Minister Klimatu i Środowiska

Rekomendacje

dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii

oraz wytyczne sektorowe dotyczące zgłaszania incydentów

Rzeczpospolita Polska
Ministerstwo Klimatu i Środowiska
Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”

Warszawa, wrzesień 2021 r.

Spis treści

1. Wprowadzenie

Przedstawiamy Państwu dokument, który będąc zbiorem dobrych praktyk i najważniejszych informacji na temat szeroko pojętego cyberbezpieczeństwa, stanowi kompendium bazowej wiedzy, której zastosowanie może przynieść pozytywne korzyści operatorom usług kluczowych, a także innym podmiotom z sektora energia, nieposiadającym tego statutu, które stoją przed wyzwaniami cyfryzacji, budowy narzędzi wymiany danych i udziału w krajowym i europejskim rynku energii. Przygotowane rekomendacje zostały wypracowane w drodze współpracy i konsultacji z CSIRT NASK, CSIRT GOV oraz CSIRT MON, a także konsultacji z operatorami usług kluczowych sektora energii, którzy dzieląc się swoim doświadczeniem i wiedzą, a także potrzebami, zapewnili większą kompletność dokumentu pod kątem zakresu tematycznego. Zaprezentowany dokument ma formę wytycznych i rekomendacji, a sama treść i kwestie w nim poruszane będą ewoluowały wraz ze zmianami i potrzebami zachodzącymi w sektorze energii.

Stabilny rozwój państwa, społeczeństwa i gospodarki jest trwale związany z niezakłóconym i nieograniczonym dostępem do informacji wykorzystywanej w procesach zarządczych, produkcyjnych i usługowych. Dlatego też sieci łączności elektronicznej, systemy informacyjne, przetwarzane w nich informacje, a także usługi świadczone za pośrednictwem tych systemów wymagają szczególnej ochrony oraz wdrożenia odpowiedniego poziomu zabezpieczeń. Dotyczy to sektora energii, jednego z krytycznych sektorów polskiej gospodarki, objętego przepisami ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (tj. Dz.U. z 2020 r. poz. 1369)[1] – dalej UKSC. Znaczenie sektora, od którego niezakłóconego działania zależy bezpieczeństwo innych sektorów gospodarki oraz bezpieczeństwo państwa, zostało wskazane w *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*[2]. Wytyczne i rekomendacje wypełniają cel główny *Strategii Cyberbezpieczeństwa*, jakim jest podniesienie poziomu odporności na zagrożenia cyberbezpieczeństwa oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym i prywatnym. Mają one również na celu wesprzeć operatorów usług kluczowych sektora energii w podniesieniu bezpieczeństwa świadczonych przez nich usług kluczowych – działanie 5.2 i 5.4 pierwszego celu szczegółowego *Strategii Cyberbezpieczeństwa*.

Rekomendacje są zbieżne z ostatnią strategią cyberbezpieczeństwa Unii Europejskiej: *Wspólny komunikat do Parlamentu Europejskiego i Rady – Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę*[3], opublikowaną 16 grudnia 2020 r. Strategia wskazuje, że sektor energii jest w coraz większym stopniu uzależniony od mocniej ze sobą powiązanych sieci i systemów informatycznych. W dokumencie zwrócono uwagę na zmieniający się poziom informatyzacji przedsiębiorstw i administracji

[1] Ustawa stanowi implementację w polskim porządku prawnym Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, tzw. Dyrektywy NIS (ang. Network and Information Services).

[2] M.P. z 30.10.2019 r. poz. 1037 dalej jako Strategia Cyberbezpieczeństwa.

[3] Join/2020/18/ final, dalej jako Strategia UE.

publicznej, co zostało spowodowane pandemią COVID-19. Szacuje się, że aż 40% pracowników UE funkcjonuje w trybie pracy zdalnej, co również przekłada się na kwestie cyberbezpieczeństwa. Strategia UE odwołuje się do wyzwań stojących zarówno przed użytkownikami, jak i producentami urządzeń. Jednym z nich są zagrożenia hybrydowe łączące cyberataki z kampaniami dezinformacyjnymi wycelowane w podmioty krytyczne dla funkcjonowania państwa. Efektem takich działań mogą być między innymi szkody fizyczne, straty finansowe, uzyskanie nieuprawnionego dostępu do danych, kradzież tajemnic handlowych czy nawet informacji ważnych z punktu widzenia państwa. W Strategii UE zidentyfikowano wyzwanie jakim jest kwestia dostępności wykwalifikowanych pracowników w dziedzinie cyberbezpieczeństwa – szacuje się, że w Europie ok. 291 000 stanowisk specjalistycznych w dziedzinie cyberbezpieczeństwa pozostaje nieobsadzonych. W dokumencie jest również mowa o odpornej infrastrukturze i usługach krytycznych, co znalazło odzwierciedlenie w kierunku nowelizacji dyrektywy NIS oraz projektach rozwiązań z zakresu tworzenia bezpiecznych produktów i usług, w tym certyfikacji cyberbezpieczeństwa[4].

Zapewnienie wysokiego poziomu cyberbezpieczeństwa, jako elementu bezpieczeństwa energetycznego państwa, znalazło się wśród celów[5] przyjętej 2 lutego 2021 r. przez Radę Ministrów *Polityki Energetycznej Polski do 2040 r.*[6], głównego dokumentu programowego transformacji polskiej energetyki, a także jej rozwoju w kierunku obniżenia emisyjności, z uwzględnieniem szeroko pojętej informatyzacji procesów technologicznych. Minister Klimatu i Środowiska jest organem odpowiedzialnym za realizację działań koncepcyjnych i operacyjnych, ukierunkowanych na rozwój innowacyjnych technologii cyfrowych (m.in. w sieciach inteligentnych), a także za nadzór nad zabezpieczeniem systemów informacyjnych służących do świadczenia nowych, innowacyjnych usług energetycznych. Dodatkowo zaproponowane w niniejszym dokumencie mechanizmy i sposoby działania, mogą być pomocne w przygotowaniu strukturalno-organizacyjnym podmiotów do nowych wymagań określonych m.in. w powstających bądź aktualizowanych Kodeksach Sieci[7]. Przykładowo, obecnie tworzone są Kodeksy Sieci w zakresie przepisów sektorowych dotyczących aspektów cyberbezpieczeństwa transgranicznych przepływów energii elektrycznej[8]. Formułowane wytyczne w obszarze wspomnianego dokumentu wskazują na konkretne kierunki i politykę działania, które mogą dominować w prawodawstwie wspólnotowym. Można wskazać, że celem działania legislacyjnego będzie rozwiązywanie, łagodzenie i zapobieganie potencjalnemu wpływowi lub materializacji zagrożeń cyberbezpieczeństwa, a także przeciwdziałanie atakom lub incydentom cyberbezpieczeństwa, które mogą mieć wpływ na operacje w czasie rzeczywistym oraz mogą spowodować efekty kaskadowe w skali transgranicznej.

Z punktu widzenia bezpieczeństwa energetycznego państwa duże znaczenie mają również sieci łączności elektronicznej. Usługi realizowane przez sieć łączności to między innymi usługi dyspozytorskie (w tym przesyłanie multimediów oraz głosu), możliwość obsługi systemów typu SCADA, czyli systemów sterowania nadrzędnego i akwizycji danych (ang. *Supervisory Control And Data Acquisition*), odczytu inteligentnych liczników czy obsługa sieci inteligentnych i odnawialnych źródeł energii. Dodatkowym wyzwaniem stojącym przed sektorem energetycznym jest również rozwijająca się

[4] Wspólny komunikat do Parlamentu Europejskiego i Rady – Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN/2020/18 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020JC0018

[5] Drugi cel szczegółowy „Rozbudowa infrastruktury wytwórczej i sieciowej energii elektrycznej".

[6] Obwieszczenie Ministra Klimatu i Środowiska z dnia 2 marca 2021 r. w sprawie polityki energetycznej państwa do 2040 r. (M.P. z 10.03.2021 r. poz. 264), dalej jako PEP2040.

[7] Kodeksy Sieci są aktami wykonawczymi UE. Są one wprowadzane przez krajowych Operatorów Systemów Przesyłowych. Kodeksy mają za zadanie eliminację barier technicznych budowy europejskiego rynku energii oraz określają zasady funkcjonowania i zarządzania systemami energetycznymi na tym rynku.

[8] Draft Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows.

technologia wymagająca coraz częściej transmisji czasu rzeczywistego, zwłaszcza w kontekście danych przesyłanych w ramach Internetu Rzeczy (IoT – ang. *Internet of Things*), przemysłowego Internetu Rzeczy (IIoT – ang. *Industrial Internet of Things*), a także szerokopasmowej transmisji danych, w tym multimediów i komunikatów głosowych. Wobec uznania sektora energii za krytyczny z punktu widzenia stabilności państwa, konieczne jest również zagwarantowanie oraz rozwijanie komunikacji krytycznej i strategicznej, działającej niezależnie od operatorów telekomunikacyjnych. Jednym z kroków podjętych w tym kierunku była nowelizacja *Prawa telekomunikacyjnego* i przydzielenie w 2018 r. dedykowanego pasma częstotliwości 450 MHz sektorowi energii.

Rekomendacje zostały także opracowane zgodnie z kierunkiem wskazanym w Zaleceniach Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. *w sprawie cyberbezpieczeństwa w sektorze energetycznym* (notyfikowana jako dokument nr C(2019) 2400)[9], w tym w oparciu o wyniki ankiety przeprowadzonej przez Ministerstwo Klimatu na przełomie kwietnia i maja 2020 r., w celu monitorowania etapu wdrożenia Zaleceń u operatorów usług kluczowych w poszczególnych państwach członkowskich. Przedmiotem Zaleceń w pkt. 2 jest wskazanie, aby państwa członkowskie zachęcały odpowiednie zainteresowane strony do poszerzania wiedzy i umiejętności związanych z cyberbezpieczeństwem w sektorze energetycznym, w szczególności poprzez strategie, przepisy ustawowe, wykonawcze i inne przepisy administracyjne. Zalecenia dzielą się na trzy obszary tematyczne: wymogi czasu rzeczywistego dotyczące elementów infrastruktury energetycznej, efekty kaskadowe oraz dotychczasowa i najnowocześniejsza technologia. Jakkolwiek wdrożenie Zaleceń nie jest obligatoryjne, ma ono na celu odpowiednie zaadresowanie szczególnych wymagań sektora energii poprzez ogólne wytyczne dla ciągłego dążenia do wyższego poziomu cyberbezpieczeństwa. Do opracowania rekomendacji wzięto pod uwagę wyniki ankiety przeprowadzonej na zlecenie Komisji Europejskiej w sprawie analizy ryzyka bezpieczeństwa systemów informacyjnych u operatorów usług kluczowych w okresie czerwiec–lipiec 2020 r., a także wyniki kwestionariusza Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) z lipca 2020 r. dotyczącej oceny zdolności operatorów usług kluczowych w sektorze energii do reagowania na incydenty teleinformatyczne. Rekomendacje uwzględniają również przeprowadzone przez Ministerstwo Klimatu i Środowiska wyniki analizy otrzymanych sprawozdań z audytów bezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej przeprowadzonych przez operatorów usług kluczowych z sektora energii zgodnie z wymaganiami UKSC.

W celu kompleksowego podejścia do opisywanych zagadnień odniesiono się również do różnych publikacji opracowanych przez ENISA, jak np. *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, Międzynarodową Agencję Energii Atomowej, opracowań dotyczących szacowania ryzyka oraz zapobiegania incydentom cyberbezpieczeństwa w sektorze energii stworzonych przez ECOFYS na zlecenie Komisji Europejskiej i inne. Pełen wykaz dokumentów, na podstawie których powstały rekomendacje znajduje się w rozdziale 2.

Systemy informacyjne w energetyce

W świetle UKSC, system informacyjny należy definiować na podstawie art. 2 pkt 14 UKSC, zgodnie z którym, system informacyjny to *system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[10], wraz z przetwarzanymi w nim danymi w postaci elektronicznej*. Zgodnie z art. 3 pkt 3 ustawy o informatyzacji, system

[9] Ich celem są zachęty do poszerzania wiedzy i umiejętności związanych z cyberbezpieczeństwem w sektorze energetycznym. Dalej jako Zalecenia.

[10] Dz.U. z 2020 r. poz. 346, 568 i 695, dalej: ustawa o informatyzacji.

teleinformatyczny to *zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy Prawo telekomunikacyjne (ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne*[11] . Telekomunikacyjne urządzenie końcowe to natomiast *urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci* (art. 2 pkt 43 Prawa telekomunikacyjnego).

Zgodnie z powyższym, system informacyjny ma zapewniać przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci komputerowe za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. Definicja opisuje więc trzy funkcjonalności systemu – przetwarzanie, przechowywanie oraz wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą urządzenia końcowego. Przepis nie wskazuje aby wszystkie trzy funkcjonalności musiały być zapewnione przez system jednocześnie.

W świetle przepisów Dyrektywy NIS, art. 4 pkt 1 jednoznacznie wskazuje, że sieci i systemy informatyczne, oznaczają:

a) sieci łączności elektronicznej w rozumieniu art. 2 lit. a) dyrektywy 2002/21/WE;
b) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych; lub
c) dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy.

Do uznania za system w świetle dyrektywy NIS, a tym samym UKSC, która implementuje dyrektywę NIS do polskiego porządku prawnego, wystarczającym jest by urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba wykonując program, dokonywały automatycznego przetwarzania danych cyfrowych.

Ustawą z dnia 20 maja 2021 r. *o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw*[12], do ustawy Prawo energetyczne został wprowadzony art. 3 pkt 71, który definiuje system informacyjny jako system w rozumieniu art. 2 pkt 14 UKSC. Dodanie wskazanej definicji jest działaniem, które zapewnia komplementarność siatki pojęciowej w regulacjach mających zastosowanie w sektorze energetycznym oraz zwiększa pewność interpretacji samej definicji systemu w kontekście świadczenia usług kluczowych sektora energii. Sam fakt dodania powyższej definicji w ustawie regulującej sektor energetyczny w Polsce, wskazuje na zbieżność tej definicji z rodzajami systemów jakie wykorzystywane są w energetyce, oraz ponownie wskazuje, iż systemem informacyjnym jest każdy system, który wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych.

W celu pełnego zrozumienia specyfiki sektora energii należy podkreślić, że do osiągnięcia pełnej operacyjności wymagane jest zastosowanie zarówno systemów technologii informacyjnej (IT – ang. *Information Technology*), jak również automatyki przemysłowej (OT – ang. *Operational Technology*), przemysłowych systemów sterowania (ICS – ang. *Industrial Control Systems*). Budowanie szeroko rozumianego bezpieczeństwa w obszarze OT jest istotnym aspektem funkcjonowania podmiotów z sektora energii. Ewentualne pominięcie tego aspektu na różnych etapach cyklu życia rozwiązań automatyki przemysłowej i sieci produkcyjnych może doprowadzić do sytuacji, w której organizacja będzie funkcjonować na nieakceptowalnym poziomie ryzyka, a jej kierownictwo nie będzie tego

[11] Dz.U. z 2021 r. poz. 576, dalej: Prawo telekomunikacyjne.
[12] Ustawa z dnia 20 maja 2021 r. o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Dz.U. 2021 poz. 1093).

świadome. W celu odpowiedniego zidentyfikowania systemów informacyjnych stosowanych w sektorze energii, należy wyróżnić pięć kategorii funkcjonalnych:

1) operacyjną,
2) biznesową,
3) bezpieczeństwa (*safety*),
4) ochrony fizycznej,
5) reagowania kryzysowego.

Każda z nich obejmuje różne zadania systemów. Zatem, kiedy jest mowa o kategorii operacyjnej należy przez to rozumieć systemy kontroli procesu, w tym systemy oprzyrządowania i kontroli (I&C – ang. *instrumentation and control systems*), sterownie systemów I&C zawierające systemy alarmowe, systemy komputerowe wykorzystywane do zbierania i przygotowania odpowiednich informacji na potrzeby sterowni, systemy do obsługi i przechowywania paliw, systemy zarządzania konfiguracją oraz utrzymania, zdalny dostęp i VPN (ang. *virtual private network*) do środowiska operatorskiego, infrastruktura służąca do komunikacji głosowej i transmisji danych, infrastruktura operatorska i systemy kontroli, środowiska testowe i programistyczne dla systemów operacyjnych.

Jeżeli chodzi o kategorię biznesową, to dotyczy ona takich aspektów jak: infrastruktura komunikacji głosowej i transferu danych, systemy służące do zarządzania zasobami ludzkimi i repozytoria danych, systemy techniczne i inżynierskie, systemy zlecania pracy i pozwolenia na pracę, systemy zamówień publicznych oraz systemy biurowe.

Do systemów kategorii bezpieczeństwa (*safety*) zalicza się systemy ochrony, systemy wykonujące działania zabezpieczające, uruchamiane przez systemy bezpieczeństwa bądź ręcznie, systemy wspomagające system bezpieczeństwa, w tym systemy zasilania awaryjnego.

W zakres kategorii ochrony fizycznej wchodzą takie systemy jak: systemy monitoringu i wykrycia włamania, system kontroli dostępu, systemy kontroli zasobów, infrastruktura służąca do przesyłania głosu i danych, systemy alarmowe, a także bazy danych zawierające informacje o posiadanych przez pracowników poświadczeniach bezpieczeństwa, używane w celu zapewnienia, że personel ma przyznany dostępu do danej strefy.

Ostatnią kategorię stanowią systemy służące do reagowania kryzysowego takie jak systemy monitorowania środowiska, systemy monitorujące promieniowanie, systemy ochrony przeciwpożarowej oraz środki komunikacji umożliwiające transmisję głosu i danych.

Należy podkreślić, że wymienione wyżej rodzaje systemów wchodzących w poszczególne kategorie funkcjonalne nie stanowią zbioru zamkniętego i w niektórych organizacjach przytoczona systematyka może być bardziej zróżnicowana. Jednakże pewne podstawy są wspólne dla wszystkich podmiotów z sektora energii.

Usługi kluczowe sektora energii

Zgodnie z art. 2 pkt 16 UKSC przez pojęcie *usługa kluczowa* rozumie się *usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych*. Wspomniany katalog, na podstawie art. 6 pkt 1 UKSC, został opracowany w formie załącznika do rozporządzenia Rady Ministrów z dnia 11 września 2018 r. *w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych* (Dz. U. z 2018 r. poz. 1806)[13].

[13] Dalej jako rozporządzenie ws. wykazu usług kluczowych.

Zgodnie z załącznikiem do rozporządzenia ws. wykazu usług kluczowych, w ramach sektora energii wyróżniono 7 podsektorów. Są to: wydobywanie kopalin, energia elektryczna, ciepło, ropa naftowa, gaz, dostawy i usługi dla sektora energii oraz jednostki nadzorowane i podległe. W ramach każdego podsektora wymieniono różne usługi kluczowe świadczone przez podmioty działające w danej branży.

Zatem, jeżeli chodzi o podsektor wydobycia kopalin to wyróżnia się tutaj następujące usługi kluczowe – wydobywanie gazu ziemnego, wydobywanie ropy naftowej, wydobywanie węgla brunatnego, wydobywanie węgla kamiennego i wydobywanie miedzi. Podmioty działające w ramach podsektora energii elektrycznej świadczą usługi kluczowe w zakresie wytwarzania energii elektrycznej, przesyłania energii elektrycznej, dystrybucji energii elektrycznej, obrotu energią elektryczną, magazynowania energii elektrycznej oraz usług systemowych, jakościowych i zarządzania infrastrukturą energetyczną. Podobne usługi kluczowe świadczone są w sektorze ciepło – wytwarzanie ciepła, obrót ciepłem, przesyłanie ciepła i dystrybucja ciepła. Kolejnym elementem jest podsektor ropy naftowej, w którym operatorzy świadczą usługi kluczowe w zakresie wytwarzania paliw ciekłych, przesyłania ropy naftowej, przesyłania paliw ciekłych, magazynowania ropy naftowej, przeładunek ropy naftowej, magazynowanie paliw ciekłych, przeładunek paliw ciekłych, obrót paliwami ciekłymi lub obrót paliwami ciekłymi z zagranicą, a także wytwarzanie paliw syntetycznych. Jeżeli chodzi o podsektor gazu, to wymieniono następujące usługi kluczowe: wytwarzanie paliw gazowych, przesyłanie paliw gazowych, obrót paliwami gazowymi i obrót gazem ziemnym z zagranicą, przesyłanie paliw gazowych, dystrybucja paliw gazowych, magazynowanie paliw gazowych oraz skraplanie i regazyfikacja LNG oraz sprowadzanie i wyładunek. Kolejny podsektor stanowią dostawy i usługi dla sektora energii, w ramach których wyróżnia się dostawy systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenie usług na rzecz sektora energii. Ostatnim podsektorem są jednostki nadzorowane i podległe, których usługi kluczowe polegają na wytwarzaniu radiofarmaceutyków, postępowaniu z odpadami promieniotwórczymi, utrzymywaniu rezerw strategicznych i zapasów ropy naftowej, produktów naftowych i gazu ziemnego, a także prace badawczo-rozwojowe lub wdrożeniowe lub badania technologiczne na rzecz sektora energii.

W załączniku do rozporządzenia w sprawie wykazu usług kluczowych, zostały również zdefiniowane progi istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej, odnoszące się bezpośrednio do każdej z wymienionych usług. Zostały one stworzone w oparciu o specyficzne uwarunkowania każdego z podsektorów.

W sektorze energii świadczonych jest wiele usług kluczowych niezbędnych do zapewnienia bezpieczeństwa energetycznego państwa. Usługi te wymagają obsługi sieci heterogenicznych i współistnienia sieci OT z IT.

Szeroki zakres podmiotowy operatorów usług kluczowych, nadzorowanych przez Ministra Klimatu i Środowiska, przekłada się na znaczne zróżnicowanie stopnia zaawansowania technologiczno-proceduralnego, przekładające się na odporność, a także gotowość do reakcji na zagrożenia pochodzące z cyberprzestrzeni. Podstawowym celem rekomendacji jest więc przedstawienie w sposób ustrukturyzowany zaleceń, których wdrożenie wewnątrz organizacji pomoże sprostać przyszłym wyzwaniom poprzez wyrównanie poziomu cyberbezpieczeństwa. Zwiększenie poziomu świadomości i dojrzałości organizacyjnej w sektorze energii, w tym zwłaszcza każdego z operatorów usług kluczowych przełoży się na wzmocnienie całego krajowego systemu cyberbezpieczeństwa. Rekomendacje pozwolą określić zalecane sposoby realizacji niektórych obowiązków nałożonych na operatorów usług kluczowych. Takie działanie pomoże zniwelować wystąpienie ewentualnych wątpliwości, jednocześnie nie ingerując w proces decyzyjny i organizacyjny podmiotu.

2. Podstawa prawna

Niniejszy dokument został przygotowany na podstawie art. 41 pkt. 1 oraz art. 42 ust. 1 pkt. 5 w związku z art. 42 ust. 8 UKSC, z udziałem CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa.

Niniejsze rekomendacje opracowano w oparciu o następujące dokumenty:

1. Akty prawne krajowe:
   a. Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. *w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024* (Dz.U. z 2019 r. poz. 1037).
   b. Ustawa z dnia 5 lipca *o krajowym systemie cyberbezpieczeństwa* (tj. Dz.U. z 2020 r. poz. 1369).
   c. Ustawa z dnia 10 kwietnia 1997 r. *Prawo energetyczne* (Dz.U. z 2021 r. poz. 1093).
   d. Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (tj. Dz. z 2020 r. poz. 1856).
   e. Ustawa z dnia 20 maja 2021 r. *o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw* (Dz.U. 2021 poz. 1093).
   f. Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. *w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych* (Dz. U. z 2018 r. poz. 1806).
   g. Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. z 2020 r. poz. 346, 568 i 695).
   h. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2021 r. poz. 576).
   i. Obwieszczenie Ministra Klimatu i Środowiska z dnia 2 marca 2021 r. w sprawie polityki energetycznej państwa do 2040 r. (M.P. z 10.03.2021 r. poz. 264).

2. Akty prawne międzynarodowe:
   a. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dz.U. L 194 z 19.7.2016),
   b. Zalecenie Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. *w sprawie cyberbezpieczeństwa w sektorze energetycznym* (notyfikowana jako dokument nr C(2019) 2400),
   c. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. *w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie*),
   d. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie*

swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

e. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1938 z dnia 25 października 2017 r. *dotyczące środków zapewniających bezpieczeństwo dostaw gazu ziemnego i uchylające rozporządzenie (UE) nr 994/2010*,

f. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/941 z dnia 5 czerwca 2019 r. *w sprawie gotowości na wypadek zagrożeń w sektorze energii elektrycznej i uchylające dyrektywę 2005/89/WE*.

g. Commission Staff Working Document Accompanying Commission Recommendation on cybersecurity in the energy sector {C(2019) 2400 final}. SWD(2019) 1240 final.

3. Publikacje:

a) Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Listopad 2017,

b) Conducting Computer Security Assessments at Nuclear Facilities, International Atomic Energy Agency, https://www.iaea.org/publications/10999/conducting-computer-security-assessments-at-nuclear-facilities,

c) Cybersecurity Incident Taxonomy (CG Publication 04/2018) by NIS Cooperation Group,

d) Cyberbezpieczeństwo. Zarys wykładu, red. Naukowa C. Banasiński, Warszawa 2018.

e) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology – April 16, 2018,

f) FRAMEWORK UDT CYBER – metodyka oceny organizacji Audyt Cyberbezpieczeństwa, wydanie 1, opublikowane 2 czerwca 2020 r,

g) Good Practices for Security of Internet of Things in the context of Smart Manufacturing, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Listopad 2018 r.,

h) Guidelines on assessing DSP and OES compliance to the NISD security requirements Information Security Audit and Self – Assessment/ Management Frameworks, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Listopad 2018 r.,

i) International Standard ISO/IEC 27019 – Information technology – Security techniques – Information security controls for the energy utility industry, Reference number ISO/IEC 27019:2017(E),

j) Ł. Kister, *Szacowanie ryzyka dla usług kluczowych opartych o systemy OT*, Nowa Energia – nr 3 (68)/2019,

k) J. Krawiec i G. Ożarek, *System Zarządzania Bezpieczeństwem Informacji w praktyce zabezpieczenia*, Polski Komitet Normalizacyjny, Warszawa 2014 r.,

l) Narodowe Standardy Cyberbezpieczeństwa Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO), Ministerstwo Cyfryzacji, v. 1.00 – luty 2020,

m) NIST SPECIAL PUBLICATION 1800-7, Situational Awareness For Electric Utilities (http://doi.org/10.6028/NIST.SP1800-7),

n) NISTIR 7628, Smart Grid Cyber Security: Vo. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, sierpień 2010,

o) Norma Europejska EN ISO 22301:2014 *Societal security – Business continuity management systems – Requirements* (ISO 22301:2012), Polski Komitet Normalizacyjny, Warszawa 2014 r.,

p) Norma Europejska EN ISO/IEC 27001:2017 *Information technology – Security techniques – Information security management systems – Requirements* (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015), Polski Komitet Normalizacyjny, Warszawa 2018 r.,

q) Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli, INTOSAI Working Group on IT Audit (WGITA), Warszawa 2016 r.,

r) Poradnik dobrych praktyk w zakresie cyberbezpieczeństwa urządzeń podlegających dozorowi technicznemu, Zespół ds. cyberbezpieczeństwa Urząd Dozoru Technicznego, 2021 r.,

s) Poradnik dla przedsiębiorstw: Jak utrzymać ciągłość działania usług/krytycznych i kluczowych systemów teleinformatycznych w stanie zagrożenia epidemicznego, Ministerstwo Cyfryzacji, marzec 2020 r.,

t) Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, Komisja Nadzoru Finansowego, Warszawa styczeń 2013 r.

u) Rekomendacje Kancelarii Premiera Rady Ministrów, cyberbezpieczeństwa dla sektora wodno-kanalizacyjnego, (R-CYBER-01/2021)r, luty 2021 r., Warszawa.

v) Rekomendacje Ministra Aktywów Państwowych z dnia 2 kwietnia 2020 r. dla podmiotów gospodarczych świadczących usługi z zakresu wytwarzania, przesyłu oraz dystrybucji energii elektrycznej.

w) Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements (IEC 62443-4-1:2018), European Comitee for Electronical Standarization (CENELEC), marzec 2018 r.

x) Smart Grid Task Force Expert Group 2, Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management, Final Report June 2019.

y) Standardy i dobre praktyki ochrony infrastruktury krytycznej automatyka przemysłowa w sektorze elektroenergetycznym, Rządowe Centrum Bezpieczeństwa, 2019 r.

z) Standardy i dobre praktyki ochrony infrastruktury krytycznej automatyka przemysłowa w sektorze ropy i gazu, Rządowe Centrum bezpieczeństwa, 2019 r.

aa) Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector, ECOFYS, https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf

ab) Wspólna Infrastruktura Informatyczna Państwa, Cyfryzacja KPRM, https://www.gov.pl/web/cyfryzacja/wspolna-infrastruktura-panstwa-wip-20

ac) Wytyczne Ministerstwa Cyfryzacji, dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, z dnia 15 grudnia 2015 r.

ad) E. Wanat, P. Ignaszak, B. Bartnicki, *Chmura obliczeniowa w energetyce*, Instytut Jagielloński, Warszawa 2021.

ae) Raport EY Law Compass II, *Chmura obliczeniowa w sektorach regulowanych: Finanse i Energetyka Wyzwania 2021*, Warszawa 2021 r.

3. Słownik użytych pojęć

Administrator Systemu – osoba zarządzająca systemem teleinformatycznym, dbająca o jego sprawne oraz bezpieczne działanie i wykorzystywanie.

Aktywa – urządzenia, systemy, obiekty, informacje i dane, procesy, dokumentacja które umożliwiają organizacji osiągnięcie celów biznesowych. Jako aktywa rozumie się także pracowników organizacji uwzględnionych w systemie zarządzania bezpieczeństwem.

Aktywa informacyjne – informacje i dane, które umożliwiają organizacji osiągnięcie celów biznesowych.

BCP – (ang. *Business Continuity Plans; pl. Plany Ciągłości Działania*) – tworzenie, modyfikacja, aktualizacja planów wznawiania działania procesów.

Bezpieczeństwo informacji – zachowanie poufności, integralności, autentyczność i dostępności informacji.

BYOD – (ang. *bring your own device)* – wykorzystywanie prywatnych urządzeń mobilnych do pracy służbowej w środowisku informatycznym danego podmiotu.

Cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

DCS – (ang. *Distributed Control System*) – rozproszony system sterowania odpowiadający za sterowanie i wizualizację procesu przemysłowego posiadający wspólną bazę danych dla sterowania i wizualizacji.

DRP – (ang. *Disaster Recovery Plan, pl. Plan odtworzenia infrastruktury teleinformatycznej)* plany odtworzenia infrastruktury teleinformatycznej oraz procesów teleinformatycznych po wystąpieniu awarii.

HMI – (ang. *Human-Machine Interface*) – Panele sterowania i pulpity nawigacyjne umożliwiające operatorom monitorowanie i sterowanie sterownikami PLC, RTU i innymi urządzeniami elektronicznymi.

ICS/IACS – (ang. *Industrial Control Systems* lub *Industrial Automation and Control System*) – systemy teleinformatyczne, które realizują funkcje nadzoru, zarządzania, sterowania, regulacji, pomiaru, monitoringu, bezpieczeństwa (lub kilku tych funkcji łącznie) dla procesów technologicznych i przemysłowych. Systemy ICS są częścią szeroko pojętego OT.

Incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

Interoperacyjność – zdolność organizacji do współdziałania na rzecz osiągnięcia celów korzystnych dla wszystkich stron, co obejmuje wymianę informacji między tymi organizacjami i dzielenie się wiedzą, poprzez realizowane przez nie procedury, za pomocą wymiany danych między ich systemami informacyjnymi.

IT – (ang. *Information Technology*) – wszelkie działania związane z wykorzystaniem urządzeń informatycznych oraz usług im towarzyszących, a także gromadzenie, przetwarzanie, udostępnianie informacji w formie elektronicznej z wykorzystaniem technik cyfrowych i wszelkich narzędzi komunikacji elektronicznej.

MITM – (ang. *Man in the Middle*) – atak sieciowy polegający na podsłuchiwaniu i modyfikacji danych wymienianych pomiędzy dwiema stronami komunikacji bez ich wiedzy, np. wymiana poprzez pocztę elektroniczną, media społecznościowe, strony internetowe. W wyniku ataku cała komunikacja przechodzi przez cyberprzestępcę, tym samym posiada on całkowity wgląd do danych przesyłanych między stronami.

MFA – (ang. *Multi-Factor Authentication*) – to uwierzytelnianie wielopoziomowe będące dodatkowym zabezpieczeniem (składnikiem) procesu autoryzacji podczas logowania do systemu informacyjnego.

Operator infrastruktury krytycznej – właściciel, posiadacz samoistny albo posiadacz zależny obiektów, instalacji urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*.

Operator usługi kluczowej – jest podmiot, o którym mowa w załączniku nr 1 do UKSC, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do UKSC.

OT – (ang. *Operational Technology*) – sprzęt i oprogramowanie wykorzystywane do sterowania i nadzoru nad procesami technologicznymi i produkcyjnymi.

Patch – poprawka oprogramowania, część kodu korygująca błędy i luki bezpieczeństwa.

PLC – (ang. *Programmable logic controller*) – najpopularniejsze urządzenie przemysłowych systemów sterowania, sterowniki swobodnie programowalne, których podstawowym zadaniem jest sterowanie urządzeniami i procesami.

RTU – (ang. *Remote Terminal Unit*) – urządzenia przemysłowych systemów sterowania, zwykle używane w podstacjach lub zdalnych lokalizacjach. Ich celem, podobnie jak w przypadku sterowników PLC, jest monitorowanie parametrów pola i wysyłanie danych do stacji centralnej.

Podatność – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa.

SCADA – (ang. *Supervisory Control and Data Acquisition*) – system informacyjny nadzorujący przebieg procesu technologicznego lub produkcyjnego obejmujący zbieranie aktualnych danych (pomiarów), ich wizualizację, sterowanie procesem, alarmowanie oraz archiwizację danych.

Sieć łączności elektronicznej – systemy transmisyjne, urządzenia przełączające lub routingowe oraz inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają przekazywanie sygnałów przewodowo, za pomocą radia, środków optycznych lub innych rozwiązań wykorzystujących fale, w tym sieci satelitarnych, stacjonarnych (komutowanych i pakietowych, w tym Internetu) i sieci ruchomych, elektroenergetycznych systemów kablowych.

SOC – *(ang. Security Operations Center)* – zespół pełniący funkcję operacyjnego centrum cyberbezpieczeństwa lub realizujący zadania z zakresu cyberbezpieczeństwa w danym podmiocie bądź na jego zlecenie. Funkcje SOC pełnią wewnętrzne lub zewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo operatora usługi kluczowej.

SIS – (ang. *Safety Instrumented System*) – przyrządowy system bezpieczeństwa, złożony z dowolnej kombinacji czujników, jednostek logicznych i elementów wykonawczych.

System informacyjny – system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i 1544), wraz z przetwarzanymi w nim danymi w postaci elektronicznej.

System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

Usługa kluczowa – usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych.

Użytkownik – upoważniona osoba fizyczna (Pracownik, Współpracownik, Kontrahent lub osoba działająca w imieniu i na rzecz Kontrahenta) korzystająca z systemów teleinformatycznych Spółki.

Wymagania czasu rzeczywistego – okoliczności charakterystyczne dla funkcjonowania elementów systemu energetycznego (np. monitorowanie pracy sieci, bilansowanie mocy oraz weryfikacji stanu stacji bazowych podczas przesyłu, a także dystrybucji energii), co wymaga funkcjonowania w „czasie rzeczywistym", tj. reagowania na polecenia w ciągu kilku milisekund.

Zagrożenie cyberbezpieczeństwa – potencjalna przyczyna wystąpienia incydentu.

4. Zarządzanie ryzykiem

4.1. Polityka Bezpieczeństwa Informacji

Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[14]. Polityka bezpieczeństwa informacji jest natomiast strategicznym dokumentem pozwalającym na efektywne i całościowe zarządzanie bezpieczeństwem danych, które zgromadzone są w organizacji, a w szczególności w jej systemach informacyjnych.

Polityka bezpieczeństwa informacji powinna zawierać spisane cele, strategie oraz działania, które w jasny i ustrukturyzowany sposób określają, jak należy zarządzać zgromadzonymi danymi, jak je chronić i rozpowszechniać. Dokument powinien ułatwiać dokładne zrozumienie celu istnienia procedur bezpieczeństwa i ma za zadanie podnosić świadomość pracowników organizacji na temat zagrożeń bezpieczeństwa i związanego z nimi ryzyka[15].

Polityka bezpieczeństwa informacji powinna być dokumentem spisanym, który jest zrozumiały i dostępny dla każdego pracownika organizacji oraz osób korzystających z jej zasobów informacyjnych. Partnerzy biznesowi powinni być zapoznawani z wybranymi i podstawowymi zasadami polityki bezpieczeństwa w zakresie wymaganym co do stopnia i zakresu korzystania przez nich z zasobów teleinformatycznych danej organizacji.

Ponadto polityka bezpieczeństwa informacji powinna zawierać ogólne, ale spójne założenia reguł i procedur dotyczących bezpieczeństwa dla danego obszaru. Szczegółowe zasady dotyczące zabezpieczeń, instrukcje reagowania na incydenty bezpieczeństwa czy opis sposobu korzystania z danych bądź przydzielania uprawnień dostępu powinny być opisane w oddzielnych dokumentach zawierających przyjęte w organizacji standardy i procedury postępowania.

Zawartość Polityki Bezpieczeństwa Informacji

Polityka bezpieczeństwa informacji powinna zawierać:

- zbiór spójnych, precyzyjnych reguł i procedur, według których dana organizacja buduje dane, dokumenty i zasoby informatyczne, zarządza nimi oraz je udostępnia;
- określenie zasobów i w jaki sposób mają być one chronione;
- opis możliwych rodzajów naruszenia bezpieczeństwa, m.in.: utraty danych, ich wycieku, nieautoryzowanego dostępu, a także scenariusze postępowania w takich sytuacjach i działania,

[14] UKSC.

[15] Norma PN-EN ISO/IEC 27001:2017.

które pozwolą uniknąć powtórzenia się danego incydentu, z odesłaniem do szczegółowych procedur obowiązujących w organizacji;

- zdefiniowane poprawne i niepoprawne korzystanie z takich zasobów, jak konta użytkowników, dostęp do danych i oprogramowania.

Projektując mechanizmy ochrony informacji, należy uwzględnić mechanizmy identyfikacji, autentykacji i zapewnienia autentyczności zarówno na poziomie fizycznym (dostęp do pomieszczeń, np. serwerowni), jak i poziomie systemów IT/OT. Dodatkowo należy wziąć pod uwagę procedury związane ze śledzeniem zdarzeń w systemie, które obejmują same mechanizmy, a także programy czy procedury stosowane do śledzenia zmian w tychże systemach.

Definiowanie Polityki Bezpieczeństwa Informacji

Dokument określający politykę bezpieczeństwa informacji organizacji powinien obejmować również kwestie przetwarzania danych osobowych oraz zarządzania nimi zgodnie z wytycznymi RODO[16]. Polityka bezpieczeństwa informacji powinna uwzględniać rekomendacje na podstawie zaleceń poaudytowych. Należy jasno zdefiniować zasady przydzielania uprawnień dostępu do poszczególnych klas informacji oraz ustalić schemat obiegu informacji w organizacji.

Elementy dobrze zdefiniowanej Polityki Bezpieczeństwa Informacji:

- jednoznaczne przypisanie uprawnień użytkownika do wykorzystywanej przez niego informacji;
- zdefiniowanie poziomu poufności informacji od chwili jej powstania aż do całkowitego usunięcia z obiegu;
- uprawniony sposób przetwarzania informacji elektronicznej;
- ograniczenie swobodnego wykorzystania obcych nośników informacji,
- klasyfikacja użytkowników, systemów, peryferii (np. zarządzanie drukiem w organizacji) oraz oprogramowania pod względem ochrony przetwarzanych informacji;
- procedury zachowania poufności danych w przypadku kradzieży lub zagubienia nośników danych, laptopów bądź urządzeń mobilnych, na których znajdowały się informacje „wrażliwe";
- wychwytywanie naruszeń polityki bezpieczeństwa;
- ewidencjonowanie dowodów naruszeń polityki bezpieczeństwa.

Podczas definiowania polityki bezpieczeństwa informacji należy uwzględnić możliwość zastosowania systemów DLP[17] oraz klasyfikacji danych, kategoryzując poszczególne poziomy dostępu do danej klasyfikacji plików.

Wdrożenie Polityki Bezpieczeństwa Informacji

Posiadając szczegółowe dane z audytu, organizacja powinna przystąpić do projektowania polityki bezpieczeństwa informacji, w której należy uwzględnić, czy organizacja będzie w stanie ponieść koszty finansowe i organizacyjne związane z wprowadzaniem zamierzonego zakresu tej polityki w życie.

[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[17] DLP (ang. *Data Loss Prevention*) – rozwiązanie informatyczne wspomagające ochronę danych w postaci elektronicznej przed kradzieżą lub przypadkowymi wyciekami.

Należy pamiętać, że podwyższanie poziomu bezpieczeństwa odbywa się często kosztem produktywności i efektywności działania, w związku z tym polityka bezpieczeństwa informacji musi być dostosowana ściśle do specyfiki organizacji, tak aby nadać jej cechy ułatwiające zastosowanie jej w praktyce.

Polityka bezpieczeństwa informacji musi obejmować wszystkie urządzenia wykorzystywane w procesie przetwarzania danych. Powinna zawierać również informacje dotyczące zasad edukacji pracowników w zakresie bezpieczeństwa i weryfikacji przestrzegania standardów organizacji w zakresie bezpieczeństwa. Ponadto, w ramach systemu bezpieczeństwa informacji powinna być podnoszona wiedza pracowników organizacji poprzez szkolenia osób zaangażowanych w proces przetwarzania informacji oraz cykliczną dystrybucję biuletynów informacyjnych.

Wdrażając politykę bezpieczeństwa, należy uwzględnić także bieżące trendy, w tym między innymi zdalny dostęp pracowników do zasobów informatycznych organizacji. Gdy pojawiają się nowe trendy, polityka musi być niezwłocznie modyfikowana. Co ważne, należy wówczas jak najszybciej przeprowadzić odpowiednie szkolenie dla pracowników i kadry zarządzającej.

Dowody kontroli:

- *dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w tym polityka Bezpieczeństwa Informacji (BI) oraz inne dokumenty stanowiące SZBI,*
- *dokumentacja z przeglądów SZBI z uwzględnieniem zmian i zdarzeń z przeszłości. Harmonogram i ogólny plan cyklu przeglądu,*
- *dokumentacja audytów z zakresu BI,*
- *certyfikacja dotycząca zgodności z normami zarządzania ryzykiem w zakresie bezpieczeństwa informacji.*

4.2. Organizacja bezpieczeństwa informacji

PN-EN ISO/IEC 27001:2017[18] to międzynarodowa norma standaryzująca wytyczne w zakresie zarządzania bezpieczeństwem informacji. Została ona opracowana na bazie brytyjskiego standardu BS 7799-2, a jej celem jest dostarczenie wymagań dotyczących ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu pozwalającego na zachowanie bezpieczeństwa informacji w każdej z organizacji.

Standard zbudowany jest z dwóch podstawowych części:

1) część podstawowa, w której zdefiniowano wymagania związane z ustanowieniem i zarządzaniem systemem bezpieczeństwa informacji, wymaganą dokumentacją, odpowiedzialnością, wewnętrznymi audytami, przeglądem zarządzania i ciągłym doskonaleniem;
2) załącznik A, w którym zdefiniowano czternaście obszarów mających bezpośredni i kluczowy wpływ na bezpieczeństwo informacji. Wśród nich są:
   - polityka bezpieczeństwa,
   - organizacja bezpieczeństwa informacji,
   - bezpieczeństwo zasobów ludzkich,
   - zarządzanie aktywami,
   - kontrola dostępu,
   - kryptografia,

[18] Dalej jako ISO 27001.

- bezpieczeństwo fizyczne i środowiskowe,
- bezpieczna eksploatacja,
- bezpieczna komunikacja,
- pozyskiwanie, rozwój i utrzymanie systemów,
- relacje z dostawcami,
- zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- aspekty bezpieczeństwa w zarządzaniu ciągłością działania,
- zgodność z wymaganiami prawnymi i własnymi standardami.

Norma może być stosowana przez przedsiębiorstwa wszystkich branż, bez względu na ich wielkość i specjalizację, jedynym warunkiem jest to, aby system stanowił część procesów realizowanych w organizacji oraz był zintegrowany ze strukturą zarządzania.

Bazą dla wszystkich działań przy jednoczesnym zapewnieniu poufności, integralności oraz dostępności informacji jest stosowanie podejścia opartego na ryzyku i odpowiednie nim zarządzanie.

Skuteczne wdrożenie, a następnie monitorowanie i doskonalenie systemu pozwala organizacji na:

- spełnienie wymagań prawnych,
- wzrost świadomości pracowników odnośnie bezpieczeństwa informacji,
- utrzymywanie stałego nadzoru nad procesami przetwarzania informacji,
- odpowiednią identyfikację zagrożeń związanych z bezpieczeństwem informacji i zmniejszenie ich wpływu na działalność organizacji,
- kompleksowe zarządzanie czynnikami ryzyka,
- zachowanie poufności, integralności i dostępności informacji, w tym tych stanowiących własność klientów,
- podniesienie wiarygodności organizacji w oczach klientów, inwestorów i innych stron zainteresowanych,
- poprawę reputacji i postrzegania marki,
- wzrost przewagi konkurencyjnej na rynku.

Jednym z kluczowych elementów wdrażania systemu jest odpowiednia organizacja bezpieczeństwa informacji. Zgodnie z normą ISO 27001 organizacja bezpieczeństwa informacji składa się na organizację wewnętrzną bezpieczeństwa informacji oraz bezpieczeństwo pracy zdalnej (telepracy) i użytkowania urządzeń mobilnych[19].

Celem organizacji wewnętrznej bezpieczeństwa informacji jest zbudowanie struktur zarządzania w celu zainicjowania, nadzorowania wdrażania i eksploatacji bezpieczeństwa informacji w organizacji.

Aby to osiągnąć, rekomenduje się realizację następujących działań:

1) Organizacja powinna przypisać odpowiednie role poszczególnym pracownikom i tym samym odpowiedzialność za bezpieczeństwo informacji.
2) Należy dokładnie określić obowiązki i odpowiedzialności pracowników tak, aby nie pozostawały ze sobą w konflikcie. Ma to na celu ograniczenie modyfikacji i nadużycia aktywów organizacji[20].

[19] Norma ISO 27001, Załącznik A, Wzorcowy wykaz celów stosowania zabezpieczeń i zabezpieczenia.

[20] Przykładowo osoba przeprowadzająca audyt bezpieczeństwa systemu informacyjnego nie może służbowo podlegać kierownikowi działu utrzymania systemów informacyjnych.

3) Organizacja powinna wyznaczyć pracownika do kontaktu z podmiotami wchodzącymi w skład Krajowego Systemu Cyberbezpieczeństwa, w tym z organem właściwym ds. cyberbezpieczeństwa w sektorze energii, a także z właściwym zespołem reagowania na incydenty bezpieczeństwa komputerowego CSIRT poziomu krajowego, tj. CSIRT GOV bądź CSIRT NASK, zgodnie z zasadami określonymi w UKSC.
4) Ponadto organizacja powinna utrzymywać stosowane kontakty z innymi podmiotami z obszaru cyberbezpieczeństwa, które stanowią doskonałe źródło informacji, m.in. o zagrożeniach, podatnościach, wskaźnikach kompromitacji (IoC – ang. *indicators of compromise*)[21], technologiach, a także wiedzę specjalistyczną w zakresie budowania i wzmacniania struktur cyberbezpieczeństwa w organizacji. Przykładem tego typu organizacji może być Centrum Wymiany i Analizy Informacji (ISAC – ang. *Information Sharing and Analysis Center*)[22].
5) Należy także uwzględnić bezpieczeństwo informacji w zarządzaniu projektami, niezależnie od rodzaju projektu.

Organizacja powinna również zapewnić bezpieczeństwo pracy zdalnej i użytkowania wszelkich urządzeń mobilnych.

W związku z tym rekomenduje się realizację następujących działań:

1) Należy wdrożyć politykę związaną ze świadczeniem pracy zdalnej oraz wdrożyć wspierające ją zabezpieczenia celem ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania pracy zdalnej (telepracy).
2) Ponadto organizacja powinna opracować i wdrożyć politykę stosowania urządzeń mobilnych, a także wdrożyć wspierające ją zabezpieczenia w celu zarządzania ryzykami, które wynikają z użytkowania tych urządzeń.

Dowody kontroli:

– regulaminy bądź procedury testowania systemów informacyjnych, obejmujące między innymi czas przeprowadzenia testów, plany testów, przypadki testowe, szablony sprawozdań z testów, a także pożądane wartości mierników bezpieczeństwa (ang. KPI - Key Performance Indicators),
– zaktualizowane regulaminy bądź procedury testowania krytycznych systemów informacyjnych, komentarze do przeglądu bądź dzienniki zmian,
– dokumentacja mierników bezpieczeństwa i ich przypisanie do systemu informacyjnego, dla którego zostały wdrożone,
– lista sprawozdań dotyczących oceny bezpieczeństwa i testów bezpieczeństwa,
– sprawozdania z poprzednich skanów bezpieczeństwa i testów bezpieczeństwa udokumentowane regulaminy bądź procedury oceny bezpieczeństwa i testowania które obejmują co najmniej następujące informacje: aktywa, które powinny zostać poddane ocenie; okoliczności, w jakich powinno to nastąpić; rodzaj przeprowadzanych ocen i testów bezpieczeństwa; częstotliwość przeprowadzania testów i ocen; zatwierdzone podmioty (wewnętrzne lub zewnętrzne); poziomy poufności na potrzeby oceny; a także wyniki testów oraz cele ocen i testów bezpieczeństwa,
– dokumentacja zmian wynikających z wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI.

[21] IoC (ang. *Indicator of Compromise*).
[22] ISAC (ang. *Information Sharing and Analysis Center*).

4.3. Metodyka zarządzania ryzykiem, szacowanie ryzyka

Organizacja powinna zarządzać ryzykiem wystąpienia incydentu cyberbezpieczeństwa w kontekście systemów informacyjnych służących do świadczenia usługi kluczowej. Proces ten jest złożony ze skoordynowanych działań w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka wystąpienia incydentu.

Na proces zarządzania ryzykiem składa się:

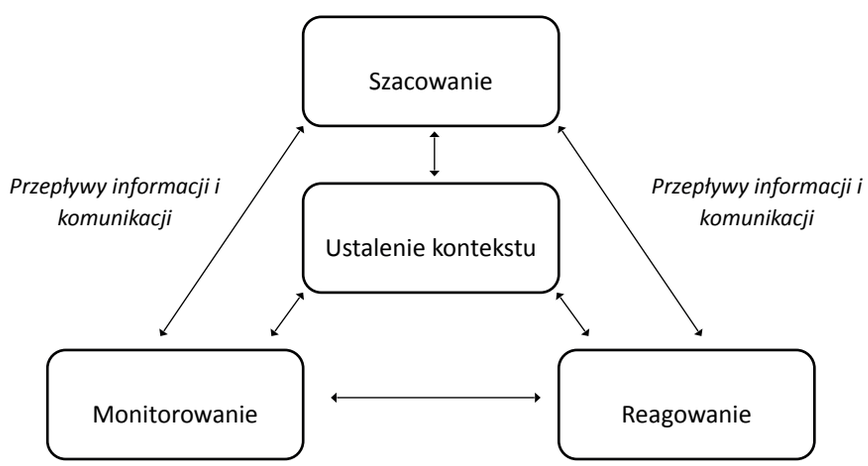
a) Ustalenie kontekstu[23] – określenie zbioru założeń, ograniczeń, tolerancji ryzyka oraz priorytetów i kompromisów, które kształtują podejście organizacji do zarządzania ryzykiem;

b) Szacowanie ryzyka – proces identyfikacji zagrożeń dla operacji prowadzonych przez organizację (w tym misji, działań, wizerunku, reputacji), zasobów organizacyjnych, jednostek i pozostałych podmiotów. Jako jeden z elementów zarządzania ryzykiem, obejmuje analizę zagrożeń i podatności na te zagrożenia oraz uwzględnia środki zaradcze zapewniane przez planowane lub już wdrożone środki bezpieczeństwa;

c) Reagowanie na ryzyko – akceptowanie, unikanie, ograniczanie, podział lub przenoszenie ryzyka na operacje organizacji (misję, funkcje, wizerunek lub reputację), zasoby organizacji, jednostki i pozostałe podmioty;

d) Monitorowanie ryzyka – utrzymanie ciągłej świadomości w zakresie ryzyk dotyczących organizacji, strategii zarządzania ryzykiem i powiązanych działań, w celu wspierania decyzji odnośnie ryzyk.

Rysunek 1 – Proces zarządzania ryzykiem.



Źródło: *opracowanie własne na podstawie NIST SP 800-30, „Guide for Conducting Risk Assessments", 2012, s. 4.*

Wzorcowo, zarządzanie ryzykiem wystąpienia incydentu cyberbezpieczeństwa w kontekście systemów informacyjnych służących do świadczenia usługi kluczowej powinno być elementem szerszego zarządzania ryzykiem w organizacji – składającego się z zarządzania ryzykiem dla realizowanych procesów oraz dla całej organizacji, co prezentuje poniższy rysunek:

[23] ang. *risk framing.*

Rysunek 2 – Wzorcowa struktura zarządzania ryzykiem w organizacji:

Źródło: *opracowanie własne na podstawie NIST SP 800-39, „Managing Information Security Risk: Organization, Mission, and Information System View", 2011, s. 32.*

Do prowadzenia zarządzania ryzykiem wystąpienia incydentu cyberbezpieczeństwa w kontekście systemów informacyjnych służących do świadczenia usługi kluczowej, czy też jego oszacowania, niezbędna jest uprzednia inwentaryzacja tych systemów informacyjnych. Propozycje w zakresie przeprowadzania inwentaryzacji systemów informacyjnych służących do świadczenia usługi kluczowej zostały przedstawione w rekomendacji dotyczącej zarządzania aktywami.

Publicznie dostępnym standardem, przedstawiającym propozycję procedury zarządzania ryzykiem jest NIST SP 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*. Składa się ona z następujących kroków:

1. Ustalenie kontekstu:
   1) Identyfikowanie założeń, które wpływają na sposób oceny ryzyka, reagowania na nie i monitorowania go w organizacji;
   2) Określenie ograniczeń dotyczących szacowania ryzyka, odpowiedzi na ryzyko oraz czynności związanych z monitorowaniem go w organizacji;
   3) Określenie poziomu tolerancji ryzyka dla organizacji;
   4) Określenie priorytetów i kompromisów rozważanych przez organizację w zarządzaniu ryzykiem.

   Wynikiem powyższych czynności powinno być sformułowanie strategii zarządzania ryzykiem, która określa, w jaki sposób organizacja zamierza oceniać, reagować i monitorować ryzyko na przestrzeni czasu. Ten krok tworzy również zestaw zasad organizacyjnych, procedur, standardów, wskazówek i zasobów obejmujących tematy dotyczące procesu zarządzania ryzykiem dla organizacji. Wyniki tego etapu stanowią bazę dla realizacji kolejnych kroków.

2. Szacowanie ryzyka:
   1) Identyfikowanie zagrożeń i podatności w zabezpieczeniach systemów informacyjnych używanych przez organizację, jak i dla środowisk w których działają systemy;
   2) Określenie ryzyka dla operacji realizowanych przez organizację, a także zasobów, jednostek, innych organizacji oraz pozostałych podmiotów, jeśli scharakteryzowane zagrożenia wykorzystują zidentyfikowane podatności w zabezpieczeniach.

Realizacja tego kroku określa ryzyka dla operacji prowadzonych przez organizację (tj. misji, funkcji, wizerunku i reputacji), jej zasobów, jednostek oraz innych podmiotów. W pewnych okolicznościach poziom ryzyka szczątkowego może doprowadzić do ponownego oszacowania ryzyka. Ponowna ocena zazwyczaj ma charakter przyrostowy (ocenia się tylko nowe informacje) oraz różnicowy (ocenia się w jaki sposób nowe informacje zmieniają ogólne określenie ryzyka).

Wyniki powyższych czynności mogą stanowić przydatne dane wejściowe dla etapów ustalania kontekstu i monitorowania ryzyka. Dla przykładu, scharakteryzowanie ryzyk może spowodować powrócenie do etapu określania tolerowanego ryzyka dla organizacji, ustalonego podczas kroku ustalania kontekstu. Jeśli organizacja ustala pewne kryteria podczas tego kroku, a gdy wyniki oceny ryzyka nie uzasadniają reakcji na ryzyko, wówczas wyniki tej oceny mogą być bezpośrednio przekazywane do etapu monitorowania ryzyka jako dane wejściowe.

3. Reagowanie na ryzyko:
   1) Określenie alternatywnych kierunków działania w celu reagowania na ryzyko zidentyfikowane w procesie szacowania ryzyka;
   2) Ocena alternatywnych kierunków działania w odpowiedzi na ryzyko;
   3) Podjęcie decyzji w sprawie odpowiednich działań w celu reagowania na ryzyko;
   4) Implementacja działań określonych w celu reagowania na ryzyko.

   Wynikiem kroku reagowania na ryzyko jest wdrożenie wybranych kierunków działania. Jednocześnie ma miejsce bieżąca komunikacja i udostępnianie informacji w zakresie ryzyka z jednostkami lub częściami organizacji, na które reakcje na ryzyko mogą mieć wpływ (w tym potencjalne działania, które musiałyby zostać podjęte przez jednostki lub części organizacji).

   Oprócz kroku monitorowania ryzyka, produkty z etapu reagowania na ryzyko mogą być użyte w etapach ustalania kontekstu i szacowania ryzyka. Na przykład możliwe jest, że analiza przeprowadzona podczas oceny alternatywnych kierunków działania może podważyć niektóre aspekty strategii reagowania na ryzyko, które są częścią strategii zarządzania ryzykiem opracowanej podczas kroku ustalania kontekstu. W takich przypadkach organizacje używają tych informacji w ustalaniu kontekstu, by powrócić do strategii zarządzania ryzykiem oraz związanej z nią strategii reagowania na ryzyko. Organizacje mogą również podczas oceny alternatywnych kierunków działania w celu reagowania na ryzyko określić, że niektóre aspekty szacowania ryzyka są niekompletne lub nieprawidłowe. Informacje te mogą być wówczas wykorzystane w etapie oceny ryzyka, co może prowadzić do dalszej analizy lub ponownego szacowania ryzyka.

4. Monitorowanie ryzyka:
   1) Opracowanie strategii monitorowania ryzyka dla organizacji obejmującej cel, typ i częstotliwość działań monitorujących;
   2) Bieżące monitorowanie systemów informacyjnych organizacji i środowisk, w których działają, w celu weryfikacji zgodności, określenia skuteczności środków reagowania na ryzyko oraz określenia zmian.

   Informacje uzyskane w trakcie etapu monitorowania ryzyka mogą być przydatne przy ustalaniu kontekstu, szacowaniu ryzyka oraz reagowaniu na nie. Na przykład wyniki monitorowania zgodności mogą prowadzić do ponownej potrzeby przeanalizowania pewnej części implementacji odpowiedzi na ryzyko, podczas gdy wyniki monitorowania skuteczności mogą ujawnić potrzebę ponownego przeanalizowania całego kroku odpowiedzi na ryzyko. Wyniki monitorowania zmian

w systemach informacyjnych i środowiskach w których działają, mogą wymagać od organizacji ponownego zbadania kroku szacowania ryzyka. Wyniki etapu monitorowania ryzyka mogą również służyć krokowi ustalania kontekstu, na przykład, gdy organizacja odkryje nowe zagrożenia lub podatności wpływające na założenia dotyczące ryzyka oraz tolerancji na nie[24].

Prócz oparcia się na dostępnych procedurach zarządzania ryzykiem i jego szacowania, jak przywołane standardy serii NIST SP 800-30 i 39 oraz normy ISO 27001, 27005 czy 31000, organizacja może opracować własne metody i procedury w tym zakresie.

Istotnym czynnikiem w zarządzaniu ryzykiem jest częstotliwość jego szacowania oraz monitorowania. Realizacja tych czynności (w formie zautomatyzowanej lub ręcznej) może być podyktowana misją organizacji, jej funkcjami biznesowymi czy też zdolnością do wykorzystania wyników monitorowania ryzyka w celu nabycia większej świadomości sytuacyjnej. Zwiększony poziom tej świadomości, w zakresie stanu bezpieczeństwa systemów informacyjnych organizacji oraz środowisk w jakich działają, pomaga organizacjom w lepszy sposób postrzegać i rozumieć ryzyko. W większości sytuacji monitorowanie jest najbardziej efektywne i opłacalne w przypadku użycia automatyzacji tego procesu. Może ono przynieść znaczne korzyści, zwłaszcza gdy takie działanie ogranicza przeciwnikom możliwość zdobycia punktu zaczepienia w organizacji (za pośrednictwem systemów informacyjnych lub środowisk, w których te systemy działają). Gdy organizacja stosuje monitorowanie w trybie ręcznym, zazwyczaj nie jest możliwe jego wykonywanie z częstotliwością, którą umożliwia automatyzacja[25]. UKSC nie precyzuje, z jaką częstotliwością powinno być prowadzone szacowanie ryzyka przez operatora usługi kluczowej. Określa jedynie, iż obowiązkiem operatora jest „prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem"[26]. *Rekomenduje się jednak, by operator usługi kluczowej przeprowadzał ten proces nie rzadziej, niż co 12 miesięcy*[27].

Dla wsparcia procesu szacowania ryzyka wystąpienia incydentu cyberbezpieczeństwa w systemach informacyjnych służących do świadczenia usługi kluczowej, został opracowany wzór formularza dla operatorów usługi kluczowej. Pozwala on określić poziom dojrzałości organizacji w zakresie cyberbezpieczeństwa, co może być pomocne w procesie szacowania ryzyka i określaniu katalogu stosowanych zabezpieczeń. Formularz został oparty o ramy doskonalenia cyberbezpieczeństwa dla infrastruktury krytycznej opracowane przez amerykański Narodowy Instytut Standardów i Technologii (ang. *National Institute of Standards and Technology*, NIST)[28].

Na tej podstawie można określić minimalną listę podstawowych wymagań cyberbezpieczeństwa, który musi spełnić operator usługi kluczowej – załączniki nr 4 i 5, a także na poziomie średnim i rozszerzonym.

Stosownie do poziomu dojrzałości cyberbezpieczeństwa organizacji oszacowanego za pomocą formularza, poziom ten można odnieść do tabeli zawartej w punkcie 14, przypisującej środki zaradcze odpowiednim poziomom dojrzałości. Dzięki temu organizacja ma możliwość określenia obecnego poziomu swej dojrzałości w tym kontekście oraz ustalenia pożądanego poziomu do osiągnięcia w przyszłości, poprzez porównanie wdrożonych i niewdrożonych zabezpieczeń.

[24] NIST SP 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*, 2011, s. 34-48.
[25] *Ibidem*, s. 47-48.
[26] Art. 8 pkt 1 UKSC.
[27] Źródło: *https://www.gov.pl/web/cyfryzacja/operatorzy-uslug-kluczowych.*
[28] NIST *Framework for Improving Critical Infrastructure Cybersecurity version 1.1*, 2018, s. 23-44.

Załącznik nr 1 – wzór formularza weryfikacji dojrzałości cyberbezpieczeństwa organizacji.

Dowody kontroli:

- *wytyczne dla personelu dotyczące oceny ryzyka, lista zagrożeń oraz dowody aktualizacji/przeglądów list i wykazów,*
- *dokumentacja procesu przeglądu i aktualizacji metodyki zarządzania ryzykiem bądź stosownych narzędzi. Harmonogram i ogólny plan cyklu przeglądu,*
- *dowody uczestnictwa personelu w szkoleniu (na przykład przyjęte zaproszenie, data i program szkolenia, podpisana lista uczestników warsztatów uświadamiających itp.),*
- *mapa ryzyka uwzględnia incydenty poważne wskazane dla sektora, w którym działa operator usługi kluczowej.*

4.4. Plan postępowania z ryzykiem

Organizacja w ramach procesu zarządzania ryzykiem i reagowania na nie, powinna ustanowić plan postępowania z ryzykiem, w szczególności dla ryzyka na poziomie wyższym niż akceptowalny.

Aktywom oraz działaniom organizacji, w szczególności tym, dla których ryzyko określone w trakcie procesu szacowania ryzyka przekroczyło akceptowalny poziom, powinny zostać przypisane środki ograniczające je, m.in. takie jak:

- wdrożenie dodatkowych zabezpieczeń,
- świadoma akceptacja ryzyka o poziomie ponad dopuszczalny przez najwyższe kierownictwo organizacji,
- przeniesienie ryzyka (np. poprzez ubezpieczenie),
- unikanie ryzyka.

Każde z powyższych działań pozwala ograniczyć oszacowane ryzyko lub je zaakceptować. Mimo to, po przedsięwzięciu powyższych środków, ryzyko może nadal być obecne na pewnym poziomie, co określa się mianem *ryzyka szczątkowego* – nie jest bowiem możliwa jego zupełna eliminacja. Z tego powodu środki ograniczające ryzyko, po ich zastosowaniu powinny zostać poddane ewaluacji pod kątem ich skuteczności.

Ponadto, najwyższe kierownictwo powinno zaakceptować i być świadome zarówno działań sformułowanych i wdrożonych w planie postępowania z ryzykiem o nieakceptowalnym poziomie, jak i istnienia oraz poziomu ryzyka szczątkowego. Bezpieczeństwo, jak każda inwestycja, niesie za sobą pewien poziom opłacalności. Istnieje bowiem zawsze pewna granica, kiedy kolejne inwestycje nie przyniosą istotnej korzyści pod kątem zwiększenia bezpieczeństwa, a ich koszty stają się niewspółmiernie wysokie[29].

Jako katalog dodatkowych zabezpieczeń, który może okazać się pomocny także przy obniżaniu poziomu ryzyka nieakceptowalnego, należy wskazać ten zawarty w formularzu weryfikacji dojrzałości organizacji pod kątem cyberbezpieczeństwa, stanowiącym załącznik nr 1 do niniejszego opracowania.

[29] J. Krawiec, G. Ożarek, *System Zarządzania Bezpieczeństwem Informacji w praktyce. Zabezpieczenia*, Warszawa 2014, s. 42-43.

Dowody kontroli:

– *wytyczne dla personelu dotyczące oceny ryzyka, lista zagrożeń oraz dowody aktualizacji/przeglądów list i wykazów,*

– *dokumentacja procesu przeglądu i aktualizacji metodyki zarządzania ryzykiem bądź stosownych narzędzi. Harmonogram i ogólny plan cyklu przeglądu,*

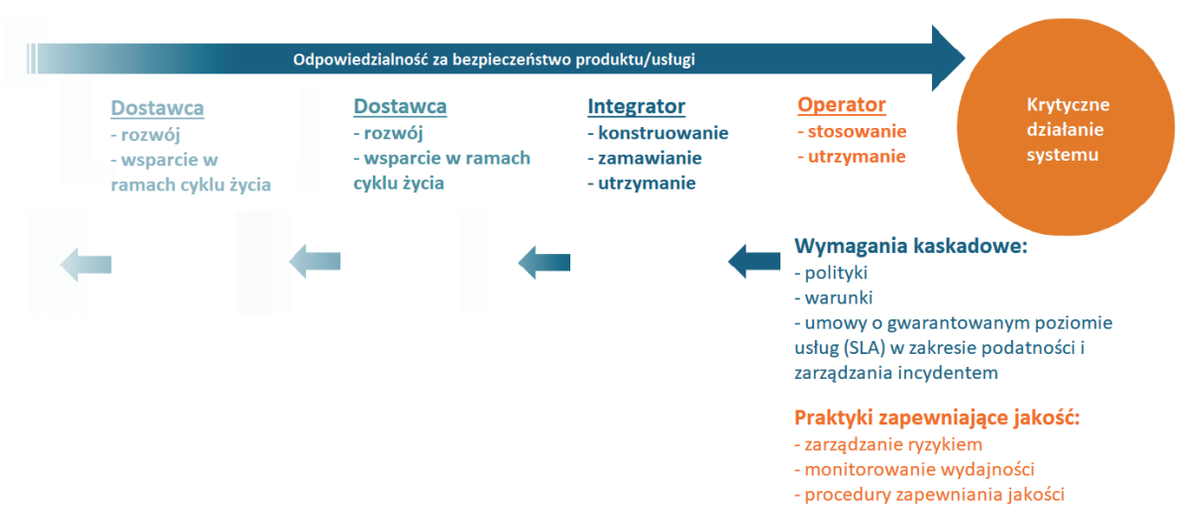
– *wykazy centralnie zarządzanych krytycznych zasobów i konfiguracji systemów, które są zarządzane i utrzymywane.*

5. Zarządzanie stroną trzecią

W warunkach globalnej gospodarki większość podmiotów gospodarczych, w tym także z sektora energii nie jest w stanie działać bez wsparcia innych firm, a ich otoczenie tworzy wiele stron trzecich wspierających realizację założeń biznesowych, dostarczających odpowiednie rozwiązania organizacyjne czy techniczne. Z racji tego, operatorzy usług kluczowych powinni posiadać odpowiednie procedury zapewniające sprawne i efektywne zarządzanie relacjami ze stronami trzecimi.

Zarządzanie relacjami ze stroną trzecią jest nierozerwalnie powiązane z bezpieczeństwem łańcucha dostaw. Ważnym aspektem tego procesu jest świadomość, że wraz z wydłużającym się łańcuchem dostaw, rozmywa się kwestia odpowiedzialności za bezpieczeństwo danego produktu czy usługi. Jest to efektem braku relacji pomiędzy poddostawcami czy podwykonawcami, a podmiotem nabywającym dany produkt czy usługę. Tę zależność przedstawia poniższy rysunek.

Rysunek 3 – Podstawy bezpieczeństwa łańcucha dostaw.



Źródło: Opracowanie własne na podstawie *Smart Grid Task Force Expert Group 2. Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity, Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management. Final Report*, 2019, https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

Głównym zadaniem operatora usługi kluczowej jest zarządzanie i utrzymanie krytycznych systemów, zazwyczaj dostarczanych przez integratora, który zbudował dany produkt czy usługę, a także je rozwija. Produkty wytworzone przez integratora opierają się na dostawach gwarantowanych przez inne podmioty, które również korzystają z produktów/usług zewnętrznych dostawców, a niejednokrotnie zlecają wykonanie danego zlecenia przez podwykonawców. Jak widać, tworzy się pewien łańcuch zależności, w którym operator usługi kluczowej powinien zarządzać cyberbezpieczeństwem

(na podstawie m.in. założeń norm ISO/IEC 27002:2013 czy ISO/IEC 27019:2017). Kontrola operatora w tym zakresie powinna obejmować polityki, wymagania, zarządzanie ryzykiem, podatnościami i zarządzanie incydentem, monitorowanie i tworzenie procedur oraz monitorowanie jakości dostarczanych produktów i usług. Bezpieczeństwo łańcucha dostaw budowane jest na zaufaniu do bezpośredniego dostawcy danego rozwiązania. Zatem, operator tworzy pewne ramy współpracy ze swoimi bezpośrednimi partnerami poprzez opracowanie m.in. polityki cyberbezpieczeństwa, wymagań względem danego produktu/usługi, umowy o zagwarantowaniu jakości usługi/produktu, w tym ważne jest ustalenie kwestii obsługi podatności bądź incydentów w ramach danej usługi czy produktu. Ponadto, operator powinien stworzyć odpowiednie procedury zarządzania ryzykiem w relacjach ze stronami trzecimi, weryfikacji jakości dostarczonego produktu lub usługi, a także monitorowania wydajności dostarczonych zamówień. Na tej podstawie, integrator bądź dostawca powinien opracować odpowiednie wymagania względem swoich dostawców i podwykonawców, a także powinien wdrożyć praktyki zapewniania jakości w ramach swojej organizacji[30].

5.1. Umowy z podmiotami trzecimi

Zaleca się by operator usługi kluczowej uwzględnił w swojej analizie ryzyka element dotyczący ryzyka prawnego wynikającego z zawieranych umów z podmiotami zewnętrznymi i dostawcami usług/sprzętu.

Analiza ryzyka (patrz rozdział 4 Rekomendacji) powinna uwzględniać wszelkie zagrożenia dla organizacji, które mogą wynikać z podpisania umów z różnymi podmiotami zewnętrznymi (np. na zakup sprzętu, oprogramowania, outsourcing usług itp.), w tym ich sytuację finansowo-ekonomiczną, kwestie właścicielskie, pozycję na rynku oraz wiarygodność (mierzona np. na podstawie wcześniejszych kontraktów). Będzie to również pomocne do określenia czy z danym podmiotem zewnętrznym należy podpisać umowę o zachowaniu poufności, zwłaszcza, jeżeli umowa, np. na dostawę oprogramowania, zawiera w sobie szczegóły tworzonego rozwiązania dedykowanego dla konkretnego operatora. Odpowiednia analiza ryzyka wesprze również proces ustalenia wysokości kar za naruszenie zapisów umowy o poufności. Właściwie przeprowadzona analiza ryzyka pomoże również operatorowi ustalić poziom uzależnienia od danego dostawcy, a tym samym uniknąć ryzyka tzw. *vendor lock*, co oznacza uzależnienie od jednego dostawcy. Taka sytuacja może wiązać się np. z niekorzystnymi zapisami dotyczącymi możliwości rozwoju czy korzystania z danego rozwiązania (produktów, usług), zwłaszcza w przypadku zerwania umowy z dostawcą bądź jego upadłości (dotyczy to przepisów w zakresie własności intelektualnej). W tym celu, operator usługi kluczowej powinien na etapie negocjowania umowy z podmiotem zewnętrznym na dostawę usługi wykonywanej na indywidualne zlecenie operatora (chodzi tu o rozwiązanie przygotowywane do wdrożenia wyłącznie w danym podmiocie, a nie powszechnie dostępnych usług czy oprogramowania) zawrzeć zapisy dotyczące przeniesienia autorskich praw majątkowych na OUK w zakresie umożliwiającym dalsze rozwijanie i modyfikowanie danego produktu, bądź zapisy dotyczące zapewnienia długotrwałej licencji gwarantującej samodzielny rozwój aplikacji czy oprogramowania przez operatora usługi kluczowej. Zastosowanie wskazanych zapisów powinno być poprzedzone analizą własnych potrzeb i możliwości danego operatora usługi kluczowej[31].

[30] Smart Grid Task Force Expert Group 2. Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity, Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management. Final Report, 2019, [PDF] s. 82-83, https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf [dostęp: 06.05.2021].

[31] Narodowy Program Ochrony Infrastruktury Krytycznej 2020. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Rządowe Centrum Bezpieczeństwa, [PDF], s. 113-114, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 11.05.2021].

Operator usługi kluczowej powinien opracować i stosować procedury zarządzania dostępem stron trzecich.

Procedura zarządzania dostępem stron trzecich do systemów operatora usługi kluczowej powinna zawierać jasno sprecyzowane zapisy dotyczące m.in. zakresu uprawnień dostawcy do systemów, sposobu realizacji połączenia w razie konieczności zdalnego świadczenia usług serwisowych czy aktualizacyjnych (np. jasno zdefiniowany kanał połączenia, sposoby uwierzytelnienia, osoby uprawnione do nawiązania takiego połączenia itd.), minimalnych wymagań monitorowania aktywności w systemie, segmentacji logicznej, kontroli i zapisów sesji itp. Wspomniane kwestie powinny również zostać uregulowane na poziomie umowy z podmiotami trzecimi, w tym także należy zawrzeć informacje dotyczące ustanowienia punktu kontaktowego (konkretne osoby) wraz ze sposobami komunikacji, w tym numery telefonów, adresy e-mail itp.[32]

Rekomenduje się by operator usługi kluczowej stworzył procedury monitorowania opracowywanych opisów zamówień publicznych i umów pod kątem ich rzetelności i bezstronności.

Opracowywane opisy zamówień publicznych i umowy powinny być sporządzane z należytą starannością, a także w sposób obiektywny. Weryfikacja tego typu dokumentów pozwoli na ograniczenie ryzyka związanego z pisaniem opisów czy umów pod kątem konkretnego produktu czy dostawcy, dzięki czemu operator będzie mógł uzyskać bardziej konkurencyjną ofertę.

Zaleca się by operator usługi kluczowej zawierał w umowach dotyczących systemów automatyki przemysłowej zapisy chroniące aktywa tych systemów.

W tym celu, operator usługi kluczowej powinien włączyć w prace nad umowami z dostawcami pracowników komórki odpowiedzialnej za bezpieczeństwo systemów, których zadaniem powinno być sprawdzenie tego rodzaju umów pod kątem ich wpływu na bezpieczeństwo już wdrożonych systemów[33], prac modernizacyjnych i remontowych, a także, w ramach możliwości, nowych systemów.

Rekomenduje się by w umowach z podmiotami trzecimi znalazły się zapisy regulujące kwestię aktualizacji oprogramowania oraz zapewnienia implementacji odpowiednich „łatek bezpieczeństwa" do systemów zakupionych od danego podmiotu.

Operator usługi kluczowej powinien mieć zapewnioną aktualizację oprogramowania i łatki bezpieczeństwa do wszystkich systemów wykorzystywanych do świadczenia usługi kluczowej, jeżeli są one nabywane od dostawcy. Zapisanie odpowiednich procedur wdrażania aktualizacji systemów i łatek bezpieczeństwa jest kluczowe w celu zapewnienia odporności na nowe zagrożenia. Takie regulacje powinny dotyczyć systemów automatyki przemysłowej, a także oprogramowania układowego, systemów sterowania i wizualizacji, aplikacji bazodanowych i innych zakupionych od podmiotów zewnętrznych[34]. W zależności od okresu wykorzystywania danych systemów, operator powinien mieć zapewnioną możliwość aktualizacji systemu i implementacji łatek bezpieczeństwa do czasu zakończenia eksploatacji systemu bądź zaprzestania jego rozwijania przez producenta.

[32] *Standardy i dobre praktyki ochrony infrastruktury krytycznej. Automatyka przemysłowa w sektorze elektroenergetycznym*, Rządowe Centrum Bezpieczeństwa, 2019, [PDF] s. 18.
[33] *Standardy i dobre praktyki ochrony infrastruktury krytycznej. Automatyka przemysłowa w sektorze elektroenergetycznym*, Rządowe Centrum Bezpieczeństwa, 2019, [PDF] s. 18.
[34] *Standardy i dobre praktyki ochrony infrastruktury krytycznej. Automatyka przemysłowa w sektorze elektroenergetycznym*, Rządowe Centrum Bezpieczeństwa, 2019, [PDF] s. 18.

Należy przy tym podkreślić, że w przypadku sektora energetycznego mogą istnieć ograniczenia dotyczące aktualizacji związane z fizyczną strukturą sieci. Wdrażanie poprawek może wymagać np. zatrzymania produkcji operacyjnej. W związku z tym, aktualizacja może być przeprowadzona tylko podczas prac konserwacyjnych i naprawczych, które mogą występować w perspektywie wieloletniej. Zatem, operatorzy powinni rozważyć środki uzupełniające, takie jak segregacja systemów lub dodanie zewnętrznych barier ochronnych, w przypadku gdy należałoby zainstalować poprawkę lub przeprowadzić aktualizację, ale nie jest to możliwe (np. w przypadku niewspieranych produktów). Krokiem w kierunku zwiększenia bezpieczeństwa jest też podział instalacji na kilka stref o różnych poziomach ryzyka i krytyczności. Ważną kwestią jest współpraca z dostawcami technologii w celu zastąpienia starszych systemów, gdy jest to korzystne ze względów bezpieczeństwa, ale z uwzględnieniem krytycznych funkcji systemu[35]. Ponadto, zaleca się by w ramach umów z dostawcami uwzględnić zapisy dotyczące procedur odbiorowych, gdzie skanowanie i analiza podatności powinna być obligatoryjna, a wykryte podatności traktowane jako wada produktu objętego umową.

Organizacja powinna posiadać wdrożone procedury związane z zachowaniem bezpieczeństwa informacji przy współpracy z podmiotami zewnętrznymi, które obejmowałyby produkty, procesy czy usługi. W zawieranych umowach z podmiotami zewnętrznymi powinny znajdować się odpowiednie zapisy w tym zakresie.

W tym celu, operator usługi kluczowej powinien nadzorować dostęp stron trzecich do warstwy kontrolnej i produkcyjnej, zezwalając na ich dostęp na żądanie w określonym przedziale czasowym, w określonym celu i z możliwie jak najmniejszymi uprawnieniami, stosownie do potrzeb. Jeżeli operator usługi kluczowej nie ma możliwości zapewnienia całodobowej i szybkiej obsługi systemów w celu przydzielenia dostępu *ad hoc*, zwłaszcza w czasie wystąpienia awarii, wówczas zaleca się wprowadzenie nadzorowanych i nagrywanych sesyjnie dostępów zdalnych z zachowaniem technik mikrosegmentacji logicznej. Ponadto, zaleca się by dostawca usług nie miał bezpośredniego połączenia do warstwy kontrolnej i produkcyjnej przedsiębiorstwa, chyba, że wymaga tego umowa serwisowa. Powinno się zezwolić im na dostęp wyłącznie do niezbędnych, określonych funkcji i części sieci.

Powinno się skłonić dostawców usług do bieżącego informowania o bezpieczeństwie przeprowadzanych procesów i usług, a także do informowania o postępach prowadzonych działań. Należy opracować wymagania bezpieczeństwa w zakresie współpracy z dostawcami i usługodawcami.

Stosowne dokumenty wraz z procedurami powinny zostać opracowane w celu zachowania komunikacji pomiędzy podmiotami zewnętrznymi a operatorem usługi kluczowej. Jest to również o tyle ważne, że działania prowadzone przez dostawców powinny być uprzednio uzgodnione z operatorem w celu wyeliminowania zagrożenia zablokowania systemów, a przede wszystkim w celu odpowiedniego przygotowania systemów do działań związanych np. z aktualizacją oprogramowania (patrz rozdział 6.5. Rekomendacji).

Zaleca się by operator usługi kluczowej w ramach zawieranych umów z podmiotami zewnętrznymi uwzględnił mechanizmy sankcyjne.

Zawarcie odpowiednich zapisów nadających operatorowi uprawnień do np. potrącenia bądź nałożenia kary umownej na podmiot zewnętrzny w przypadku niewywiązywania się z zapisów umowy,

[35] Zalecenia Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. *w sprawie cyberbezpieczeństwa w sektorze energetycznym* i Commission Staff Working Document Accompanying Commission Recommendation on cybersecurity in the energy sector {C(2019) 2400 final}.

gwarantuje jakość wykonania zlecenia. Dodatkowo, operator powinien również mieć zagwarantowane prawo do rozwiązania umowy w przypadku rażących naruszeń zawartej umowy. Ponadto, w umowie powinny znaleźć się zapisy dotyczące procedury, kiedy powyższe mechanizmy można zastosować[36]. Ponadto, operator usługi kluczowej powinien rozważyć możliwość opracowania i wdrożenia procedury kwalifikacji zaimplementowanej w proces odbiorowy, co może podnieść prawdopodobieństwo dostawy żądanych produktów i usług na zadawalającym poziomie.

Umowy dotyczące oprogramowania systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej zawierane z podmiotami zewnętrznymi powinny zawierać odpowiednie zapisy mające na celu zwiększenie bezpieczeństwa tych systemów.

Umowy w zakresie oprogramowania systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych powinny zawierać m.in.:

- Zobowiązanie dostawcy do sprawdzenia danego oprogramowania pod kątem posiadanych luk bezpieczeństwa i poinformowanie operatora o istniejących lukach,
- Deklarację, że architektura dostarczonego oprogramowania umożliwia usunięcie ewentualnych luk bezpieczeństwa wykrytych w ramach cyklu życia oprogramowania,
- Wykaz wszystkich komponentów dostarczonego oprogramowania,

Deklaracje producentów oprogramowania co do stosowanych przez nich zasad usuwania wykrytych luk bezpieczeństwa, zasad informowania użytkowników o wykrytych lukach bezpieczeństwa oraz zasad dystrybucji poprawek[37].

Dowody kontroli:

– udokumentowana analiza ryzyka w kontekście umów z podmiotami zewnętrznymi,

– udokumentowana polityka bezpieczeństwa dotycząca relacji z podmiotami zewnętrznymi,

– wykazy wszystkich umów z podmiotami zewnętrznymi,

– wymagania dotyczące bezpieczeństwa są wyraźnie uwzględnione w umowach z podmiotami zewnętrznymi dostarczającymi produkty IT, usługi IT, procesy biznesowe, pomoc techniczną, itp.

[36] Narodowy Program Ochrony Infrastruktury Krytycznej 2020. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Rządowe Centrum Bezpieczeństwa, [PDF], s. 115, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 13.05.2021].

[37] Narodowy Program Ochrony Infrastruktury Krytycznej 2020. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Rządowe Centrum Bezpieczeństwa, [PDF], s. 115, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 14.05.2021].

5.2. Monitorowanie usług świadczonych przez strony trzecie, weryfikacja rozwiązań w oparciu o uzgodnione kryteria

Rekomenduje się by zapisy w umowach oraz ich realizacja opierała się m.in. na przeprowadzonym wcześniej szacowaniu ryzyka w organizacji. Analiza ryzyka powinna także pomóc w zidentyfikowaniu obszarów krytycznych, np. eksploatacji systemu informacyjnego, ciągłości działania usługi kluczowej, które powinny zostać uwzględnione w umowach, a które do tej pory były pomijane. Wykonana analiza ryzyka powinna objąć również uwarunkowania sytuacji losowych sił wyższych (np. epidemii), gdzie firma trzecia świadcząca usługę może nie być w stanie zapewnić pełnienia usługi na wystarczająco wysokim poziomie.

W umowach ze stronami trzecimi powinno się zawrzeć zapisy dotyczące monitorowania usług świadczonych przez strony trzecie oraz kryteria do weryfikacji rozwiązań, w szczególności dotyczących elementów zidentyfikowanych w procesie wyżej wspomnianej analizy ryzyka. W ramach analizy ryzyka operator powinien sklasyfikować systemy informacyjne i przetwarzane w nich informacje, a następnie powinien dokonać pewnej selekcji w zakresie identyfikacji i wyboru funkcjonalności oraz zabezpieczeń usługi, wybrać model danej usługi, przeprowadzić ocenę dostawców w celu dokonania odpowiedniego wyboru w oparciu o spełnienie przez dany podmiot określonych wymagań, by w końcu przystąpić do negocjacji poziomu usługi i określenia wymagań bezpieczeństwa. Ponadto, operator usługi kluczowej powinien dysponować personelem posiadającym doświadczenie i certyfikaty, który będzie w stanie opracować rzetelny i obiektywny opis zamówienia publicznego. Po podpisaniu umowy, operator powinien odpowiednio postępować z ryzykiem poprzez monitorowanie wdrożenia zabezpieczeń przez dostawcę, a następnie dokonanie oceny wdrożonych rozwiązań. W rezultacie operator może podjąć decyzję o uruchomieniu danej usługi. Następnie, operator powinien monitorować funkcjonowanie zabezpieczeń zarządzanych przez siebie, a także dokonać ich ponownej oceny i ewentualnej akredytacji.

Rekomendowane jest monitorowanie wskazanych w umowie ram czasowych realizacji umowy, np. wdrażania usługi, oraz wskazanie kryteriów do monitorowania i oceny realizacji umowy.

Zaleca się by organizacja wdrożyła wewnętrzne, formalne procedury bądź instrukcje dotyczące zakresu monitorowania i weryfikacji zawartych umów ze stronami trzecimi w celu ujednolicenia działań związanych z umowami, a także w celu udoskonalania wdrażanych rozwiązań zwiększających skuteczność i bezpieczeństwo działań w zakresie świadczonych usług. Wskazane jest także zdefiniowanie celów bezpieczeństwa. W zakresie zapisów umów, jak i własnych wewnętrznych procedur, rekomendowane jest by zidentyfikować najważniejsze kryteria oceny poszczególnych etapów realizowania umowy (oparte m.in. o wcześniejsze szacowanie ryzyka) pod kątem m.in. skuteczności oraz bezpieczeństwa rozwiązań. W zakresie najważniejszych kryteriów przy umowach dotyczących usług cyfrowych rekomendowane jest by znalazły się m.in. te dotyczące bezpieczeństwa danych (zarówno ważnych dla organizacji, jak i regulowanych przez ustawy), bezpiecznej lokalizacji (a w przypadku usług chmurowych – zgodności z przepisami prawa w zakresie lokalizacji przechowywania danych), bezpiecznego dostępu do usług (np. przy usłudze chmurowej unikanie tzw. pojedynczego punktu awarii czy też kwestie dostępu do danych zarówno własnych pracowników, jak i pracowników strony trzeciej), czy też elementów dotyczących bezpieczeństwa pod kątem utrzymania ciągłości świadczenia usługi kluczowej.

Rekomendowane jest wprowadzenie regulacji wewnętrznych w organizacji, a także regulacji w umowach dla kontrahentów realizujących zadania z wykorzystaniem systemów i usług informacyjnych organizacji, zobowiązujących pracowników do zgłaszania wszelkich zaobserwowanych lub możliwych do wystąpienia słabości związanych z bezpieczeństwem informacji w systemach lub usługach.

Rekomenduje się także wdrożenie wewnątrz organizacji procedur dot. monitorowania i audytowania dostawców usług i uwzględnienie tego w zapisach umów z dostawcami.

Zaleca się by operatorzy usług kluczowych w zakresie zawieranych kontraktów ze stroną trzecią stosowali umowy o gwarantowanym poziomie świadczenia usług (SLA – ang. Service Level Agreement) w celu ustalenia odpowiednich kryteriów monitorowania usługi świadczonej przez dostawcę.

Service Level Agreement to umowa pomiędzy odbiorcą i dostawcą danej usługi, w której definiuje się jakość świadczonych usług, a zwłaszcza określa się na jakim minimalnym poziomie dostawca będzie świadczyć daną usługę odbiorcy. Dokument ten powinien zawierać zapisy dotyczące specyfikacji technicznej poziomu świadczonych usług przez stronę trzecią, sposób kontrolowania poziomu usług oraz ustalenia dotyczące kwestii finansowych i prawnych. SLA powinna również regulować kwestię wymaganego poziomu dostępności (zazwyczaj określany poprzez procent dostępności danej usługi w ciągu roku), procedurę zgłaszania problemów związanych z działaniem danej usługi, a także proces nadzoru nad działaniem usługi, czyli monitorowanie usługi i raportowanie jej poziomu. Kluczowymi wskaźnikami w przypadku umów SLA są: czas reakcji i rozwiązania zgłoszonych problemów bądź zakłóceń oraz ustalenie wysokości kar finansowych za niewypełnienie ustaleń zawartych w SLA[38]. Ponadto, umowa SLA powinna również regulować takie kwestie jak, m.in. procedurę informowania o wykrytych lukach bezpieczeństwa, usuwanie wykrytych podatności, dystrybucja poprawek, aktualizacje oprogramowania itp. SLA ma również gwarantować stabilność działania procesu technologicznego realizowanego w oparciu o dostarczone rozwiązanie, zachowującego swoje parametry we wskazanych przez technologów granicach parametrycznych pracy poszczególnych komponentów, segmentów procesu i całości procesu. Ważne jest by w SLA wpisać również zasady zlecenia podwykonawcom realizacji różnych zadań związanych z świadczeniem danej usługi przez dostawcę, w tym wymóg stosowania równorzędnych zabezpieczeń wpisanych do umowy SLA[39].

Dowody kontroli:

- *udokumentowane uwagi lub dzienniki zmian polityki bezpieczeństwa dotycząca podmiotów zewnętrznych,*
- *wdrożony i utrzymywany regulamin bądź procedura oceny ryzyka dostawcy/zarządzania ryzykiem. Udokumentowane zmiany lub zakończenie relacji z podmiotami zewnętrznymi charakteryzującymi się wysokim ryzykiem,*
- *dokumentacja procesu przeglądu polityki bezpieczeństwa dotyczące podmiotów zewnętrznych, uwzględniające przeszłe zdarzenia.*

[38] *Service level agreements overview*, IBM, https://www.ibm.com/docs/en/control-desk/7.6.1.2?topic=application-service-level-agreements-overview [dostęp: 04.05.2021 r.]

[39] Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, 2020, s. 113-115, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 04.05.2021 r.].

5.3. Korzystanie z usług chmurowych

Środki bezpieczeństwa dotyczące korzystania z usług chmurowych powinny obejmować uwzględnienie aspektów bezpieczeństwa w umowach z dostawcami tego typu usług, a także unikania tzw. pojedynczych punktów awarii. Przy korzystaniu z usług chmurowych należy zabezpieczyć dane, które mają być przechowywane w chmurze.

1. Odpowiedzialność

Usługi chmurowe różnią się między sobą zarówno zestawem funkcji, jak i tym, kto dokładnie ponosi odpowiedzialność za zabezpieczenie poszczególnych elementów. W przypadku usług SaaS (ang. *Software as a Service*)[40] to operator zwykle dba o bezpieczeństwo aplikacji czy przesyłanych danych. W środowiskach IaaS (ang. *Infrastructure as a Service*[41]) to klient ma pełną kontrolę nad infrastrukturą, tj. oprogramowaniem, konfiguracją danych i aplikacji, kontrolą dostępu czy uwierzytelnieniem, i to klient jest wyłącznie odpowiedzialny za ich zabezpieczenie.

2. Zabezpieczanie danych

Poważnym zaniedbaniem administratorów jest przechowywanie w chmurze nieszyfrowanych danych. Większość dostawców chmury rekomenduje szyfrowanie danych i dostarcza niezbędne do tego narzędzia oraz usługi, które stanowią dodatkową, bardzo skuteczną warstwę zabezpieczeń, która chroni dane przed odczytaniem, nawet gdy dojdzie do wycieku lub kradzieży. Jeśli dostawca usług chmurowych zapewnia narzędzia kontroli bezpieczeństwa, które można włączyć, wówczas powinno się ich użyć. Niewybranie odpowiednich opcji zabezpieczeń może narazić organizację na materializację ryzyka. Jeśli to możliwe, należy też zachować pełną kontrolę nad kluczami szyfrującymi.

W celu ograniczenia ryzyka powiązanego z atakiem na chmurę, należy stosować zasadę wiedzy zerowej (ang. zero-knowledge) i zabezpieczyć wszystkie dane, zarówno te, które są przechowywane w chmurze, jak i te, które są w stanie transmisji. Należy planować wdrażanie funkcji związanych z bezpieczeństwem już na bardzo wczesnym etapie tworzenia czy implementowania danego rozwiązania.

Zabezpieczanie środowisk chmurowych powinno być procesem wieloetapowym, w którym należy stosować wiele różnych, nakładających się technologii z dziedziny bezpieczeństwa. Dzięki temu nawet jeśli któraś z warstw zostanie spenetrowana lub dojdzie do błędu użytkownika, wciąż jest duża szansa, że nasze zasoby pozostaną nienaruszone. Dlatego tak ważne jest np. korzystanie z uwierzytelniania wieloetapowego, znacznie wzmacniającego standardowe zabezpieczenie z wykorzystaniem loginu i hasła.

Ponadto należy pamiętać o tym, aby nie przechowywać danych organizacji w chmurze bez uzyskania uprzedniej zgody przełożonego. Przechowywanie danych organizacji w chmurze może nie tylko naruszyć zasady obowiązujące w organizacji, ale także naruszać prawa krajowe, narażając organizację na prawne konsekwencje.

Dodatkowo nawet jeśli dostawca usług chmurowych tworzy kopie zapasowe danych, warto zaplanować regularne tworzenie własnych, lokalnych kopii zapasowych. To nie tylko ochroni dane organizacji na wypadek zniknięcia usługodawcy, ale także sprawi, że łatwiej będzie odzyskać duże ilości danych z lokalnej kopii zapasowej niż pobranie danych z usługi chmurowej.

[40] SaaS – oprogramowanie jako usługa

[41] IaaS – infrastruktura jako usługa

3. Szacowanie ryzyka

Organizacja powinna w procesie szacowania ryzyka uwzględnić potencjalną możliwość[42]:

1) korzystania ze zweryfikowanych, aktualizowanych źródeł informacji o zagrożeniach specyficznych dla stosowania usług chmury obliczeniowej, w tym również w odniesieniu do konkretnych (nazwanych) usług;

2) korzystania z pomocy ze strony podmiotów lub osób o specjalistycznych kompetencjach zarówno w obszarze cyberbezpieczeństwa jak i usług chmury obliczeniowej, szczególnie w sytuacji braku takich kompetencji wewnątrz własnej organizacji;

3) przeanalizowania dostępnych wyników audytów zewnętrznych dostawców usług chmury obliczeniowej w odniesieniu do usług chmury obliczeniowej oraz procesu zarządzania bezpieczeństwem informacji, poszerzając zakres analizy o dostępne certyfikaty wystawione dostawcy usług chmury obliczeniowej potwierdzające spełnienie wymagań;

4) uprzedniego testowania usług chmury obliczeniowej, także przy wykorzystaniu scenariuszy warunków skrajnych, zarówno w zakresie sposobu działania usługi jak i jej konfiguracji.

Wyniki szacowania ryzyka powinny zostać formalnie zatwierdzone oraz podlegać okresowej weryfikacji i aktualizacji.

Uruchomienie produkcyjne stosowania usług chmury obliczeniowej powinien poprzedzać okres testowy, podczas którego na danych testowych (generowanych maszynowo lub w inny przypadkowy sposób), w udokumentowanym procesie, testowane są scenariusze adekwatne do oszacowanego ryzyka.

Organizacja powinna posiadać udokumentowany, przetestowany plan wycofania swojego zaangażowania w przetwarzanie informacji w usługach chmury obliczeniowej danego dostawcy (również w sytuacji awaryjnej), bez uszczerbku dla zachowania zgodności swojego działania z wymaganiami prawa.

Organizacja powinna posiadać udokumentowany plan ciągłości działania uwzględniający potencjalną możliwość utraty kontroli nad przetwarzanymi informacjami u danego dostawcy usług chmury obliczeniowej oraz możliwość przerwania ciągłości działania usługi. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej dostawców usług chmury obliczeniowej, organizacja powinna regularnie weryfikować własną zdolność do utrzymania deklarowanych założeń, w szczególności zgodność konfiguracji usług i odtwarzalności środowiska teleinformatycznego, zwłaszcza po zmianach technologicznych u jednego z dostawców usług chmury obliczeniowej.

4. Ochrona danych logowania

Hasła i klucze dostępu do usług chmurowych powinny być traktowane bardzo poważnie. Dla każdej aplikacji, zasobu, czy usługi należy tworzyć oddzielne, unikalne i odpowiednio silne hasła, a także pamiętać o ich regularnym zmienianiu. Dzięki temu nawet jeśli dojdzie do wycieku czy kradzieży danych, to jest duża szansa, że włamywacze przejmą nieaktualne hasło. Ważne jest również, by precyzyjnie przydzielać uprawnienia i nadawać użytkownikom dostęp tylko do niezbędnych zasobów wynikających z zakresu realizowanych zadań, a także w miarę możliwości stosować uwierzytelnienie wieloskładnikowe (ang. MFA).

W miarę możliwości należy zrezygnować z używania w codziennej pracy z wbudowanego konta systemowego *administrator/root*, nawet do zadań administracyjnych. Do tego celu należy wykorzystać konto

[42] Urząd Komisji Nadzoru Finansowego, Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, Warszawa, 23 stycznia 2020 r.

użytkownika z odpowiednio wysokim do wykonania danego zadania poziomem uprawnień. Takie konta powinny podlegać dedykowanej *polityce kont z wysokimi uprawnieniami*, która określa m.in. warunki korzystania z tych kont oraz odpowiednio skomplikowaną złożoność i długość hasła. Należy też regularnie sprawdzać, czy w systemie istnieją nieaktywne konta użytkowników. Jeśli tak, należy je usuwać.

5. Umowy z dostawcą usługi chmurowej

Jeżeli przeprowadzona analiza ryzyka dopuściła do zastosowania w danej organizacji usługi chmurowe, to należy dokładnie zapoznać się z umową o warunkach świadczenia usług i licencji SLA (ang. *Service Level Agreement* – szerzej w rozdziale 5.2) i EULA (ang. *End User License Agreement*) przed zapisaniem się do usługi. Powinno się także rozważyć podpisanie umowy z innymi dostawcami, jeśli istnieją warunki w umowie, których realizacja nie została wystarczająco precyzyjnie opisana/wyjaśniona dla prawidłowej oceny ich skutków dla organizacji.

W związku z powyższym należy zadbać o to, aby w umowach z dostawcami usług chmurowych uwzględnić, w szczególności, aspekty bezpieczeństwa i dostępności tych usług, a także przepisy prawa krajowego i unijnego oraz wewnętrzne regulacje danej organizacji[43]*. W szczególności w przypadku podmiotów uznanych za operatorów usługi kluczowej w sektorze energia dla usług chmurowych dla środowisk OT bądź serwerów przesiadkowych*[44] *(tzw. jump box) należy stosować poziom uzasadnienia zaufania o poziomie wysoki i odpowiadające im krajowe bądź europejskie programy (schematy) certyfikacji w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 (Aktu o cyberbezpieczeństwie).*

6. Pojedyncze punkty awarii

Pojedynczy punkt awarii, inaczej SPOF (ang. *single point of failure*)[45], jest potencjalnym ryzykiem związanym z wadą w projekcie, implementacji lub konfiguracji systemu, w którym jedna usterka lub awaria powoduje zatrzymanie działania całego systemu. Definicja SPOF obejmuje także krytyczny składnik systemu, który ma możliwość zatrzymania operacji systemowych podczas przełączania systemowego.

W przypadku przetwarzania w chmurze pojedynczy punkt awarii występuje zarówno w układzie sprzętowym, jak i programowym. Redundancja i klastry o wysokiej dostępności są kluczowymi czynnikami pozwalającymi na uniknięcie SPOF-ów. Do osiągnięcia tego celu potrzebna jest zarówno redundancja logiczna, jak i fizyczna. Gdy składnik systemu ulegnie awarii, inny składnik powinien natychmiast przejąć rolę uszkodzonego składnika. Przykładem może być konfiguracja bazy danych z wieloma lokalizacjami.

W przypadku użytkowania aplikacji opartych na chmurze oraz systemów scentralizowanych, należy unikać pojedynczych systemowych punktów awarii.

Dowody kontroli:

- *wytyczne, wzorcowe konfiguracje, opisy zasad, itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji;*
- *dokumentacja dotycząca zasad zbierania logów w związku z przetwarzaniem informacji w chmurze obliczeniowej stosownie do zakresu używanych usług,*
- *dokumentacja dotycząca certyfikacji dostawcy lub poddostawcy usług chmury obliczeniowej.*

[43] Agencja Unii Europejskiej ds. Cyberbezpieczeństwa ENISA, Good Practices for Security of Internet of Things in the context of Smart Manufacturing, 2018

[44] System zdalnego połączenia, który pozwala operatorowi zyskać dostęp do sieci OT z sieci korporacyjnej.

[45] Agencja Unii Europejskiej ds. Cyberbezpieczeństwa ENISA, Good Practices for Security of Internet of Things in the context of Smart Manufacturing, 2018

6. Cykl życia systemów informacyjnych

W obszarze technologicznym można wyróżnić kilka istotnych elementów, które wpływają na bezpieczeństwo systemu informacyjnego. Kluczowym elementem w obszarze technologicznym jest bezpieczeństwo oprogramowania, definiowanie jako występowanie błędów, które mogą pozwalać na przejęcie kontroli nad aplikacją, urządzeniem bądź systemem. W tym zawiera się również odporność systemu transmisyjnego na zakłócenia, czyli zabezpieczenie transmisji danych przed przechwyceniem lub zniekształceniem informacji. Ponadto w obszarze technologicznym należy uwzględnić takie czynniki jak odporność na warunki pracy i wpływ środowiska, a także niezawodność funkcjonowania w cyklu życia urządzenia, czyli czas do pierwszej awarii. Przemysłowe systemy sterowania funkcjonujące w większości polskich firm energetycznych projektowane były przede wszystkim z wykorzystaniem starych technologii, których głównym zadaniem było zapewnienie ciągłości i jakości procesów technologicznych, a bezpieczeństwo było rozumiane jako zachowanie bezpieczeństwa procesu, ludzi i środowiska (bezpieczeństwo w znaczeniu *safety*). Ze względu na otoczenie, w którym funkcjonowały (odseparowanie urządzeń i systemów OT od sieci IT – *air gap*), aspekty cyberbezpieczeństwa rzadko były brane pod uwagę przy ich projektowaniu, dlatego są one tak podatne na cyberataki – co więcej, niektóre elementy ICS są same w sobie podatne na tego rodzaju zagrożenia. Z tego względu, odpowiednio zaplanowana architektura i topologia sieci spełniają bardzo ważną funkcję[46].

6.1. Analiza i specyfikacja wymagań bezpieczeństwa

Z racji integralnego charakteru dużej części zabezpieczeń, krytycznymi etapami cyklu życia systemów jest etap ich projektowania i wdrożenia, więc wymagania bezpieczeństwa systemów powinny być definiowane na wczesnym etapie cyklu życia oraz powinny być spójne z modelem biznesowym. Chcąc działać zgodnie z zasadą *security* oraz *privacy by design* kluczową kwestią jest przewidzenie potencjalnych podatności, które urządzenie może wprowadzić do systemu. Sama analiza wymagań powinna koncentrować się na wymaganiach technicznych zamawianego lub modernizowanego rozwiązania, a także powinna brać pod uwagę ewentualne powiązania pomiędzy nowym systemem a już wykorzystywanymi i badać ich interoperacyjność oraz kompatybilność. Należy również przeprowadzić analizę, której wynikiem będzie spis funkcjonalności danego systemu, a także przykładowe warianty jego wykorzystania. Zaleca się także przeprowadzenie analizy wymagań względem dostawców i uzupełnienie standardowych wymagań z zakresu cyberbezpieczeństwa jakie musi spełniać dostawca[47].

[46] Na podstawie *Cyberbezpieczeństwo. Zarys wykładu*, red. naukowa C. Banasiński, Warszawa 2018 i Poradnik dobrych praktyk w zakresie cyberbezpieczeństwa urządzeń podlegających dozorowi technicznemu, Zespół ds. cyberbezpieczeństwa Urząd Dozoru Technicznego, 2021 r.,

[47] J. Krawiec, G. Ożarek, *System Zarządzania Bezpieczeństwem Informacji w Praktyce. Zabezpieczenia*, Polski Komitet Normalizacyjny, Warszawa 2014, s. 77-78.

Organizacja powinna uwzględnić aspekty bezpieczeństwa na wszystkich etapach życia systemów informacyjnych oraz oprogramowania, a także dostosować architekturę do wymagań prawnych.

Organizacja powinna mieć na uwadze dostosowanie środowiska oraz systemów informacyjnych do wymagań prawnych, w szczególności do wymagań wynikających z UKSC rozporządzeń wykonawczych i zmian wprowadzonych do Prawa energetycznego, ukierunkowanych na budowę zdecentralizowanego rynku energii.

Należy dokonać standaryzacji wymagań względem poziomu bezpieczeństwa systemów, a także zwiększać jego poziom poprzez modernizację i inwestycję w nowe rozwiązania.

W celu standaryzacji poziomu bezpieczeństwa powinno się stworzyć standardy i wytyczne dla modyfikowanych lub nowych systemów informacyjnych, które będą definiowały minimalne wymagania bezpieczeństwa. Przy definiowaniu minimalnych wymagań należy uwzględniać wymagania Zaleceń Komisji *w sprawie cyberbezpieczeństwa w sektorze energetycznym,* właściwych norm oraz dobrych praktyk cyberbezpieczeństwa, np. ISO 27001, NERC, NIST, IEC 62351, ISO 62443.

W szczególności operatorzy sieci energetycznych powinni ustanowić kryteria projektowe i architekturę na potrzeby odpornej sieci, co można osiągnąć poprzez:

- *wprowadzenie w każdym obiekcie środków ochrony w głąb (ang. Defence-In-Depth) dostosowanych do krytyczności danego obiektu,*
- *identyfikację węzłów krytycznych, zarówno pod względem zdolności wytwórczych, jak i wpływu na klienta. Funkcje krytyczne sieci powinny być zaprojektowane w taki sposób, aby poprzez rozważenie redundancji, odporności na wahania fazy i ochrony przed kaskadowymi wyłączeniami mocy ograniczyć ryzyko, które może wywołać efekty kaskadowe,*
- *współpracę z innymi właściwymi operatorami i dostawcami technologii w celu zapobiegania efektom kaskadowym poprzez zastosowanie odpowiednich środków i usług,*
- *projektowanie i budowę sieci łączności i sterowania w celu ograniczenia skutków wszelkich błędów fizycznych i logicznych do ograniczonych części sieci oraz zapewnienia odpowiednich i szybkich środków łagodzących.*

Ponadto, organizacja powinna dążyć do unifikacji i standaryzacji architektury rozwiązań, również poprzez modernizację lub wdrażanie nowych systemów w miejsce starszych, już wykorzystywanych. Szczególnie istotną kwestią jest stopniowe wycofanie systemów informacyjnych, które z racji swojego wieku i długiej eksploatacji nie są objęte procesem aktualizacji, dostarczania poprawek bezpieczeństwa oraz tych, które są niekompatybilne z innymi systemami odpowiadającymi za bezpieczeństwo, mając na uwadze możliwe korzyści i straty wynikające z planowanej modernizacji. Przy wdrażaniu nowych systemów informacyjnych, należy zwrócić uwagę, aby inwestycje bazowały na najnowszych rozwiązaniach w zakresie bezpieczeństwa, jak i na różnice dotyczące wymagań bezpieczeństwa stawiane urządzeniom IT oraz OT. Ponadto, powinno się także stosować uzupełniające środki bezpieczeństwa w starszych systemach, które już wykazują niewystarczający poziom cyberbezpieczeństwa, m.in. poprzez zapewnienie dodatkowych środków bezpieczeństwa fizycznego, jak na przykład środki ochrony przeciwpożarowej, systemy sygnalizacji włamania i napadu, kontroli dostępu, ochrony obwodowej, czy poprzez przeniesienie rozliczalności dostępu (np. do centralnej

nastawni i znajdujących się tam systemów) z kont logicznych SCADA na systemy kontroli dostępu i monitoringu (CCTV).

Organizacja powinna stworzyć jednolity model postępowania w fazie zamawiania nowych rozwiązań informatycznych, uściślając modele współpracy z dostawcami oraz minimalne wymagania jakie powinny być spełnione.

Organizacja powinna prosić dostawcę o informacje dotyczące zabezpieczeń przedmiotów przetargu, o potwierdzenie zgodności przedmiotu z obowiązującymi standardami cyberbezpieczeństwa, a także o zapewnionym ciągłym ostrzeganiu o zagrożeniach, łatkach i środkach zaradczych w stosunku do odkrytych podatności. Powinien być ustanowiony zakres odpowiedzialności dostawcy w przypadku wystąpienia cyberataku lub incydentu, a rozwój współpracy z dostawcami technologii powinien dotyczyć także zgłaszania potrzeb rozwojowych i pozyskania nowych funkcjonalności. Dodatkowo, organizacja powinna wprowadzić stałą analizę ryzyka związaną z dostawcami i łańcuchem dostaw, a także monitoringiem ryzyka po stronie dostawców i oceny ich dojrzałości w zarządzaniu ryzykiem (patrz rozdział 4 i 5 Rekomendacji).

W zależności od rodzaju zamawianego systemu, ważnym elementem etapu prac projektowych może być wczesne zdefiniowanie rodzajów przetwarzanych danych w zamawianych rozwiązaniach informatycznych, o ile jest to możliwe. Organizacja powinna przywiązywać wagę do prywatności i ochrony danych, w tym danych osobowych już na etapie projektowania rozwiązań, procesów i procedur.

Gromadzenie danych wyłącznie w sytuacji ich obligatoryjnego charakteru jest metodą zmniejszającą ryzyko wystąpienia negatywnych skutków w wyniku ewentualnego zdarzenia prowadzącego do naruszenia atrybutów informacji, szczególnie poufności informacji. Zdefiniowanie zakresu i rodzaju gromadzonych danych, niezbędnych do prowadzenia danego procesu, pozwoli na uniknięcie zbierania danych pozornie potrzebnych. Powyższe zalecenia należy stosować wyłącznie do systemów, w których takie działanie jest możliwe ze względu na ich specyfikę i rodzaj. W innym przypadku ograniczenie danych powinno następować dopiero po pełnej integracji systemów analityki, wdrożeniu zespołów SOC[48] itp. Realizowanie tego zagadnienia na etapie projektu może obniżyć poziom bezpieczeństwa poprzez degradację danych źródłowych.

W miarę możliwości, należy wyznaczyć konkretną lokalizację przechowywania danych, a także określić, między którymi podmiotami jakie dane będą udostępniane, ponadto należy zapewnić dostęp do danych wyłącznie upoważnionemu personelowi. Dodatkowo, należy wziąć pod uwagę problem posiadania danych kluczowych przez generalnych dostawców lub też producentów komponentów, lub całych rozwiązań.

Organizacja powinna wziąć pod uwagę konieczność modyfikacji dostępu do danych względem pracownika, który zmienił stanowisko lub zakończył świadczenie pracy dla organizacji.

Jest to działanie, które powinno mieć wysoki priorytet w działaniach o charakterze organizacyjnym. Wyłączanie dostępu do danych pracownikom, którzy zakończyli współpracę powinno być wpisane w standardowy model działań obiegowych wykonywanych w tym procesie. Należy także wziąć pod uwagę konta systemowe, brygadowe, zespołowe, techniczne, w stosunku do których np. zmiana haseł

[48] Patrz rozdział 13.1.

może wprowadzić obniżenie zdolności reakcyjnych zespołów i tym samym powodować zagrożenie (źródło ryzyk) o wysokim poziomie wpływu na dane zakładu lub segment technologiczny. Czynności i zalecenia powinny być dokonywane po uwzględnieniu zarówno ryzyk, jak i korzyści z danego działania i powinny być adekwatne do charakterystyki systemu na którym są implementowane.

Organizacja powinna przeprowadzić analizę oceny skutków przetwarzania danych w konkretnych urządzeniach związanych ze świadczeniem usługi kluczowej. Działanie to może być zintegrowane z procesem zarządzania ryzykiem organizacji.

Należy zabezpieczyć dane m.in. poprzez szyfrowanie transmisji w środowiskach niezaufanych przy transmisji danych zewnętrznych (chmura, operator).[49]

W przypadku korzystania z rozwiązania dostarczanego przez podmioty zewnętrzne, zasada *privacy by design* powinna być wyraźnie eksponowana i egzekwowana już na etapie rozmów i zamówień z dostawcą lub wykonawcą rozwiązania.

Dowody kontroli:

- *dokumenty wprowadzające stosowanie zabezpieczeń, dokumentacja zabezpieczeń, w tym: procedury stosowania zabezpieczeń, dokumentacja wykonywania ww. procedur, plan postępowania z ryzykiem, dokumentacja zabezpieczeń, w tym: procedury stosowania zabezpieczeń i dokumentacja wykonywania ww. procedur,*
- *dokumenty definiujące proces utrzymania minimalnych wymogów bezpieczeństwa systemów informacyjnych.*

6.2. Cykl życia systemów informacyjnych

Z uwagi na szerokie spektrum rodzajów systemów stosowanych w sektorze energii, a także ze względu na różny zakres i poziom samodzielności operatorów usług kluczowych w rozwoju, utrzymaniu czy modyfikacji tych systemów, zalecenia odnoszące się do cyklu życia systemów informacyjnych nie mają charakteru katalogu zamkniętego. Podstawą jest zasada zapewnienia bezpieczeństwa systemu informacyjnego oraz przetwarzanych w nim danych w każdym z cyklów życia, poprzez zastosowanie mechanizmów dopasowanych do uwarunkowań funkcjonujących w danej organizacji.

Faza nabywania

Określenie wymagań bezpieczeństwa już na etapie zamówienia jest metodą, która w sposób efektywny i wydajny pozwoli na implementację minimalnych wymagań, a także pozwoli na zaoszczędzenie kosztów, które organizacja mogłaby ponieść w przypadku konieczności modyfikacji mechanizmów bezpieczeństwa w późniejszych cyklach życia systemu. Na tym etapie organizacja przeprowadza analizę zasadności posiadania ustanowionych procedur zawierania, modyfikacji i rozwiązywania umów z dostawcami rozwiązań informatycznych. Procedury powinny co najmniej zawierać kwestie związane z usystematyzowanym zakresem odpowiedzialności w kwestiach

[49] ENISA, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, 2018 r.

bezpieczeństwa, ponadto w kwestiach finansowych i prawnych powinny zawierać klauzule dotyczące możliwości rozwiązania umowy i ewentualnego odszkodowania. Kwestie związane z odpowiedzialnością powinny być uwzględniane na etapie tworzenia umowy, opisu przedmiotu zamówienia, programu funkcjonalno-użytkowego oraz procedur kwalifikacji. Stosownie do możliwości, zaleca się uwzględnienie procedury nabywania rozwiązań IT, OT w ogólnym procesie zaopatrzenia organizacji (jeśli taki istnieje).

- Ustanowione procedury powinny określać ogólne ramy działania, jednakże ostateczna ocena rozwiązania oraz opinia na temat zasadności jego pozyskania powinna być dokonana przez kierowników/specjalistów zajmujących się cyberbezpieczeństwem, którzy na podstawie swojego doświadczenia i praktyki są w stanie obiektywnie zaproponować podjęcie najbardziej właściwych działań.
- Należy określić środki bezpieczeństwa zamawianego produktu dopasowane do posiadanych lub stosowanych już rozwiązań, określić kontekst użycia nowego rozwiązania oraz jego relacje z innymi elementami infrastruktury oraz jego kompatybilność.
- Należy rozważyć obligatoryjne zawieranie umów o zachowaniu poufności przed podpisaniem umów na konkretne rozwiązanie.
- Na etapie zamawiania powinno się określić wymagania zawierające kryteria bezpieczeństwa wskazujące na charakterystykę biznesową dostawcy, dającą rękojmię prawidłowej realizacji dostarczenia danego rozwiązania.
- Organizacja powinna korzystać z usług dostawcy lub producenta danego rozwiązania, który charakteryzuje się odpowiednim doświadczeniem, a także posiada wdrożone powszechnie uznawane standardy i normy odnoszące się do bezpieczeństwa przetwarzanych informacji.
- W razie możliwości zaleca się stworzenie listy akredytowanych (przez producenta) i zaufanych dostawców rozwiązań, mając jednak na uwadze zjawisko tzw. vendor lock – uzależnienia od rozwiązań jednego dostawcy. Należy więc rozważyć także oddzielenie zagadnień cyberbezpieczeństwa od głównych wykonawców systemów technologicznych w tym kontekście.
- Należy przedstawić dostawcy danego rozwiązania sprecyzowane wymagania, zawierające m.in.: wymogi funkcjonalne, wymagania w zakresie cyberbezpieczeństwa, bezpieczeństwa informacji, a także zakresu wsparcia produktowego podczas całego jego cyklu życia – należy zawrzeć umowy wsparcia serwisowego i technicznego. Umowy te powinny dawać zamawiającemu pełną możliwość monitorowania wszystkich komponentów OT, jak i wszystkich danych. Należy również w nich wskazać, iż wszystkie dane wygenerowane w ramach pracy danego rozwiązania stanowią własność zamawiającego.
- Każda zmiana treści procedowanej umowy w trakcie procesu jej negocjacji powinna być ocenioną pod kątem wpływu na bezpieczeństwo.
- W procesie zamówienia powinni brać udział eksperci ds. bezpieczeństwa oraz cyberbezpieczeństwa, którzy posiadają odpowiednie doświadczenie w kontekście charakteru przedmiotu zamówienia (systemów OT lub IT) oraz będą w stanie ocenić zaproponowane oferty i sugerować wybór tych najbardziej optymalnych. Ponadto w procesie powinny brać udział osoby odpowiedzialne za kwestie prawne, które będą w stanie ocenić zgodność z wymaganiami prawnymi.

- Należy upewnić się czy dostawca danego rozwiązania zapewnia dokumentację obejmującą kwestie cyberbezpieczeństwa, procesów i procedur, które są powiązane z tym produktem i składają się, np. z procedur konserwacji, procesów instalacji poprawek, procedur zawierających bazowe konfiguracje, kontrolę zmian.
- Aspekty bezpieczeństwa zawarte w umowach powinny być stale monitorowane, a w razie stwierdzenia ich uchybienia powinny zostać podjęte działania naprawcze zmierzające do usunięcia niezgodności.
- Wymiana informacji o konkretnie stosowanych rozwiązaniach oraz ich wersjach w przedsiębiorstwie powinna być udostępniana po uzyskaniu zapewnienia lub potwierdzenia zachowania tych informacji w poufności.

Faza wdrożenia

- Organizacja powinna budować kompetencje wymagane przy rozwoju, wdrożeniu, modyfikacji czy eksploatacji danego rozwiązania poprzez zapewnienie dostępu do szkoleń dla pracowników odpowiedzialnych za obsługę tego rozwiązania.
- Zaleca się przygotowanie planu wdrożenia rozwiązania.
- Zaleca się stworzenie bezpiecznego środowiska testowego, odpowiadającego najważniejszymi aspektami np. bezpieczeństwa, danych, obciążeń, środowisku produkcyjnemu, któremu dedykowane jest rozwiązanie.
- Należy nadzorować proces implementacji rozwiązania przez dostawcę, w tym proces rozwiązywania problemów związanych z implementacją. Może to być zrealizowane np. poprzez wprowadzenie zespołu zajmującego się cyberbezpieczeństwem po stronie Inwestora.
- Należy zweryfikować ocenę ryzyka i podatności związanych z wdrażanym rozwiązaniem, na podstawie wewnętrznych procedur OUK zgodnych z odpowiednimi normami.
- Zaleca się przygotować i wdrożyć zaplanowany proces konwersji i migracji danych, o ile jest to możliwe.
- O ile istnieje taka możliwość, organizacja powinna przeprowadzić serię testów mających na celu walidację wdrożonego rozwiązania. W przypadku wystąpienia błędów, należy je usunąć. Takie działanie powinno dać pewność poprawności działania rozwiązania przed skierowaniem go do środowiska produkcyjnego. Dla rozwiązań w zakresie elektroenergetyki, wystarczającym poziomem jest poziom kwalifikacji, np. w oparciu o DQ, IQ, OQ, i PQ (ang. *Design Qualification, Installation Qualification, Operational Qualification, Performance Qualification*).
- Powinno nastąpić przygotowanie poprawek w celu rozwiązania specyficznych problemów.
- Zaleca się opracowanie mechanizmu przeprowadzenia przeglądu powdrożeniowego, na przykład w trybie kwalifikacji DQ, IQ, OQ, PQ.

Faza użytkowania

- Należy zapewnić bezpieczeństwo procedur i procesy konserwacji, zarówno w aspektach fizycznych, jak i oprogramowania i danych.
- Organizacja powinna przeprowadzać okresowe, zaplanowane audyty bezpieczeństwa systemów – patrz rozdział 8.

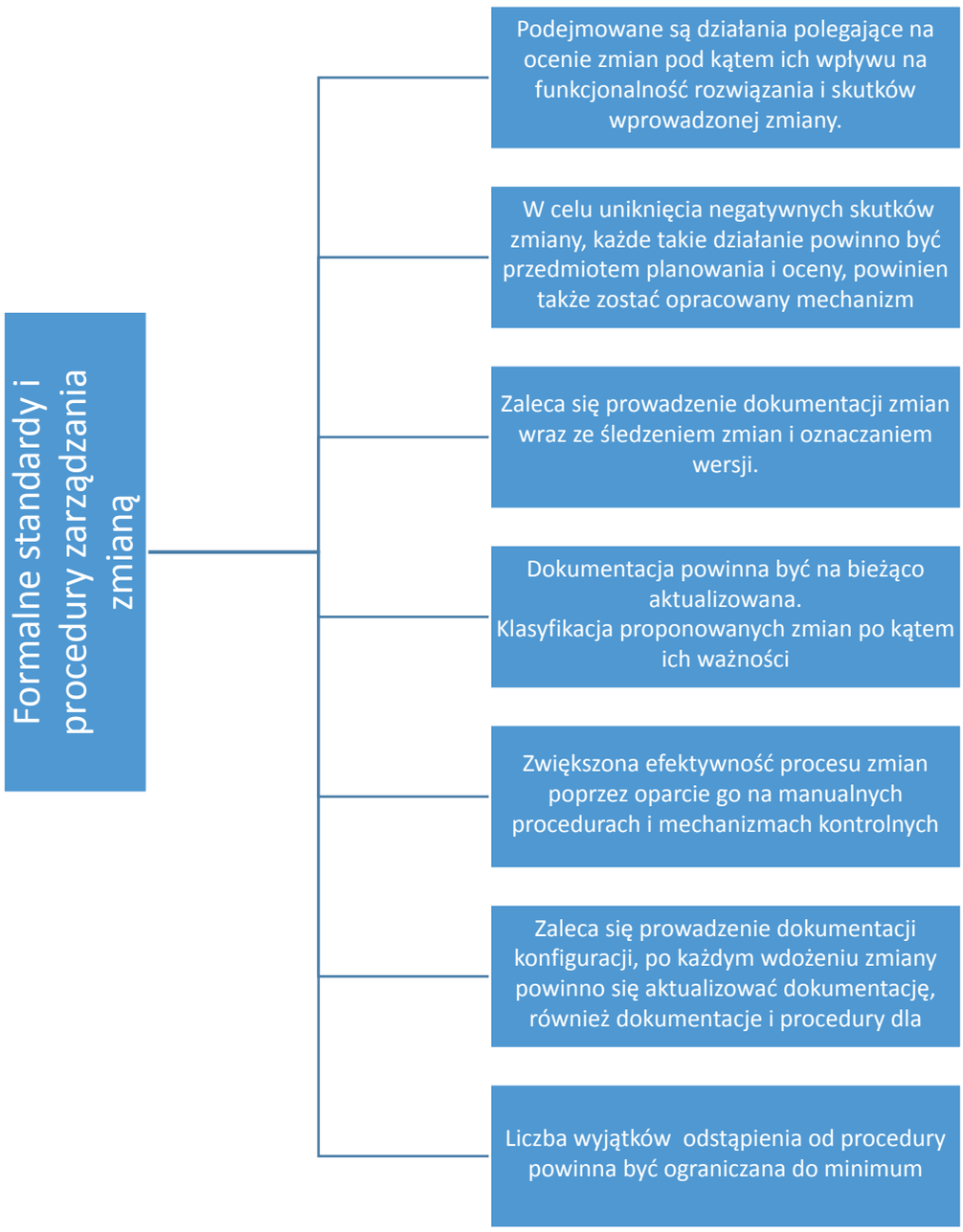
- Należy zapewnić odpowiednią aktualizację oprogramowania i wdrażanie poprawek, z wcześniejszym uwzględnieniem potrzeb, krytyczności takiego działania i oszacowaniu ryzyka dotyczącego ewentualnych zmian.
- Potrzeby i względy bezpieczeństwa powinny wpływać na wdrażanie uszeregowanych pod względem ważności ulepszeń procesów, modeli i procedur.
- Raporty o incydentach i problemach powinny być uwzględniane w procesie określania skuteczności i wagi zabezpieczeń w pracach konserwacyjnych.
- W zależności od możliwości organizacja powinna wykonywać konserwację zapobiegawczą, wyprzedzającą możliwość wystąpienia zdarzenia mającego wpływ na bezpieczeństwo.
- W czasie planowanych postojów lub modernizacji systemów zaleca się przeprowadzanie testów bezpieczeństwa, a także dokonywanie przeglądów pod kątem bezpieczeństwa po wprowadzeniu zmian w rozwiązaniach.
- W przypadku zlecania na zewnętrz prac rozwojowych, zaleca się nadzorowanie i monitorowanie tych prac oraz ich efektów.

Faza wycofania systemu (IT)

- Z odpowiednim wyprzedzeniem powinno się zapewnić zastępowalność likwidowanego rozwiązania oraz poczynić kroki w celu migracji do nowych rozwiązań (w razie kontynuowania procesu).
- Informacje generowane podczas cyklu życia systemu powinny podlegać szczególnej ochronie, a także powinny zostać w odpowiedni sposób zarchiwizowane.
- Należy dochować szczególnej staranności, aby elementy systemu podlegającego wycofaniu, nie trafiły powtórnie do łańcucha dostaw w sytuacji, gdy doprowadziłoby to do możliwości ujawnienia danych np. danych konfiguracyjnych.
- W celu uniknięcia wycieku informacji przetwarzanych w wycofywanym rozwiązaniu zaleca się wdrożenie formalnych procedur bezpiecznego wycofania rozwiązania. Procedury powinny być współmierne do wrażliwości informacji przetwarzanych przez rozwiązanie, którego dotyczą.
- Podczas wycofywania systemu, powinno się zapewnić dostępność danych archiwalnych, jeżeli nie mogą być one przechowywane w innych systemach, a jedynie w wycofywanym systemie.

Ponadto rekomenduje się zwrócenie szczególnej uwagi na proces zarządzania zmianą. Zaleca się nadzorowanie zmian w systemach podczas procesu ich rozwoju, a także uprzednie opracowanie formalnych procedur dokonywania zmian. Wszystkie zmiany dokonywane w funkcjonującym rozwiązaniu (w środowisku produkcyjnym) powinny podlegać formalnemu zarządzaniu. Każda zmiana powinna być oceniana i zatwierdzana przed wdrożeniem, rejestrowana, a także zaleca się dokonanie oceny po wdrożeniu i weryfikacji skutków pod kątem planowanych rezultatów. Działania powinny być prowadzone w celu uniknięcia negatywnego wpływu na stabilność funkcjonowania.

Rysunek 4 – Formalne standardy i procedury zarządzania zmianą.



Dowody kontroli:

- *dokumentacja wdrożeń nowych systemów teleinformatycznych, dokumentacja wprowadzanych zmian w systemach eksploatowanych, dokumentacja monitorowania systemów teleinformatycznych oraz działań zapobiegawczych będących wynikiem dostrzeżonych problemów podczas monitorowania,*
- *dokumentacja wprowadzanych zmian w systemach eksploatowanych,*
- *dokumentacja monitorowania systemów teleinformatycznych oraz działań zapobiegawczych będących wynikiem dostrzeżonych problemów podczas monitorowania.*

6.3. Zarządzanie aktywami

Organizacja powinna zarządzać aktywami w zakresie świadczonej usługi kluczowej. Czynności te powinny być realizowane przy użyciu odpowiednich rozwiązań organizacyjnych oraz zautomatyzowanych rozwiązań technicznych.

Zarządzanie aktywami, jako element Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą ISO 27001, jest złożone z następujących obszarów:

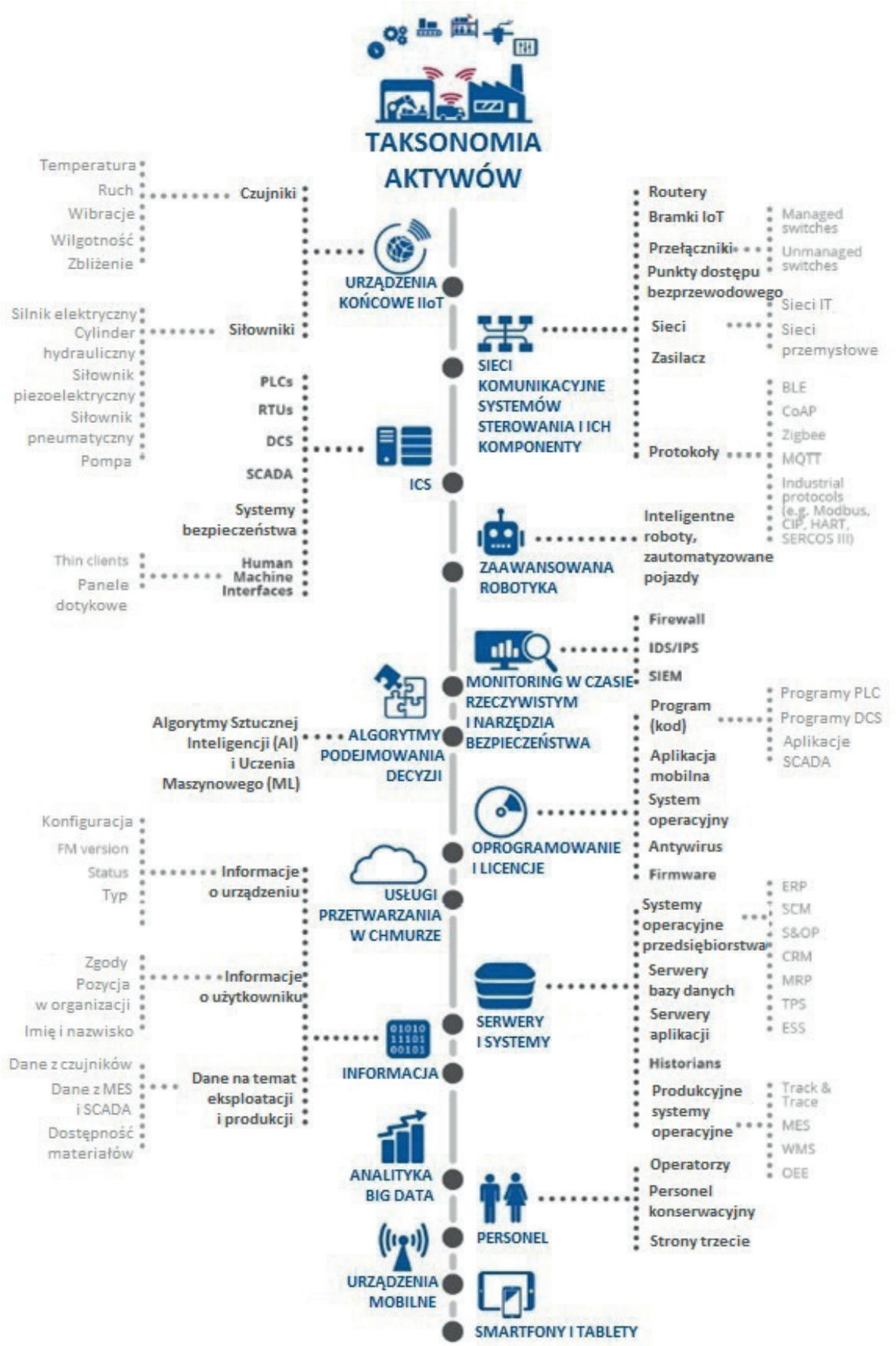
1. *Odpowiedzialność za aktywa:*
   1.1. Inwentaryzacja aktywów,
   1.2. Własność aktywów,
   1.3. Akceptowalne użycie aktywów,
   1.4. Zwrot aktywów.
2. *Klasyfikacja informacji:*
   2.1. Klasyfikowanie informacji,
   2.2. Oznaczanie informacji,
   2.3. Postępowanie z aktywami informacyjnymi.
3. *Postępowanie z nośnikami:*
   3.1. Zarządzanie nośnikami wymiennymi,
   3.2. Wycofywanie nośników,
   3.3. Przekazywanie nośników[50].

Mając na uwadze powyższe, a także specyfikę funkcjonowania sektora energii, w którym świadczenie usługi kluczowej najczęściej zależy od urządzeń automatyki przemysłowej (OT), czynności wskazane w treści normy powinny się odnosić nie tylko do informacji przetwarzanych przez organizację (aktywów informacyjnych), lecz również do sieci i urządzeń (zatem aktywów jako całości). Celem realizowanych czynności powinno być więc zidentyfikowanie aktywów oraz określenie odpowiedzialności w zakresie ich ochrony, przydzielenie im odpowiedniego jej poziomu, stosownie do krytyczności aktywów, a także przeciwdziałanie nieuprawnionemu ujawnieniu, modyfikacji, usunięciu czy zniszczeniu aktywów informacyjnych[51].

Należy podkreślić znaczenie procesu identyfikacji aktywów w kontekście realizacji pozostałych zadań organizacji dotyczących cyberbezpieczeństwa świadczonej usługi kluczowej. W szczególności dotyczy to procesu zarządzania ryzykiem wystąpienia incydentu cyberbezpieczeństwa systemów informacyjnych służących do jej świadczenia, który to proces wymaga uprzedniej identyfikacji aktywów, by móc zarządzać występującym w ich zakresie ryzykiem.

[50] PN-EN ISO/IEC 27001:2017-06 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania*., 2018, s. 16.
[51] *Ibidem*.

Rysunek 5 – Taksonomia aktywów.



Źródło: *ENISA, Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, 2018, s. 20.

Katalog zinwentaryzowanych aktywów powinien być aktualny i aktualizowany. Aktualny katalog oznacza dokonanie inwentaryzacji zgodnie ze stanem faktycznym wszystkich wymaganych aktywów na czas jej przeprowadzenia. Aktualizowanie katalogu oznacza późniejsze ponowne oraz cykliczne powtarzanie tego procesu, względem pierwotnie posiadanego rejestru aktywów.

Można wyróżnić cztery główne metody dokonywania inwentaryzacji, ukierunkowane na środowiska automatyki przemysłowej i sterowania:

a) inspekcja fizyczna (spis z natury),
b) pasywne wykrywanie,
c) analiza konfiguracji,
d) aktywne wykrywanie (należy mieć na uwadze, iż może ono często prowadzić do awaryjnego odstawienia segmentów technologicznych)[52].

Inspekcja fizyczna

Inspekcja fizyczna polega na przeglądzie sieci i urządzeń w całym obiekcie, w celu weryfikacji podłączonych systemów. Przeprowadzona prawidłowo, zazwyczaj pozwala stworzyć pełny obraz wykorzystywanych aktywów i odkrywa zasoby, których nie można zidentyfikować za pomocą innych środków. Realizację tej metody warto rozpocząć od najbardziej nadrzędnego punktu sieci (np. firewalla organizacji), następnie śledząc przewody, które rozdzielają się w kierunku poszczególnych urządzeń, aż do pożądanej warstwy modelu IACS. Należy jednak mieć na uwadze, iż wiele systemów nie ma połączenia do sieci niezaufanych. Inwentaryzację należy rozpocząć od systemów nazwanych, jak np. DCS, PCS, HART, MIOS, HVAC, nawęglanie, regulatory turbin i pozostałe.

Inspekcja fizyczna cechuje się szczególną efektywnością w przypadku sporządzania wstępnego katalogu aktywów. Niestety, w zestawieniu z pozostałymi metodami nie oferuje takich korzyści, jak łatwość aktualizacji katalogu (wykrywanie aktywne/pasywne) czy rozszerzony kontekst prowadzonej inwentaryzacji, co ma miejsce w przypadku analizy konfiguracji. Jest to również najbardziej pracochłonna z metod, co czyni ją jednocześnie najbardziej kosztowną[53].

Wykrywanie pasywne

Wykrywanie pasywne opiera się na wykorzystaniu sieci pasywnej, bezprzewodowego oraz szeregowego monitorowania zasobów komunikujących się w systemie, w celu ich identyfikacji. Wymogiem jest implementacja technologii monitorowania pasywnego w sieci, jednak po jej zastosowaniu, jest to jedna z technik o najmniejszym wpływie na inwentaryzowane aktywa. Może być wówczas stosowana nie tylko w celu ciągłego ich monitorowania, lecz również do wytyczania i nadzoru komunikacji sieciowej. Narzędzia do pasywnego wykrywania są bardziej niezawodne przy stosowaniu ich w odniesieniu do tradycyjnych technologii i protokołów sieciowych, jak TCP/IP, a ich wykorzystywanie jest obarczone większym ryzykiem błędu przy protokołach przemysłowych, jak Modbus czy Profibus. Niektóre urządzenia OT nie generują dużego ruchu sieciowego w trakcie wykonywania standardowych operacji, przez co mogą zostać pominięte przez rozwiązania pasywne. Kluczowe jest również monitorowanie pasma bezprzewodowego w organizacji, gdyż mogą w niej występować urządzenia komunikujące się poprzez Wi-Fi, Zigbee, Bluetooth czy WirelessHART, które nie są uwidaczniane przy

[52] M. Bristow, *ICS Asset Identification: It's More Than Just Security*, SANS Institute Information Security Reading Room, 2020, s. 2.
[53] *Ibidem*.

stosowaniu innych technik analizy. Należy uporządkować te protokoły na poziomie grup i przypisać do obszarów stosowania mapując je na model IACS. Prócz powyższego, starsze urządzenia sieciowe, często występujące w środowiskach OT, mogą nie posiadać wystarczających zasobów lub mocy obliczeniowej dla konfiguracji *port mirroringu*, co może prowadzić do powstawania opóźnień, utraty ramek lub nawet restartu czy zawieszenia się urządzenia. Należy również mieć na uwadze, iż dzisiejsze urządzenia aktywne, dedykowane dla przemysłu nie wspierają *port mirroringu*, a jeśli go wspierają to tylko w bardzo ograniczonym zakresie – np. dwa porty na jeden. Z tego powodu nie powinno się stosować wykrywania pasywnego jako wyłącznej techniki przy inwentaryzacji środowisk automatyki przemysłowej i sterowania, jednak może być ona stosowana jako rozwiązanie uzupełniające w połączeniu z innymi technikami[54]. Tam, gdzie techniki aktywne nie powinny być stosowane, należy stosować jedynie techniki pasywne w architekturze przepływowej, właściwie oprogramować funkcje diagnostyczne na przełącznikach zarządzalnych, zastosować techniki DiD dla segmentacji granic procesu, itp.

Analiza konfiguracji

Analiza konfiguracji to kolejna metoda inwentaryzacji aktywów, polegająca na pobieraniu istniejących danych konfiguracyjnych z systemów kontroli, urządzeń sieciowych, diagramów procesów oraz innych źródeł konfiguracji w celu stworzenia obrazu zasobów. Może być przeprowadzana w sposób całkowicie pasywny, analogicznie do wykrywania (wykorzystując konfiguracje statyczne) lub bardziej aktywny (wykorzystując automatyzację do ciągłej oceny konfiguracji). W przeciwieństwie do inspekcji fizycznej, ta metoda może być w szybki sposób skalowana do całej instalacji, poprzez normalizowanie (wprowadzenie typoszeregów urządzeń i zbudowanie matrycy normalizacyjnej) i kompilowanie funkcjonujących konfiguracji. Wiele przełączników w OT jest jednak niezarządzalnych. Należy zauważyć, iż wiele przełączników jest wbudowanych w urządzenia przemysłowe (np. PLC, IED), gdzie nie są funkcyjnie obsługiwane przez programistów.

Przeważająca część technik i narzędzi do analizy konfiguracji dostępnych na rynku skupia się na zasobach IT, jak switche czy konfiguracje firewalla. W środowiskach OT urządzenia te są jednak często skonfigurowane w sposób bardzo otwarty, aby nie ograniczać ruchu sieciowego, przez co mogłyby nie dostarczyć danych o wystarczającej jakości w zakresie ich konfiguracji. W tych środowiskach, bogate zbiory danych do analizy konfiguracji najczęściej pochodzą z systemów nadzoru i kontroli. Należy jednak mieć na uwadze konieczność zapewnienia wiedzy w zakresie korelacji obiektów fizycznych do obiektów logicznych, które stanowią większość obiektów w środowisku OT, osobom odpowiedzialnym za realizację zadań związanych z tą metodą inwentaryzacji. Kolejnym wyzwaniem związanym z analizą danych konfiguracyjnych, jest pobieranie ich z niejednolitych środowisk kontroli, często pochodzących od różnych dostawców lub modeli urządzeń, w celu ich normalizacji do użytecznego formatu. Normalizacja i przekształcenie tych danych jest skomplikowaną czynnością, szczególnie w organizacjach o rozbudowanej strukturze, jednak istnieją komercyjne rozwiązania wspomagające ten proces. Pomimo wysokiego stopnia trudności tych działań, raz przeprowadzona transformacja danych znacznie przyspieszy ten proces w przyszłości.

Jako, że dane konfiguracyjne opierają się na konfiguracji stworzonej przez operatora systemu i odzwierciedlają pewien stan w określonym czasie, nie pozwolą wykryć pozostałych, nieautoryzowanych systemów w środowisku (jak na przykład stacji roboczej nie będącej częścią oficjalnej konfiguracji

[54] *Ibidem*, s. 2-3.

zakładu, lecz zainstalowanej przez pracowników terenowych). Na rynku istnieją narzędzia umożliwiające wykonywanie analizy zarządzania konfiguracją w sposób ciągły (aktywny), często opierające się na pozyskiwaniu danych bezpośrednio z kontrolerów, co pozwala aktualizować katalog zasobów w czasie rzeczywistym, analogicznie jak w metodach pasywnego oraz aktywnego wykrywania. Jest to jedna z najlepszych technik, dzięki której można uzyskać kompleksowe informacje o zasobach OT, rozszerzone o kontekst ich funkcjonowania, co nie jest możliwe w przypadku pozostałych metod. Może to być także jedna z niewielu możliwości pozyskania tego typu informacji z odizolowanych i zamkniętych środowisk, jak systemy bezpieczeństwa[55].

Aktywne wykrywanie

Ostatnią z głównych metod dokonywania inwentaryzacji jest aktywne wykrywanie. Używa ona aktywnej komunikacji sieciowej do identyfikacji urządzeń w środowisku. Wykorzystywane sondy mogą mieć ogólny charakter dla technologii komunikacyjnych, jak polecenie ICMP *ping*, lub też szczególny dla danego protokołu, jak skanowanie identyfikatorów urządzeń Modbus TCP (*unit ID*). Metoda ta jest w stanie zidentyfikować urządzenia, które bywają uśpione w sieci. Może ona jednak pomijać te zasoby, których zadaniem jest reagowanie tylko w określonych okolicznościach, takich jak wystąpienie odpowiedniego identyfikatora urządzenia typu *master*. Aktywne wykrywanie może powodować negatywne skutki w niektórych starszych urządzeniach z powodu niezgodności protokołów, co może prowadzić do zablokowania ich interfejsów sieciowych lub wyczerpania zasobów procesora. W związku z tym, organizacja powinna przetestować tę metodę na reprezentatywnej, testowej konfiguracji sprzętowej przed zastosowaniem jej w środowisku produkcyjnym. Zastosowanie tej techniki może także wprowadzać dodatkowe opóźnienia w komunikacji w danym środowisku, co może mieć negatywny wpływ na realizowany proces w sieciach o niskiej przepustowości oraz wysokich opóźnieniach – problematyczny może być także brak zasobów w urządzeniach w środowisku OT i tym samym brak oprogramowania obsługującego nieznane typy komunikacji, sygnalizacji, enkapsulacji, itp., co powoduje zawieszanie się systemów na poszczególnych komponentach ICS, jak PLC czy elementach związanych z tak zwaną inteligentną sensoryką. Wiele z narzędzi do aktywnego skanowania w środowiskach OT zostało przekształconych z analogicznych narzędzi dla rozwiązań IT, przez co mogą nie zapewniać kompleksowej identyfikacji urządzeń korzystających z protokołów innych niż TCP/IP lub szeregowych.

W ostatnich latach opracowano jednak wyspecjalizowane narzędzia do wykrywania zasobów OT, pozbawione ryzyk związanych z zastosowaniem narzędzi wywodzących się ze środowisk IT w środowiskach automatyki przemysłowej i sterowania. Korzystają one z protokołów stosowanych w OT do nasłuchiwania środowiska, przez co pozwalają ująć kontekst tych systemów podczas skanowania. Analogicznie, narzędzia te nie powinny być jednak używane bezpośrednio w środowisku produkcyjnym, bez uprzedniego sprawdzenia ich działania w reprezentatywnej konfiguracji testowej (jak laboratorium, które posiada pełne układy sterowania, jak np. kompletne systemy DCS podłączone do systemów warstw 0-2 modelu IACS).[56]

W związku z powyższym, wzorcowo organizacja powinna korzystać z narzędzi pozwalających przeprowadzać inwentaryzację oraz aktualizację katalogu aktywów w sposób zautomatyzowany oraz ciągły, umożliwiający możliwie efektywne i rzetelne realizowanie tego procesu, poprzez połączenie różnych metod odpowiednich dla charakterystyki i złożoności jej instalacji.

[55] *Ibidem*, s. 4-5.
[56] *Ibidem*, s. 5.

Przy niewielkiej liczbie aktywów lub braku możliwości zastosowania aktywnych metod ich inwentaryzacji, możliwe jest przeprowadzenie tego procesu ręcznie, jednak nie jest to rekomendowane ze względu na czasochłonność oraz wysokie ryzyko pomyłki.

Katalog aktywów powinien uwzględniać także ich krytyczność dla przedsiębiorstwa oraz stanowić scentralizowaną bazę. Krytyczność dla procesów może zostać określona poprzez stworzenie matrycy z funkcją czasu i faz poszczególnych procesów. Na przykład proces nawęglania podzielony jest na wiele etapów i każdy z nich będzie klasyfikowany na innym poziomie krytyczności.

Krytyczność aktywów może być określona zgodnie z podziałem na:

a) krytyczne – w razie ich niedostępności nie jest możliwe świadczenie usługi kluczowej,
b) ważne – w razie ich niedostępności usługa kluczowa będzie świadczona, lecz o obniżonej jakości i/lub ciągłość jej świadczenia zostanie przerwana,
c) pomocnicze – niedostępność tych aktywów nie będzie miała wpływu na jakość i/lub ciągłość świadczenia usługi kluczowej, lecz w pewien sposób usprawnia lub ułatwia ten proces.

Baza zawierająca informacje na temat zinwentaryzowanych aktywów, powinna docelowo zawierać również dane o właściwościach urządzeń, jak:

a) adresy IP (ze szczególnym uwzględnieniem adresacji warstwy 1, 2 oraz 5 wg modelu OSI, gdyż te adresacje są najważniejsze i stanowią większość adresów w środowisku OT),
b) wykorzystywane porty,
c) wykorzystywane protokoły komunikacyjne (oraz protokoły przemysłowe),
d) dostępny rodzaj/model urządzenia,
e) wersja firmware'u i software'u,
f) informacje diagnostyczne,
g) dane o wydajności,
h) właściciel/administrator/osoba odpowiedzialna za urządzenie,
i) lokalizacja urządzenia,
j) funkcja pełniona przez urządzenie,
k) informacja o urządzeniu – maszyna wirtualna czy fizyczna,
l) informacja czy do urządzenia posiadają dostęp osoby trzecie,
m) informacja na temat kopii zapasowej,
n) krytyczność zasobu na bazie szacowania ryzyka,
o) lokalizacja fizyczna i logiczna,
p) informacja na temat redundancji,
q) informacja czy zasób może być aktywnie skanowany.

Dodatkowo w przypadku sektora energetycznego, zwłaszcza w przypadku występowania starych i nowych technologii na poziomie obiektów i instalacji, należy przyjąć założenie przeprowadzenia odrębnej analizy ryzyka w podziale na klasy aktywów w odniesieniu do najnowszych i małych instalacji. To zalecenie zakłada, że istnieje pewna standaryzacja między zasobami tego samego typu w najnowszych obiektach i instalacjach. Natomiast w przypadku większych zakładów, które są wynikiem

zupełnie różnych projektów, a ich modernizacje były planowane niezależnie, należy ograniczyć stopień, w jakim można przeprowadzić analizę ryzyka „według klasy aktywów"[57].

Ponadto organizacja powinna także posiadać ewidencję aktywów informacyjnych istotnych z punktu widzenia bezpieczeństwa informacji oraz posiadać wdrożone procedury określające akceptowalne użycie tego rodzaju aktywów.

Należy podkreślić, iż są już także dostępne rozwiązania *open source* w zakresie identyfikacji aktywów w środowiskach OT oraz IT. Są to m.in.:

a) Snipe-IT – jest platformą do zarządzania i śledzenia zasobów IT. Nie jest to narzędzie przystosowane do śledzenia zasobów OT, ale jest konfigurowalne i może zastąpić podstawowe arkusze kalkulacyjne często używane w tym celu,

b) GRASSMARLIN – to narzędzie do pasywnego wykrywania, które pozwala wizualizować zasoby OT do formy mapy z możliwością eksportu. Może nasłuchiwać ruch sieciowy na żywo, przechwytywać pakiety, także stosować inne techniki analizy pasywnej.

Dowody kontroli:

– spis aktywów podstawowych (procesy i działania podstawowe, informacje), spis aktywów wspierających (sprzęt, oprogramowanie, sieć, personel, siedziba, struktura organizacyjna),

– udokumentowane formalnie sposób zarządzania aktywami oprogramowania i sprzętem.

6.4. Utrzymanie systemów informacyjnych

Rekomendowane jest przeprowadzenie szacowania bezpieczeństwa systemów informacyjnych pod kątem bezpiecznej eksploatacji systemu, uwzględniającej zagrożenia wynikające np. z wieku systemu, ograniczonej liczby osób posiadających wiedzę o systemie.

Jeżeli wcześniej w organizacji nie były realizowane procedury dot. bezpieczeństwa systemów informacyjnych to w celu oceny poziomu wiedzy o systemie wskazane jest przeprowadzenie szacowania ryzyka, w trakcie którego należy przyjrzeć się takim obszarom jak:

– kompletność dokumentacji – czyli w jakim stopniu dokumentacja systemu jest pełna i gdzie występują braki informacji o systemie. Należy zastosować procedury kwalifikacji,

– informacje dot. kopii zapasowych – czy w systemie istnieje możliwość tworzenia kopii zapasowych, gdzie są przechowywane te kopie. Istotne jest tworzenie kopii w ujęciu procesowym, a nie komponentowym,

– czy istnieją dzienniki modyfikacji/aktualizacji systemu (kiedy były wykonywane czynności, co dokładnie było modyfikowane), czy jest możliwość ponownej instalacji systemu,

– dokumentacja zagrożeń wynikających ze sposobu pracy systemu oraz identyfikacja obszarów dot. pracy systemu, o których niewiele wiadomo, jakie są możliwości konserwacji systemu i koszty utrzymania infrastruktury systemu, itp.

[57] Zalecenie Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r.

Rekomendowane jest gromadzenie wiedzy o systemie i jej zabezpieczanie.

W celu zabezpieczenia wiedzy wskazane jest m.in. utrzymywanie repozytorium z pełną dokumentacją dot. systemu (konfiguracji oprogramowania, szczegółowej dokumentacji zmian czy też aktualizacji systemu, sposobu przechowywania haseł, informacji o testach bezpieczeństwa, listy osób mających dostęp do systemu oraz zakresu dostępu i okresu czasu) czy też zabezpieczenie wiedzy, którą posiada administrator systemu np. poprzez zapewnienie zastępowalności pracowników administrujących oraz obsługujących system (szczególnie istotne przy wieloletnich systemach), aby przy odejściu pracownika informacje dot. systemu w pełnym zakresie pozostały dostępne dla organizacji.

Wskazane jest na przykład prowadzenie rejestru zdarzeń dostępu do konfiguracji urządzeń – na podstawie rozwiązań bezpieczeństwa wyposażonych w mechanizmy rejestracji oraz analizy dzienników systemowych czy śladów audytowych. Takie rozwiązania pozwalają np. na podjęcie działań chroniących konfigurację zanim zostanie ona zmodyfikowana.

Rekomendowane jest zawieranie w umowach ze stronami trzecimi klauzul dotyczących szczegółów w zakresie zapewnienia obsługi systemu, jak i ciągłości wiedzy dot. systemu.

W przypadku świadczenia usługi przez stronę trzecią w zakresie obsługi systemu informacyjnego wskazane jest zawarcie w umowie ze stroną trzecią klauzul, które zabezpieczą utrzymanie systemu informacyjnego, m.in. zabezpieczenie obsługi systemu na okres czasu, w którym pracownicy organizacji będą w stanie poznać system, aby po zakończeniu umowy posiadać wystarczającą wiedzę na temat prawidłowego utrzymania systemu. Innym rozwiązaniem może być zawarcie zapisów regulujących przekazanie po zakończeniu umowy dokumentacji dotyczącej systemu informacyjnego.

Rekomendowana jest realizacja wdrożonych zapisów procedur/instrukcji dot. bezpieczeństwa systemu informacyjnego w organizacji.

Wskazane jest by na bieżąco realizować zapisy procedur/instrukcji, które mają na celu zapewnienie bezpieczeństwa pracy systemu informacyjnego, także w celu późniejszego sprawnego utrzymywania procesów technologicznych w organizacji, poprzez właściwie podejmowane działania, a także poprzez zbieranie szczegółowych informacji dotyczących pracy systemów i jej zakresu (informacje dot. m.in. aktualizacji dokumentacji systemu, bieżącego monitoringu systemu, przeprowadzania testów systemu, wraz z regularnymi wewnętrznymi audytami w zakresie realizowania tych procedur/instrukcji i sprawozdań z tych działań dla zarządu).

Rekomendowane jest regularne przeprowadzanie testów systemów informacyjnych.

W organizacji powinny być wdrożone procedury/instrukcje dot. przeprowadzania testów systemów informacyjnych i w ich zakresie powinny być regularnie przeprowadzane testy systemów w celu zarówno wykrywania ich potencjalnych błędów, jak i weryfikowania skuteczności działania. Takie testy powinny być zaplanowane m.in. na podstawie szacowania ryzyka i określania wrażliwych obszarów działania (np. sytuacji, gdy system ponownie się nie uruchomi), natomiast nie należy ograniczać się tylko do tych obszarów.

Przy projektowaniu nowego systemu informacyjnego wskazane jest uwzględnienie elementów dotyczących utrzymywania systemu w późniejszym czasie.

Ze względu na to, że w sektorze energii systemy informacyjne są projektowane na dłuższy okres, to należy także pamiętać o elementach dotyczących utrzymywania systemu po planowanym czasie. Elementy te obejmują zarówno zakres pracy ciągłej, jaki i informacje niezbędne do realizacji późniejszych działań (m.in. dostęp do historycznych danych dot. pracy systemu, system wsparcia technicznego, przewidzenie możliwości rozbudowy systemu itp.).

Dowody kontroli:

- *procedura utrzymania bezpieczeństwa systemu informacyjnego odpowiednio udokumentowana i zatwierdzona przez kierownictwo wyższego szczebla,*
- *formalnie udokumentowane wymagania dotyczące oprogramowania i sprzętu zapewniające kompatybilność,*
- *zapisy umów serwisowych oraz umów dotyczących rozwoju systemów teleinformatycznych,*
- *jasno określony i udokumentowany proces utrzymania minimalnego bezpieczeństwa.*

6.5. Aktualizacja oprogramowania

Operator usługi kluczowej powinien wdrożyć w swojej organizacji proces aktualizacji oprogramowania.

Prowadzenie aktualizacji oprogramowania jest procesem ciągłym, który bez odpowiedniego przygotowania i zautomatyzowania może spowodować wiele niekorzystnych skutków dla organizacji. Operator usługi kluczowej powinien na bieżąco monitorować bazy danych aktualizacji rekomendowanych przez producentów oprogramowania. Następnie, powinien dokonać analizy własnego środowiska pod kątem brakujących aktualizacji, by na podstawie wyników tej analizy ustalić priorytetowe obszary do zaktualizowania, a także opracować odpowiedni harmonogram aktualizacji, uwzględniający np. konieczność przerwania procesu świadczenia usługi kluczowej. Po wykonaniu tych czynności, operator powinien odpowiednio przygotować się do zaktualizowania poszczególnego oprogramowania (w tym m.in. wykonać kopię zapasową oprogramowania), a następnie przetestować wgrane aktualizacje pod kątem sprawności systemów w środowisku testowym. Jeżeli test zaktualizowanego oprogramowania wyjdzie poprawnie, wówczas podmiot powinien zainstalować aktualizacje w środowisku produkcyjnym. Po zakończonej instalacji należy zweryfikować poprawność zainstalowanych aktualizacji. W przypadku wystąpienia błędów po aktualizacji, operator powinien posiadać przygotowaną kopię zapasową systemów, aby w razie konieczności można było przywrócić poprzednią wersje systemu i tym samym cofnąć aktualizację powodującą błędy. Po dokonaniu instalacji aktualizacji, operator powinien zarejestrować informacje o zmianie w odpowiednich dokumentach, aby były one zawsze aktualne. Po zakończonym cyklu, rozpoczyna się kolejny. Poniżej, znajduje się wizualizacja tego procesu.

Rysunek 6 – Wizualizacja procesu aktualizacji oprogramowania.

Źródło: I. Tarnowski, *Procesy zarządzania aktualizacjami systemów i oprogramowania*, IT Professional, http://www.it-professional.pl/bezpieczenstwo/artykul,7986,procesy-zarzadzania-aktualizacjami-systemow-i-oprogramowania.html [dostęp: 20.04.2021 r.].

Należy podkreślić, że proces zarządzania aktualizacjami powinien obejmować m.in. serwery produkcyjne i testowe, urządzenia sieciowe, stacje robocze, urządzenia typu appliance, urządzenia mobilne, urządzenia IoT i IIoT, aplikacje (seryjne, własne itd.)[58]. Operator usługi kluczowej powinien objąć specjalnym nadzorem oprogramowanie wykorzystywane do świadczenia usługi kluczowej, a także mające wpływ na jej jakość i dostępność. Należy przy tym podkreślić, że mogą istnieć ograniczenia dotyczące aktualizacji w sektorze energetycznym, związane z fizyczną strukturą sieci, wymagania czasu rzeczywistego, konieczności zatrzymania produkcji operacyjnej, omówione w rozdziale 5.1.

Zaleca się by operator usługi kluczowej opracował i utrzymywał aktualny katalog oprogramowania zawierający informacje na temat posiadanych zasobów.

Posiadanie i aktualizowanie katalogu oprogramowania powinno być elementem wspierającym proces zarządzania aktualizacjami i łatkami bezpieczeństwa. Powinny się w nim znajdować informacje na temat m.in. rodzaju systemu operacyjnego i jego wersji, adresach IP, rzeczywistej lokalizacji urządzeń, zainstalowanym oprogramowaniu, osobach odpowiedzialnych za dany system wraz z danymi kontaktowymi itd.[59] Oczywiście, każdy operator powinien dostosować zakres katalogu do swoich potrzeb i przetwarzanych informacji.

[58] I. Tarnowski, *Procesy zarządzania aktualizacjami systemów i oprogramowania*, IT Professional, http://www.it-professional.pl/bezpieczenstwo/artykul,7986,procesy-zarzadzania-aktualizacjami-systemow-i-oprogramowania.html [dostęp: 20.04.2021].

[59] I. Tarnowski, *Procesy zarządzania aktualizacjami systemów i oprogramowania*, IT Professional, http://www.it-professional.pl/bezpieczenstwo/artykul,7986,procesy-zarzadzania-aktualizacjami-systemow-i-oprogramowania.html [dostęp: 20.04.2021].

Jednym ze sposobów zarządzania aktualizacjami jest np. posiadanie bazy danych zarządzania konfiguracją CMDB (ang. *Configuration Management DataBase*), która jest jednym z elementów standardów ITIL (ang. *Information Technology Infrastructure Library*). ITIL jest zbiorem najlepszych praktyk w zakresie zarządzania usługami IT. Jednym z podstawowych założeń metodyki ITIL jest zapewnienie spójności pomiędzy usługami IT a celami biznesowymi, nawet w sytuacji, gdy cele te ulegną zmianie. Baza CMDB dostarcza informacji na temat wszelkich komponentów, w tym usług, oprogramowania, komponentów IT, dokumentów, użytkowników i sprzętu, którymi należy zarządzać, aby świadczyć usługi IT. Ponadto, CMDB pozwala na śledzenie lokalizacji i wszelkich zmian zasobów, a także ich atrybuty i relacje z innymi zasobami[60]. Posiadając bazę zawierającą informacje o posiadanych zasobach przez organizację, możliwe jest wprowadzenie pewnej automatyzacji procesów zarządzania systemami IT w organizacji, a także łatwiejsze zarządzanie sprzętem, cyklem życia oprogramowania, w tym aktualizacjami, oraz przyspieszenie rozwiązania problemów z uwagi na zidentyfikowane powiązania pomiędzy poszczególnymi zasobami[61].

Zaleca się regularne przeprowadzanie aktualizacji oprogramowania z uwzględnieniem analiz podatności i zaleceń producenta, a także poziomu krytyczności poszczególnych aktualizacji.

Zasadne jest by regularnie aktualizować oprogramowanie wykorzystywane do świadczenia usług kluczowych, jednakże proces ten powinien opierać się na szczegółowej analizie, a decyzja o przeprowadzeniu aktualizacji powinna zostać podjęta świadomie. Jest to ważny element zwłaszcza w systemach automatyki przemysłowej, obsługujących proces technologiczny w trybie ciągłym, a także działających w ramach odseparowanych sieci, gdzie aktualizacja oprogramowania niejednokrotnie może być dokonana wyłącznie w czasie planowanych postojów bądź przez serwis producenta. Co więcej, w ramach systemów automatyki przemysłowej często występuje zróżnicowane oprogramowanie, w tym starsze programy, które już nie są wspierane przez producenta, ale na podstawie przeprowadzonej analizy ryzyka, operator dopuszcza ich funkcjonowanie.

Rekomenduje się bieżące obserwowanie informacji o wydawanych przez producentów oprogramowania łatkach bezpieczeństwa, w celu poprawienia bezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej. Zaleca się przygotowanie i wdrożenie procedury instalacji poprawek bezpieczeństwa.

Te działania wiążą się bezpośrednio z zarządzaniem podatnościami, ponieważ poprawki bezpieczeństwa (ang. *patch*) to aktualizacje oprogramowania mające na celu wyeliminowanie wykrytych podatności i zwiększenie bezpieczeństwa ich funkcjonowania[62]. Informacje na temat pojawiających się podatności powinny być czerpane z zaufanych źródeł, jak np. CVE czy NVD NIST (patrz rozdział 13.3.). Jest to to tyle ważne, że każda zidentyfikowana podatność ma przypisany odpowiedni poziom klasyfikacji zależny od różnych czynników zdefiniowanych w zależności od metodyki, np. w przypadku CVSS ocena danej podatności jest podawana w skali od 0–10, gdzie wynik 0 oznacza brak wpływu, a 9–10 dotyczy krytycznej podatności. Od tego również zależy zalecenie instalacji danej poprawki bezpieczeństwa – od opcjonalnej po krytyczną. Jednakże, każdy podmiot powinien mieć na uwadze, że kwestia instalacji danej poprawki powinna być przeanalizowana przez pryzmat kluczowych systemów zidentyfikowanych w ramach procesu świadczenia usługi kluczowej, ponieważ w takich systemach, nawet mało znacząca podatność może spowodować daleko idące konsekwencje, a nawet uniemożliwić świadczenie usługi kluczowej, dlatego zalecane jest indywidualne podejście do każdej poprawki bezpieczeństwa dotyczącej kluczowych systemów informacyjnych.

[60] *IT Infrastructure Library*, IBM, https://www.ibm.com/cloud/learn/it-infrastructure-library [dostęp: 22.04.2021].
[61] W. Pawłowicz, *Automat do zarządzania*, Computerworld, https://www.computerworld.pl/news/Automat-do-zarzadzania,321005.html [dostęp: 22.04.2021].
[62] Definicja słowa *patch*, *Słownik języka polskiego*, https://sjp.pl/patche [dostęp: 20.04.2021].

Zaleca się by w przypadku braku opracowania przez producenta poprawek bezpieczeństwa eliminujących daną podatność, operator usługi kluczowej przeprowadził analizę ryzyka i podjął odpowiednie działania nakierowane na zminimalizowanie ryzyka wystąpienia incydentu.

Należy mieć na uwadze, że nie wszystkie zidentyfikowane luki bezpieczeństwa w oprogramowaniu są łatwe do załatania (patrz także rozdział 5.1). Z tego powodu, poprawki bezpieczeństwa często pojawiają się z opóźnieniem. Zatem, operator usługi kluczowej powinien do czasu pojawienia się odpowiedniej poprawki przeprowadzić analizę ryzyka wystąpienia incydentu, a także przygotować i wdrożyć odpowiednie środki do tego, aby w jaki największym stopniu ograniczyć możliwość wykorzystania danej podatności.

Dowody kontroli:

– *dokumentacja zarządzania sprzętem i oprogramowaniem, w tym: rejestr zasobów informatycznych, procedury prowadzenia rejestru zasobów informatycznych, procedury przydzielania, zwrotu sprzętu i oprogramowania, procedury korzystania z zasobów informatycznych przez użytkowników oraz dokumentacja wykonywania ww. procedur.*

6.6. Zarządzanie licencjami

Rekomenduje się by operator usługi kluczowej dokonał inwentaryzacji posiadanego przez siebie licencjonowanego oprogramowania.

Operator powinien znać wersje oprogramowania, okres obowiązywania licencji, ilość posiadanych licencji, koszty odnowienia licencji, zakres stosowania licencji itp. Ponadto operator powinien dokonać inwentaryzacji oprogramowania wykorzystywanego przez pracowników. Dzięki temu będzie mógł zidentyfikować oprogramowanie, które już nie jest potrzebne, a tym samym przyczyni się to do oszczędności finansowych. Należy pamiętać, żeby w czasie inwentaryzacji uwzględnić także usługi dostarczane przez dostawców zewnętrznych[63].

W przypadku zakupu oprogramowania, operator powinien uwzględnić rzeczywiste zapotrzebowanie i zdefiniować wymagania techniczne.

Odpowiednie dostosowanie zakupu do potrzeb procesów i użytkowników przyczyni się do efektywniejszego wykorzystania środków finansowych, a także pozwoli uniknąć sytuacji, w której zakupione oprogramowanie wraz z licencjami byłoby bezużyteczne. Ponadto operator powinien pamiętać, by zakupić odpowiednią ilość licencji danego oprogramowania, a także by były one dopasowane do użytku biznesowego. Rekomenduje się również by licencje były jak najbardziej elastyczne, tak aby bez problemu można było je przekazywać między użytkownikami.[64]

[63] T. Cygan, *Podstawowe zasady zarządzania licencjami*, IT Professional, http://www.it-professional.pl/zarzadzanie-i-prawo-it/artykul,8347,podstawowe-zasady-zarzadzania-licencjami.html [dostęp: 31.03.2021].

[64] T. Cygan, *Podstawowe zasady zarządzania licencjami*, IT Professional, http://www.it-professional.pl/zarzadzanie-i-prawo-it/artykul,8347,podstawowe-zasady-zarzadzania-licencjami.html [dostęp: 31.03.2021].

Rekomenduje się by operator usługi kluczowej posiadał system zarządzania licencjami oprogramowania.

Z uwagi na ilość posiadanego oprogramowania, a także różnorodność jego dostawców i poziomu skomplikowania umów licencyjnych dany podmiot może skorzystać z różnego rodzaju narzędzi dostępnych na rynku, jak np. typu SAM (ang. *Software Asset Management*), czyli zarządzanie oprogramowaniem w organizacji zgodne z normą ISO/IEC 19770-1:2006 i ITIL. W rezultacie, operator będzie miał pełną wiedzę na temat zakupionych licencji, ich ilości, instalacji, terminie wygaśnięcia subskrypcji itp., a także zgodności użycia oprogramowania z zakupioną licencją[65]. Prawidłowo wdrożone zarządzanie licencjami i oprogramowaniem ma na celu przede wszystkim poprawę bezpieczeństwa systemów i aplikacji, zredukowanie kosztów utrzymania i zakupu oprogramowania, a także lepsze przygotowanie do audytów[66].

Dowody kontroli:

– *dokumentacja systemu zarządzania licencjami, spis oprogramowania wykorzystywanego w przedsiębiorstwie.*

6.7. Testowanie systemów i komponentów

Organizacja powinna testować systemy i komponenty dotyczące systemów informacyjnych, od których zależy świadczenie usługi kluczowej.

Testowanie systemów i komponentów odpowiedzialnych za realizację usługi kluczowej pozwala upewnić się, że spełniają one założenia ustanowione przez organizację oraz pozostałe określone wymogi związane z ich cyberbezpieczeństwem. Metodyki i kryteria czynności wykonywanych w tym zakresie powinny mieć spójny oraz ustandaryzowany charakter, gdyż wówczas pozwoli to uzyskać obiektywne i powtarzalne efekty. Ponadto, umożliwi to przedstawienie informacji na temat prawidłowości wdrożenia wymagań, ich funkcjonowania zgodnie z intencją oraz osiągania pewnych pożądanych wartości dotyczących bezpieczeństwa systemów informacyjnych i ich komponentów. Świadomość w zakresie efektywności implementacji wymagań bezpieczeństwa dla systemów informacyjnych oraz środowisk ich funkcjonowania ma podstawowe znaczenie dla określenia ryzyka związanego z funkcjonowaniem organizacji.[67]

Testowanie w zakresie cyberbezpieczeństwa i związane z nim działania powinny być prowadzone w koordynacji z testami interoperacyjności, w celu zapewnienia, że zmiany w tych obszarach nie będą miały na siebie wzajemnego, negatywnego wpływu. W związku z powyższym, jeżeli zostanie opracowane rozwiązanie umożliwiające interoperacyjność, może wówczas zaistnieć ryzyko, iż jednocześnie mogły zostać wprowadzone nowe potencjalne podatności w zabezpieczeniach. Zapewnienie koordynacji pomiędzy testami cyberbezpieczeństwa a testami interoperacyjności, może pozwolić zidentyfikować i zaradzić błędom, które mogły zostać popełnione w fazie projektowania,

[65] M. Marciniak, *Zarządzanie legalnością oprogramowania – to nie takie proste*, IT WIZ., https://itwiz.pl/zarzadzanie-legalnoscia-oprogramowania-nie-takie-proste/ [dostęp: 01.04.2021].

[66] *Software Asset Management*, Deloitte, https://www2.deloitte.com/pl/pl/pages/technology/topics/SoftwareAssetManagement.html [dostęp: 02.04.2021].

[67] NIST NISTIR 7628 Rev. 1 *Guidelines for Smart Grid Cybersecurity. Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*, 2014, s. 214.

wdrażania lub funkcjonowania, a których skutkiem może być utrata informacji, dostępności lub uzyskanie nieautoryzowanego dostępu[68].

Jednym z nadrzędnych celów testowania systemów informacyjnych oraz komponentów jest wykrycie związanych z nimi podatności, aby móc podjąć działania zaradcze. Identyfikacja podatności może nastąpić w trakcie czynności takich, jak:

a) przeprowadzanie audytów i testów bezpieczeństwa, na które składają się: testy podatności, testy penetracyjne, audyty zgodności z wymaganiami norm bezpieczeństwa, audyty weryfikujące spełnienie wymagań bezpieczeństwa, ćwiczenia realizacji planów zapewnienia ciągłości działania oraz ćwiczenia typu *red teaming*, czyli kontrolowany atak na własną organizację,

b) przegląd systemu zarządzania bezpieczeństwem informacji i przegląd planów zapewnienia ciągłości działania,

c) przeprowadzanie modelowania zagrożeń i analizy ryzyka,

d) zarządzanie zdarzeniami bezpieczeństwa oraz proaktywne monitorowanie bezpieczeństwa systemów,

e) zarządzanie incydentami bezpieczeństwa (podatność jako przyczyna zgłoszonego incydentu bezpieczeństwa),

f) konsekwencja aktywnego poszukiwania informacji o podatnościach typu *zero-day* pasujących do bazy aktywów organizacji.[69]

W związku z powyższymi czynnościami należy przywiązać szczególną wagę do skanowania podatności. Wykorzystuje się w tym celu wyspecjalizowane narzędzia, zróżnicowane pod kątem zasięgu, zaawansowania technicznego, czy konieczności ich pogłębionej konfiguracji przez osobę przeprowadzającą test. W praktyce, wyniki skanowania są jednak głównie uzależnione od doświadczenia testera. Należy również mieć na uwadze, iż skanowanie podatności w elementach środowisk OT może nieść za sobą szereg ryzyk i niebezpieczeństw, ze względu na wrażliwość ich komunikacji.

Skanowanie podatności należy odróżnić od testów penetracyjnych – są one przeprowadzane w sposób zautomatyzowany i nie posiadają cechy bycia ukierunkowanymi na dedykowane, mniej znane autorskie systemy lub aplikacje. Skaner podatności pozwala uzyskać informacje o słabościach odnoszących się do popularnych rozwiązań, ponieważ wykorzystuje on bazę znanych już podatności. Należy jednak mieć na uwadze, iż przeprowadzenie skanowania powinno być skonsultowane z administratorami, w celu zaplanowania okna serwisowego dla takich działań. Ponadto, powinno ono także obejmować monitoring stabilności skanowanych systemów oraz uwzględniać konieczność informowania osoby przeprowadzającej skanowania o wszelkich nieprzewidzianych nieprawidłowościach[70].

Należy przy tym wyróżnić dwa rodzaje skanowania:

a) uwierzytelnione – realizowane z uwzględnieniem informacji dotyczących uwierzytelniania, dostępu itp.,

b) nieuwierzytelnione – wykonywane w taki sposób, jakby badana infrastruktura była nasłuchiwana z „zewnątrz”[71].

[68] *Ibidem*, s. 215.
[69] C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo*, 2020, s. 152
[70] *Ibidem*, s. 154.
[71] *Ibidem*.

Testy penetracyjne również stanowią istotny element weryfikacji bezpieczeństwa systemów i komponentów, będąc kontrolowaną próbą przełamania ich zabezpieczeń. Działania realizowane w związku z nimi, symulują ataki hakerów czy crackerów, a ich celem jest ujawnienie podatności w danym systemie, która umożliwiłaby pokonanie zabezpieczeń, włamanie się lub przejęcie kontroli nad systemem. Badanie jego odporności na ataki, jest procesem złożonym z pięciu etapów:

I. Zdobycie informacji na temat badanego obiektu lub obszaru,

II. Skanowanie – przegląd urządzeniem elektronicznym badanego obiektu lub obszaru punkt po punkcie,

III. Enumeracja – zdobywanie informacji na temat systemów, na których bazuje usługa. Polega na nawiązaniu aktywnego połączenia oraz wysłaniu zapytania na temat zasobów systemu udostępniającego daną informację, z pominięciem weryfikacji uprawnienia audytora do otrzymania takich danych,

IV. Eksploracja, pozyskiwanie, ekstrakcja, drążenie i wydobywanie wiedzy z baz danych. Polega ono na sprawdzeniu możliwości ich pozyskania bez odpowiednich uprawnień,

V. Raportowanie mocnych i słabych stron testowanego systemu wraz z oceną krytyczności tych słabych[72].

Można wyróżnić trzy typy wykonywanych testów penetracyjnych:

a) Black-Box – stanowi próbę przełamania zabezpieczeń bez jakiejkolwiek wiedzy na temat badanego systemu. Audytor posiada informacje jedynie na temat celu ataku, starając się przełamać zabezpieczenia, wiernie odwzorowując działania hakera,

b) Gray-Box – to próby przełamania zabezpieczeń z fragmentaryczną wiedzą w zakresie atakowanego systemu. Atakujący używa technik wykorzystywanych prze hakerów, lecz posiada także dodatkową wiedzę, aby dokładniej penetrować zabezpieczenia,

c) White-Box – atakujący ma kompletną wiedzę dotyczącą atakowanego systemu i stara się na tej podstawie przełamać zastosowane zabezpieczenia, w celu zdobycia jak najszerszych informacji o badanym systemie[73].

Testy tego typu pozwalają uzyskać wiele cennych informacji dotyczących bezpieczeństwa systemów poddawanych analizie, jak m.in.:

- potencjalny zbiór możliwych wektorów ataku,
- zidentyfikowane podatności wysokiego ryzyka, powstające w wyniku połączenia i wykorzystania w określonej kolejności luk niskiego ryzyka,
- zidentyfikowane luki, mogące być trudne lub niemożliwe do wykrycia za pomocą automatycznych narzędzi do skanowania pod kątem podatności sieci lub aplikacji,
- ocena skali potencjalnych strat biznesowych i operacyjnych w wyniku wystąpienia skutecznego ataku,

[72] *Ibidem*, s. 156.
[73] Ibidem, s. 157.

- zbadane zdolności sieciowych systemów ochrony do skutecznego wykrywania i reagowania na ataki,
- argumenty związane z koniecznością inwestowania w personel i technologie rozwiązań w zakresie cyberbezpieczeństwa[74].

Dowody kontroli:

– dokumentacja z zrealizowanych testów podatności, testów penetracyjnych, audytów zgodności z wymaganiami norm bezpieczeństwa, audytów weryfikujące spełnienie wymagań bezpieczeństwa.

[74] *Ibidem*.

7. Bezpieczeństwo osobowe, podnoszenie świadomości, szkolenia

7.1. Program podnoszenia kompetencji z zakresu cyberbezpieczeństwa

Zaleca się, żeby operator usługi kluczowej opracował odpowiednio dopasowany do swoich potrzeb program podnoszenia kompetencji z zakresu cyberbezpieczeństwa wśród swoich pracowników.

Operator usługi kluczowej powinien zatrudniać specjalistów posiadających kwalifikacje w zakresie cyberbezpieczeństwa, aby zapewnić odpowiedni poziom cyberbezpieczeństwa świadczonej usługi kluczowej. Jednakże, szybkość zmieniających się technologii i pojawiających się nowych cyberzagrożeń powoduje, że osoby zajmujące się kwestią cyberbezpieczeństwa powinny regularnie podnosić swoje kompetencje, a operator usługi kluczowej powinien swoim pracownikom zagwarantować odpowiednią ścieżkę rozwoju. Dodatkowo, możliwość doskonalenia umiejętności wpływa pozytywnie na stabilność zatrudnienia specjalistów w danym podmiocie.

Zalecane jest by program szkoleń był odpowiednio dostosowany do potrzeb danego podmiotu, a także do poziomu dojrzałości organizacji i ilości wykorzystywanych systemów do świadczenia usługi kluczowej, a także ich złożoności i różnorodności. Z racji tego, operator powinien dopasować program szkolenia do konkretnych stanowisk, nie tylko związanych stricte z cyberbezpieczeństwem, ponieważ oprócz automatyków czy administratorów systemów informacyjnych, ważne jest np. odpowiednie opracowanie opisu zamówień publicznych pod kątem zachowania standardów bezpieczeństwa i kompatybilności nowych urządzeń czy oprogramowania z już posiadanymi zasobami.

Ministerstwo Klimatu i Środowiska, w załączniku do niniejszych rekomendacji, wskazuje przykładowe obszary tematyczne obejmujące kwestie, których wzmocnienie może przełożyć się na większy poziom cyberbezpieczeństwa, niezależnie od podsektora, w którym funkcjonuje dany podmiot. Jednakże, operator usługi kluczowej powinien zapewnić szkolenia, które będą właściwe ze względu na rodzaj świadczonej przez niego usługi oraz będą dopasowane do potrzeb kompetencyjnych pracowników.

Załącznik nr 2 – przykładowa lista szkoleń dla pracowników operatorów usług kluczowych.

Dowody kontroli:

– dokumentacja kontroli referencji zawodowych kluczowego personelu.

7.2. Podnoszenie kompetencji i kwalifikacji

W pakiecie szkoleń podstawowych, dedykowanych nowo przyjętym pracownikom, organizacja powinna uwzględnić szkolenia z zakresu cyberbezpieczeństwa.

Podmiot powinien zagwarantować podobny poziom wiedzy bazowej wszystkich pracowników swojej organizacji w zakresie tematyki cyberbezpieczeństwa. Z racji tego, rekomenduje się by uwzględnić szkolenia z podstaw cyberbezpieczeństwa w ramach wdrożenia nowych pracowników, które pozwolą zapoznać się zarówno z procedurami i wymaganiami cyberbezpieczeństwa funkcjonującymi w danym przedsiębiorstwie, jak i wyrównać poziom wiedzy w tym zakresie. Ważne jest również budowanie świadomości sytuacyjnej personelu, zwłaszcza w kontekście potencjalnych kampanii phishingowych, spearphishingowych czy innych nietypowych zdarzeń. Zaleca się również zapoznanie nowych pracowników z procedurą zgłaszania incydentów cyberbezpieczeństwa do odpowiednich struktur w organizacji.

Organizacja powinna zapewnić kompleksowe podejście do szkoleń i działań mających na celu podniesienie świadomości cyberbezpieczeństwa swoich pracowników niezależnie od komórki organizacyjnej w jakiej pracują.

Poza szkoleniem nowozatrudnionych pracowników, operator usługi kluczowej powinien również prowadzić cykliczne szkolenia dla wszystkich zatrudnionych osób, aby regularnie budować świadomość cyberbezpieczeństwa w ramach swojej organizacji. Operator również powinien zidentyfikować różne grupy docelowe szkoleń – od podstawowych użytkowników systemów po osoby bezpośrednio zajmujące się bezpieczeństwem sieci i systemów IT i OT. Zakres szkoleniowy powinien być odpowiednio dopasowany w zależności od kompetencji potrzebnych do realizacji zadań na danym stanowisku.

Proces podnoszenia świadomości z zakresu cyberbezpieczeństwa wśród użytkowników systemów informacyjnych powinien być procesem ciągłym, aby utrwalać ich wiedzę i przypominać informacje na temat cyberzagrożeń i podstawowych zasad bezpieczeństwa.

W celu utrzymania odpowiedniego poziomu wiedzy dotyczącej cyberbezpieczeństwa w organizacji, zaleca się przeprowadzanie cyklicznych szkoleń przypominających najważniejsze kwestie związane z cyberbezpieczeństwem. Z racji tego, że każdy najlepiej uczy się na swoich błędach, rekomenduje się również przeprowadzanie co jakiś czas praktycznych szkoleń, poprzez np. organizację wewnętrznych niezapowiedzianych ćwiczeń z wyłapywania kampanii phishingowych. Poza walorem szkoleniowym, na podstawie wyników z organizacji tego typu ćwiczeń, podmiot może zbadać poziom dojrzałości swojej organizacji w zakresie cyberbezpieczeństwa, a także procedury zgłaszania potencjalnych incydentów. Dodatkowo w celu zbadania efektywności szkoleń podstawowych dla wszystkich pracowników, organizacja powinna przeprowadzać niezapowiedziane symulacje zagrożeń z wykorzystaniem m.in. socjotechniki.

Pracownicy w których zakresie obowiązków wymagana jest zaawansowana wiedza z zakresu cyberbezpieczeństwa, powinni mieć zapewniony dostęp do cyklicznych szkoleń i odpowiednich ścieżek rozwoju.

Rozwój nowych technologii i wdrażanie ich do przedsiębiorstw ma bezpośredni wpływ na zmianę otoczenia technologicznego, a tym samym na nowe wektory cyberataków. Z tego powodu rekomenduje się, opracowanie odpowiedniego programu szkoleń dla specjalistów zajmujących się cyberbezpieczeństwem, aby poziom ich wiedzy był na wysokim poziomie, co będzie gwarancją lepszego przygotowania na wystąpienie potencjalnego cyberataku i odpowiedniej reakcji.

Zaleca się uczestnictwo w międzynarodowych forach współpracy w zakresie bezpieczeństwa, które powstały w celu umożliwienia dyskusji, współpracy i wymiany informacji w ramach grupy zaangażowanych podmiotów, w celu poprawienia świadomości zagrożeń.

Ze względu na mocne powiązanie ze sobą różnych sektorów, część zdarzeń w jednej branży może mieć wpływ na inne podmioty w kraju, jak i zagranicą. W rezultacie, rekomenduje się, aby operatorzy usług kluczowych brali aktywny udział w różnych forach wymiany informacji, zarówno na poziomie krajowym, jak i międzynarodowym. Przyczyni się to do budowy zaufania pomiędzy uczestnikami takich gremiów, a także do szybszego przekazywania informacji o potencjalnych zdarzeniach i zagrożeniach.

Rekomenduje się by operatorzy usług kluczowych brali aktywny udział w organizowanych krajowych ćwiczeniach cyberbezpieczeństwa, jak również, w ramach możliwości, w tych organizowanych na poziomie międzynarodowym.

Ćwiczenie i doskonalenie procedur przyczynia się do sprawniejszej reakcji na pojawiające się zagrożenie. Ponadto, umożliwia wymianę doświadczeń i dobrych praktyk z innymi podmiotami, a także przetestowanie swoich własnych zdolności. W takich ćwiczeniach zazwyczaj bierze udział wiele podmiotów z różnych sektorów – administracji publicznej, energii, finansów, dostawców usług cyfrowych itd. Co więcej, podczas ćwiczeń istnieje możliwość przetestowania ścieżki kontaktu z CSIRT poziomu krajowego czy CSIRT sektorowym.

Organizacja powinna dokumentować przeprowadzanie szkoleń dla pracowników.

Dokumentowanie szkoleń oraz innych aktywności, których celem jest podniesienie lub zrównanie kompetencji pracowników jest działaniem, które pozwoli na bardziej sprawne zarządzanie tym procesem. Posiadanie odpowiedniej dokumentacji potwierdzającej udział osób zatrudnionych w poszczególnych aktywnościach szkoleniowych wspomoże ich rozwój, zwłaszcza, gdy dalsza edukacja, w tym udział w szkoleniach zakończonych różnego rodzaju certyfikatami, wymaga posiadania potwierdzonego zakresu wiedzy i lat doświadczenia.

Dowody kontroli:

– *dowody uczestnictwa personelu w szkoleniu (na przykład przyjęte zaproszenie, data i program szkolenia, podpisana lista uczestników warsztatów uświadamiających, materiały informacyjne itp.).*

7.3. Weryfikacja personelu, zmiany kadrowe

Jak wskazują statystyki opublikowane w raporcie[75], ponad 85% nadużyć w firmach powodowanych jest przez ludzi z wewnątrz. W związku z powyższym, należy zwrócić uwagę na bezpieczeństwo i wiarygodność osób, które zatrudniamy, tym samym dopuszczając do informacji, stanowiących aktywo informacyjne przedsiębiorstwa.

W związku z powyższym, należy podejmować co najmniej poniższe rodzaje działań:

Przygotowanie procesu dokładnego weryfikowania pracowników

Przedsiębiorstwo powinno posiadać procedurę rekrutacji opisującą przebieg całego procesu zatrudnienia pracownika. Organizacja powinna podjąć działania zmierzające do zebrania jak największej informacji o kandydacie na dane stanowisko. Historię kandydatów na dane stanowiska należy zweryfikować zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi w sposób proporcjonalny do wymagań biznesowych i klasyfikacji informacji do których będzie dany pracownik miał dostęp.[76] Zebrane informacje powinny być zestawione z przygotowanym wcześniej profilem kandydata (profilem kompetencyjnym), gdzie określone będą obowiązki i wynikająca z nich konieczność dostępu do różnych kategorii informacji oraz pomieszczeń. Szczególnie ważne jest weryfikowanie tych osób, które mogą mieć dostęp do informacji niejawnych, czy też informacji stanowiących tajemnicę przedsiębiorstwa lub innych krytycznych informacji. Weryfikacja może opierać się m.in. na sprawdzeniu czy taka osoba nie była karana (wymaganie od kandydatów zaświadczenia o niekaralności), ze szczególnym naciskiem na przestępstwa związane z informacjami stanowiącymi tajemnicę handlową. Dodatkowym atutem u kandydatów może być uzyskanie poświadczenia bezpieczeństwa w rozumieniu ustawy z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych*[77]. W przypadku stwierdzenia jakichkolwiek nieprawidłowości lub zastrzeżeń do kandydata, zaleca się odstąpienie od dalszego procesu rekrutacyjnego. W sytuacji, gdy kandydat rekrutowany jest na stanowisko, które z racji swojej krytyczności czy rodzajów przekazywanych informacji *może* stwarzać większe prawdopodobieństwo zmaterializowania się ryzyka (np. administratorzy, programiści), organizacja powinna przedsięwziąć szczególne środki ostrożności. Weryfikacja tożsamości kandydata powinna odbywać się na podstawie oryginałów przedstawionych dokumentów, zawierających pełne dane ich posiadacza, a także podpis i zdjęcie. Same dokumenty powinny być również sprawdzone pod kątem ich ważności, właściwości organu, który je wydał. Zaleca się, aby organizacja wymagała od kandydata na takie stanowiska dokumentów, które z racji swoich zabezpieczeń są trudne do podrobienia, tj. dowód osobisty, paszport, prawo jazdy. Pracownicy dokonujący weryfikacji takich dokumentów powinni mieć wiedzę na temat sposobu ich skutecznej analizy[78]. *Również dane zawarte w dokumentach dostarczonych przez kandydata, które mają potwierdzać jego doświadczenie lub kompetencje, powinny być weryfikowane pod kątem wiarygodności. Przykładowo, należy zwrócić uwagę czy kursy, szkolenia, certyfikaty, którymi legitymuje się kandydat, nie są wydane przez podmioty, które posiadając nazwy podobne do wiodących i uznanych miejsc kształcenia, oferują znacznie niższy poziom nauczania*[79].

[75] Ernst & Young 9th International Fraud Survey – IX Badania Nadużyć Gospodarczych – Ryzyko Nadużyć na Rynkach Wschodzących.
[76] Norma PN-EN ISO/IEC 27001 s. 15.
[77] tj. Dz. U. z 2019 r. poz. 742.
[78] RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej Załącznik 1*, s. 60.
[79] *Ibidem*, s. 61.

Proces uświadamiania pracowników i kandydatów

Jednym z najlepszych środków ochrony aktywów organizacji są pracownicy świadomi zagrożeń, a także wagi przetwarzanych informacji. Pracownik, który nie jest do końca świadomy konsekwencji, np. ujawnienia pewnych informacji, może w sposób nieintencjonalny wykonać czynność, której negatywny skutek odbije się na organizacji. Proces cyklicznego uświadamiania i szkoleń może być działaniem, które stworzy prewencyjną ochronę przed takimi zdarzeniami. Szkolenia dla pracowników nowozatrudnionych jak i obecnych, powinny obejmować co najmniej informacje związane z bezpieczeństwem informacji w organizacji, a także informacje specyficzne dla danego stanowiska pracy[80]. Zaleca się, aby same szkolenia przyjmowały formę ciekawą dla słuchacza, która pozwoli nie tylko na bierne otrzymywanie wiedzy w danym zakresie, ale także zapewni możliwość dyskusji. Ponadto, w razie możliwości powinno się stosować przykłady naruszeń wraz ze wskazaniem konsekwencji jakie wystąpiły lub mogły wystąpić. Najlepiej już w ramach procesu rekrutacyjnego, poinformować osobę rekrutowaną, że po zatrudnieniu będzie odpowiedzialna za przetwarzanie informacji dla danego przedsiębiorstwa, uświadomić taką osobę o wadze tego faktu, a także zastanowić się nad ewentualnym spisaniem stosownej umowy o zachowaniu poufności, w której kary umowne za jej naruszenie powinny być nie tylko adekwatne do zjawiska, ale także mieć charakter odstraszający od chęci chociażby sprzedaży informacji na czarnym rynku.

Zaleca się rozważenie zaimplementowania metody polegającej na zamieszczaniu w umowach podpisywanych z nowymi pracownikami, zapisów określających zakres odpowiedzialności dotyczącej bezpieczeństwa informacji danej organizacji.

Zapisy w umowach powinny być sformułowane w sposób egzekwowalne oraz powinny pozwalać na działania:

1. Wskazywać zbiory informacji, które podlegają ochronie,
2. Wskazać przewidywany czas trwania umowy, wraz z przypadkami, w których obowiązek zachowania poufności jest bezterminowy,
3. Określać obszary dozwolonego użycia informacji poufnych lub „wrażliwych",
4. Zapewniać prawo do monitorowania działań związanych z informacjami poufnymi lub wrażliwymi,
5. Wskazywać sposób powiadamiania i raportowania w przypadku nieuprawnionego ujawnienia informacji,
6. Określać działania w momencie zakończenia umowy[81].

Ponadto, dodatkowe szkolenia sprawdzające reakcję na incydenty i utrwalające właściwe wzorce zachowań oraz postępowania z poufnymi informacjami będą procesem wzmacniającym komplementarność działań prewencyjnych.

Przeciwdziałanie

Zabezpieczeniem wartym zastosowania w danej organizacji jest właściwe finansowanie specjalistów, adekwatne do realiów rynkowych względem postawionych wymagań, jak i wprowadzanie monitorowania, który pracownik ma dostęp do poszczególnych kategorii informacji. Dzięki takiemu,

[80] J. Krawiec, G. Ożarek, *System Zarządzania Bezpieczeństwem Informacji w Praktyce. Zabezpieczenia*, Polski Komitet Normalizacyjny, Warszawa 2014, s. 27.
[81] *Ibidem*, s. 26.

w przypadku wycieku danych, organizacja może określi kto jest odpowiedzialny za dany wyciek oraz oszacować skalę zjawiska. W przypadku informacji przetwarzanych w systemach informacyjnych, po przeprowadzeniu szacowania bezpieczeństwa informacji oraz określeniu wartości przetwarzanych informacji, warto rozważyć wykorzystanie systemów DLP – (ang. *Data Leak/Leakage/Loss Protection/Prevention*). Oprogramowanie tego typu służy do ochrony danych przed wyciekiem, dotyczy to zarówno wycieków przypadkowych, wynikających na przykład z nieostrożności pracowników oraz działań celowych.

Organizacja powinna także podejmować kroki w celu wszczęcia postępowania dyscyplinarnego wobec pracowników, którzy naruszają podstawowe zasady bezpieczeństwa informacji. Postępowania te powinny być prowadzone zgodnie z przedstawionymi wcześniej i ustalonymi zasadami. Jest to działanie o charakterze nie tylko sankcyjnym lecz również prewencyjnym, gdyż może przyczynić się do zwrócenia uwagi na ten aspekt przez pozostałych pracowników[82].

W celu zabezpieczenia interesów organizacji podczas procesu zmiany zatrudnienia przez pracownika lub jego zakończenia, powinno określić się i przedstawić pracownikowi jakie zakresy odpowiedzialności w zakresie bezpieczeństwa informacji będą aktualne po zmianie statusu zatrudnienia. Powinno zwrócić się szczególną uwagę na konieczny zwrot aktywów informacyjnych przez pracowników w momencie zakończenia zatrudnienia[83].

Ponadto, organizacja powinna prowadzić ocenę ryzyka zakłócenia jej funkcjonowania z powodu nielegalnego wykorzystania informacji przez pracowników. Wyniki takiej analizy mogą przyczynić się do zmian procedury zatrudniania na bardziej dostosowaną do prawdopodobieństwa wystąpienia zdarzenia niepożądanego[84].

Dowody kontroli:

- *lista nominacji (na stanowiska dyrektorów ds. bezpieczeństwa informacji, inspektorów ds. ochrony danych itp.) oraz opis obowiązków i zadań dla stanowisk związanych z bezpieczeństwem. Istnieje schemat organizacji, opisy stanowisk pracy podpisane przez kluczowy personel, przeprowadzono stosowne szkolenia dotyczące pełnionych ról,*
- *dokumentacja zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym procedury nadawania, zmiany i odbierania uprawnień do pracy w systemach teleinformatycznych i dokumentacja wykonywania ww. procedur.*

[82] Norma PN-EN ISO/IEC 27001 s. 15

[83] *Ibidem*, s. 16.

[84] RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej Załącznik 1*, s. 60.

8. Audyty bezpieczeństwa systemów informacyjnych

8.1. Audyty bezpieczeństwa systemów informacyjnych

UKSC nałożyła na operatora usługi kluczowej obowiązki wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniającego prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem, wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych zapewniających:

– utrzymanie i bezpieczną eksploatację systemu informacyjnego,

– bezpieczeństwo fizyczne i środowiskowe, w tym kontrolę dostępu,

– ciągłość działania usług kluczowych,

– objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

Realizację tych obowiązków można osiągnąć poprzez wdrożenie systemu zarządzania bezpieczeństwem systemu informacyjnego w organizacji, służącego weryfikacji zgodności z normami np. ISO 27001, NIST SP 800-53[85], PCI DSS itd.

UKSC nałożyła też obowiązek przeprowadzenia audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej w terminie roku od dnia doręczenia decyzji administracyjnej o uznaniu za operatora, a następnie co najmniej raz na 2 lata.

Cele i zakres audytu bezpieczeństwa

W tym kontekście audyt bezpieczeństwa systemów informacyjnych będzie stanowić niezależny przegląd i badanie zapisów systemowych, realizowanych działań w systemie informacyjnym i związanych z nimi dokumentów. Audyt jest ukierunkowany na podniesienie poziomu bezpieczeństwa informacji, właściwe wdrożenie wymagań bezpieczeństwa systemów informacyjnych do poziomu obiektów fizycznych i logicznych oraz optymalizacja skuteczności zabezpieczeń i procesów bezpieczeństwa[86]. Wśród głównych celów audytu powinna się znaleźć identyfikacja i klasyfikacja systemów informacyjnych oraz aktywów organizacji, ocena ryzyka, weryfikacja zgodności wszystkich systemów i procesów organizacji z istniejącymi ramami regulacyjnymi, a także politykami i normami związanymi z IT i OT. W wymiarze praktycznym może służyć jako metoda okresowego przeglądu logów sieciowych i innych wskazanych, uprawnień kontroli dostępu, konfiguracji aktywów, a w konsekwencji wykrywania naruszeń w systemach informacyjnych.

Zakres audytu bezpieczeństwa informacji obejmuje szereg elementów, wśród których można wymienić między innymi opis fizycznych lokalizacji, jednostek organizacyjnych, powiązanych działań i procesów, a także harmonogram przeprowadzenia audytu. Określenie zakresu audytu stanowi element ogólnego procesu planowania audytu i z tego powodu powinien skupiać się na następujących elementach:

- określeniu obszarów narażonych na ryzyko, wytycznych regulacyjnych i koncentrować się na obszarach wysokiego ryzyka;

[85] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[86] https://www.isaca.org/Journal/archives/2016/volume-5/Pages/information-systems-security-audit.aspx

- krytycznych komponentach systemów informacyjnych, służących zapewnieniu odporności na poziomie operacyjnym i wykorzystywanym w procesie odbudowy;
- systemach stanowiących środowisko złożone z komponentów realizujących zadania i dostarczających funkcje w konkretnym otoczeniu środowiskowym, a także
- charakterze prowadzonej działalności operatora usługi kluczowej (podsektorze) i wpływu procesu audytu i technik audytu na tą działalność.

Zaleca się, aby operator usługi kluczowej:

1) *Określił w ramach ogólnej polityki bezpieczeństwa informacji zasady prowadzenia programów audytów bezpieczeństwa systemów informacyjnych względem personelu i krytycznych aktywów informacyjnych, w tym cele audytów, polityki, odpowiedzialności i procedury (patrz rozdział 4.1).*
2) *Uwzględnił w programowaniu audytu bądź w programach audytu wyniki szacowania ryzyka bezpieczeństwa systemów informacyjnych, w tym szacowanie ryzyka wystąpienia incydentu – (patrz rozdział 4.3).*
3) *Uwzględnił w programach audytu – w zależności od poziomu dojrzałości operatora – wymagania regulacyjne wynikające z UKSC, przepisów Prawa energetycznego[87], Zalecenia Komisji Europejskiej 2019/553 z dnia 3 kwietnia 2019 r. w sprawie cyberbezpieczeństwa w sektorze energetycznym.*

Formy audytów i wymagane kompetencje audytorów

Z punktu widzenia systemowego i stosowanej praktyki, wyróżnia się trzy główne formy audytu bezpieczeństwa systemów informacyjnych[88]:

- *Audyt wewnętrzny (audyt pierwszej strony)* to wewnętrzne procedury realizowane przez członka organizacji lub grupę członków w ramach organizacji. Celem audytu wewnętrznego jest zapewnienie, że proces lub zbiór procesów w systemie bezpieczeństwa informacji spełnia wymagania proceduralne określone przez operatora usług kluczowych. Audyt wewnętrzny może być przeprowadzany przez właściciela procesu, wówczas proces audytu nazywany jest samoocena. W imieniu operatora, audytor prowadzi działania wewnątrz organizacji i dokonuje dogłębnej kontroli, w celu znalezienia obszarów problemowych, w których występują niezgodności, a także określa możliwości poprawy.
- *Audyt drugiej strony* ma miejsce, gdy operator przeprowadza audyt dostawcy usługi (strony trzeciej) w celu upewnienia się, że ten spełnia wszystkie wymagania określone w umowie pomiędzy obiema stronami.
- Audyt przeprowadzany przez stronę trzecią tzw. *audyt strony trzeciej*, ma miejsce wówczas, gdy jest prowadzony przez niezależny podmiot w celu weryfikacji i zatwierdzenia zgodności organizacji z wymaganiami bezpieczeństwa. Najczęściej tego typu audyt jest przeprowadzany przez jednostki certyfikujące, w celu porównania i weryfikacji, czy zapewniona jest ciągłość świadczenia usługi kluczowej, odpowiedni poziom bezpieczeństwa systemów informacyjnych służących do jej świadczenia oraz czy system bezpieczeństwa informacji operatora usługi kluczowej spełnia wszystkie kryteria i wymagania ujęte w danej normie i kontroluje, czy dany podmiot spełnia wymagania w bieżącej działalności operacyjnej.

[87] Dotyczy w szczególności przepisów prawa w zakresie ochrony informacji pomiarowej.

[88] ENISA (Agencja ds. Cyberbezpieczeństwa): *Wytyczne dotyczące oceny zgodności dostawców usług cyfrowych oraz operatorów usług kluczowych z wymogami bezpieczeństwa stawianymi przez dyrektywę NIS*, listopad 2018

UKSC wprowadza natomiast wymagania kompetencyjne względem audytorów. I tak, zgodnie z art. 15 ust. 2 UKSC, audyt może być realizowany przez:

- jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku[89], w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych[90];
- co najmniej dwóch audytorów posiadających certyfikaty określone w przepisach wydanych na podstawie art. 15 ust. 8 UKSC i rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. *w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu*[91], lub co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;
- sektorowy zespół cyberbezpieczeństwa, ustanowiony w ramach sektora lub podsektora.

Ważnym elementem określonym ustawowo, będącym również standardem w działalności audytowej, jest obowiązek dotyczący postępowania z informacjami „wrażliwymi", gdzie audytor jest obowiązany do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych. Ma to szczególne znaczenie w sektorze energii, gdzie jako operatorzy usług kluczowych mogą być identyfikowane podmioty z krytycznymi systemami informacyjnymi. Tworzy to podwyższone wymagania ochrony informacji audytowej przed dostępem, modyfikacją i usunięciem.

Rekomenduje się, aby operatorzy usług kluczowych, będący operatorami systemów przesyłowych, dystrybucyjnych, Jednostki Wytwórcze Centralnie Dysponowane z podsektora energii elektrycznej, a także operatorzy systemów przesyłowych, dystrybucyjnych i obejmujące inne elementu procesu technologicznego w sektorach gazu, ropy i paliw, a także niektóre duże zakłady przemysłowe przeprowadzali audyt bezpieczeństwa systemów informacyjnych zgodnie z wymaganiami UKSC:

1) *przez wewnętrzne struktury podmiotu,*
2) *podmiot uznany za operatora usługi kluczowej z grupy kapitałowej,*
3) *zewnętrzny podmiot (tzw. audyt stron trzeciej), określony w art. 15 ust. 2 UKSC, pod warunkiem bycia akredytowaną jednostką oceniającą zgodność bądź dysponujący audytorami legitymującymi się doświadczeniem i certyfikatami uprawniającymi do przeprowadzenia audytu w obszarze automatyki systemów przemysłowej,.*
4) *kwalifikacje audytora określone w programie audytów w ramach organizacji.*

Rekomenduje się, aby operatorzy usług kluczowych wprowadzili wymóg niezależności w opisie przedmiotu zamówienia, w przypadkach realizacji audytu przez podmiot zewnętrzny.

[89] Dz. U. z 2019 r. poz. 544 oraz z 2020 r. poz. 1086.
[90] Tak sformułowany przepis dotyczy tylko systemów informatycznych (IT).
[91] Dz. U. z 2018 r. poz. 1999.

Proces audytowania

Integralną częścią programów audytów są wytyczne przygotowania i prowadzenia audytów. Na etapie planowania gromadzone są informacje potrzebne do przeprowadzenia wstępnej oceny bezpieczeństwa (między innymi lista ocenianych aktywów, główne zagrożenia dotyczące aktywów, zabezpieczenia stosowane w celu ograniczenia tych zagrożeń itp.). W sektorze energetycznym wstępna ocena bezpieczeństwa winna uwzględniać przeprowadzoną wcześniej analizę wpływu i analizę źródeł ryzyka w oparciu o metodyki HAZOP lub FMEA.

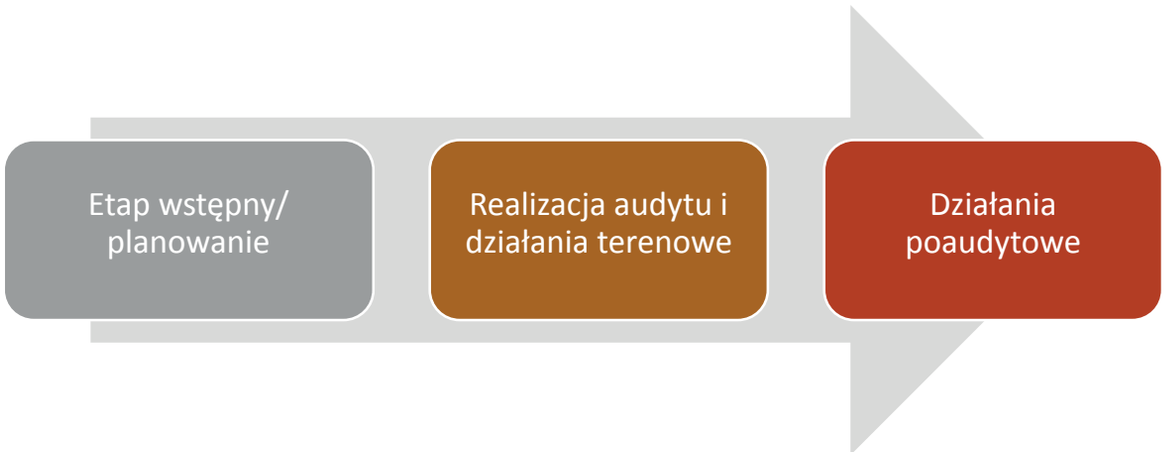
Metodyka HAZOP (ang. *Hazard and Operability Study*) stanowi analizę zagrożeń i zdolności operacyjnych w obszarze przemysłowych systemów sterowania i jest wykonywana w oparciu o normę PN-IEC 61882:2016-07 – *Badania zagrożeń i zdolności do działania (badania HAZOP) – Przewodnik zastosowań*. HAZOP sprawdza jak duży jest wpływ błędnie działającego elementu układu obiektowego na kolejny element obiektowy. Przykładem może być niewłaściwa informacja, która płynie z PLC. Badanie rozpoczyna się od podziału całego systemu na węzły. Dla poszczególnych węzłów zostają określone parametry, takie jak np. przepływ, temperatura, ciśnienie itp. Zestawienie tych parametrów wraz ze słowami kluczowymi pozwoli na zbadanie odchyleń parametrów od normy. Dla każdego odchylenia identyfikuje się przyczyny, dokonuje oceny prawdopodobieństwa wystąpienia odchylenia i określa zagrożenia przez nie spowodowane. Ocenia się także, czy stosowane zabezpieczenia sprzętowe i proceduralne są wystarczające wobec skutków niepożądanych zdarzeń. Z metodyki HAZOP powinny wypływać dyrektywy generalne – opis globalnych zasad w przedsiębiorstwie, np. gdzie można wprowadzić nadzór automatyczny itd. HAZOP pozwala stwierdzić kiedy, pomimo wykrycia anomalii, trzeba reagować. Istotność tych odchyleń bada natomiast metodyka FMEA (ang. *Failure Mode and Effects Analysis*) – analiza rodzajów i skutków możliwych błędów. Metoda ta ma na celu zapobieganie skutkom wad, które mogą wystąpić w fazie projektowania oraz w fazie wytwarzania.

Opracowana, na podstawie powyższej analizy wpływu, wstępna ocena bezpieczeństwa powinna składać się z planu zarządzania projektem audytu, określenia konkretnych celów i zadań, zakresu, wymagań, ról i obowiązków członków zespołu, ograniczeń, założeń, wyzwań, ram czasowych i rezultatów. Należy również ustalić charakter i skalę audytu, organizację przydzielonych zasobów, a także ustalić zrozumiały plan audytu, biorąc pod uwagę cele i ograniczenia wynikające chociażby z operacyjnych zadań podmiotu.

Zaleca się, aby operator usługi kluczowej:

1) *Opracował, w oparciu o ocenę ryzyka (patrz rozdział 4.3 i 4.4), listę usług kluczowych i systemów informacyjnych podlegających audytowi, uwzględniając realizowane procesy w ramach świadczenia usługi kluczowej, istniejącą architekturę bezpieczeństwa, procedury wprowadzania zmian i utrzymania, a także przeszłe zdarzenia i incydenty.*
2) *Przeprowadził audyt uwzględniający elementy/zależności łańcucha dostaw, a także zmiany konfiguracji systemów informacyjnych – dotyczy tylko organizacji o najwyższym poziomie dojrzałości, ustalony w oparciu o tabelę w pkt 14.*

Rysunek 7 – Fazy audytu.



Na *etapie realizacji audytu* będącej główną fazą audytu, wdrażana jest założona metodyka audytu (patrz rozdział 8.2) oraz przyjęta technika oceny. Podmiot przeprowadzający audyt ocenia dostępne dane, w tym ekstrakcję ze strumieni, logi komponentów OT, dane z zainstalowanych agentów, dane z systemów opomiarowania, dane systemowe i technologiczne z układów diagnostyki, dane z zewnętrznych i wewnętrznych systemów bezpieczeństwa z systemów informacyjnych organizacji oraz określa jakość świadczenia usługi kluczowej (tzn. czy istnieją przesłanki świadczące o tym, że wdrożone mechanizmy działają skutecznie zgodnie z określonym poziomem wymagań bezpieczeństwa). Źródła wybieranych do audytu informacji, zależne od zakresu i specyfiki audytu powinny obejmować:

- rekordy zdarzeń z systemów informacyjnych, w tym dane dotyczące daty i godziny zdarzenia, komponentu systemu informacyjnego, w którym doszło do zdarzenia, rodzaju i wyniku zdarzenia, właściciela zasobu[92],
- dokumentację, w tym polityki, plany, procedury, normy, instrukcje, licencje, pozwolenia, specyfikacje, zamówienia, umowy,
- zapisy, w tym protokoły, raporty własne, wyniki pomiarów,
- analizy, wskaźniki skuteczności i wnioski,
- badania i raporty pochodzące z innych źródeł,
- strony internetowe,
- plany i procedury pobierania i nadzorowania procesów pobierania próbek i pomiarów,
- wywiady z pracownikami,
- obserwacje środowiska pracy[93].

Rekomenduje się, aby operatorzy usług kluczowych:

1) *określili w polityce bezpieczeństwa informacji bądź w programie audytu zasady i warunki korzystania z informatycznych narzędzi audytowych, a także zapewnili ochronę dostępu do tych narzędzi celem zapobieżenia ewentualnym nadużyciom i ujawnieniu danych audytowych,*
2) *stosowali rozwiązania potwierdzające niezaprzeczalność zebranych w czasie audytu danych, takie jak podpisy elektroniczne, znaczniki czasu, uwierzytelnienie w systemach.*

[92] Zakres danych musi być wcześniej uzgodniony między podmiotem audytowanym a jednostką audytującą.

[93] Opracowano na podstawie NISTIR 7628: *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements* oraz J. Krawiec, G. Ożarek, *Certyfikacja w informatyce*, Polski Komitet Normalizacyjny, Warszawa 2014.

Po zakończeniu etapu realizacji, w *ramach działań poaudytowych* audytorzy powinni określić słabe punkty systemów informacyjnych, sieci łączności elektronicznej i procesów organizacyjnych. Na tym etapie ma miejsce analiza zidentyfikowanych słabych punktów, identyfikacja podstawowych przyczyn, zalecenia dotyczące środków zaradczych.

Zgodnie z obowiązującymi przepisami UKSC, na podstawie zebranych dokumentów i dowodów, audytor sporządza pisemne sprawozdanie z przeprowadzonego audytu i przekazuje je operatorowi usługi kluczowej wraz z dokumentacją z przeprowadzonego audytu.

Rekomenduje się, aby dokumentacja wyników audytu składała się z:

1) *Raportu z audytu zawierającego specyfikację celu audytu, opis realizacji przedsięwzięcia audytowego, podsumowanie wyników dla kadry kierowniczej (często wyodrębniane jako osobny dokument), specyfikację punktów sprawdzeń wraz z wynikami, zalecenia poaudytowe.*
2) *Wyniki badań technicznych (tzw. dowody audytowe): przeglądy konfiguracji, analiza wyników testów penetracyjnych przeprowadzonych przez organizację bądź inny podmiot na zlecenie organizacji, itp.*

Ponadto w myśl przepisów UKSC, operator usługi kluczowej przekazuje kopię sprawozdania z przeprowadzonego audytu na uzasadniony wniosek organu właściwego do spraw cyberbezpieczeństwa, dyrektora Rządowego Centrum Bezpieczeństwa (w przypadku, gdy operator usługi kluczowej jest jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*) lub Szefa Agencji Bezpieczeństwa Wewnętrznego.

Wynikiem audytu winna być ocena skuteczności zaprojektowanych i wdrożonych zabezpieczeń na poziomie organizacyjnym, proceduralnym, a także technicznym, jak również ocena podjętych działań ograniczających ryzyko dla systemów informacyjnych. Dlatego też w związku z przeprowadzonym audytem należy uzyskać:

- informacje i dowody na zgodność lub niezgodność ze wszystkimi wymogami wynikającymi z obowiązującego prawa bądź norm;
- wyniki monitoringu jakości usługi, pomiary i raporty oraz analiza wyników w odniesieniu do kluczowych wskaźników skuteczności i założonych celów;
- dane nt. systemów zarządzania oraz wyniki w zakresie zgodności z obowiązującym prawem;
- przegląd zaprojektowanych zabezpieczeń i jakości usługi kluczowej z punktu widzenia wszystkich wdrożonych zabezpieczeń organizacyjnych bądź technicznych;
- dane nt. realizacji ładu korporacyjnego wobec usługi kluczowej,
- analizy wszelkich stosownych wymogów prawnych, obowiązków i kompetencji personelu;
- analizy operacji, procedur, danych dotyczących wyników oraz ustaleń i wniosków z audytu wewnętrznego.

Rekomenduje się, aby operator usługi kluczowej określił jednocześnie w ogólnej polityce bezpieczeństwa informacji zasady implementacji na poziomie organizacji zaleceń poaudytowych.

8.2. Metodyki audytu systemów informacyjnych

Przepisy UKSC nie wskazują metodyki przeprowadzenia audytu, obecnie istnieje kilka dostępnych metodyk przeprowadzenia audytu bezpieczeństwa informacji, stworzonych i proponowanych do zastosowania przez organizacje/instytucje zarówno polskie, jak i europejskie tj.: ISO, ISA, Urząd Dozoru Technicznego, ENISA czy ISSA Polska. Kilka przykładowych metodyk przeprowadzenia audytu bezpieczeństwa informacji przez operatora usługi kluczowej to:

– ISO 27001[94],
– ISA/IEC 62443,
– UDT Framework,
– ISSA Polska/IIA Polska,
– ENISA Framework.

ISO 27001

ISO 27001 jest normą bezpieczeństwa informacji. Ramy audytu opisane zostały w normie ISO 27001, stanowiącą jeden z elementów rodziny norm ISO/IEC 27000, wywodzącą się z normy BS 7799 część 2, opublikowaną po raz pierwszy przez British Standards Institute w 1999 roku. Norma ISO/IEC 27001 została zmieniona w 2013 roku, co pozwoliło na dostosowanie jej do innych norm systemów zarządzania ISO. Norma jest publikowana przez Międzynarodową Organizację Normalizacyjną (ISO) i Międzynarodową Komisję Elektrotechniczną (IEC) w ramach wspólnego komitetu ISO i IEC.

Norma ISO/IEC 27001 określa program audytu systemu zarządzania bezpieczeństwem informacji (SZBI) audytowanego podmiotu. Program ten obejmuje wszystkie istotne informacje dotyczące audytów pierwszej strony, audytów przeprowadzanych przez klientów i audytów przeprowadzony przez niezależną stronę trzecią w stosownych przypadkach.

Procedura audytu zewnętrznego jest realizowana za pomocą szeregu list kontrolnych:

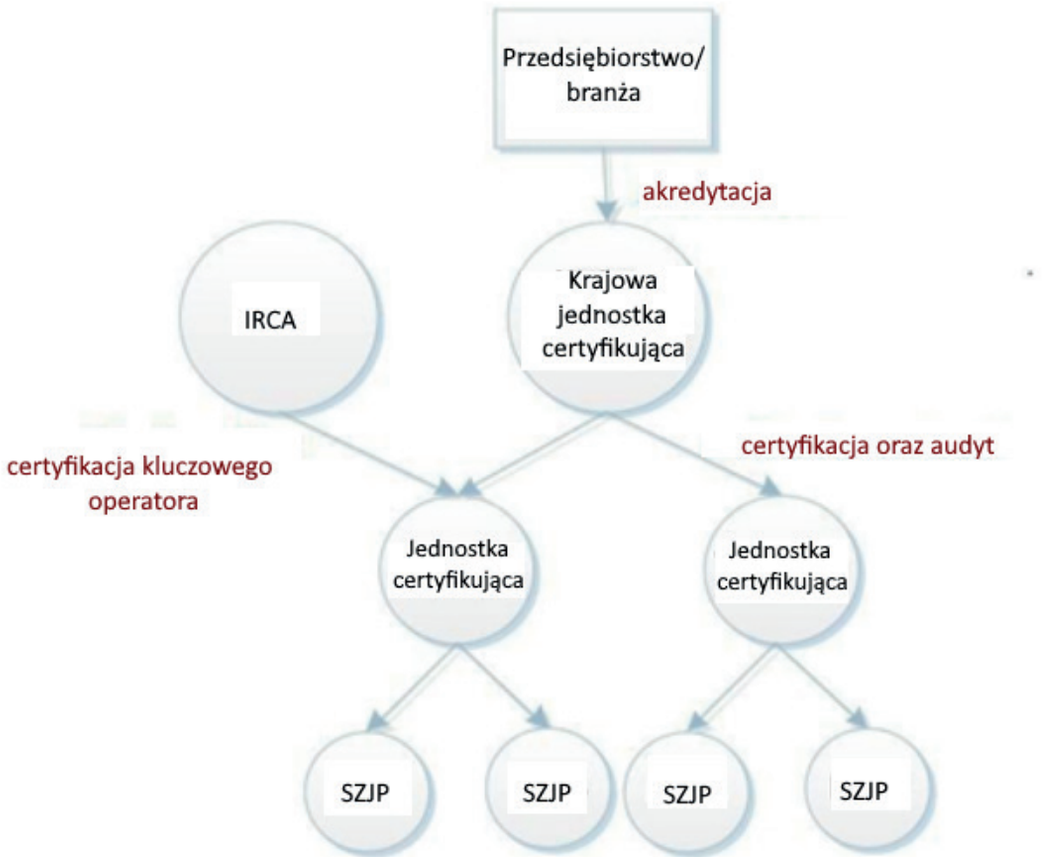
– listy kontrolnej audytu/formularza obserwacji, zawierającego określone pozycje dotyczące jednostki organizacyjnej podlegającej audytowi;
– wymagań systemowych, obejmujących pozycje odnoszące się do wymagań normy ISO/IEC 27001:2013 i każdorazowo dostosowanych do specyfiki audytowanego podmiotu;
– wymagań dotyczących zabezpieczeń: obejmuje zabezpieczenia przedstawione w Załączniku A do normy ISO/IEC 27001:2013, opisane w normie ISO/IEC 27002:2013.42

Należy wspomnieć, że norma ISO 27001 oferuje audytorom pewien stopień swobody w celu zapewnienia skutecznego i efektywnego wdrożenia SZBI zgodnie ze szczególnymi wymaganiami dotyczącymi bezpieczeństwa informacji w danej organizacji.

Poniżej przedstawiony został schemat ram audytu ISO 27001.

[94] https://www.iso.org/standard/54534.html

Rysunek 8 – Schemat ram audytu ISO 27001.



ISA/IEC 62443

ISA/IEC 6244346 to seria norm, sprawozdań technicznych i związanych z nimi informacji, które wyznaczają procesy stosowania środków bezpieczeństwa w strefach przemysłowych i stanowi jedną z najbardziej kompleksowych norm bezpieczeństwa systemów automatyki przemysłowej i sterowania. Wytyczne tej normy odnoszą się do użytkowników końcowych (tj. osób odpowiedzialnych za aktywa), integratorów systemów, praktyków bezpieczeństwa i producentów systemów kontroli odpowiedzialnych za produkcję, projektowanie, wdrażanie lub zarządzanie systemami automatyki przemysłowej i sterowania.

W serii norm ISA/IEC 62443 zaproponowano i wprowadzono nowatorskie koncepcje „stref" (*zones*) i „przewodów" (*conduits*), które stanowią sposób na rozdzielenie różnych podsystemów w ramach systemu kontroli. Strefy stanowią połączenie aktywów fizycznych lub logicznych, które charakteryzują wspólne wymogi bezpieczeństwa związane z czynnikami takimi jak konsekwencje i kluczowy charakter. Dodatkowe środki bezpieczeństwa, takie jak wdrożenie dodatkowych technologii lub zasad, są wymagane, jeżeli stwierdzony poziom bezpieczeństwa sprzętu nie jest równy lub wyższy od poziomu wymaganego.

Normy ISA/IEC 62443 stanowią również ramy dla przemysłu w celu osiągnięcia i utrzymania poprawy bezpieczeństwa w całym cyklu życia, który obejmuje projektowanie, wdrażanie, monitorowanie i ciągłe doskonalenie. Ramy te oferują rozwiązania w zakresie bezpieczeństwa przemysłowego oraz możliwość łagodzenia zagrożeń dotyczących bezpieczeństwa informacji pojawiających się w ramach posegmentowanej sieci kontroli dla stref i przewodów przez interesariuszy.

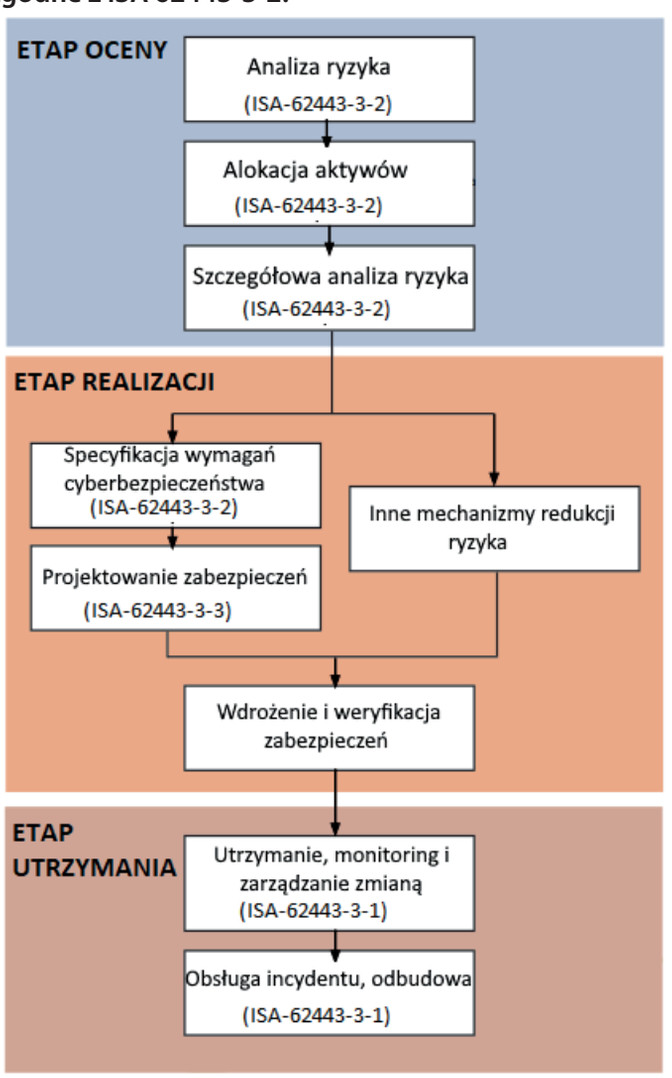
Obecnie nie istnieje ocena ryzyka/zarządzania ryzykiem lub certyfikacja bezpieczeństwa informacji oparta na normach ISA/IEC 62443. Trwają prace nad powiązanymi procesami audytu i oceny, których celem jest umożliwienie organizacjom oceny stanu bezpieczeństwa informacji w odniesieniu do rodziny norm ISA/IEC 62443. Obecnie i do czasu opublikowania własnościowego standardu audytu ISA 62443, organizacja ISA proponuje standardy atestacyjne dla stron trzecich: Są to:

a) w odniesieniu do atestów produktów:
   i. ISO/ IEC 15408;
   ii. ISO/ IEC 19790 (podobny do NIST FIPS 140-2);
   iii. ISO/ IEC TR/19791.

b) w odniesieniu do atestów procesu:
   i. ISO/ IEC 21827;
   ii. ISO/ IEC 17799;
   iii. COBIT5;
   iv. Projekt normy ISA S99, obejmujący koncepcje i wytyczne dotyczące procesów.

a) w odniesieniu do ochrony środowiska:
   i. Seria norm ISO 9000.

Rysunek 9 – Etapy audytu zgodne z ISA 62443-3-2.



Framework UDT

Poniższy wykres ilustruje proponowany przez Urząd Dozoru Technicznego (Framework UDT) zakres audytu bezpieczeństwa informacji.

Rysunek 10 – Zakres audytu bezpieczeństwa informacji proponowany przez UDT.

Metodyka Urzędu Dozoru Technicznego oparta została na 7 głównych modułach, istotnych z punktu widzenia bezpieczeństwa informacji u operatora usługi kluczowej. Każdy z modułów obejmuje przypisane obszary poddawane ocenie przez audytora. Moduł „organizacja" obejmuje obszary związane ze strukturą organizacyjną, zasobami ludzkimi i zarządzanie nimi, strategią bezpieczeństwa informacji czy systemami zarządzania. Moduł „ochrona" to przede wszystkim kwestie bezpieczeństwa informacji, ochrona aktywów, zarządzanie dostępem (w tym dostępem strony trzeciej), szacowanie ryzyka, czy samej eksploatacji zasobów fizycznych. Moduł „kontrola" stanowią sprawy związane z monitorowaniem sieci, wykrywaniem i raportowaniem podatności, podejmowaniem działań operacyjnych i prewencyjnych, zapewnieniem odpowiedniego poziomu bezpieczeństwa. Moduł „reagowanie" obejmuje kwestie wykrywania incydentów, zarządzanie incydentami i zagrożeniami, monitorowanie zachowań użytkowników, analizę skutków zdarzeń czy komunikacji o zdarzeniach. Część „Przywracanie do działania" obejmuje obszary systemów zarządzania ciągłością działania, reagowanie po wystąpieniu zagrożenia, postępowanie z ryzykiem, raportowanie i ocenę planów w procesie ciągłości działania, a także doskonalenie procesu odtwarzania. Do zakresu modułu „doskonalenie" należy monitorowanie wdrożonych systemów, przegląd zarządzania, audyty wewnętrzne i zewnętrzne, kontrole i nadzór, przyjęcie właściwego modelu oceny dojrzałości organizacji. Ostatni moduł skierowany jest na obszary bezpośrednio dotyczące wymagań nałożonych na OUK przepisami UKSC, w tym obszary struktury organizacyjnej OUK, zarządzania i szacowania ryzyka, działań związanych z minimalizacją ryzyka, obsługą incydentów, audytu bezpieczeństwa czy podnoszeniem stopnia świadomości o zagrożeniach przez użytkowników systemu.

Urząd Dozoru Technicznego przeprowadza audyty cyberbezpieczeństwa jako audytor zewnętrzny (audyt trzeciej strony) według ustalonych kryteriów i obszarów zdefiniowanych w ramach Framework UDT*Cyber* i jest jednostką akredytowaną w ramach normy PN-EN ISO/IEC 27001.

ISSA Polska/IIA Polska

Podobny zakres audytu bezpieczeństwa informacji przygotowany został przez ISSA Polska w ramach dokumentu *Szablon Raportu Audytu KSC*[95]. Szablon został stworzony jako propozycja sprawozdawcza z raportów audytowych wyczerpująca podstawowe założenia UKSC na potrzeby ujednoliconego wykonywania sprawdzenia poprawności implementacji systemu zapewnienia cyberbezpieczeństwa i realizacji obowiązków sprawozdawczych względem organu właściwego. Poniższy schemat przedstawia proponowany w Szablonie model kluczowych 10 obszarów, które powinny zostać ujęte w audycie bezpieczeństwa informacji u operatora usługi kluczowej.

Rysunek 11 – Model kluczowych obszarów audytu bezpieczeństwa informacji zaproponowanych w „Szablonie Raportu Audytu KSC".

Dokument został przygotowany, pod nadzorem organów rządowych, przez ISSA Polska (Stowarzyszenie do spraw Bezpieczeństwa Systemów Informacyjnych) oraz IIA Polska (Instytut Audytorów Wewnętrznych). Opracowano szablony sprawozdań zgodne z ustawą KSC. Istnieją dwie wersje szablonu sprawozdania z audytu. Pierwszy dedykowany jest operatorom, którzy świadczą tylko jedną usługę kluczową, natomiast drugi adresowany jest do operatorów, którzy świadczą dwie lub więcej usług kluczowych. Szablony zostały przygotowane na potrzeby ujednoliconego wykonywania sprawdze-

[95] https://issapolska.github.io/Audyt_KSC/

nia poprawności implementacji systemu ochrony przestrzeni cyfrowej u OUK przez ministra właściwego dla danego sektora oraz właściwy CSIRT w czasie incydentu. Wzory szablonów zostały udostępnione na rządowej witrynie internetowej pod adresem: *https://www.gov.pl/web/baza-wiedzy/szablony-audytu-dla-operatorow-uslug-kluczowych*

ENISA Framework

Rysunek 12 – Zakres audytu bezpieczeństwa informacji zaproponowany w ramach ENISA Framework.

W Wytycznych ENISA wymienia się 4 kluczowe obszary, które powinny zostać ujęte w audycie bezpieczeństwa informacji OUK. Szczegółowy opis każdego z obszarów i elementów koniecznych do uwzględnienia podczas audytu BI znajduje się w załączniku nr 3.

Powyżej przedstawiony został schemat kluczowych obszarów, proponowanych przez ENISA do uwzględnienia w zakresie audytu.

W swych *Wytycznych* ENISA przedstawiła wytyczne dla organów właściwych do spraw cyberbezpieczeństwa dotyczące prowadzenia audytu bezpieczeństwa informacji w OUK. Na stronie internetowej Agencji Unii Europejskiej ds. Cyberbezpieczeństwa zostało udostępnione narzędzie, które w prosty sposób wskazuje zalecane normy i standardy w związku z realizowaniem wymagań bezpieczeństwa wynikających z dyrektywy NIS, w tym wymagań dotyczących przeprowadzania audytów bezpieczeństwa systemów informacyjnych. Narzędzie jest dostępne pod adresem https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services. Narzędzie zawiera listę pytań podzielonych na kategorie według środków bezpieczeństwa, a każdemu pytaniu towarzyszą orientacyjne informacje i dane, które umożliwią organowi przeprowadzającemu audyt (zgodnie z art. 14 UKSC) ocenę, czy każde zabezpieczenie zostało wdrożone zgodnie z jego założeniami. W Załączniku do niniejszego dokumentu przedstawiono wykaz obszarów i pytań, stosowanych w narzędziu proponowanym przez ENISA.

Załącznik nr 3 – szablon audytu opracowany przez ENISA.

Dowody kontroli:

– regulamin bądź procedury audytu bezpieczeństwa formalnie udokumentowane i regularnie utrzymywane.

9. Zachowanie ciągłości działania i odbudowa

Zarządzanie ciągłością działania przedsiębiorstwa jest czynnością, której celem jest m.in. zapewnienie działania danego podmiotu poprzez ochronę krytycznych procesów przed skutkami incydentów w obszarze procesu technologicznego, jak i ochrony aktywów informacyjnych niezbędnych do realizacji tych procesów. Samą ciągłość działania można zdefiniować jako zdolność przedsiębiorstwa do przewidywania i reagowania na zakłócenia procesu biznesowego w celu utrzymania prowadzonej działalności na akceptowalnym, ustalonym poziomie. Zarządzanie ciągłością działania powinno być priorytetem każdego przedsiębiorstwa. W związku z tym zaleca się, aby organizacja opracowała metodyki zachowania ciągłości działania, z uwzględnieniem aspektów, które zgodnie ze specyfiką organizacyjną danego przedsiębiorstwa mogą mieć wpływ na tą ciągłość, rozumianą jako podtrzymanie kluczowych procesów pozwalających na świadczenie usługi kluczowej. Ze względu na duże zróżnicowanie organizacyjne przedsiębiorstw funkcjonujących w sektorze energii, organizacja powinna sama określić, które udokumentowane informacje powinny być uwzględnione w tworzonych mechanizmach zachowania ciągłości działania dla efektywności tych mechanizmów. Opracowane metodyki ciągłości działania powinny co najmniej identyfikować m.in. kluczowe usługi realizowane przez przedsiębiorstwo zależne od systemów informacyjnych, a także produkty rozumiane jako świadczenie usługi kluczowej oraz inne powiązane działania związane z usługą kluczową. Zaleca się, aby plan ciągłości działania był opracowany dla każdego rodzaju zagrożenia, które zgodnie z analizą ryzyka może wystąpić. Zaleca się, aby uwzględnić również zagrożenia związane z działalnością człowieka[96].

9.1. Ciągłość świadczenia usług kluczowych

Ciągłość działania usługi kluczowej należy traktować jako priorytet, a opracowane procedury powinny przyczynić się do ograniczonego ryzyka wystąpienia incydentu, zapewnić minimalny poziom zdolności operacyjnej, a także zminimalizować czas odtworzenia po katastrofie[97]. Podstawowym aspektem w procesie zarządzania ciągłością działania w sektorze energii i ogólnie sektorach przemysłowych jest zapewnienie bezpieczeństwa systemów sterowania przemysłowego i ich komponentów w znaczeniu *„safety"* i *„security"*. Bezpieczeństwo w znaczeniu *„safety"* oznacza, że są one bezpieczne dla otoczenia (ludzi, mienia, środowiska i samego procesu), tzn. działają prawidłowo, nie ulegają awarii, są niezawodne. Natomiast bezpieczeństwo systemów automatyki i ich komponentów w znaczeniu *„security"* oznacza ochronę przed zagrożeniami płynącymi z zewnątrz, ze strony otaczającego środowiska, w któ-

[96] *Ibidem.*
[97] *Ibidem,* s. 94.

rym system pracuje i/lub z którym ma powiązania[98]. W rezultacie, szacowanie ryzyka w kontekście zarządzania ciągłością działania powinno dotyczyć szerokiego wachlarza procesów biznesowych, stosowanych zabezpieczeń, a także kompatybilności technologicznej oprogramowania, komponentów układów automatyki, infrastruktury komunikacyjnej i systemów sterowania. Zdarzenia, które mogą spowodować przerwanie ciągłości działania, jak np. incydenty teleinformatyczne oraz awarie sprzętu i oprogramowania, akty terroryzmu i cyberatak, katastrofy naturalne, zamierzona lub nieświadoma działalność ludzka, powinny być wzięte pod uwagę podczas szacowania ryzyka oraz opracowania dokumentacji związanej z zachowaniem ciągłości działania. Wyniki takiej analizy ryzyka powinny być podstawą do opracowania strategii ciągłości działania oraz planu wdrożenia tej strategii.

Powinno się stworzyć plan ciągłości działania obejmujący m.in. opracowane procedury ciągłości działania wraz ze zdefiniowanym zakresem odpowiedzialności, uzgodnieniem akceptowalnego poziomu strat, warunkami jakie muszą wystąpić do zainicjowania planów (z podziałem na konkretne procesy), opracowanymi procedurami odtworzenia procesów kluczowych, uzgodnionym procesem szkolenia personelu w zakresie procedur kryzysowych, testowaniem planów ciągłości działania wraz z harmonogramem [99].

Opracowany plan ciągłości działania powinien posiadać swojego właściciela oraz przypisane odpowiedzialne osoby za każdy z elementów tego planu. Dokumenty – kopie opracowanych planów ciągłości działania powinny być przechowywane w bezpieczny sposób. Optymalnym rozwiązaniem jest przechowywanie kopii poza siedzibą przedsiębiorstwa, jednakże w takiej lokalizacji, która posiada takie same zabezpieczenia pomieszczenia przechowywania kopii planu, jak miejsce w którym przechowywany jest oryginał. Kopie planów ciągłości działania należy traktować jednakowo jak oryginał dokumentu. W planach ciągłości działania oraz odbudowy należy wziąć pod uwagę aspekt strony trzeciej. Właściwe zarządzanie stronami trzecimi oraz kontrola ich wpływu na firmę jest niezbędne w celu zachowania jej ciągłości działania.

Organizacja powinna zidentyfikować krytyczne systemy informacyjne służące do świadczenia usług kluczowych, a także systemy informacyjne o charakterze wspomagającym, w których ewentualne zdarzenie może wpłynąć na te krytyczne. Ponadto, zaleca się, aby identyfikacja wskazywała również na dane przekazywane w konkretnym systemie. Należy także zidentyfikować krytyczne procesy technologiczne oraz biznesowe, a także określić ich wpływ na ciągłość działania przedsiębiorstwa. Ponadto zaleca się dokonanie priorytetyzacji realizowanych usług, z uwzględnieniem usługi kluczowej jako tej krytycznej. Dodatkowo, powinno się określić parametry istotne dla ciągłości działania danego przedsiębiorstwa, takie jak: Cel Czasu Odbudowy (ang. recovery time objective – RTO), Cel Punktu Odbudowy (ang. recovery point objective – RPO), maksymalny akceptowalny czas braku dostaw (ang. maximum tolerable outage – MTO) and Minimalny Cel Ciągłości Działania (ang. minimum business continuity objective – MBCO)[100] (patrz rozdział 9.3).

[98] *Poradnik dobrych praktyk w zakresie cyberbezpieczeństwa urządzeń podlegających dozorowi technicznemu*, Zespół ds. cyberbezpieczeństwa Urząd Dozoru Technicznego, 2021 r

[99] *Ibidem*.

[100] ENISA, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, s. 63.

Przykładowy (uproszczony model) procesu identyfikacji.

L.p.	System informacyjny	Usługa kluczowa/ usługa wspomagająca	Krytyczność usługi realizowanej przez system	Osoba odpowiedzialna na system/usługę	Kontakt do osoby odpowiedzialnej
1					
2					
3					

Identyfikacja kluczowych elementów mających wpływ na ciągłość działania przełoży się na sprawniejsze projektowanie procesów i procedur. Dokumentacja tego typu powinna być regularnie weryfikowana i aktualizowana. Dla każdego ze zidentyfikowanych systemów krytycznych powinno opracować się ocenę potencjalnych skutków wystąpienia zdarzenia cyberbezpieczeństwa lub awarii oraz procedury lub mechanizmy przywrócenia poprawnego działania procesów, których efektem jest świadczenie usługi kluczowej. W razie możliwości zaleca się zaznaczenie ram czasowych, w jakich będą wykonywane konkretne czynności zmierzające do przywrócenia prawidłowej funkcjonalności systemu. Krytyczność usługi kluczowej w krajowym systemie cyberbezpieczeństwa oraz jej znaczny wpływ na niezakłócone funkcjonowanie państwa, społeczeństwa, gospodarki lub samej organizacji, powoduje, *iż* należy jej zapewnić priorytet w ramach podejmowanych działań.

Zaleca się stworzenie oraz rozwijanie procedur mających na celu wykrywanie i monitorowanie ewentualnych zdarzeń cyberbezpieczeństwa, a także procedur pozwalających na usystematyzowanie innych działań, związanych z reakcją na zdarzenie, np. usystematyzowanie procesu komunikacji wewnętrznej, scenariuszy awaryjnych. W oparciu o przeprowadzony audyt bezpieczeństwa systemu informacyjnego organizacja powinna rozważyć niezbędne modernizacje sprzętowe, oprogramowania lub dokonanie zakupu nowych rozwiązań wspomagających zachowanie ciągłości działania.

W celu wsparcia działań o charakterze prewencyjnym, może być konieczne zainwestowanie w dedykowane rozwiązania wspomagające takie procesy. W przypadku stwierdzenia konieczności zaopatrzenia się w rozwiązania narzędziowe do wczesnego ostrzegania o zagrożeniach, np. narzędzia typu IPS/IDS (ang. *Intrusion Detection System/Intrusion Prevention System*[101]) lub jakiekolwiek inne narzędzia, które zostaną uznane za pomocne, kierownictwo organizacji powinno uwzględnić przedstawione potrzeby, jednocześnie traktując cyberbezpieczeństwo oraz wzmocnienie procesów ciągłości działania jako inwestycję.

Powinno się dokonać oszacowania czasu na jaki system informacyjny służący do świadczenia usługi kluczowej może być niedostępny, tak, aby ta niedostępność nie niosła za sobą istotnych konsekwencji (z ewentualnym uwzględnieniem konkretnych funkcji danego systemu).

Wskazane oszacowanie może być pomocne w procesie ustalania czasów reakcji na zagrożenie związane z danym systemem. Może także pomóc w ustaleniu ewentualnych negatywnych konsekwencji związanych z niedostępnością systemu i przerwaniem świadczenia usługi kluczowej. Zebrane informacje mogą być pomocne przy kwalifikacji incydentu do rangi incydentu poważnego zgodnie z Rozporządzeniem Rady Ministrów z dnia 31 października 2018 r. *w sprawie progów uznania incydentu za poważny* (Dz. U. 2018 poz. 2180).

[101] Więcej w pkt. 13.1–13.3

Organizacja powinna zadbać o mechanizmy podnoszenia świadomości pracowników o funkcjonujących mechanizmach ciągłości działania, zagrożeniach, ewentualnych zadaniach pracowników podczas incydentu, a także, wkładu pracowników w efektywne zapewnienie ciągłości działania.

W celu podniesienia efektywności procedur pracownicy odpowiedzialni za ich realizację, ale także pracownicy bezpośrednio niezaangażowani w działanie powinni mieć możliwość zapoznania się z procedurami, które ze względu na rodzaj wykonywanych przez nich obowiązków mogą ich dotyczyć.

Kierownictwo organizacji powinno wyznaczyć osoby odpowiedzialne za zidentyfikowane procesy kluczowe, a także osoby odpowiedzialne za realizowanie zadań mających na celu zapewnienie ciągłości działania. Ponadto, kierownictwo swoim działaniem powinno dążyć do usprawnienia procesu zarządzania ciągłością działania.

Czynne zaangażowanie kierownictwa w proces tworzenia, utrzymywania oraz rozwijania planów ciągłości działania wskaże na istotne znaczenie tego procesu, jednocześnie zwiększając priorytet tego typu działań oraz wskazując ich kluczowe znaczenie pracownikom zaangażowanym. Ponadto, kierownictwo powinno rozdzielić odpowiedzialność. Dla efektywnej realizacji procedur i procesów ciągłości działania, kierownictwo, w tym najwyższe kierownictwo, organizacji powinno podejmować wszelkie działania wzmacniające efekt zaimplementowanych rozwiązań. Zaleca się podejmowanie działań nie tylko zarządczych i decyzyjnych, ale także inwestycyjnych.

Zaleca się wcześniejsze przygotowanie wymagań dla komunikacji i wymiany informacji związanej z ciągłością działania, wskazujących na najważniejsze aspekty związane m.in. ze stronami komunikacji.

Wcześniejsze zdefiniowanie metod oraz stron komunikacji w procesie zachowania ciągłości działania może usprawnić realizowanie procesów w trakcie zdarzenia. Rozwinięcie tematu znajduje się w rozdziale 9.2.

Przygotowane procedury i mechanizmy ciągłości działania (np. plany ciągłości działania), w celu bieżącego utrzymania ich aktualności i przydatności, powinny być cyklicznie testowane i weryfikowane, a także ulepszane.

W celu maksymalizacji efektywności opracowanych procedur, należy je regularnie weryfikować i testować za pomocą ćwiczeń w kontrolowanych warunkach. Plany ciągłości działania powinny być aktualizowane i testowane zgodnie ze zdefiniowanym harmonogramem. Organizacja powinna w miarę możliwości przeprowadzać symulację przerw w działalności oraz omawiać warianty jej przywracania, a także sprawdzać sposób postępowania personelu zaangażowanego w realizację zadań związanych z ciągłością działania. Należy także weryfikować kwalifikacje personelu pod kątem odpowiednich kompetencji i umiejętności do działania po wystąpieniu incydentu. Należy także sprawdzać m.in. skuteczność przywrócenia systemów informacyjnych do stanu przed awarii. Wyniki testów powinny być uwzględniane w procesie doskonalenia opracowanych procedur. Ponadto organizacja powinna rejestrować i dokumentować przeprowadzane przeglądy procedur.

Zaleca się również wdrożenie mechanizmów, które mogą pozwolić na sprostanie wyzwaniom związanym z koniecznością zapewnienia ciągłości działania w dobie pandemii . Mając na uwadze to, iż obecnie trwające zagrożenie epidemiologiczne związane z pandemią koronawirusa SARS-CoV-2 niejednokrotnie determinowało działania OUK, których celem było zachowanie ciągłości działania, w wielu przypadkach zostały wypracowane procedury właściwe dla tego rodzaju zagrożenia. W celu

podjęcia działań prewencyjnych oraz systemowego wdrożenia pewnych rozwiązań na wypadek wystąpienia podobnych zagrożeń epidemiologicznych w przyszłości, zaleca się podjęcie wskazanych poniżej czynności. Jeżeli organizacja ma już wdrożony system zarządzania ciągłości działania, zaleca się uwzględnienie niektórych rozwiązać we właściwych mechanizmach lub procedurach.

Rekomenduje się opracowanie procedur postępowania w sytuacjach awaryjnych związanych z zagrożeniem epidemiologicznym zawierających co najmniej:

1) Plany działania na wypadek nagłej utraty możliwości operacyjnych spowodowanych niedostępnością dużej liczby pracowników w jednym czasie,
2) Ustalenie sposobów komunikacji pomiędzy osobami zaangażowanymi,
3) Opracowanie procedury doszkalania pracowników o zbliżonych kompetencjach i przenoszenia ich w razie potrzeby do realizowania usług o wyższym priorytecie, czego celem powinno być utrzymanie świadczenia usługi kluczowej,
4) Opracowanie mechanizmów pracy w trybie zmianowym, z uwzględnieniem potrzeby zastosowania bezkontaktowej rotacji pracowników,
5) W miarę możliwości zaleca się wypracowanie procedur zastępowania kluczowych pracowników poprzez nawiązanie kontaktu z byłymi pracownikami (będącymi na emeryturze) i stworzenie mechanizmów ich awaryjnego zatrudniania. Tego rodzaju działanie powinno być stosowane w przypadku krytycznej niedostępności kluczowych pracowników,
6) Mechanizmy koszarowania kluczowych pracowników na wypadek wystąpienia poważnego kryzysu epidemiologicznego,
7) Zaopatrzenie się organizacji w środki ochrony osobistej, jak np.: maseczki, środki dezynfekujące, odzież ochronna, inne środki zalecane przez odpowiednie organy państwowe,
8) Opracowanie mechanizmów pracy zdalnej, zakup sprzętu umożliwiającego pracę zdalną i oddelegowanie pracowników, którzy mogą taki rodzaj pracy wykonywać do jej świadczenia w miejscu zamieszkania,
9) Ograniczenie dostępu osobom trzecim do siedziby organizacji, z uwzględnieniem wyjątków, takich jak np. osób z zespołów typu CSIRT.

Dowody kontroli:

– *formalnie udokumentowana strategia ciągłości usług, w tym cele dotyczące czasu przywracania usług kluczowych i towarzyszących procesów,*

– *dokumentacja wykonywania kopii zapasowych w tym: procedury wykonywania, przechowywania i testowania kopii zapasowych oraz dokumentacja wykonywania ww. procedur.*

9.2. Wymagania dla komunikacji i wymiany informacji związanych z ciągłością działania

Jednym z elementów utrzymania ciągłości działania jest wprowadzenie procedur/instrukcji dotyczących zasad komunikacji i wymiany informacji. W związku z tym rekomendowane jest, aby zawrzeć w takich zasadach poniższe zagadnienia komunikacji w zakresie utrzymania ciągłości działania:

1) Jednoznaczne wskazanie etapów działań i ich charakterystycznych cech (w miarę możliwości: zakresów działań, przedziałów czasowych, zdarzeń granicznych, ról głównych i pomocniczych),
2) Określenie jednoznacznego podziału ról i ich zakresów działań (w tym uwzględnienie zastępstw), na każdym zdefiniowanym etapie realizacji działań związanych z utrzymaniem ciągłości działania tak, by sposób i rodzaj komunikacji był jednoznaczny dla uczestników działań,
3) Ustalenie zastępowalności personelu w sytuacjach nieprzewidzianych takich jak brak komunikacji z osobą zastępującą w przypadku braku osoby zastępowanej. Uwzględnienie rezerw personelu ponad standardową zastępowalność,
4) Uwzględnienie sytuacji przerwania komunikacji i wskazanie postępowania w takich przypadkach,
5) Opisanie sposobu komunikacji na poszczególnych etapach realizowania działań oraz zakresu komunikatów,
6) Wprowadzenie obowiązku zapoznania się wszystkich pracowników z procedurami dot. działań w zakresie utrzymania ciągłości, w tym komunikacji wraz z okresowym testowaniem znajomości procedur,
7) Regularne testowanie wszystkich kanałów komunikacji wskazanych do utrzymania ciągłości działania i potwierdzone sprawozdaniami,
8) Stworzenie co najmniej dwóch kanałów komunikacji w sytuacji kryzysowej (podstawowego i zastępczego) oraz rozpisania działań dot. zmiany kanału komunikacji,
9) Wskazanie w procedurach lub instrukcjach wykonawczych listy danych kontaktowych niezbędnych do realizacji działań (dane kontaktowe w zakresie podmiotu, jak i dane kontaktowe służb zewnętrznych tj. straż pożarna, pogotowie) wraz z regularnym aktualizowaniem tej listy.

Wskazane jest, by procedury w zakresie utrzymania ciągłości działań, jeśli to możliwe, były na poziomie poszczególnych czynności, by komunikacja w czasie działań nie była nadmiarowa.

Przykładowa tabela[102] rozpisująca role/osoby biorące udział w procesie zapewnienia ciągłości działania:

[102] Ministerstwo Cyfryzacji, *Poradnik dla przedsiębiorstw: Jak utrzymać ciągłość działania usług/krytycznych i kluczowych systemów teleinformatycznych w stanie zagrożenia epidemicznego?* – bibliografia.

Tabela 1 – Poszczególne role/osoby biorące udział w procesie zapewnienia ciągłości działania.

Lp.	Funkcja/stanowisko	Rola osoby	Przykładowe zadania
1.	Koordynator działań dotyczących utrzymania ciągłości działania	Nadzór nad realizacją zadań związanych z działaniami dotyczących utrzymania ciągłości działania	1. Analiza informacji o zagrożeniu. 2. Weryfikacja źródła. 3. Decyzja o uruchomieniu Planu Ciągłości Działania. 4. Powołanie Sztabu Kryzysowego. 5. Powiadomienie pracowników. 6. Powiadomienie odpowiednich służb. 7. Powiadomienie Zarządu. 8. Wydanie odpowiednich dyspozycji dla personelu.
2.	Kadra kierownicza	Wsparcie obsługi wewnętrznej, kontrola realizacji zadań zgodnie z zaleceniami.	1. Kontrola przestrzegania ustalonych zasad realizacji zadań. 2. Informowanie koordynatora o sytuacjach zagrożenia lub potencjalnie niebezpiecznych. 3. Rekomendacje działań zapobiegawczych mających na celu ograniczenie ryzyka związanych z wystąpieniem zagrożenia. 4. Zgłaszanie zapotrzebowania na sprzęt do odpowiednich zespołów, dodatkowe wyposażenie stanowisk pracy w celu zapewnienia ciągłości pracy w przypadku konieczności pracy zdalnej. 5. Przygotowanie personelu do realizacji zadań w formie pracy zdalnej.
3.	Personel przedsiębiorstwa – rozpisanie tego punktu na poszczególne role/ stanowiska pełnione w procesie realizowania usługi kluczowej	Realizacja zadań związanych z realizacją celu przedsiębiorstwa – dla poszczególnych ról/ stanowisk	Zadania wynikające z obowiązków służbowych pracowników przypisanych do konkretnych ról/ stanowiskach, procedur dot. działań w zakresie ciągłości działania oraz poleceń przełożonych/osób pełniących zdefiniowane role.

Dowody kontroli:

– dokumentacja poszczególnych działań szkoleniowych dotyczących ciągłości funkcjonowania systemu, a także sprawozdania po zakończeniu ćwiczeń.

9.3. Odbudowa, plan odbudowy po katastrofie (DRP)

Organizacja powinna zdefiniować i utrzymywać parametry odbudowy systemów informacyjnych służących do świadczenia usługi kluczowej, zawarte w posiadanym planie odbudowy po katastrofie.

Nieodłączną częścią zdolności organizacji do utrzymania ciągłości jej działania jest opracowanie planu odbudowy po katastrofie (ang. *Disaster Recovery Plan* – DRP). Opracowanie takiego planu jest procesem, w którym formułuje się strategię uszczegóławiającą kluczowe działania wymagane do przywrócenia usług informatycznych w ramach przyjętych celów odbudowy, które mają zostać osiągnięte po przerwaniu działalności biznesowej w wyniku katastrofy[103].

[103] Jako „katastrofę" należy rozumieć niespodziewane lub nagłe zdarzenie o znaczących skutkach dla realizacji procesów biznesowych organizacji (także ich przerwaniu), jak np. awaria, katastrofa naturalna, akt terroryzmu czy błąd ludzki.

Dla świadczonej usługi kluczowej, zależnej od systemów informacyjnych, niezwykle istotne jest objęcie planem odbudowy po katastrofie właśnie tych systemów. Mając powyższe na uwadze, wśród możliwych zagrożeń prowadzących do katastrofy w ich kontekście, należy wymienić między innymi:

a) działalność przestępczą/cyberatak/nadużycie,
b) podsłuchanie/przechwycenie sesji,
c) atak fizyczny,
d) nieumyślne uszkodzenie (wypadek),
e) wadliwe działanie/awarię,
f) przerwę w dostawie (np. energii elektrycznej),
g) zagrożenia od strony prawnej,
h) katastrofy naturalne[104].

W opracowanym planie, organizacja powinna określić parametry odbudowy systemów informacyjnych służących do świadczenia usługi kluczowej, co najmniej takie jak:

a) Cel czasu odbudowy (ang. *recovery time objective* – RTO);
b) Cel punktu odbudowy (ang. *recovery point objective* – RPO);
c) Maksymalny akceptowalny czas przerwania procesów (ang. *maximum tolerable outage* – MTO);
d) Minimalny cel ciągłości działania (ang. *minimum business continuity objective* – MBCO)[105].

Cel czasu odbudowy (RTO) jest parametrem określającym czas, w którym organizacja musi przywrócić działanie systemów informacyjnych po katastrofie. Proces odzyskiwania z nim związany obejmuje kroki, które musi podjąć organizacja, aby przywrócić systemy i dane do stanu sprzed katastrofy. W przypadku systemów i danych o wysokim priorytecie, wskaźnik ten może być wyrażony w sekundach, o ile organizacja zainwestowała w odpowiednie usługi i zabezpieczenia z nimi związane. Określanie RTO wymaga, aby organizacja w pierwszej kolejności przyznawała pierwszeństwo systemom i danym stosownie do ich krytyczności oraz ryzyka biznesowego dla organizacji. W kolejnym kroku przypisuje się tym aktywom odpowiednią ilość potrzebnych zasobów, jak środki finansowe, czas czy wymagana infrastruktura. Przy ustanawianiu parametru RTO, należy określić także ogólne potrzeby organizacji, jak i również czas, jaki będzie ona w stanie przetrwać bez infrastruktury i usług w zakresie systemów informacyjnych. RTO powinny być opracowywane zgodnie z możliwościami organizacji w zakresie przywracania, bowiem wskaźnik ten określony np. na 30 minut nie będzie możliwy do spełnienia, jeżeli rzeczywisty minimalny czas przywracania wynosi na przykład 1 godzinę[106].

RPO – cel punktu odbudowy, to wskaźnik określający czas od awarii, katastrofy lub porównywalnego zdarzenia powodującego straty. Odwołuje się on do momentu, w którym dane były zachowane w postaci nadającej się do użytku, a więc najczęściej będzie to najnowsza kopia zapasowa. Proces odtwarzania zazwyczaj zachowuje wszelkie zmiany danych zastosowane przed awarią lub katastrofą. Jeżeli kopie zapasowe danych w organizacji są tworzone w sposób automatyczny, wówczas odpowiednie odstępy czasowe między nimi mogą być wystarczające do osiągnięcia celów RPO[107].

[104] ENISA, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, 2018, s. 80.
[105] *Ibidem*.
[106] NIST, *SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems*, 2010, s. 17.
[107] *Ibidem*.

Maksymalny czas przerwania procesów (MTO, czasem także jako MTD) definiuje całkowity czas, przez jaki organizacja jest gotowa zaakceptować przerwę lub zakłócenie realizowanych procesów biznesowych i zawiera wszelkie możliwe skutki z tym związane. Określenie tego parametru jest ważne, gdyż determinuje on działania związane z wyborem odpowiedniej metody i obszaru odtwarzania wymaganych przy opracowywaniu treści oraz zakresu tych procedur[108].

Parametr MBCO – minimalny cel ciągłości działania, to minimalny poziom usług, który jest możliwy do zaakceptowania przez organizację, by osiągać jej cele biznesowe w trakcie zakłóceń[109]. W ustanowieniu MBCO może być pomocny opracowany wskaźnik RPO. Poziom tego parametru może być zmienny w zależności od charakteru usługi/działalności organizacji. Wskaźnik ten powinien być osiągnięty w określonym czasie po wystąpieniu zakłócenia. Może być konieczne opracowanie kilku MBCO dla różnych okresów po incydencie, jak i dla każdej usługi/działalności ujętej w zakresie planu ciągłości działania.

Prócz powyższych podstawowych wskaźników, organizacja może ująć w swoim planie odbudowy dodatkowe wskaźniki według własnego uznania, mając jednak na uwadze, iż parametry te powinny być realne do osiągnięcia oraz utrzymywane. Takimi dodatkowymi wskaźnikami mogą być m.in. MDL (ang. *maximum data lost*), określający maksymalną utratę danych z uwzględnieniem dodatkowych możliwości odtwarzania, czy NRO (ang. *network recovery objective*), uwzględniający czas od momentu katastrofy do nawiązania awaryjnych połączeń sieciowych, niezbędnych do inicjacji odtwarzania danych, wznowienia odtwarzania lub ustanowienia docelowych połączeń sieciowych po katastrofie.

W związku z powyższym, niezbędne jest również utrzymywanie opracowanych parametrów przez organizację. Oznacza to zapewnienie ciągłej zdolności do odbudowy zgodnie ze zdefiniowanymi parametrami, w tym zapewnienie usług oraz zabezpieczeń tak, aby w razie nastąpienia katastrofy organizacja mogła osiągnąć te parametry.

Plan odbudowy po katastrofie powinien być regularnie testowany. Testowanie polega na upewnieniu się, że plan spełnia potrzeby organizacji. Celem weryfikacji nie powinno być jednak udowodnienie, że plan działa. Czynność ta powinna ujawnić niedoskonałości i braki w opracowanym planie, aby osiągnąć maksymalny poziom gotowości na nieprzewidziane zdarzenia. Wnioski z przeprowadzonych testów umożliwią podjęcie decyzji na przykład w zakresie uniknięcia nieuzasadnionych kosztów, jak w przypadku stosowania dodatkowych środków zapobiegawczych, kiedy oszacowane skutki zdarzenia mogłyby być niewielkie lub prawdopodobieństwo jego wystąpienia jest bardzo niskie. Analogicznie, jeżeli wykryte słabe punkty okażą się prawdopodobne lub ich skutek mógłby być znaczący, informacje te pozwolą podjąć odpowiednie decyzje biznesowe w zakresie implementacji dodatkowych środków i zabezpieczeń[110].

Lista kontrolna planu może zawierać takie pytania, jak na przykład:

- Czy przypisane zostały funkcje systemów do konsekwencji biznesowych? Czy przypisano im wartość pieniężną stosownie do ich znaczenia?
- Czy definicja określona przez organizację obejmuje zdarzenia o wysokim prawdopodobieństwie/niskich konsekwencjach, które powodują większość katastrofalnych zakłóceń biznesowych?
- Czy można obliczyć nie tylko potencjalne straty, lecz także i oczekiwane straty? Czy te obliczenia odzwierciedlają zarówno bieżące środki zaradcze, jak i prawdopodobieństwo wystąpienia zdarzeń?

[108] *Ibidem*.

[109] PN-EN ISO 22301:2014-11 *Bezpieczeństwo powszechne. Systemy zarządzania ciągłością działania. Wymagania*, 2014, s. 5.

[110] VERITAS, *Disaster Recovery Planning Guide: The Business persons Handbook for ensuring Business Continuity*, 2015, s. 8.

Czy masz odpowiedni model powielania danych, odzwierciedlający potrzeby związane z ich odzyskiwaniem?

Czy rozwiązania w zakresie odzyskiwania, stosowane w organizacji, pozwalają przywracać każdą warstwę w złożonych, wielowarstwowych zastosowaniach, automatycznie i we właściwej kolejności?[111]

Zaleca się aktualizowanie planu odbudowy. Powinno to być dokonywane w razie potrzeby – taka potrzeba może się pojawić w szczególności po przeprowadzonych testach planu lub zmianach/rozbudowie czy aktualizacji w zakresie systemów informacyjnych służących do świadczenia usługi kluczowej, czy też w przypadku zmian w strukturze lub działaniu organizacji.

Opracowanie planu odbudowy po katastrofie dla systemów krytycznych w zakresie usługi kluczowej, jako części planu ciągłości działania organizacji, pozwala uniknąć wydłużenia lub nawet uniemożliwienia odtworzenia ich po wystąpieniu incydentu lub innego zdarzenia związanego z tymi systemami. Tym samym, pozwala to uniknąć lub znacznie obniżyć ewentualne straty finansowe, jak i wizerunkowe dla organizacji. Może to również zapobiec eskalacji zaistniałego incydentu w incydent poważny lub krytyczny, przy nieodpowiedniej zdolności organizacji (lub jej braku) w zakresie odbudowy jej kluczowych systemów informacyjnych, a tym samym braku możliwości przywrócenia i dalszej przerwie w prawidłowej realizacji jej celów biznesowych.

Dowody kontroli:

- *plany awaryjne dla kluczowych systemów, obejmujące jasne kroki i procedury w przypadku typowych zagrożeń, mechanizmy aktywacyjne, kroki i czas przywrócenia pełnej sprawności,*
- *środki stosowane w przypadku awarii i katastrof, takie jak mechanizmy przejmowania funkcji w innych regionach, tworzenie kopii zapasowych najważniejszych danych w zdalnych lokalizacjach itp.,*
- *dokumentacja poszczególnych szkoleń, dotyczących odtwarzania awaryjnego.*

[111] *Ibidem*.

10. Bezpieczeństwo fizyczne

10.1. Bezpieczeństwo fizyczne

W przypadku obowiązywania regulacji prawnych nakładających obowiązki na obszary opisane poniższymi rekomendacjami, operatorzy usług kluczowych w pierwszej kolejności zobowiązani są do wdrożenia zabezpieczeń opisanych tymi regulacjami prawnymi[112]. Poniższe rekomendacje mają spełnić rolę komplementarną do obowiązujących aktów prawnych, lub w przypadku braku takich przepisów, formę zaleceń do wdrożenia w celu podniesienia poziomu bezpieczeństwa fizycznego.

Informacje przetwarzane w procesie świadczenia usługi kluczowej, jak i sama usługa powinna podlegać szczególnej ochronie również w aspekcie bezpieczeństwa fizycznego. Skutki zakłócenia świadczenia usługi kluczowej lub naruszenie atrybutów bezpieczeństwa informacji (w zależności od poziomu tych naruszeń i rodzajów informacji), mogą mieć poważne skutki nie tylko dla przedsiębiorstwa, lecz także dla społeczeństwa, gospodarki czy państwa.

Procedury wzmacniające bezpieczeństwo fizyczne[113]

Zaleca się, aby organizacja przygotowała system bezpieczeństwa fizycznego określający m.in.:

- ustalenie elementów, które podlegać będą ochronie,
- minimalny poziom bezpieczeństwa dla różnych obszarów, np. obszaru zewnętrznego, ogólnodostępnych miejsc w siedzibie przedsiębiorstwa w przypadku dużej liczby pomieszczeń, w których realizowane są procesy związane z usługą kluczową, oznaczonych różnym poziomem oszacowanego ryzyka, zaleca się wydzielenie stref ochronnych zróżnicowanych pod kątem poziomu zabezpieczeń. Zaleca się utworzenie strefy ograniczonego dostępu oraz strefy ściśle chronionej,
- zróżnicowanie personelu pod względem kategorii, która jednocześnie wskazuje na poziomy dostępowe do różnych stref ochronnych lub pomieszczeń,
- ustalenie zasadności zastosowania oraz wskazanie środków zabezpieczenia technicznego,
- określenie procedur pracy systemu, również zasad pracy osób.

[112] Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* oraz rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. *w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*.

[113] RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej Załącznik 1*, s. 22-40 oraz rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. *w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*.

Wszystkie wypracowane procedury i systemy działania powinny być okresowo testowane, a także weryfikowane pod kątem aktualności i spełniania postawionych celów.

Organizacja powinna wdrożyć środki bezpieczeństwa fizycznego pomieszczeń, w których realizowane są zadania z zakresu cyberbezpieczeństwa usługi kluczowej, a także prowadzone są procesy których efektem jest świadczenie usługi kluczowej, adekwatne do przeprowadzonej analizy ryzyka uwzględniającej czynniki, mogące mieć wpływ na cyberbezpieczeństwo.

Przy analizie ryzyka powinno się uwzględnić co najmniej czynniki mogące mieć wpływ na ciągłość działania związaną z rodzajem przekazywanych informacji w systemach informacyjnych, liczbą osób mających lub mogących mieć dostęp do pomieszczenia, a także posiadane przez nich uprawnienia, zasadność dostępu do pomieszczeń dla osób, które mają do nich dostęp. Dodatkowo, należy uwzględnić sposoby działania w przypadku braku dostępu do tego rodzaju pomieszczeń w przypadku zdarzeń nieprzewidzianych np. pandemia. Zaleca się również opracowanie mechanizmu zabezpieczenia działania jednostki monitorującej w przypadku konieczności działań zdalnych. Ponadto powinno się szacować poziom zagrożenia działań mających znamiona sabotażu, działań o charakterze terrorystycznym i innych działań przestępczych – również dla osób z zewnątrz realizujących zlecenia. Powinno się określić zasady na jakich będzie przyznawany oraz odbierany dostęp do poszczególnych pomieszczeń lub stref ochronnych dla m.in. pracowników, kontrahentów, wykonawców, podwykonawców, gości, a także zasady poruszania się po obiekcie, zasady przechowywania kluczy oraz ich wydawania, procedurę okresowej wymiany kodów dostępu, tryb przyznawania i wydawania kart dostępu.

Organizacja powinna ustanowić procedury reagowania ochrony lub pracowników odpowiedzialnych za bezpieczeństwo fizyczne na wypadek wystąpienia awarii, braku dostępności wdrożonych systemów bezpieczeństwa, na przykład systemu kontroli dostępu.

Organizacja powinna ustanowić procedury ewakuacyjne w razie zmaterializowania się zagrożeń wynikających z analizy ryzyka, a także ustanowić formalny proces kontaktu ze służbami ratunkowymi, jak i proces wewnętrznej komunikacji o zagrożeniach. Powinna zostać również uwzględniona konieczność niepozostawienia krytycznych pomieszczeń z możliwością swobodnego wstępu podczas ewakuacji.

W przypadku korzystania z usług firm zewnętrznych świadczących usługi z zakresu zapewnienia bezpieczeństwa fizycznego obiektów, zaleca się przygotowanie planu ochrony obiektu zgodnie z ustawą z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia*[114].

Środki ochrony budowlano-mechanicznej i elektronicznej[115]

Zaleca się uwzględnienie w przeprowadzanej analizie ryzyka aspektów związanych z zagrożeniami mogącymi mieć wpływ na konieczność dostosowania pomieszczeń pod kątem:

– odpowiedniej odporności ścian i stropów pomieszczeń na zagrożenia związane z pożarem poprzez zastosowanie odpowiednich wymagań dotyczących klasy odporności ogniowej. Rekomenduje się zastosowanie zabezpieczeń odporności ogniowej o klasie co najmniej EI 60, zgodnie z normą PN-EN 13501,

[114] tj. Dz. U. z 2020 r. poz. 838, z 2021 r. poz. 469.

[115] RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej Załącznik 1*, s. 22-40 oraz rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. *w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*.

– odpowiedniej klasy drzwi do pomieszczeń wyposażonych w adekwatne do przeprowadzonej analizy ryzyka klasy zamków do drzwi. Rekomenduje się zastosowanie drzwi o klasie 2 zgodnie z normą PN-EN 1627 oraz zamków spełniających wymagania klasy 4 zgodnie z normą PN-EN 12209,
– zastosowania właściwego rodzaju okien zewnętrznych, których klasa jest zgodna z zagrożeniem wynikającym z oszacowanego ryzyka. Rekomenduje się zastosowanie okien o klasie 2 zawartej w normie PN-EN 1627,
– wyposażenia pomieszczeń w odpowiedniej klasy szafy, służące do przechowywania zarówno dokumentacji papierowej, jak i informatycznych nośników danych, zapewniające określoną odporność na próby włamań oraz pożary. Klasa powinna być dostosowana do wyników przeprowadzonej analizy ryzyka. Rekomenduje się zastosowanie szaf o podwyższonej (większej niż standardowa) odporności ogniowej oraz podwyższonej odporności na próby włamania,
– odpowiedniego zabezpieczenia dostępu do pomieszczeń z ewentualną implementacją systemu kontroli dostępu wejścia i wyjścia. Zaleca się, aby wdrożony system posiadł funkcje rozpoznawania osoby uprawnionej uzyskującej dostęp do pomieszczeń lub wychodzącej z tych pomieszczeń, poprzez odczyt identyfikatora lub cech biometrycznych. Zaleca się również, aby system rejestrował tego rodzaju zdarzenia oraz posiadał zdefiniowane grupy użytkowników. Dla większego bezpieczeństwa zaleca się również implementację funkcjonalności w systemie SKD sygnalizującą niedomknięte drzwi lub weryfikację aktualności kart dostępowych,
– odpowiedniego systemu sygnalizacji napadu i włamania, adekwatnego do oszacowanego ryzyka. Rekomenduje się zaimplementowanie systemu spełniającego wymagania 2 stopnia określone w normie PN-EN 50131-1,
– adekwatnego do oszacowanego ryzyka systemu sygnalizacji pożarowej. Rekomenduje się wdrożenie systemu składającego się z urządzeń sygnalizacyjno-pomiarowych, służących do samoczynnego wykrywania i przekazywania informacji o pożarze,
– właściwego do oszacowanego ryzyka systemu chłodzenia pomieszczeń, utrzymywania odpowiedniej temperatury oraz wilgotności i wentylacji pomieszczeń (np. w serwerowniach),
– zainstalowania systemu automatycznego gaszenia pożaru w przypadku wystąpienia takiego zdarzenia. Rekomenduje się również uwzględnienie funkcji automatycznego przekazania informacji do straży pożarnej,
– objęcia systemem (SSV) CCTV wejść do pomieszczeń kluczowych,
– objęcia systemem (SSV) CCTV pomieszczeń, w których występuje ryzyko nieuprawnionego dostępu osób niezwiązanych stanowiskiem pracy ze świadczeniem usługi kluczowej oraz jej cyberbezpieczeństwem – szczególnie w sytuacji braku możliwości wdrożenia któregoś z wyżej wymienionych zabezpieczeń w sposób dający duży stopień pewności skuteczności tego rozwiązania.
– w razie możliwości, powinno się zapewnić zapasowe źródło zasilana dla posiadanych systemów VSS, systemu kontroli dostępu oraz systemu sygnalizacji włamania i napadu.

Zaleca się, aby organizacja w przeprowadzanej analizie ryzyka uwzględniła zagrożenia fizyczne związane z siedzibą przedsiębiorstwa. Analiza ryzyka powinna być przeprowadzona pod kątem konieczności zastosowania środków ochrony obwodowej, takich jak:

- odpowiedniej klasy i rodzaju ogrodzenie minimalizujące ryzyko zmaterializowania się zidentyfikowanych zagrożeń. Zaleca się wzięcie pod uwagę możliwej konieczności konstrukcyjnego zmodyfikowania ogrodzenia w sposób utrudniający wspinanie się, np. dodanie elementów z drutu kolczastego na ogrodzeniu, modyfikację utrudniającą jego przecinanie czy inne naruszenie integralności,
- środków ochrony perymetrycznej, np. barier mikrofalowych lub podczerwieni,
- odpowiedniego oznakowania terenu działającego w sposób prewencyjny (w przypadku wyznaczenia stref wewnątrz budynku, zaleca się także wywieszanie informacji na drzwiach do wejścia tych stref),
- rozszerzenie (lub wdrożenie) systemu VSS (CCTV) w sposób umożliwiający monitorowanie słabiej zabezpieczonych obszarów, obszarów trudno dostępnych, a także wejść i wyjść z obiektu, zabezpieczenie nagrań na odpowiednio długi okres, zabezpieczenie samych kamer przed dewastacją, zastosowanie kamer odpowiedniej jakości.

Środki ochrony fizycznej[116]

Powinno się zdefiniować wymagania wobec podmiotów zewnętrznych świadczących usługi ochrony fizycznej obiektu lub wobec wewnętrznych komórek świadczących takie usługi, które to wymagania mogą obniżać poziom oszacowanego ryzyka.

Działaniem takim może być np. cykliczne monitorowanie terenu przedsiębiorstwa (patrole), cykliczna weryfikacja stanu ogrodzenia, szczególnie w miejscach trudno dostępnych, nieobjętych systemem VSS (CCTV) lub tych gdzie zgodnie z planem ochrony lub innym dokumentem występuje potencjalne ryzyko, a także patrolowanie o losowych godzinach. Dodatkowo, powinno się weryfikować stan bramy wjazdowej, stan zamknięć drzwi zewnętrznych. Rekomenduje się również zaimplementowanie systemu elektronicznej kontroli wartowników. Oprócz powyższych działań doraźnych, powinno się przeprowadzać zaplanowane, kompleksowe przeglądy stanu zewnętrznego chronionego obiektu oraz stanu ogrodzenia.

Przy wejściu do obiektu powinno znajdować się stanowisko ochrony obiektu, gdzie pracownicy ochrony mogą weryfikować wszystkie osoby wchodzące na teren, sprawdzając ich tożsamość z możliwością kontroli bagażu.

Powinno się zapewnić dostateczne oświetlenie terenu organizacji, jak i wewnętrznego obszaru budynku (w kluczowych miejscach) w taki sposób, aby obraz utrwalony przez system wizyjny był wystarczająco dobrej jakości.

Rekomenduje się wypracowanie procedur stałego nadzoru nad osobami nie biorącymi udziału w wykonywaniu zadań operatora usługi kluczowej, ale przebywającymi w pomieszczeniach, w których realizowane są wrażliwe procesy (osoby trzecie względem procesów krytycznych, jak i osoby spoza organizacji).

[116] RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej Załącznik 1*, s. 22-40 oraz rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. *w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*.

Operator powinien posiadać prawo do wyłącznego korzystania z pomieszczeń, które są miejscem stałego i ciągłego wykonywania obowiązków operatora usługi kluczowej, w szczególności tych związanych z zarządzaniem incydentami, obsługą incydentu oraz prowadzeniem komunikacji i wymiany informacji z jednostkami CSIRT poziomu krajowego.

Powinno się przygotować procedurę szybkiego zapoznania się z zasadami bezpieczeństwa w obiekcie, dedykowaną osobom trzecim wchodzącym na jego teren. Osoby te powinny zostać poinformowane o dozwolonych i zabronionych czynnościach oraz zasadach BHP.

Organizacja powinna stworzyć rejestr osób uprawnionych do dostępu do pomieszczeń, w których realizowane są krytyczne procesy związane z usługą kluczową, a także stworzyć rejestr tych pomieszczeń.

Dowody kontroli:

- *dokumenty potwierdzające zabezpieczenie przed nieautoryzowanym fizycznym dostępem do obiektów i infrastruktury oraz wprowadzenie środków zapobiegawczych mających na celu ochronę przed nieautoryzowanym dostępem (np. włamaniem, pożarem, powodzią itp.).*
- *lista personelu posiadającego dostęp oraz stosowne uprawnienia,*
- *udokumentowane regulaminy w zakresie środków bezpieczeństwa fizycznego i zabezpieczeń środowiskowych, w tym opis obiektów i systemów,*
- *lista personelu posiadających dostęp oraz stosowne uprawnienia,*
- *udokumentowane regulaminy w zakresie środków bezpieczeństwa fizycznego i zabezpieczeń środowiskowych, w tym opis obiektów i systemów.*

10.2. Bezpieczeństwo fizyczne stron trzecich

Podmioty realizujące zadania z zakresu cyberbezpieczeństwa na rzecz operatora usługi kluczowej powinny spełnić wymagania określone w rozdziale 10.1 niniejszego dokumentu, w takim zakresie, w jakim zasadność ich wdrożenia wynika z analizy ryzyka. Ponadto operator usługi kluczowej znając krytyczność danych przetwarzanych przez te podmioty, powinien kierować się kryteriami definiującymi minimalne wymagania związane z bezpieczeństwem fizycznym, przy wyborze usługodawcy. W sytuacji konieczności skorzystania przez operatora usługi kluczowej z usługi doraźnej, świadczonej przez stronę trzecią, która wymaga udzielenia dostępu do obiektów przedsiębiorstwa będącego OUK, zaleca się:

- zachowanie podwyższonej czujności podczas obecności pracowników wykonawcy na terenie należącym do operatora,
- zaleca się uwzględnienie w przeprowadzanej analizie ryzyka sytuacji nielegalnego wykorzystania informacji pozyskanej przez osoby trzecie, a także sytuacji dostępu do pomieszczeń o podwyższonym standardzie zabezpieczeń,
- rekomenduje się weryfikację statusu podwykonawcy danego działania, m.in. pod kątem jego rozpoznawalności, spełniania odpowiednich standardów. Ponadto, w razie możliwości proponuje się pozyskanie personalnych rekomendacji oraz opinii na temat danej strony trzeciej wykonującej usługę doraźną,
- zakres usługi powinien być jasno określony i zakomunikowany wszystkim pracownikom usługodawcy świadczącego usługę doraźną, którzy będą mieli dostęp do obiektów i pomieszczeń

należących do operatora usługi kluczowej. Ponadto, powinno się zapewnić krótkie szkolenie informujące o procedurach i zasadach panujących na terenie organizacji. Po dokonaniu tych czynności powinno się określić ewentualny dostęp i wydać przepustki dla pracowników podwykonawcy,

– w sytuacji wykonywania prac, które ze względu na swój charakter lub ze względu na miejsce w jakim są prowadzone mogą spowodować zmaterializowanie się zagrożeń związanych z działaniem osób trzecich względem organizacji, operator usługi kluczowej powinien zapewnić stały nadzór wizyjny lub osobowy nad pracownikami podwykonawcy,
– należy zwracać szczególną uwagę na niestandardowe zachowania pracowników strony trzeciej realizujących usługę na terenie przedsiębiorstwa.

Dowody kontroli:

– dokumenty potwierdzające zabezpieczenie przed nieautoryzowanym fizycznym dostępem do obiektów i infrastruktury.

11. Bezpieczeństwo sieci łączności elektronicznej

11.1. Segmentacja sieci, protokoły, szyfrowanie

Organizacja powinna stosować segmentację i separację sieci w zakresie systemów informacyjnych służących do świadczenia usługi kluczowej, o ile nie spowoduje to utrudnień lub zakłóceń w funkcjonowaniu tych systemów oraz sieci, a także samego świadczenia usługi kluczowej.

Architektura sieci oraz sposób jej projektowania jest jednym z działań, które bezpośrednio wpływają na podwyższenie standardów bezpieczeństwa. Wyrazem maksymalizacji poziomu bezpieczeństwa sieci może być jej budowa zgodnie ze strategią *Defence-in-Depth*, co przekłada się na segmentację sieci poprzez zastosowanie m.in. stref bezpieczeństwa. Im bardziej efektywna jest segmentacja, tym zmniejsza się prawdopodobieństwo rozszerzenia zagrożenia na większy obszar atakowanej sieci, a także zwiększa się bezpieczeństwo świadczenia usługi kluczowej, poprzez ograniczenie dostępu do krytycznych danych i systemów.

Sieci łączności elektronicznej, w których funkcjonują systemy automatyki przemysłowej oraz przetwarzane są kluczowe dane powinny podlegać szczególnej ochronie. Organizacja powinna utworzyć strefy bezpieczeństwa sieci, które odseparują poszczególne segmenty sieci, a komunikacja pomiędzy tymi strefami będzie kontrolowana. Przy tworzeniu stref bezpieczeństwa powinno się mieć na uwadze, iż wydzielona strefa, w której funkcjonują systemy automatyki przemysłowej powinna być tą najbardziej chronioną. Prowadzone działania powinny być oparte o realizację zasady „najmniejszych uprawnień". Utworzenie strefy bezpieczeństwa, określanej również jako strefa zdemilitaryzowana (DMZ), powinno obligatoryjnie mieć miejsce pomiędzy siecią biznesową, a siecią przemysłową. Sieci te powinny zawsze komunikować się przez DMZ, podlegającą zasadzie *zero-trust*, ponadto ruch pomiędzy każdą ze stref powinien być kontrolowany przez firewall.

Organizacja powinna stosować mikrosegmentację sieci w ramach jednej sieci. Segmentacja powinna być oparta o zasadę minimalnej wiedzy i dostępu, a ruch sieciowy pomiędzy segmentami powinien być kontrolowany za pomocą m.in. firewalli. Takie działanie będzie korzystne w przypadku np. infekcji, przekładając się na zapobieganie dalszemu rozprzestrzenianiu się zagrożenia na sieć. Mikrosegmentacja może być osiągnięta poprzez m.in. wydzielenie w ramach sieci fizycznej lokalnych sieci wirtualnych, czyli sieci wydzielonych w sposób logiczny (sieci VLAN), filtrowanie ruchu sieciowego na różnych poziomach, fizyczną separację sieci. Zaleca się, aby zastosowanie wirtualnych sieci lokalnych VLAN (ang. *Virtual Local Area Network*) wiązało się również z zastosowaniem kontroli ruchu na podstawie adresów MAC oraz w oparciu o standard bezpieczeństwa IEEE 802.1X, a także o politykę filtrowania pakietów IP[117]. W celu

[117] Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, 2020, s. 83.

ochrony sieci, a także urządzeń zaleca się stosowanie mechanizmów kontroli dostępu do sieci (NAC), które powinny być dostosowane do najnowszych wymagań i standardów oraz spełniać kryteria:

- mechanizmy kontroli dostępu powinny być skonfigurowane w taki sposób, aby widziały wszystkie rodzaje urządzeń końcowych oraz mogły je ocenić przed podłączeniem do sieci. Dodatkowo, NAC powinny mieć zdolność kategoryzacji urządzeń, a także oceny ryzyka związanego z urządzeniem oraz użytkownikiem, dokonywanej również po podłączeniu do sieci[118],
- mechanizmy NAC powinny także posiadać funkcję określania krytycznych lub w zabezpieczeniach danego urządzenia, np. nieaktualna wersja oprogramowania[119],
- po dokonaniu identyfikacji urządzenia i użytkownika, narzędzie NAC powinno obsłużyć segmentację opartą na celach biznesowych, czego skutkiem będzie automatyczne stosowanie zasad zabezpieczeń[120],
- zastosowane mechanizmy NAC powinny mieć możliwość integracji z innymi rozwiązaniami w ramach stosowanej architektury zabezpieczeń[121],
- mechanizmy NAC powinny ułatwiać reagowanie na zagrożenia w czasie rzeczywistym, pozwalać na automatyzację procesów, np. samodzielne przydzielanie zasobów przez użytkownika, wysyłanie użytkownikowi odpowiednich zaleceń w sytuacji, gdy dane urządzenie nie będzie spełniało minimalnych standardów bezpieczeństwa. Dodatkowo, powinny zapewniać skalowalność i elastyczność[122].

Implementacją techniczną jest protokół 802.11.x. w warstwie użytkownika i urządzenia.

W procesie wdrażania różnych rozwiązań zapewniających kontrolę dostępu do sieci organizacja powinna mieć na uwadze również negatywne aspekty przyjętych rozwiązań w postaci ich wad, niedoskonałości lub niekompletnej funkcjonalności, co z kolei powinno przełożyć się na uwzględnienie tego rodzaju inwestycji lub zmian w procesie szacowania ryzyka. Ponadto, organizacja powinna mieć świadomość konieczności uzupełniania się mechanizmów filtrowania adresów MAC i zastosowania systemu NAC, które działając wspólnie mogą zapewnić pewną komplementarność. Filtrowanie po adresach MAC powinno być zastosowane szczególnie do urządzeń, które nie są objęte systemem NAC, należy także mieć świadomość, które to są urządzenia.

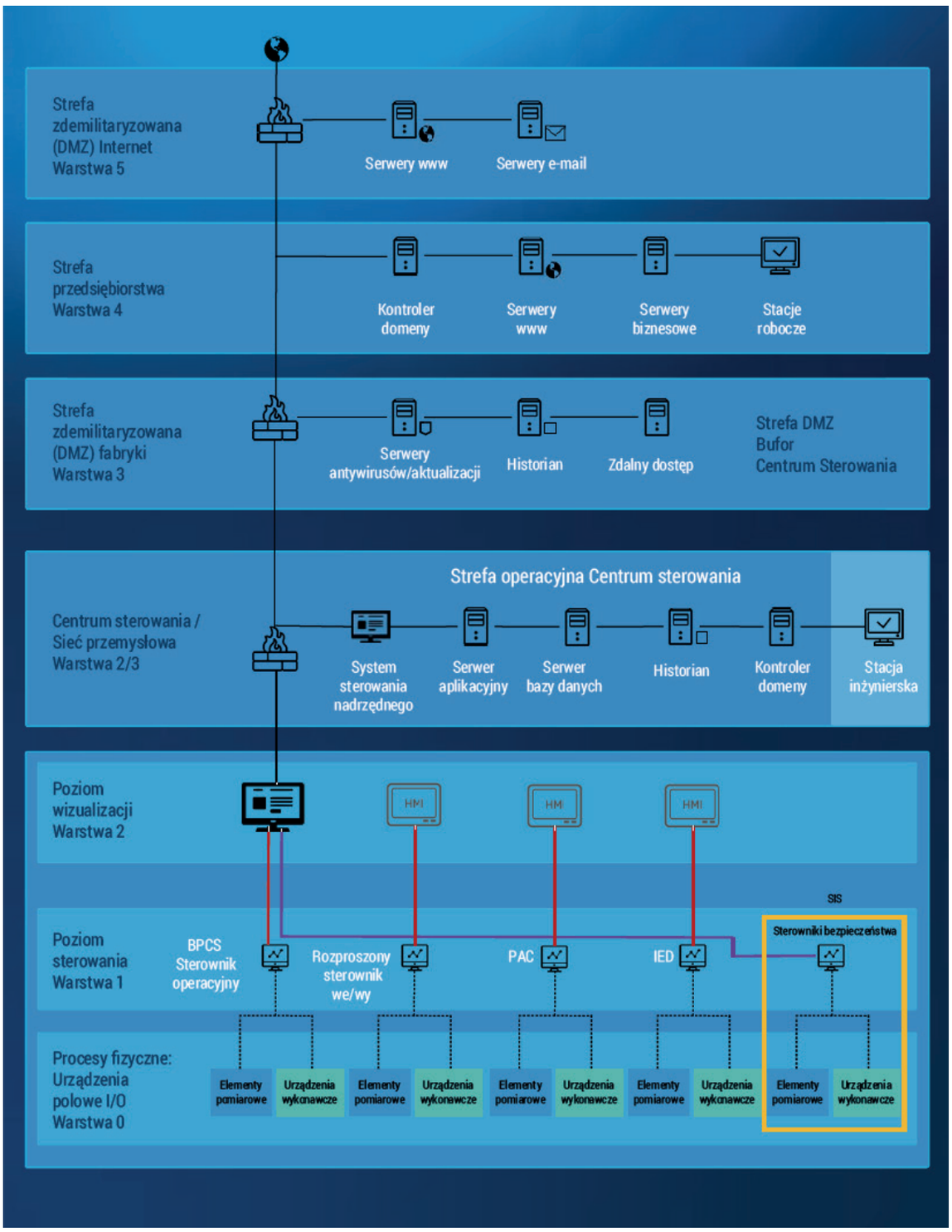
Zastosowanie rozwiązań typu firewall w postaci odpowiedniego oprogramowania lub dedykowanego urządzenia i jego oprogramowania, również powinno być metodą stosowaną przez organizację. Powyższe rozwiązania pozwolą także uniknąć rozprzestrzeniania się potencjalnego szkodliwego oprogramowania pomiędzy segmentami sieci.

W przypadku korzystania z sieci bezprzewodowych, organizacja powinna dokonać separacji ruchu z taką siecią. Powinno się wyłączyć możliwość komunikacji sieci bezprzewodowych z sieciami, w których przetwarzane są informacje krytyczne dla procesu technologicznego oraz sieciami, w których komunikują się urządzenia związane ze świadczeniem usługi kluczowej. Ponadto, komunikacja bezprzewodowa powinna wykorzystywać szyfrowanie zgodnie z rekomendowanymi i powszechnie uznanymi standardami, np. WPA2. W celu zminimalizowania prawdopodobieństwa wystąpienia zagrożenia, zaleca się także podjęcie działań o charakterze prewencyjnym. Przykładem może być wyłą-

[118] Publikacja: Fortinet, *Mechanizmy kontroli dostępu do sieci (NAC) w erze Internetu rzeczy i BYOD*, 2020 r.
[119] *Ibidem*.
[120] *Ibidem*.
[121] *Ibidem*.
[122] *Ibidem*.

czenie rozgłaszania identyfikatora sieciowego (wyłączenie rozgłaszania SSID), co przełoży się na potencjalne utrudnienia w wykryciu sieci. Organizacja powinna również zastosować kontrolę dostępu do sieci bezprzewodowych, poprzez zdefiniowanie dozwolonych adresów fizycznych MAC urządzeń, które mogą się przyłączyć do sieci, także w oparciu o IEEE 802.1X.[123]

Rysunek 13 – Wizualizacja struktury segmentacji sieci.



Źródło: *Urząd Dozoru Technicznego, „Poradnik dobrych praktyk w zakresie cyberbezpieczeństwa urządzeń podlegających dozorowi technicznemu", 2021, s. 34.*

[123] *Ibidem*, s. 94.

W celu zapewnienia możliwości sprawnego zarządzania systemem informacyjnym, organizacja powinna ograniczyć liczbę protokołów zaimplementowanych do danego środowiska, a także wyłączyć wszystkie nieużywane i domyślne usługi sieciowe.

Organizacja powinna zapewnić zdolności ochronne oraz interoperacyjność pomiędzy protokołami, kiedy są one implementowane dla różnych urządzeń w ramach tego samego systemu. Jedną z przykładowych metod osiągnięcia tego celu jest używanie dedykowanych bram sieciowych, które zapewniają konwersję (ang. *translation*) protokołów. Brama ta może konwertować niezabezpieczony protokół, na współczesny, bezpieczniejszy protokół, zanim wyśle go dalej, tym samym zmniejszając możliwości w zakresie ewentualnego ataku.

W sytuacji, gdy organizacja wykorzystuje lub wdraża w ramach swojej struktury technologie IIoT, powinna wykorzystywać już wypróbowane protokoły ze zdolnościami ochronnymi, które określają ustanowione standardy i rekomendacje techniczne. Powinno się wybierać takie rozwiązania, które podczas pracy wykorzystują protokoły uznane za bezpieczne oraz unikać tych, które wykorzystują protokoły o stwierdzonych podatnościach.

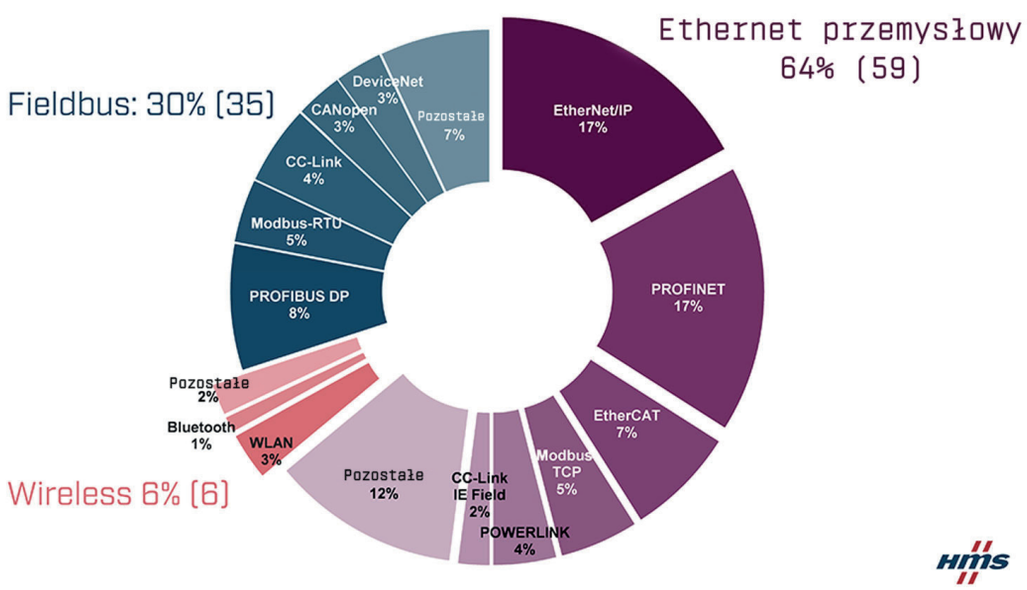
Organizacja powinna zastosować rozwiązania służące do pasywnego monitorowania środowisk IT i OT. Zaleca się stworzenie punktu odniesienia w postaci standardowego ruchu w sieci, w celu wykrywania ewentualnych anomalii w postaci odstępstw od stanu bazowego.

Organizacja powinna stosować szyfrowanie danych, informacji oraz komunikacji w zakresie świadczonej usługi kluczowej, a także uwzględnić ewentualność stosowania szyfrowania w środowiskach systemów informacyjnych służących do jej świadczenia, o ile nie spowoduje to utrudnień lub zakłóceń w funkcjonowaniu tych systemów, a także samego świadczenia usługi kluczowej.

Metoda szyfrowania danych i informacji powinna być dostosowana do ich charakterystyki oraz wykorzystania – zależnie od tego, czy są to dane w stanie spoczynku (np. przechowywane do celów archiwalnych), czy te, co do których istnieje wymóg krótkiego czasu dostępu lub danych będących w przesyle.

Należy mieć na uwadze, iż szyfrowanie komunikacji pomiędzy urządzeniami OT nie zawsze jest możliwe ze względu na używane protokoły i specyfikę działania systemów czasu rzeczywistego.

Rysunek 14 – Najczęściej spotykane protokoły komunikacyjne w sieciach przemysłowych.



Źródło: *https://sterowniki.elmark.com.pl/rynek-protokolow-2020-wg-hms/ (na podstawie analizy globalnego rynku nowo instalowanych urządzeń sieciowych w zakładach przemysłowych).*

Sieci sterowania przemysłowego korzystają z dwóch głównych standardów komunikacyjnych – Fieldbus oraz Ethernet. W standardzie Fieldbus (sieci polowe) najpopularniejszymi protokołami są PROFIBUS DP oraz MODBUS-RTU, a wśród tych opartych w przemyśle o Ethernet najczęściej używany jest EtherNet/IP, PROFINET, EtherCAT oraz MODBUS TCP czy POWERLINK Ethernet.

PROFIBUS-DP jest jednym z wariantów protokołu PROFIBUS, ukierunkowanym na sterowanie urządzeniami za pośrednictwem systemu centralnego. PROFIBUS-PA dedykowany jest zaś rozwiązaniom monitorującym urządzenia pomiarowe za pośrednictwem systemu sterowania procesem, w szczególności w strefach niebezpiecznych jak „Ex". PROFIBUS może działać zarówno w warstwie aplikacji, sieci jak i fizycznej. Komunikacja w tym protokole jest oparta o hybrydowe rozwiązanie polegające na technologii *master-slave* wraz z przekazywaniem tokena, co zapobiega jednoczesnemu komunikowaniu się urządzeń. Nie przeciwdziała to jednak atakom typu DoS czy *traffic injection*. Podobnie, jak w przypadku innych protokołów opartych o sieci polowe, PROFIBUS nie zapewnia uwierzytelniania oraz dodatkowych zabezpieczeń, przez co wymaga odizolowania magistrali od pozostałych składników sieci. Należy więc zwrócić uwagę na środki ochrony obwodowej, które powinny być bardzo surowe, aby uniknąć nieautoryzowanego lub podejrzanego ruchu sieciowego.[124]

MODBUS jest jednym z najwcześniej wdrożonych do funkcjonowania protokołów sterowania w przemyśle. Działa on jako protokół komunikacyjny osadzony w warstwie aplikacji, oparty o tryb klient-serwer, umożliwiając łączność pomiędzy różnymi rodzajami urządzeń oraz techniki na niższych warstwach, obejmując m.in. warstwę protokołu TCP/IP. MODBUS, jako protokół opracowany do komunikacji w ściśle nadzorowanych środowiskach, nie przewiduje sam w sobie żadnych zabezpieczeń w postaci uwierzytelniania czy szyfrowania. Do przesłania poprawnego komunikatu za jego pomocą wystarczy jedynie prawidłowy adres sieciowy oraz kod funkcji[125]. Ponadto, w zastosowaniach szeregowych komendy MODBUS są przekazywane poprzez rozgłaszanie, przez co wszystkie połączone urządzenia mogą zostać dotknięte za pośrednictwem jednego ataku typu DoS. Jako protokół opracowany do programowania urządzeń typu PLC oraz RTU, możliwe jest również zaimplementowanie za jego pomocą złośliwego kodu w tego typu urządzeniach. Tym samym należy mieć na uwadze, iż komunikacja za pomocą MODBUS powinna podlegać nadzorowi. Może to zostać zrealizowane na przykład za pomocą wdrożenia analizy ruchu sieciowego, która weryfikowałaby, czy komunikaty są transmitowane tylko z określonych urządzeń oraz w zakresie funkcji, jakie zostały dozwolone. Prócz powyższego, pakiety MODBUS TCP w transmisji na porcie 502, posiadające nieprawidłowe dane na temat ich wielkości lub budowy powinny być weryfikowane. Sprawdzeniu powinny podlegać także wysyłane komunikaty wywołujące funkcję przejścia urządzeń typu *slave* w tryb nasłuchu, a także funkcje reinicjujące komunikację, kasujące lub resetujące informacje diagnostyczne[126].

EtherNet/IP stanowi implementację protokołu CIP (*Common Industrial Protocol*) dla TCP/IP, który zawiera w sobie zbiór usług i komunikatów dotyczących m.in. kontroli, bezpieczeństwa, synchronizacji, konfiguracji czy informacji, które mogą zostać zintegrowane z sieciami Ethernet oraz Internetem. Ten protokół, jako bazujący na sieci Ethernet, charakteryzuje się również wszystkimi podatnościami związanymi z tą siecią, jak kradzież tożsamości czy przechwytywanie ruchu. Dla komunikacji i transmisji danych w czasie rzeczywistym, używana jest komunikacja UDP z zastosowaniem adresacji *multicast*, przez co nadzór transmisji jest znacznie utrudniony. Tym samym istnieje możliwość wygenerowania

[124] INCIBE, *Protocols and Network Security in ICS Infrastructures*, 2015, s. 26-28.

[125] Kod funkcji – w protokole MODBUS jest to odpowiedni kod używany w żądaniu, by przekazać urządzeniu podrzędnemu, do jakiego rodzaju pamięci ma uzyskać dostęp oraz jaką wykonać na niej akcję (np. zapis lub odczyt). Na przykład kod funkcji „4" oznacza odczyt rejestrów wejściowych.

[126] INCIBE, *op. cit.*, s. 22-23.

złośliwego ruchu sieciowego oraz manipulacji tej transmisji poprzez IGMP[127]. Aby zwiększyć bezpieczeństwo użytkowania tego protokołu, powinny zostać uwzględnione wszelkie mechanizmy bezpieczeństwa przewidziane zarówno dla interfejsu Ethernet, jak i dla IP. Korzystny wpływ będzie miało również zastosowanie rozwiązań w zakresie pasywnego monitorowania sieci, co pozwoli upewnić się, iż ruch dotyczy wyłącznie wskazanych urządzeń i nie pochodzi spoza sieci[128].

PROFINET stanowi adaptację protokołu PROFIBUS dla interfejsu Ethernet i podobnie jak w jego pierwowzorze, komunikacja opiera się na przekazywaniu tokena. Ponadto, transmisja za jego pośrednictwem zapewnia wszelkie funkcjonalności TCP/IP dla transmisji danych, pozwalając na wdrożenie go w zastosowaniach bezprzewodowych, a także tych o wysokiej przepustowości sieci. Jako, że pierwotnie protokół ten został opracowany do komunikacji za pośrednictwem sieci polowych typu Fieldbus, sam w sobie nie oferuje on uwierzytelniania oraz innych cech bezpieczeństwa. Z tego powodu, przy jego wykorzystaniu wymagana jest fizyczna separacja sieci, choć mogą zostać zaimplementowane także rozwiązania w zakresie uwierzytelniania komponentów w sieci oraz szyfrowania komunikacji, na wzór tych stosowanych pierwotnie w IT. Podobnie jak w przypadku innych protokołów, sieć powinna podlegać ochronie i monitorowaniu w celu uniknięcia ruchu o niejasnym lub niebudzącym zaufania pochodzeniu.[129]

EtherCAT (ang. *Ethernet for Control Automation Technology*) jest protokołem charakteryzującym się otwartym kodem oraz realizującym transmisję za pośrednictwem Ethernet. Jest wykorzystywany w systemach automatyki wymagających krótkich cykli aktualizacji danych (poniżej 100 mikrosekund) oraz jitterze (zmiana opóźnienia pakietu) niższym niż 1 mikrosekunda, co czyni go najszybszym protokołem spośród obecnie dostępnych. Jak każdy inny protokół oparty o Ethernet, jego stosowanie niesie za sobą wszelkie jego słabości, m.in. ryzyko rozległego ataku typu DoS. Ponadto, komunikację EtherCAT można w łatwy sposób modyfikować, wprowadzając pakiety danych Ethernet w sposób zakłócający synchronizację i umożliwiający ich preparowanie, jak i dokonanie ataku typu *Man-in-the-Middle*. Jak w przypadku pozostałych protokołów opartych o interfejs Ethernet, ruch wykorzystujący EtherCAT powinien być monitorowany oraz chroniony[130].

Coraz popularniejszym standardem w zakresie protokołów komunikacyjnych jest także OPC UA opracowany przez OPC Foundation[131]. Jego pozytywną cechą jest przede wszystkim możliwość zaimplementowania w dowolnych systemach operacyjnych, platformach sprzętowych czy środowiskach chmurowych, z wykorzystaniem różnych języków programowania.

Bezpieczeństwo tego protokołu opiera się na certyfikatach w standardzie X.509, które mają trzy zastosowania:

1) Podpisywanie komunikatów, co pozwala uwierzytelniać wymianę informacji oraz zapewniać jej integralność – aplikacja używa swojego prywatnego klucza by wygenerować hash przesyłanego komunikatu, który może zostać zweryfikowany za pomocą odpowiedniego certyfikatu klucza publicznego. Jeżeli weryfikacja się powiedzie oznacza to, iż komunikat pochodzi z odpowiedniej aplikacji. Modyfikacja komunikatu w trakcie transmisji (jak w przypadku ataków *Man-in-the-Middle)*, skutkowałaby tym, iż hash komunikatu nie byłby już poprawny;

[127] IGMP – protokół ze zbioru protokołów TCP/IP, służący do zarządzania grupami transmisji zbiorowej (*multicast*).
[128] *Ibidem*, s. 16, 20-21.
[129] *Ibidem*, s. 28-29.
[130] *Ibidem*, s. 33-34.
[131] https://opcfoundation.org/

2) Szyfrowanie komunikatów, które zabezpiecza przed odczytaniem ich przez nieuprawnione podmioty – w ten sam sposób, jak klucz publiczny może być używany do podpisywania komunikatów by zagwarantować, że został wygenerowany przez uwierzytelnioną aplikację, klucz publiczny może być użyty do jej zaszyfrowania. Jeżeli klucz publiczny zostanie użyty do zaszyfrowania wiadomości, tylko aplikacja z odpowiadającym mu kluczem prywatnym jest w stanie go odszyfrować. Nawet w przypadku, gdyby atakujący posiadał kopię certyfikatu publicznego, nie byłby w stanie odszyfrować wiadomości, gdyż klucz publiczny jest używany tylko do szyfrowania – nie może być użyty do odszyfrowania wiadomości,
3) Identyfikację aplikacji, która stanowi środek zapewniający wiarygodność – powyższe środki nie miałyby odpowiedniego zastosowania, gdyby nie było możliwe ustalenie do kogo należy dany certyfikat. Każdy certyfikat w komunikacji OPC UA pozwala ustalić w jakiej aplikacji został on wygenerowany, kiedy zostało to dokonane, przez kogo, do czego może zostać użyty, jak długo jest ważny, gdzie został wygenerowany, jak i wiele innych informacji. W momencie nawiązania komunikacji pomiędzy dwiema aplikacjami za pośrednictwem OPC UA, wymieniają się one swoimi kluczami publicznymi (certyfikatami), nie ujawniając swoich kluczy prywatnych. To zarówno po stronie klienta, jak i serwera leży odpowiedzialność za zaufanie danemu certyfikatowi publicznemu. Należy mieć jednak na uwadze odpowiednie zweryfikowanie certyfikatu, któremu chce się zaufać[132].

Ważnym aspektem w kontekście komunikacji, poza tą związaną z wymianą informacji pomiędzy urządzeniami, jest także ich wymiana pomiędzy jednostkami w organizacji, jak i pomiędzy samymi organizacjami. Należy wskazać, iż najczęściej taka komunikacja odbywa się za pośrednictwem poczty e-mail. Dla zapewnienia odpowiednich cech związanych z jej bezpieczeństwem, jak integralność, autentyczność, a w szczególności poufność, organizacja powinna stosować odpowiednie zabezpieczenia dla takiej komunikacji, jak m.in. szyfrowanie za pośrednictwem PGP. PGP poza swoją komercyjną implementacją, jest także narzędziem występującym w wersji powszechnie dostępnej i opartej o otwarte oprogramowanie, pozwalającej szyfrować poza samymi wiadomościami również m.in. przesyłane pliki[133].

[132] https://opcconnect.opcfoundation.org/2020/06/exploring-opc-ua-security-concepts/
[133] Jedną z takich implementacji opartych o OpenPGP jest GnuPG, dostępne pod adresem https://gnupg.org/.

Tabela 2 – Tabela porównawcza cech bezpieczeństwa protokołów wykorzystywanych w systemach sterowania przemysłowego.

Protokół		Szyfrowanie	Uwierzytelnianie	Warstwa IP/ transportowa	Warstwa aplikacji	Bezpieczeństwo i zalecenia
Common Industrial Protocol (CIP)	DeviceNet	Nie	Nie	Protokół zamknięty **DeviceNet™**	CIP	CIP posiada technologię w warstwie aplikacji **CIP Safety™** Rekomendowane jest uzupełnienie powyższego poprzez ogólne środki segmentacji i izolacji sieci sterowania przemysłowego
	ControlNet	Nie	Nie	Protokół zamknięty **ControlNet™**		
	CompoNet	Nie	Nie	Protokół zamknięty **CompoNet™**		
	Ethernet/IP	Nie	Nie	TCP/IP		
MODBUS	Modbus szeregowy	Nie	Nie	Nie ma zastosowania (transmisja szeregowa)	Modbus (niezabezpieczony)	Jeżeli to możliwe, należy użyć szyfrowania (SSL, VPN) lub środków analizy ruchu sieciowego (np. Snort), IPS (np. Tofino) lub podobne
	Modbus--TCP	Nie	Nie	TCP/IP	Modbus (niezabezpieczony)	
DNP3		Tylko poprzez Secure DNP	Tylko poprzez Secure DNP	Secure DNP	Secure DNP	Rekomendowana jest implementacja Secure DNP
Profibus		Nie	Nie	Nie ma zastosowania (transmisja szeregowa)	Nie posiada wbudowanych środków	Powinny zostać zastosowane ogólne zalecenia dotyczące segmentacji, analizy ruchu sieciowego oraz szyfrowania
Profinet		Nie	Nie	TCP/IP UDP/IP	Nie posiada wbudowanych środków	*Profinet Security Guide*
PowerLink Ethernet		Nie	Nie	Nie posiada wbudowanych środków	Nie posiada wbudowanych środków	PowerLink jest protokołem opartym o Ethernet z zastosowaniem komunikacji w czasie rzeczywistym Rekomendowane są środki oparte o segmentację dla architektury
OPC		OPC UA	OPC UA	Bazowe TCP/IP OPC UA	OPC UA	*Implementation of OPC UA*
EtherCAT		Nie	Nie	Nie posiada wbudowanych środków	Nie posiada wbudowanych środków	Zaleca się zastosowanie środków opartych o segmentację oraz ochronę perymetryczną

Źródło: INCIBE, op. cit., s. 35.

Dowody kontroli:

– *dokumentacja dotycząca sposobu wdrożenia rozdzielenia krytycznych systemów informacyjnych i danych, w tym rysunki i mapy topologii sieci.*

11.2. Monitorowanie sieci łączności elektronicznej

W celu właściwego monitorowania prac sieci należy przeprowadzić inwentaryzację zasobów oraz urządzeń działających w sieciach.

Podstawą do aktualności i utrzymania wysokiej jakości monitorowania jest wiedza dotycząca aktualności posiadanych aktywów.

Inwentaryzacja zasobów powinna uwzględnić wszystkie elementy monitorowanej sieci oraz podłączone do niej urządzenia, a także powinna zawierać informację o połączeniach pomiędzy urządzeniami, wykorzystywanych protokołach, portach itd. Dodatkowo inwentaryzacja powinna uwzględniać elementy które są czasowo podłączane do sieci. Inwentaryzacja powinna być przeprowadzona indywidualnie dla każdej z sieci odseparowanych. Powinna być ona regularnie przeprowadzana w celu aktualizacji informacji o sieciach. Zaleca się wspieranie systemem informatycznym pozwalającym śledzić zmiany i trendy.

Rekomenduje się rezygnację z urządzeń niezarządzalnych, niskich warstw sieci, nie wspierających funkcji monitorowania i zarządzania.

W celu realizacji skutecznego monitorowania sieci należy określić krytyczność poszczególnych zasobów w sieci i oszacować dla nich ryzyka.

Zaleca się jednakowe traktowanie każdego zidentyfikowanego zasobu sieci, który sam w sobie może stać się wektorem potencjalnego ataku czy źródłem innych problemów z działaniem sieci.

Uwzględniając fakt, że nie zawsze jest możliwe wdrożenie monitorowania całej infrastruktury sieciowej rekomenduje się identyfikację zasobów krytycznych dla działania kluczowych procesów OUK, oszacowanie ryzyka dla każdego z tych zasobów oraz określenie stopnia istotności objęcia monitoringiem danego zasobu.

Zasoby krytyczne powinny być wskazane po analizie uwzględniającej m.in. szacowanie ryzyk dla całej organizacji, to jest jej celów, otoczenia biznesowego itp. Następnie dla krytycznych zasobów powinno być przeprowadzone szczegółowe szacowanie ryzyk.

Rekomendowane jest monitorowanie zasobów oraz ruchu pomiędzy nimi, w tym zalecana jest automatyzacja monitoringu oraz scentralizowanie do jednego systemu zarządzającego.

Ze względów bezpieczeństwa zarówno w obszarze cyberbezpieczeństwa, jak i bezpieczeństwa realizacji celów organizacji należy wdrożyć monitorowanie zasobów i komunikacji między nimi.

Zalecana jest centralizacja zarządzania monitoringiem w celu zwiększenia skuteczności analizy dużej ilości danych, jak i umożliwienie analizy w czasie rzeczywistym (np. wdrożenie SIEM).

Monitoring powinien być realizowany z uwzględnieniem analizy elementów i zdarzeń na poszczególnych warstwach sieci (OSI, tj. warstwa aplikacji, transportowa, sieciowa, itd.).

Zalecane jest śledzenie trendów w zakresie pracy poszczególnych sieci w celu przewidywania późniejszych ograniczeń zasobów (np. przepełnienie stosów protokołów).

Rekomendowane jest wydzielenie sieci wewnętrznej do realizacji zadań w zakresie monitorowania sieci.

Ze względów bezpieczeństwa system monitoringu powinien być odseparowany od sieci monitorowanej oraz sieci zewnętrznych (Internetu). Budowa systemu monitorowania powinna posiadać nadmiarowość w celu eliminacji pojedynczych punktów awarii.

Ze względu na konieczność zabezpieczenia zbieranych informacji o stanie i działaniu sieci, należy wykorzystać mechanizmy, takie jak diody danych (przekazywanie danych tylko w jedną stronę) oraz systemy archiwizacji zebranych informacji. Diody danych separują sieci fizycznie (jest to także izolacja galwaniczna) oraz fizycznie zapewniają jednokierunkowość transmisji, co, innymi słowy, pozwala na przepływ informacji między sieciami tylko w jednym kierunku.

Uwzględniając fakt, że zagrożenia bezpieczeństwa mogą także dotyczyć systemu monitoringu, zalecane jest wdrożenie rozwiązań umożliwiających monitorowanie oraz analizę zdarzeń w zakresie samych działań związanych z monitoringiem (np. informacje o dostępie do danych z urządzeń, analiza wadliwości wdrożonych funkcjonalności monitoringu).

Rekomendowane jest wdrożenie funkcjonalności umożliwiającej zbieranie i korelację zdarzeń w czasie rzeczywistym na podstawie zebranych informacji. System powinien także zbierać dane z wielu źródeł, a także uwzględniać dane przekazywane off-line uzyskane z odseparowanych sieci.

System monitorowania powinien móc realizować zadanie korelacji zdarzeń w czasie rzeczywistym (funkcjonalność systemu SIEM) – szerzej w rozdziale 13.1.

Rekomendowane jest zbudowanie wzorcowego obrazu sieci (ruchu) w prawidłowo działających sieciach, mające na celu m.in. zwiększenie możliwości wykrywania zdarzeń na podstawie anomalii względem wzorca.

Wskazane jest zbudowanie modelu analitycznego wynikającego z mapy komunikacji systemów o znane porty, usługi i urządzenia, który byłby poszerzany dynamicznie w zakresie rejestrowanego normalnego ruchu, w celu łatwego wykrywania anomalii (ruchu odbiegającego od wzorca np. w postaci ruchu wygenerowanego przez intruza).

Rekomendowane jest wdrożenie narzędzi do monitorowania, które będzie miało możliwość reagowania na wykryte zdarzenia (alarm czy też działania defensywne w czasie rzeczywistym).

Narzędzie do monitoringu powinno umożliwiać ostrzeganie oraz reakcję na zidentyfikowane niepożądane działanie lub anomalię. Narzędzie to powinno posiadać takie funkcjonalności jak: monitorowanie anomalii wskazujących podejrzaną aktywność, reagowanie w przypadku zarejestrowania takich anomalii (IDS, np. alerty), korelację zdarzeń, wykrywanie nietypowych dostępów i ruchów do sieci czy też nieautoryzowane zmiany konfiguracji, analizę przyczyn zdarzeń (SIEM), a przy atakach – możliwość odcięcia zagrożonego obszaru, ale również możliwość utrzymania procesu świadczenia usługi w przypadku ataku na urządzenie sieciowe (IPS) oraz możliwość wyodrębnienia fragmentu sieci do przeprowadzenia testów i analizy działania podejrzanego wykrytego pakietu.

Rekomendowane jest aktualizowanie informacji dot. procesu monitorowania zasobów w sieci oraz aktualizacja danych po każdej zmianie w zidentyfikowanych do monitorowania obszarach.

Aby zachować akceptowalny poziom bezpieczeństwa, należy wskazać częstotliwość aktualizacji informacji dotyczącej składowych sieci oraz jej pracy. Dodatkowo, zaleca się aktualizację informacji przy każdej zmianie w obszarach monitorowanych (tj. przy zmianie ruterów, aplikacji użytkowych na stacjach roboczych czy urządzeń końcowych). A także ponowną analizę elementów krytycznych i niezbędnych do włączenia w zakres monitorowania.

W przypadku, gdy jest ograniczona możliwość monitorowania sieci, ze względu np. na monitorowanie sieci odseparowanych fizycznie, zalecane jest wykorzystanie innych metod zbierania informacji do uzupełnienia informacji dotyczących bezpieczeństwa zdarzeń w sieci w czasie rzeczywistym.

Ze względu na to, że w sieciach OT nie zawsze jest możliwe monitorowanie poszczególnych komponentów sieci (czy też monitorowania ich stanu), to monitoring powinien być wzbogacony o dodatkowe elementy monitorujące, jak np. kamery CCTV (telewizję przemysłową) ustawione w pomieszczeniach technicznych czy też czujniki badające parametry środowiskowe (np. pomiar napięcia układu podłączonego do elementu w sieci odseparowanej fizycznie, temperatury itp.).

Dowody kontroli:

- *dokumenty potwierdzające ustanowienie struktur odpowiedzialnych za realizację monitoringu sieci i systemów informacyjnych, w tym wykonywanie ocen bezpieczeństwa (testów penetracyjnych),*
- *dowody przeprowadzonych w przeszłości ćwiczeń cyberbezpieczeństwa,*
- *dokumentacja dotycząca narzędzi wykorzystywanych do stałego monitoringu sieci i systemów informacyjnych,*
- *raporty z monitoringu sieci łączności elektronicznej i krytycznych systemów informacyjnych.*

12. Bezpieczeństwo systemów informacyjnych

12.1. Ochrona danych

Współczesne systemy biznesowe IT wymagają zwykle łączności z siecią OT, aby móc uzyskać dostęp do danych operacyjnych lub wyeksportować dane do zewnętrznych systemów zarządzania. Systemy SCADA są włączane do infrastruktury, której przez wzgląd na oczekiwania biznesowe nie da się w pełni odizolować od środowisk publicznych. Elementy sieci OT, takie jak serwery obsługujące raporty oraz stacje kontrolne, często umieszczane są w sieci biznesowej (IT), z połączeniem do sieci OT, a nie bezpośrednio w sieci OT. Przestały być systemami całkowicie wyizolowanymi i stają się częścią infrastruktury działającej w oparciu o protokół IP. Taka ewolucja usprawnia działanie oraz zarządzanie systemami przemysłowymi, a jednocześnie eksponuje je na zagrożenia, z uwagi na dotychczas zakładany wyizolowany charakter systemów przemysłowych[134].

Rekomendowana jest identyfikacja danych dot. systemów IT/OT, szczególnie tych „wrażliwych", na podstawie analizy ryzyka przeprowadzonej w organizacji uwzględniające oprócz wrażliwości z poziomu realizowanych zadań także przepisy prawa (m.in. RODO, dot. infrastruktury krytycznej).

W przypadku systemów przemysłowych IT/OT identyfikacja powinna dotyczyć przetwarzanych danych na wszystkich warstwach systemu informacyjnego (patrz także rozdział 11.1), a więc:

- danych na temat eksploatacji i produkcji: obejmuje to informacje o działaniu systemu IIoT i danych produkcyjnych, takich jak dane z czujników, dane DCS i SCADA itp.,
- informacji o urządzeniu: obejmuje to informacje takie jak model, typ, konfiguracja, wersja oprogramowania układowego, status, adres IP, lokalizacja fizyczna itp.; spis zasobów zawiera te informacje o wszystkich urządzeniach systemowych,
- informacji o użytkowniku, a więc takich informacji jak imię i nazwisko, rola, uprawnienia itp.

Dodatkowo w przypadku systemów przemysłowych należy uwzględnić występowanie analityki Big Data. Termin ten opisuje proces badania ogromnych ilości różnych zestawów danych generowanych w czasie rzeczywistym przez inteligentne czujniki, urządzenia, pliki dziennika, wideo i audio. Dane te są tworzone na wszystkich poziomach automatyzacji, w tym w zakładach produkcyjnych, aplikacjach transakcyjnych itp. Big Data jest analizowane w celu wykrycia ukrytych wzorów, nieznanych korelacji, trendów i innych przydatnych informacji, które mogą pomóc w podejmowaniu bardziej świadomych i przemyślanych decyzji[135].

[134] Na podstawie *Cyberbezpieczeństwo. Zarys wykładu*, red. naukowa C. Banasiński, Warszawa 2018 i Poradnik dobrych praktyk w zakresie cyberbezpieczeństwa urządzeń podlegających dozorowi technicznemu, Zespół ds. cyberbezpieczeństwa Urząd Dozoru Technicznego, 2021 r.,

[135] Good Practices for Security of Internet of Things in the context of Smart Manufacturing, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Listopad 2018 r.,

Analiza ryzyka bezpieczeństwa informacji powinna zostać przeprowadzona pod kątem utraty poufności, integralności, dostępności i autentyczności (szczegółowo opisane w rozdziale 4.3) z uwzględnieniem wymagań prawnych, wartości, wrażliwości na ujawnienie lub niewłaściwe wykorzystanie i krytyczności.

Przy analizie ryzyka należy zdefiniować poziomy wrażliwości danych, w tym danych osobowych i dokonać przypisania poziomów ochrony oraz właściwego poziomu dostępu.

Rekomendowane jest stworzenie procedur/instrukcji dotyczących zasad postępowania z danymi w czasie ich przetwarzania, przechowywania, kopiowania czy też transmisji, a także zasad postępowania z nośnikami na których znajdują się dane (urządzenia w sieci, urządzenia końcowe, nośniki zewnętrzne, itp.).

Zaleca się opracowanie procedur dot. ochrony informacji w zakresie sposobu postępowania z nimi jak i ich przechowywania. Dodatkowo zaleca się, zgodnie z klasyfikacją dokonaną na podstawie analizy ryzyka, wprowadzenie zasad oznaczania informacji i sposobu postępowania. Istotne jest także zapewnienie jednoznacznej identyfikacji użytkownika w zakresie dostępu do danych, w tym danych osobowych, a także stosowanie zasady minimalnego niezbędnego dostępu (szczególnie przy dostępie do danych stron trzecich) i kontroli oraz monitorowania dostępu do danych. Przy tworzeniu lub modyfikowaniu systemów rekomendowane jest uwzględnienie mechanizmów działań z danymi wynikających z przepisów prawa (np. RODO – mechanizmy anonimizacji danych, czy też prawo do zapomnienia, jeżeli tego prawa nie ograniczają inne przepisy) oraz mechanizmów zabezpieczeń, np. poprzez odpowiednią budowę bazy danych, możliwości i sposoby kategoryzacji ról, monitorowania dostępu oraz aktualności uprawnień. W przypadku dostępu stron trzecich do danych należy stosować zasadę minimalizacji uprawnień.

Rekomendowane jest stworzenie procedur dotyczących kopii zapasowych.

Zalecane jest wdrażanie zasad bezpieczeństwa w zakresie tworzenia, usuwania oraz przechowywania kopii zapasowych zarówno na poziomie administratora, jak i zwykłych użytkowników.

Rekomendowane jest udoskonalanie systemu w zakresie bezpieczeństwa danych we współpracy z pracownikami organizacji, np. poprzez przeprowadzanie cyklicznych szkoleń lub też budowanie systemu wymiany informacji między kierownictwem a pracownikami m.in. w celu uzyskiwania informacji o lukach bezpieczeństwa danych w działającym systemie.

Wskazane jest także wprowadzenie obowiązkowego zapoznania się pracowników z zasadami zachowania bezpieczeństwa informacji i uczestnictwa w regularnych szkoleniach z zakresu procedur organizacji oraz wiedzy o ogólnych zagrożeniach. Ponadto, powinno się włączyć pracowników w proces cyklicznej analizy bezpieczeństwa danych, w tym ochrony bezpieczeństwa danych osobowych.

Dowody kontroli:

- *właściwie udokumentowana i zatwierdzona przez kierownictwo wyższego szczebla procedura bezpieczeństwa informacji,*
- *dostosowane i udokumentowane konta administracyjne z określonymi uprawnieniami dostępu przyznanymi stosownym pracownikom,*
- *upoważnienia do przetwarzania danych osobowych (jeśli są przetwarzane w systemie),*
- *szczegółowy spis obejmujący zasoby sprzętowe i programowe wykorzystywane do celów administracyjnych,*
- *wyspecjalizowany personel jest odpowiedzialny za zarządzanie i konfigurację danych.*

12.2. Zarządzanie uprawnieniami

W związku ze znacznym zróżnicowaniem rzeczywistości organizacyjnej oraz technologicznej OUK, która częściowo warunkowana jest rodzajami systemów służących do świadczenia usługi kluczowej, wskazane zalecenia powinny być stosowane tam, gdzie ich implementacja będzie możliwa i zasadna.

W zakresie zarządzania uprawnieniami rekomendowane jest wprowadzenie polityki dotyczącej nadawania, modyfikowania i odbierania uprawnień oraz nadzorowania tych działań.

Uprawnienia powinny być nadawane zgodnie z polityką, w minimalnym zakresie niezbędnym do realizacji zadań, w sposób ustrukturalizowany, przy akceptacji wskazanych w polityce ról, np. akceptacji przez przełożonego pracownika, osoby pełniącej rolę pełnomocnika do spraw bezpieczeństwa informacji oraz administratora systemu. W polityce należy uwzględnić także zasady związane z dostępem do systemu przez strony trzecie, np. nadanie uprawnień poprzez podpisanie imiennej umowy z zewnętrznym pracownikiem w odpowiednim zakresie dostępu.

Rekomendowane jest stworzenie procedur dotyczących nadawania/odbierania uprawnień, ich aktualizowania, regularnego ich przeglądu z równoczesnym wskazaniem osób/ról odpowiedzialnych za realizację tych zadań.

Wskazane jest wykorzystanie systemu zarządzania tożsamością integrującego zarządzanie zakresem uprawnień w całej organizacji lub też stworzenie mechanizmów, które automatyzowałyby aktualizację informacji o uprawnieniach, np. w przypadku, gdy pracownicy kończą stosunek pracy z organizacją lub też następuje zmiana zakresu ich zadań i w związku z tym, powinny być im odebrane lub zmodyfikowane uprawnienia w określonym czasie. Należy także wdrożyć mechanizm pozwalający na natychmiastowe odebranie uprawnień. Zalecenie powinno być implementowane w systemach, których charakterystyka na to pozwala lub nie spowoduje negatywnych efektów.

Rekomendowane jest by uprawnienia były nadawane zgodnie z zasadą minimalnego dostępu określonego przez zakres realizowanych zadań.

Należy zweryfikować dostęp do systemów oraz danych do zakresu realizacji zadań przez użytkowników. Wskazane jest wydzielenie osobnych kont administracyjnych dla obszarów takich jak: zarządzanie stacjami roboczymi, zarządzanie domenami czy też zarządzanie urządzeniami serwerowymi. Zalecane jest by działania te zostały sformalizowane w postaci procedur.

*Rekomendowane jest wdrożenie rozwiązań dotyczących jednoznacznej identyfikacji użytkowników***.**

Należy wdrożyć rozwiązania techniczne oraz organizacyjne, które pozwolą na jednoznaczną identyfikację użytkownika, np. poprzez imienne konta dostępowe. W sytuacji, gdy nie ma możliwości korzystania z kont imiennych, zalecane jest wdrożenie dodatkowych mechanizmów kontrolnych wraz z procedurami pomocniczymi, np. prowadzenie książki pracy z informacjami o harmonogramie prac operatorów. Dodatkowo, w infrastrukturze OT występują problemy związane z kontami grupowymi i dostępem przez konto *root*. Ze względu na specyfikę tych rozwiązań, nie zawsze istnieje możliwość zmiany, w związku z tym zaleca się zwrócić szczególną uwagę na kwestię zabezpieczenia kont grupowych.

W przypadku kont zakładanych na potrzeby firm zewnętrznych, należy w miarę możliwości stosować konta imienne lub inne mechanizmy jednoznacznej identyfikowalności użytkowników zewnętrznych. Zalecenia powinny być wdrożone w systemach, których charakterystyka pracy to umożliwia, a zaimplementowanie rekomendacji nie wpłynie np. na ciągłość działania.

Dla kont administratorskich rekomendowane jest nadawanie uprawnień administratorom tylko w systemach im podlegających oraz ograniczeniu możliwości dostępu do danych przetwarzanych w systemach.

W celu ograniczenia zagrożeń w postaci nadmiernych działań lub możliwości przejęcia kontroli przy ataku nad wieloma systemami i obszarami równocześnie należy wdrożyć procedury nadawania uprawnień administratorskich tylko w zakresie zadań pracownika, a także ograniczyć dostęp do danych wytwarzanych w systemach, do których administrator nie powinien mieć wglądu.

Rekomendowane jest wdrożenie zasady wielopoziomowego uwierzytelnienia dostępu, szczególnie do kont administratorskich.

Przy realizacji dostępu do systemu zaleca się wprowadzanie uwierzytelniania, a tam gdzie jest to możliwe, to uwierzytelnienia wielopoziomowego (np. weryfikacji dwuetapowej).

Rekomendowane jest stworzenie procedur dotyczących zastępstw w sytuacjach zarówno planowanych, jak i o charakterze nagłym, zarówno dotyczących kont administratorskich, jak i zwykłych użytkowników, wraz z rejestrowaniem takich zdarzeń, przeglądem rejestrów i ich odpowiednim przechowywaniem.

W celu kontroli dostępu, należy wprowadzić procedury dotyczące zastępstw, szczególnie w zakresie prac na kontach administracyjnych lub dyspozytorskich. Należy także uwzględniać je przy regularnych przeglądach dotyczących bezpieczeństwa dostępu do systemów oraz chronić przed utratą.

Rekomendowane jest prowadzenie rejestru prac w systemach oraz dokonywanych zmian, ich regularny przegląd oraz odpowiednie zabezpieczenie przed utratą.

W celu monitorowania prac oraz zmian w systemach, należy prowadzić rejestry działań realizowanych przez administratorów, operatorów czy użytkowników w systemach, a w przypadku administratorów i operatorów wraz z nagrywaniem sesji. Powinno się wprowadzić procedury w zakresie regularnego przeglądu takich tych zapisów wraz z odpowiednim ich zabezpieczeniem przed nieuprawnioną modyfikacją bądź utratą.

Dowody kontroli:

- *dokumentacja dotycząca zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym procedury nadawania, zmiany i odbierania uprawnień do pracy w systemach teleinformatycznych i dowody wykonywania ww. procedur typu: rejestry uprawnień, dowody regularnych przeglądów uprawnień dla ról/użytkowników, w tym upoważnienia do przetwarzania danych osobowych (jeśli są przetwarzane w systemie),*
- *udokumentowany proces zarządzania kontami administracyjnymi,*
- *dostępne dzienniki aktywności kont administratorów.*

12.3. Kontrola dostępu do danych

Organizacja powinna stworzyć procedury (polityki) zarządzania uprawnieniami i dostępem do systemów dla pracowników organizacji, a także sposobu wnioskowania o dostęp oraz ustalonej ścieżki akceptacji. Przygotowane dokumenty powinny obejmować role, grupy, uprawnienia dostępu, procedury przyznawania i cofania uprawnień. W celu zapewnienia większej przejrzystości przyznanych praw, zaleca się stworzenie m.in. matrycy związanej z kontrolą dostępu, np. matryca kontrolna podziału obowiązków, kontrola dostępu zdalnego itp. Przy opracowaniu procedur zarządzania dostępem, należy mieć na uwadze konieczność restrykcyjnego podejścia do przydzielania uprawnień, co wiąże się z zasadnością ograniczania praw dostępu do systemów, sieci lub ich części tam gdzie to możliwe[136].

W celu uregulowania oraz określenia jasnych zasad przydzielania dostępu do systemów, organizacja powinna przygotować, wdrożyć oraz regularnie aktualizować procedurę zarządzania dostępem do danych oraz zarządzania uprawnieniami. Uprawnienia powinny być nadawane po wysłaniu wniosku w systemie i jego akceptacji przez ustaloną osobę. Modyfikacja, zawieszenie, przywrócenie lub usunięcie dostępu dla użytkownika również powinno odbywać się na podstawie wniosku. Zakres przyznanych uprawnień powinien być adekwatny do zajmowanego stanowiska. W celu zapewnienia kompleksowej efektywności stworzonych procedur, powinny być one regularnie weryfikowane i aktualizowane. Zakres przyznanych uprawnień powinien być adekwatny do zajmowanego stanowiska i do obowiązków z niego wynikających. Zaleca się utworzenie grup użytkowników. Dodatkowo, przy określaniu zakresów uprawnień, należy zwrócić uwagę, aby korzystanie z uprzywilejowanych programów narzędziowych, które umożliwiają obejście zabezpieczeń systemów i aplikacji, było ściśle nadzorowane oraz ograniczane.

Należy stworzyć procedurę zarządzania dostępem do systemów dedykowaną dostawcom usług – stronom trzecim.

W przypadku nadawania dostępu podmiotom zewnętrznym, zaleca się, aby każde takie działanie było umocowane w sposób formalny, np. umową. Ponadto, gdy umowa jest zwarta na określony czas, należy ściśle przestrzegać terminów cofnięcia uprawnień. W sytuacji, gdy umowa zawarta jest na dłuższy okres, organizacja powinna umieścić w opracowywanej procedurze cykliczną weryfikację uprawnień, nawet w przypadku trwania umowy. Zaleca się, aby organizacja przy określaniu dostępu sprecyzowała i wskazała pracownikowi lub osobie trzeciej względem organizacji, które obowiązki pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, a także określiła sposób ich egzekwowania.

Organizacja powinna cyklicznie weryfikować prawa dostępu do systemów i sieci, zgodnie z przygotowanym harmonogramem. Powinno się także przeprowadzać doraźne weryfikacje przyznanych uprawnień. Dodatkowo, powinny zostać określone zasady usuwania nieaktywnych/nieużywanych kont.

W przypadku zmian kadrowych lub innych zmian, które mogą mieć wpływ na zasadność przyznanych uprawnień, powinno się dokonać doraźnej weryfikacji. Ponadto, czynności te powinny być wykonane zgodnie z założonym harmonogramem i nie powinny być uzależnione wyłącznie od zaistnienia ewidentnej potrzeby modyfikacji dostępu na skutek, np. zmian kadrowych. Wraz z rozwiązaniem stosunku pracy z pracownikiem, dostępy powinny być natychmiastowo odbierane. Ponadto, w pro-

[136] RCB, *Narodowy Program Ochrony Infrastruktury Krytycznej Załącznik 1*, s. 82.

cesie sprawdzania aktualności przyznanych dostępów, powinno się również weryfikować poprawność przydzielonych już dostępów.

Dodatkowo zaleca się, aby w przypadku zmiany przełożonego (osoby, która akceptowała lub wnioskowała o uprawnienia dla pracowników podległych), nowy przełożony rozpoczął proces weryfikacji nadanych uprawnień i ich zakresów osobom, które są w jego kompetencji nadzorczej. Gdy nie będzie miało to wpływu na ciągłość działania, zaleca się wdrożenie mechanizmu odwołania uprawnień po zmianie przełożonego do czasu złożenia ponownie wniosków przez nowego przełożonego.

W razie możliwości zaleca się skonfigurowanie, w systemach obsługujących usługę kluczową, dedykowanych kont administracyjnych z dostępem dla administratorów przeprowadzających konkretne operacje, np. konserwacje, instalacje. Ponadto, proces zarządzania kontami administracyjnymi powinien być udokumentowany, a także powinny być dostępne dzienniki aktywności kont administratorów. Zaleca się stworzenie dostosowanych i udokumentowanych kont administracyjnych z określonymi uprawnieniami dostępu przyznanymi właściwym pracownikom[137].

Tylko konta administratorskie powinny mieć dostęp do danych administracyjnych w systemach, konta powinny być imienne i nie powinny mieć dostępu do danych wykorzystywanych w systemach. Ponadto, zaleca się, aby konta administratorskie posiadały uprawnienia jedynie w systemach im podlegających. Powinien być stworzony szczegółowy spis obejmujący zasoby sprzętowe i programowe wykorzystywane do celów administracyjnych.

Należy unikać stosowania kont współdzielonych i zamiast nich stosować konta imienne dla administratorów oraz użytkowników.

Nie powinno się dopuścić do sytuacji w której kilku użytkowników korzysta z jednego konta współdzielonego, na przykład w przypadku pracy zmianowej. Każdy z użytkowników powinien mieć konto imienne, skonfigurowane zgodnie z zasadami określonymi m.in. w stworzonej polityce przyznawania dostępów. Na ten aspekt należy zwrócić uwagę szczególnie w przypadku paneli dyspozytorskich.

Powinno unikać się przyznawania dostępu „na chwilę", na czas wykonania jednej, konkretnej czynności lub zadania.

Przyznawanie dostępów „na chwilę" może być utożsamiane z pewnego rodzaju zagrożeniem. W związku z tym, zaleca się unikać tego typu sytuacji. Jednak, w przypadku zaistnienia konieczności udzielenia takiego dostępu, powinien on być udzielony z czasowym ograniczeniem kontrolowanym automatycznie lub manualnie.

W razie możliwości zaleca się wdrożenie narzędzi umożliwiających wspieranie procesów zarządzania dostępem fizycznym i logicznym oraz odpowiedniej separacji dostępów w zależności od poziomu uprawnień.

Narzędzia powinny uwzględniać możliwość m.in. automatycznego odbierania dostępów, cyklicznego wymuszania przeglądów uprawnień. Dodatkowo, zaleca się wdrożenie rozwiązań umożliwiających zarządzanie uprzywilejowanym dostępem. Powyższe procedury powinny określać również zasady dostępu do systemów w sposób zdalny (patrz pkt. 12.4).

[137] *RCB, Standardy i dobre praktyki ochrony infrastruktury krytycznej – automatyka przemysłowa w sektorze elektroenergetycznym*, s. 19.

Przydzielanie haseł do tworzonych kont, powinno funkcjonować jako formalny proces, który pozwoli na sprawowanie kontroli nad tą czynnością.

Pracownicy powinni podpisywać zobowiązania do zachowania haseł w tajemnicy, takie zobowiązanie może być integralną częścią np. umowy o pracę. Dodatkowo, w projektowanym procesie należy uwzględnić wymuszenie zmiany hasła przy pierwszym logowaniu, a także okresowe zmiany hasła. W przypadku konieczności przyznawania haseł tymczasowych, czynność ta powinna być zakończona potwierdzeniem odbioru takiego hasła przez pracownika. Co najważniejsze, wymagania względem haseł powinny odpowiadać standardom zwiększającym ich odporność na odszyfrowanie w przypadku wycieku. Należy sprecyzować minimalne wymagania dla haseł, określające ich minimalną długość, minimalną liczbę różnych typów znaków, określić wyrazy niedozwolone (np. imię, nazwisko pracownika, adres, numer telefonu, a także modyfikacje haseł używanych w przeszłości)[138].

Zaleca się wdrożenie kontroli dostępu do sieci poprzez m.in. zastosowanie odpowiedniej architektury sieci (np. wirtualnych sieci lokalnych), a także wdrożenie systemów NAC.

Separacja ruchu sieciowego poprzez wydzielenie wirtualnych sieci lokalnych (sieci VLAN) jest jedną z metod wpływających na kontrolę dostępu. Ponadto, zaleca się zastosowanie kontroli ruchu na podstawie adresów MAC oraz opracowanie polityki filtrowania pakietów IP. Należy również rozważyć wdrożenie metodyki weryfikacji klienta podczas dostępu do sieci, pod kątem posiadania przez niego aktualizacji zgodnych z założeniami administratora (patrz rozdział 11.1). W przypadku negatywnego wyniku, klient powinien być przekierowany do innej podsieci celem dokonania niezbędnej aktualizacji.

Dowody kontroli:

- *regulamin kontroli dostępu obejmujący role, grupy, uprawnienia dostępu, procedury przyznawania i cofania uprawnień dostępu do systemów informacyjnych,*
- *określone zasady dotyczące usuwania nieaktywnych/nieużywanych kont,*
- *matryce związane z kontrolą dostępu (np. matryca kontrolna podziału obowiązków, kontrola dostępu zdalnego itp.),*
- *rozdział dotyczący uprawnień dostępu zawarty w regulaminie/procedurach kontroli dostępu,*
- *wykaz mapowania praw dostępu do odpowiednich zasobów bądź procesów zawartych w regulaminie kontroli dostępu.*

[138] J. Krawiec, G. Ożarek, *System Zarządzania Bezpieczeństwem Informacji w Praktyce. Zabezpieczenia*, Polski Komitet Normalizacyjny, Warszawa 2014, s. 45.

12.4. Dostęp zdalny i urządzenia mobilne

W kontekście obecnego podejścia do zdalnego dostępu można wyróżnić trzy aspekty – pracę zdalną i konieczność zapewnienia dostępu do zasobów przedsiębiorstwa pracownikom przebywającym poza siedzibą firmy, dostęp zdalny zapewniony stronom trzecim oraz zdalny dostęp do urządzeń i systemów OT. Upowszechnienie pracy zdalnej zwiększyło się pod wpływem pandemii koronawirusa SARS-CoV-2, w czasie której, w bardzo krótkim czasie, duża część pracowników została wysłana na pracę zdalną. W rezultacie, operatorzy usług kluczowych stoją przed wyzwaniem, jakim jest zapewnienie bezpieczeństwa zdalnego dostępu i urządzeń mobilnych (np. laptopów, tabletów, smartfonów itd.).

Zaleca się by dostęp do zasobów przedsiębiorstwa odbywał się poprzez szyfrowane kanały, a także by stosowane było uwierzytelnienie wieloskładnikowe.

W celu zagwarantowania bezpieczeństwa dostępu do zasobów operatora, powinno się wybrać odpowiednie protokoły szyfrujące (takie jak np. TLS[139] – ang. *Transport Layer Security*), odporne na ataki kryptograficzne. Zaleca się również stosowanie uwierzytelnienia wieloskładnikowego (ang. *multi-factor authentication* – MFA). MFA ma na celu zapewnienie dodatkowej ochrony i weryfikacji użytkownika w czasie logowania. Gdy użytkownik chce uzyskać dostęp do zasobów przedsiębiorstwa, wówczas przeprowadzana jest dodatkowa weryfikacja w oparciu o dane biometryczne (np. odcisk palca), token, kod SMS, połączenie głosowe, klucz zewnętrzny itp. W ten sposób eliminuje się ryzyko nieuprawnionego dostępu poprzez posiadanie wyłącznie loginu i hasła (zwłaszcza w przypadku wycieku danych bądź zainstalowania oprogramowania szpiegującego). W ten sposób, użytkownik dokonuje podwójnej weryfikacji swojej tożsamości, gdyż poza znanym mu hasłem, musi wprowadzić dodatkowe dane do logowania, które są wcześniej ustalone w ramach polityki bezpieczeństwa danego podmiotu[140].

W ramach pracy zdalnej zaleca się by pracownicy pracowali na sprzęcie firmowym wykorzystującym wirtualne sieci prywatne (ang. Virtual Private Network – VPN) oraz by był on odpowiednio zaopatrzony w niezbędne oprogramowanie (służące do pracy i chroniące dane urządzenie mobilne).

Zastosowanie VPN na urządzeniach mobilnych jest zalecane, ponieważ VPN tworzy prywatny, szyfrowany kanał do dostawcy usługi VPN, którą wybrał dany operator, chroniąc w ten sposób prywatność danego użytkownika. W rezultacie generowany ruch jest dużo trudniejszy do monitorowania przez np. cyberprzestępców. VPN pozwala na bezpieczny dostęp do zasobów danego przedsiębiorstwa, umożliwiając w ten sposób realizację zadań przez pracowników. Operator usługi kluczowej powinien wybrać zaufanego dostawcę usługi VPN, co zagwarantuje bezpieczeństwo komunikacji pomiędzy urządzeniami mobilnymi a zasobami firmy. Przy wyborze dostawcy VPN należy zwrócić uwagę m.in. na:

- sposób logowania do usługi VPN – powinno się zwrócić uwagę na to, by usługa stosowała uwierzytelnienie wieloskładnikowe, a także by operator mógł przechowywać logi przez okres zgodny z politykami retencji danych uwierzytelniających, logowania itp.,

[139] TLS – ang. *Transport Layer Security*, protokół zapewniający integralność i poufność przesyłanych danych w Internecie, a także pozwalający na odpowiednie uwierzytelnienie serwera i klienta. Patrz szerzej: RFC 8446 – The Transport Layer Security (TLS) Protocol Version 1.3. – https://datatracker.ietf.org/doc/html/rfc8446 [dostęp: 14.05.2021].

[140] *Zabezpieczanie dostępu do zasobów za pomocą uwierzytelniania wieloskładnikowego*, Microsoft, https://www.microsoft.com/pl-pl/security/business/identity-access-management/mfa-multi-factor-authentication [dostęp: 14.05.2021].

– lokalizację siedziby przedsiębiorstwa – zaleca się by operator usługi kluczowej upewnił się, że dostawca usługi VPN rezyduje i posiada infrastrukturę w kraju zapewniającym prawo do prywatności,
– lokalizację serwerów – zwrócić uwagę na umiejscowienie serwerów w celu zapewnienia najkrótszych tras komunikacyjnych w publicznej sieci Internet,
– kompatybilność danego rozwiązania z już zainstalowanym oprogramowaniem na urządzeniach mobilnych[141].

Dodatkowo, w celu zabezpieczenia samych urządzeń mobilnych zaleca się zainstalowanie na nich oprogramowania antywirusowego oraz odpowiednią konfigurację firewall.

Operator usługi kluczowej musi być pewny, że wybrane korporacyjne rozwiązanie VPN skaluje się i jest w stanie utrzymać dużą liczbę połączeń jednocześnie. Wszystkie aplikacje biznesowe powinny być dostępne za pośrednictwem zaszyfrowanych kanałów komunikacji, taki jak np. SSL VPN, IPSec VPN i inne[142].

Zaleca się by operatorzy usług kluczowych zmieniali domyślne hasła i nazwy użytkowników skonfigurowane w poszczególnych urządzeniach, w tym w urządzeniach mobilnych. Rekomenduje się opracowanie stosownej polityki zarządzania hasłami – sposoby ich tworzenia, wymagania co do ich złożoności (np. ilość znaków, wielka litera, znak specjalny itd.), a także wymuszali na użytkownikach regularną zmianę haseł. Operator powinien zapoznać cały personel z wewnętrzną polityką zarządzania hasłami.

Jednym ze słabych punktów całej architektury sieci mogą być urządzenia, które nie mają zmienionych domyślnie ustawionych nazw użytkowników i haseł (np. login: *admin*, hasło *admin* itd.). Zaleca się, by w przypadku podłączenia nowego urządzenia do sieci zaktualizować login i hasło w sposób zgodny z wewnętrzną polityką zarządzania hasłami. Z racji tego, rekomenduje się by każdy operator opracował taki dokument, w którym zostaną ustalone zasady tworzenia haseł, wymagania co do ich złożoności (w tym np. uwzględnienie wielkiej litery, znaku specjalnego itd.) oraz harmonogram ich aktualizacji. Posiadając taki dokument, operator usługi kluczowej może zapoznać personel z przyjętą polityką, a także ograniczyć ryzyko tworzenia prostych haseł przez użytkowników[143].

Rekomenduje się by operator usługi kluczowej dokonał segregacji dostępu zdalnego poprzez np. opracowanie zestawu zasad komunikacji zdalnej.

Zestaw zasad komunikacji zdalnej powinien zawierać informację o tym, do których systemów można mieć zdalny dostęp. Rozróżnienie powinno zostać opracowane na podstawie przeprowadzonej analizy ryzyka i technicznych możliwości. Powinny zostać opracowane mechanizmy dostępu do środowiska danego przedsiębiorstwa. Dokument powinien również zawierać informację o wymaganych uprawnieniach dostępu do poszczególnych systemów (szerzej ta tematyka została opisana w rozdziałach 12.2 i 12.3). W ramach zasad komunikacji zdalnej powinny również znaleźć się kwestie dotyczące możliwości rejestracji ruchu generowanego przez użytkowników łączących się z systemami zdalnie, jak również zakres odpowiedzialności poszczególnych użytkowników tych systemów[144].

[141] *Wirtualne Sieci Prywatne (VPN)*, OUCH! Security Awareness Newsletter Biuletyn Bezpieczeństwa Komputerowego, lipiec 2019, SANS Institute, przekład CERT Polska, https://www.sans.org/sites/default/files/2019-06/201907-OUCH-July-Polish.pdf [dostęp: 21.05.2021].
[142] *Tips for cybersecurity when working from home*, ENISA, https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home [dostęp: 26.05.2021].
[143] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, ENISA 2017, [PDF] s. 50, 71, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot [dostęp: 21.05.2021].
[144] Good Practices for Security of Internet of Things in the context of Smart Manufacturing, ENISA, 2018, [PDF], s. 42, 86-87, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot [dostęp: 25.05.2021].

W celu kontroli dostępu zaleca się stworzenie tzw. „czarnych list", które zawierają informacje na temat adresów e-mail, IP czy domen, które nie powinny być dozwolone w ruchu przychodzącym do sieci danego przedsiębiorstwa.

Jednym z elementów ochrony przez złośliwym oprogramowaniem jest zdefiniowanie adresów e-mail, IP czy domen, które są traktowane jako niebezpieczne. Często pracownicy nie są w stanie zidentyfikować fałszywych stron internetowych czy akcji phishingowych, ważna jest więc bieżąca aktualizacja takiej listy. Informacje na temat adresów e-mail rozsyłających złośliwe oprogramowanie, czy o podejrzanych adresach IP można znaleźć w biuletynach dystrybuowanych m.in. przez CSIRT GOV. To działanie może również zostać wykorzystane do ustalania praw dostępu do poszczególnych aplikacji. Możliwe jest również analogiczne opracowanie tzw. „białej listy" zawierającej informacje o akceptowanych adresach[145].

Zaleca się unikać używania dzielonych kont przez różnych użytkowników do urządzeń i systemów w celu lepszego monitorowania aktywności poszczególnych osób, a także możliwości powiązania danego działania z konkretnym użytkownikiem.

W sytuacji, gdy stosowane są dzielone konta między różnych użytkowników, to w momencie wystąpienia niepożądanego zdarzenia może dojść do rozmycia odpowiedzialności, ponieważ nie można będzie ustalić kto w danym momencie podejmował działania na współdzielonym koncie[146].

Rekomenduje się by operator usługi kluczowej opracował stosowną politykę w zakresie udzielania dostępu zdalnego podmiotom zewnętrznym.

Podmiot zewnętrzny może potrzebować zdalnego dostępu do niektórych systemów czy aplikacji w celu dokonania, np. aktualizacji czy też implementacji łatek bezpieczeństwa. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa środowiska operatora, zaleca się by objąć stosownym nadzorem i zaimplementować zabezpieczenia komunikacji dostępu dla firm serwisujących oprogramowanie lub urządzenia. Należy zauważyć, że często zdalny dostęp stron trzecich odbywa się na ich warunkach, więc zdarza się, że stosowane zabezpieczenia organizowane są tak, by serwisanci mieli łatwy dostęp, a to nie zawsze może być spójne z zabezpieczeniami stosowanymi przez operatora. W tym kontekście, zdalny dostęp stron trzecich do systemów automatyki przemysłowej powinien być przyznawany tylko w uzasadnionych przypadkach i po uprzednim dokonaniu analizy ryzyka. Jeżeli taki dostęp zostanie przydzielony firmie zewnętrznej, wówczas powinien być szczegółowo monitorowany i rejestrowany, a kanał zdalnego dostępu powinien być każdorazowo zamykany i otwierany na nowo dopiero w przypadku uprzedniego zgłoszenia przez podmiot zewnętrzny takiej potrzeby i uzyskaniu zgody osoby odpowiedzialnej za dane oprogramowanie/system/urządzenie[147].

[145] Narodowy Program Ochrony Infrastruktury Krytycznej 2020. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Rządowe Centrum Bezpieczeństwa, [PDF], s. 86, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 20.05.2021].

[146] Good Practices for Security of Internet of Things in the context of Smart Manufacturing, ENISA, 2018, [PDF], s. 72-73, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot [dostęp: 24.05.2021].

[147] Narodowy Program Ochrony Infrastruktury Krytycznej 2020. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Rządowe Centrum Bezpieczeństwa, [PDF], s. 85, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 20.05.2021].

Zaleca się by urządzenia mobilne, na których pracuje personel były odpowiednio skonfigurowane i posiadały zainstalowane oprogramowanie chroniące, jak np. program antywirusowy, firewall itp.

Urządzenia mobilne powinny być chronione przed zagrożeniami pochodzącymi z cyberprzestrzeni, jak również na wypadek ich zgubienia bądź kradzieży. Należy korzystać z blokady ekranu, którą można odblokować za pomocą numeru PIN bądź danymi biometrycznymi (np. odcisk palca). Urządzenia mobilne powinny mieć również ustawioną automatyczną aktualizację, aby dysponować najnowszym oprogramowaniem i móc automatycznie implementować poprawki bezpieczeństwa. Zaleca się również by aplikacje zainstalowane na urządzeniach mobilnych pochodziły z zaufanych źródeł, co pozwala zredukować ryzyko pobrania aplikacji ze złośliwym oprogramowaniem. Przed pobraniem konkretnej aplikacji można również zapoznać się z opiniami wystawionymi przez innych użytkowników, a także zweryfikować ilość pobrań. Rekomenduje się również, by przy instalacji aplikacji i programów sprawdzić ich ustawienia prywatności oraz do jakich danych będą miały dostęp na urządzeniu mobilnym (np. lokalizacja, książka telefoniczna, zdjęcia itd.), a następnie ograniczyć do minimum ilość zbieranych danych przez aplikacje. Użytkownicy powinni również regularnie tworzyć kopie zapasowe swoich urządzeń, aby w przypadku ich kradzieży, zgubienia bądź uszkodzenia móc odtworzyć zawartość danego urządzenia[148]. Jeżeli dany podmiot zgadza się na wykorzystanie przez swoich pracowników służbowych urządzeń mobilnych do celów prywatnych, zaleca się odseparowanie środowiska służącego do pracy od środowiska używanego do celów prywatnych. Urządzenia mobilne również powinny być zaopatrzone w programy antywirusowe, firewall i inne oprogramowanie wzmacniające ich bezpieczeństwo.

Urządzenia mobilne po zakończeniu ich eksploatacji powinny być utylizowane z zachowaniem standardów bezpieczeństwa i ochrony polityki prywatności.

Korzystając z urządzeń mobilnych, takich jak m.in. tablety, smartfony, gromadzona jest na nich duża ilość informacji dotycząca danego użytkownika, a także przedsiębiorstwa, w którym pracuje. Dane te mogą dotyczyć np. odwiedzanych lokalizacji, danych kontaktowych innych pracowników, kontrahentów i partnerów, historię połączeń i wiadomości, pocztę wraz z historią e-maili, zapisane pliki, zdjęcia czy filmy, historię przeglądanych stron internetowych, hasła zapisane do kont itp. To duży zbiór informacji, które nieodpowiednio zabezpieczone mogą być źródłem różnych nieprzewidzianych zdarzeń. Z tego powodu, przed utylizacją urządzenia należy wyczyścić je ze wszystkich ww. danych, poprzez np. przywrócenie ustawień fabrycznych, ponieważ samo ich usuniecie nie zawsze jest skuteczne. Dodatkowo, zaleca się sprawdzenie czy pamięć na urządzeniu jest szyfrowana, ponieważ przechowywanie danych w takiej postaci gwarantuje ich większe bezpieczeństwo. Należy pamiętać, że urządzenia mobilne zawierają w sobie również karty SIM (ang. *Subscriber Identity Module*), które także przechowują wiele danych, jak np. numery telefonów, a przywrócenie ustawień fabrycznych nie ingeruje w żaden sposób w dane zapisane na karcie SIM. Zatem, przed utylizacją danego urządzenia należy wyjąć kartę SIM i przenieść do innego urządzenia, a jeżeli karta SIM jest już niepotrzebna, wówczas zaleca się jej fizyczne zniszczenie. Część urządzeń może zapisywać dane również na zewnętrznych karach pamięci typu SD (ang. *Secure Digital*), wówczas przed utylizacją danego urządzenia należy przełożyć ją do innego urządzenia bądź w przypadku, gdy jest niezdatna do dalszego użytku poddać fizycznemu zniszczeniu[149].

[148] *Zabezpieczanie urządzenia mobilnego*, OUCH! Security Awareness Newsletter Biuletyn Bezpieczeństwa Komputerowego, luty 2018, SANS Institute, przekład CERT Polska, https://www.sans.org/sites/default/files/2018-02/201802-OUCH-February-Polish.pdf [dostęp: 25.05.2021].

[149] *Utylizacja urządzenia mobilnego*, OUCH! Security Awareness Newsletter Biuletyn Bezpieczeństwa Komputerowego, marzec 2019, SANS Institute, przekład CERT Polska, https://www.sans.org/sites/default/files/2019-03/201903-OUCH-March-Polish_0.pdf [26.05.2021].

W ramach zdalnego dostępu do zasobów organizacji, ważne jest również zapewnienie bezpieczeństwa wideokonferencji (dla funkcji audio i wideo, a także przesyłanych plików i komunikatorów).

W związku z tym, że zorganizowanie fizycznego spotkania w stanach epidemii, zagrożenia epidemicznego bądź w stanach nadzwyczajnych jest utrudnione, konferencje poszczególnych komórek organizacyjnych przeniosły się do cyberprzestrzeni, gdzie odbywają się widekonferencje. W czasie tych spotkań, pracownicy poruszają wiele bardzo wrażliwych tematów dotyczących organizacji, dlatego operatorzy usług kluczowych powinni zapewnić im bezpieczne narzędzia do komunikacji – wideokonferencji, przesyłania plików, czy do bieżącej wymiany wiadomości. Operator powinien zagwarantować każdemu pracownikowi dostęp do takich narzędzi, aby nie korzystali z publicznie dostępnych kanałów do komunikacji (np. media społecznościowe). Ponadto operator usługi kluczowej przy wyborze narzędzi, powinien kierować się analizą ryzyka oraz analizą pod kątem podatności, niezawodności oraz możliwości danego rozwiązania. Ponadto, należy poinformować pracowników o tym, by nie udostępniali publicznie adresów URL wirtualnych spotkań[150].

Zaleca się by w czasie pracy zdalnej, pracownicy mieli zapewniony odpowiedni poziom wsparcia technicznego (procedury, instrukcje, serwis itp.).

W celu sprawnego realizowania zadań w czasie pracy zdalnej, pracownicy powinni mieć zagwarantowany dostęp do serwisu zajmującego się oprogramowaniem i sprzętem, aby szybko rozwiązać problemy techniczne. Ponadto, personel powinien być przeszkolony z procedur i instrukcji związanych z pracą zdalną, takich jak, np. reagowanie na incydenty bezpieczeństwa i naruszenia danych osobowych, zdalna zmiana haseł dostępowych, sposób rejestracji czasu pracy itd. Dzięki znajomości tych elementów, pracownicy są w stanie sprawnie realizować swoje działania, a przy okazji zachować czujność w przypadku podejrzanych aktywności (np. gdy zadzwoni cyberprzestępca i wskaże inną procedurę zmiany hasła dostępowego)[151]. W tym kontekście ważne jest również wspieranie informatyzacji wielu procesów, w tym np. wprowadzenie podpisów elektronicznych[152].

Operator usługi kluczowej powinien również zapewnić swój personel przebywający na pracy zdalnej, że przetwarzanie danych w kontekście telepracy (jak np. rejestr czasu pracy) jest zgodne z ramami prawnymi UE dotyczącymi ochrony danych osobowych.

Odpowiednio poinformowani pracownicy wiedzą jakie przepisy są stosowane w ramach realizacji pracy zdalnej, a w rezultacie unika się ryzyk naruszeń[153].

Pracownicy przebywający na pracy zdalnej również powinni być poinformowani o zagrożeniach płynących z pracy zdalnej.

W związku z przejściem na pracę zdalną, pracownicy narażeni są na większa ilość cyberzagrożeń, z uwagi na brak bezpośredniego kontaktu ze współpracownikami, nie są w stanie zweryfikować różnych elementów, jak np. fałszywe e-maile. Ważne jest prowadzenie szkoleń, ponieważ zwiększają poziom świadomości wśród pracowników na różne nietypowe zdarzenia, jak np. kampanie phishin-

[150] *Tips for cybersecurity when working from home*, ENISA, https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home [dostęp: 26.05.2021].
[151] *Tips for cybersecurity when working from home*, ENISA, https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home [dostęp: 26.05.2021].
[152] *Top Tips for Cybersecurity when Working Remotely*, ENISA, https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely [dostęp: 26.05.2021].
[153] *Tips for cybersecurity when working from home*, ENISA, https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home [dostęp: 26.05.2021].

gowe, socjotechnikę itp.[154]. Ponadto, spora część pracowników nie wie o wielu zagrożeniach, których można uniknąć stosując proste rozwiązania, jak np. kwestia korzystania z publicznie dostępnych sieci bądź starszych sieci lokalnych, które nie mają odpowiedniego zabezpieczenia[155]. Więcej informacji na temat szkoleń i podnoszenia klasyfikacji znajduje się w rozdziale 7.

Pracownicy powinni dysponować narzędziami szyfrującymi w celu zachowania bezpiecznej komunikacji z podmiotami zewnętrznymi.

Część informacji, którymi wymieniają się pracownicy operatora z podmiotami zewnętrznymi, w tym z Ministerstwem Klimatu i Środowiska są krytyczne, więc wysłanie ich otwartym kanałem komunikacji może narazić dany podmiot na liczne konsekwencje. Z tego powodu na urządzeniach pracowników powinny być dostępne programy pozwalające na szyfrowanie wiadomości[156].

Dowody kontroli:

– dowód wdrożenia odpowiednich procesów kryptograficznych,

– dokumenty potwierdzające istnienie narzędzi chroniących tajność kluczy prywatnych,

– dokumentacja dotycząca zarządzania urządzeniami przenośnymi i pracą na odległość, w tym: procedury bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, dokumentacja wykonywania ww. procedur.

12.5. Bezpieczeństwo systemów automatyki przemysłowej, sieci inteligentnych

System informacyjny służący do świadczenia usługi kluczowej pełni szczególną rolę z punktu widzenia zapewnienia ciągłości świadczenia tej usługi, co przekłada się na konieczność zaimplementowania bazowych standardów bezpieczeństwa w celu maksymalizacji procesu ochrony. Z racji szerokiego przekroju zastosowanych rozwiązań w sektorze, przedstawione rekomendacje powinny być traktowane jako zbiór podstawowych zasad, który powinien być rozszerzany o bardziej zaawansowane działania właściwe dla danego rodzaju systemów informacyjnych. Kluczowym wnioskiem z zaleceń powinno być dążenie do zapewnienia jak największego bezpieczeństwa systemów informacyjnych, jednakże należy zwrócić uwagę na to, aby poziom bezpieczeństwa nie wpłynął na obniżenie funkcjonalności tych systemów. Wskazane w niniejszym dokumencie rekomendacje stanowią swoisty wyraz zalecenia realizacji koncepcji ochrony warstwowej, która poprzez zaprojektowanie i wprowadzenie wielu niezależnych warstw zabezpieczeń, powinna przyczynić się do zwiększenia ogólnego bezpieczeństwa oraz zminimalizować ryzyko uzyskania dostępu do kluczowych zasobów.

[154] *Tips for cybersecurity when working from home*, ENISA, https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home [dostęp: 26.05.2021].
[155] *Top Tips for Cybersecurity when Working Remotely*, ENISA, https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely [dostęp: 26.05.2021].
[156] *Top Tips for Cybersecurity when Working Remotely*, ENISA, https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely [dostęp: 26.05.2021].

Rekomenduje się stworzenie polityki bezpieczeństwa systemów OT.

Stworzona polityka bezpieczeństwa systemów OT może być częścią przyjętej polityki bezpieczeństwa funkcjonującej w organizacji lub funkcjonować jako osobna polityka. Stworzona polityka bezpieczeństwa powinna być zatwierdzona przez zarząd, a także zakomunikowana pracownikom i podmiotom, których będzie dotyczyć. Ponadto polityka bezpieczeństwa systemów OT powinna podlegać regularnym przeglądom w celu weryfikacji jej aktualności. Zaleca się opracowanie standardów i procedur określających zarządzanie bezpieczeństwem OT, np. proces aktualizacji systemów operacyjnych w OT. Wspomniane polityki, stanowiąc element bezpieczeństwa informacji organizacji, powinny być poddane tym samym działaniom weryfikacyjnym i aktualizacyjnym, co inne procedury i polityki funkcjonujące w danym przedsiębiorstwie. W celu zmaksymalizowania efektywności opracowanych procedur, poprzez budowanie obrazu dojrzałości cyberbezpieczeństwa w oparciu o większą liczbę źródeł, zaleca się posiadanie i aktualizowanie co najmniej następujących dokumentów:

1. wdrożonej i utrzymywanej procedury bądź regulaminu konfiguracji systemów/ tabele konfiguracji systemów/ harmonogram i plan cykli przeglądu konfiguracji systemów,
2. dokumentacji dotyczącej sposobu wdrożenia rozdzielenia krytycznych systemów informacyjnych i danych,
3. sprawozdania z monitorowania kluczowych sieci i systemów informacyjnych,
4. udokumentowanej polityki w zakresie procedur monitorowania, w tym minimalne wymogi dotyczące monitorowania,
5. dowodów wdrożenia narzędzi służących do monitorowania systemów,
6. udokumentowanych testów krytycznych systemów informacyjnych zrealizowanych w przeszłości/ harmonogram i plan przeglądów konfiguracji bezpieczeństwa.

Wskazane we wcześniejszej części dokumentu zalecenia o charakterze organizacyjnym oraz fizycznym, znajdują dopełnienie w ogólnych zaleceniach bezpieczeństwa teleinformatycznego, stanowiąc wspólnie spójny system warstwowej ochrony. Co za tym idzie, bezpieczeństwo systemów automatyki przemysłowej należy traktować jako proces, na który składają się elementy opisane w całości niniejszego dokumentu.

Przykładowo, w kontekście zapewnienia bezpieczeństwa fizycznego w rozumieniu bezpieczeństwa systemów OT, organizacja powinna zapewnić ochronę zarówno urządzeniom PLC/PAC /RTU, stacjom HMI, a także stacjom operatorskim SCADA/DCS. Urządzenia typu PLC/PAC[157]/ RTU powinny być umieszczane w szafach elektrycznych zapewniających rozwiązania wspomagające stabilizację warunków pracy, np. klimatyzację. Jednakże, w większości przypadków urządzenia tego typu są przystosowane do działania w ciężkich warunkach, w związku z tym podejmowane działania powinny dążyć do minimalizacji utrzymaniowej. Ponadto, powinny być umiejscowione w pomieszczeniach technicznych, do których dostęp jest ściśle kontrolowany. Podobne działania zalecane są w stosunku do stacji HMI, które w celu zwiększenia bezpieczeństwa powinny być umieszczane tam, gdzie dostęp jest ściśle kontrolowany. Porty fizyczne urządzeń HMI powinny być zabezpieczone przed dostępem, a operatorzy powinni mieć dostęp tylko do interfejsów użytkownika. Dodatkowo zaleca się, aby organizacja

[157] PAC – ang. *Programmable Automation Controller* – programowalny sterownik automatyki.

stosowała ścisłą kontrolę nad nośnikami USB i innymi mediami lub blokowała porty w stacjach roboczych tam gdzie to możliwe. Działania powinny być podejmowane w celu uniknięcia ewentualnych negatywnych wpływów na środowisko OT, zarówno od strony warunków funkcjonowania tych systemów, tj. odpowiednia temperatura, wilgotność itd., a także od strony nieautoryzowanego dostępu fizycznego.

Również systemy typu SCADA/DCS, które w swoich podstawowych konfiguracjach służą do monitorowania procesów, archiwizacji danych pomiarowych i przekazywania poleceń operatorów, powinny być zabezpieczone od strony fizycznej. Należy zwrócić szczególną uwagę na zapewnienie odpowiedniego poziomu dostępu do pomieszczeń sterowni, definiując precyzyjnie zakres osób mogących mieć dostęp do tego pomieszczenia.

Także procedura zarządzania dostępami powinna zawierać zagadnienia związane z wymienionymi wyżej rozwiązaniami. Zarówno dostęp do programu urządzenia PAC/PLC/RTU, jak i dostęp do urządzeń HMI lub innych rozwiązań OT powinien być zabezpieczony.

Stacje inżynierskie nie powinny być wykorzystywane do innych celów niż te związane z procesem technologicznym.

Zaleca się także zabezpieczenie i dostęp do kopii programów urządzeń w wersjach edytowalnych, z definicją konfiguracji sprzętowej i innymi danymi, które przyczynią się do zwiększenia wartości użytkowej tego rodzaju kopii. Powinno się również zapewnić dostęp do instrukcji użytkownika danych rozwiązań OT, np. stacji HMI, zarówno instrukcji dla operatorów, jak i instrukcji dla inżynierów[158]. Również zmiany w programach powinny być przeprowadzanie w sposób zapewniający możliwość odtworzenia aplikacji pierwotnej, a ewentualne nowe programy powinno się testować w środowisku testowym. Również w systemach typu SCADA/DCS zmiany, poprawki i aktualizacje powinno przeprowadzać się po weryfikacji ewentualnego wpływu takiego działania na ciągłość procesu technologicznego.

Komunikacja sieciowa pomiędzy warstwą systemów biznesowych funkcjonujących w przedsiębiorstwach[159], powinna być monitorowana na styku z siecią OT, a także posiadać zaimplementowany system wykrywania ataków sieciowych na styku sieci IT i OT. Ponadto, zaleca się zapewnienie funkcjonowania systemu kontroli plików na zawartość złośliwego kodu oraz monitorowanie zdarzeń mogących mieć wpływ na bezpieczeństwo. Organizacja powinna również wdrożyć system zarządzania podatnościami oraz aktualizacjami bezpieczeństwa, podjąć działania zmierzające do zapewnienia poufności i wiarygodności komunikatów sterujących.

Organizacja powinna przeprowadzać testy bezpieczeństwa systemów OT.

Przeprowadzone testy (analiza bezpieczeństwa obszaru automatyki przemysłowej) powinny uwzględniać co najmniej weryfikację architektury środowiska OT, konfigurację systemów operacyjnych, skuteczność zabezpieczeń brzegowych, bezpieczeństwo fizyczne. Ponadto zaleca się opracowanie i wdrożenie planów przeprowadzania testów bezpieczeństwa w sposób cykliczny.

[158] NPOIK s. 92

[159] Warstwa ta wspiera część biznesową działalności podmiotów poprzez zapewnienie funkcjonowania rozwiązań typu ERP, CRM, APS itd.

Zaleca się zapoznanie z instrukcjami wskazanymi w dokumentach:

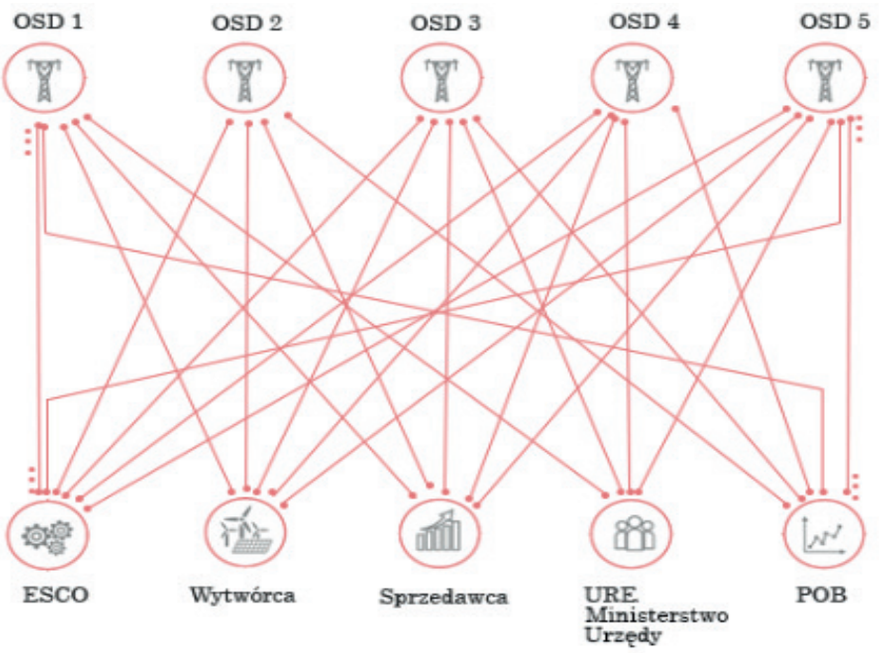
1. Rządowego Centrum Bezpieczeństwa – S*tandardy i dobre praktyki ochrony Infrastruktury Krytycznej – automatyka przemysłowa w sektorze elektroenergetycznym*,
2. Rządowego Centrum Bezpieczeństwa – *Standardy i dobre praktyki ochrony Infrastruktury Krytycznej – automatyka przemysłowa w sektorze Ropy i Gazu*,
3. Załącznik nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej – *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje.*

Rozwój polskiej energetyki oraz postępujący proces jej informatyzacji, skutkuje większą podatnością świadczonych usług na zagrożenia cyberbezpieczeństwa. Zmiany Prawa energetycznego, wprowadzone w 2021 r. określają nie tylko kierunek rozwoju polskiego systemu energetycznego, ale także umożliwią dalszą bezpieczną integrację odnawialnych źródeł energii w systemie oraz wykorzystanie synergii w sektorze – w tym, zwiększenie elastyczności systemu energetycznego oraz wykorzystanie potencjału aktywnych odbiorców. Dodatkowo, należy wspomnieć o zaproponowanych kompleksowych rozwiązaniach usuwających bariery prawne dla rozwoju magazynów energii umożliwiające dalszy rozwój energetyki rozproszonej (prosumenckiej) i OZE (odnawialne źródła energii). Jednakże, co kluczowe z punktu widzenia cyberbezpieczeństwa, przygotowane rozwiązania są niezbędnym punktem wyjścia do transformacji sektora energetycznego, opartej między innymi o jego cyfryzację, inteligentne sieci i inteligentne liczniki zdalnego odczytu, a także tworzą ramy prawne dla funkcjonowania systemu inteligentnego opomiarowania w elektroenergetyce.

Inwestycje w rozwój inteligentnych sieci, w tym liczniki zdalnego odczytu stanowią ogólny kierunek przyjęty w Unii Europejskiej, skutkujący powstaniem obowiązku instalacji przez operatorów systemów dystrybucyjnych do końca 2028 roku liczników inteligentnych u co najmniej 80% odbiorców końcowych. Zaproponowane zmiany dostosują także element zarządczy, w którego właściwości jest ta część systemu energetycznego kraju, co skutkuje powołaniem Operatora Informacji Rynku Energii (OIRE) odpowiedzialnego m.in. za zarządzanie i administrowanie Centralnym Systemem Informacji Rynku Energii (CSIRE). CSIRE jest systemem informacyjnym służącym do przetwarzania informacji rynku energii na potrzeby realizacji procesów rynku energii elektrycznej oraz wymiany informacji pomiędzy użytkownikami systemu – zbieranie oraz przetwarzanie informacji i danych pomiarowych z zainstalowanych liczników. Ponadto Operator Informacji Rynku Energii będzie zajmował się opracowaniem oraz aktualizacją standardów wymiany informacji CSIRE, wspieraniem procesów rynku energii oraz udostępnianiem zgromadzonych informacji uprawnionym użytkownikom systemu CSIRE.

Dotychczasowy model wymiany informacji składał się ze skomplikowanej siatki połączeń i zależności, co przedstawia poniższy schemat:

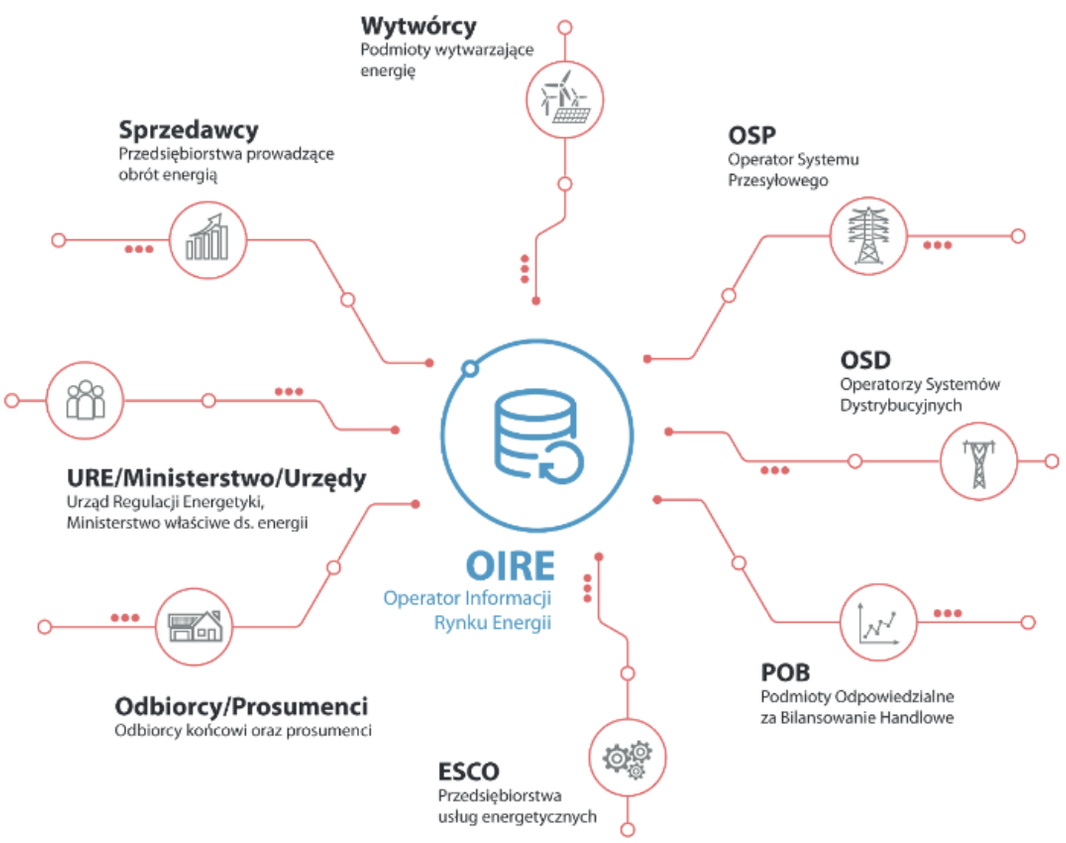
Rysunek 15 – Dotychczasowy model wymiany informacji w ramach rynku energii.



Źródło: *https://www.pse.pl*

Wdrażany model wymiany informacji z Operatorem Informacji Rynku Energii:

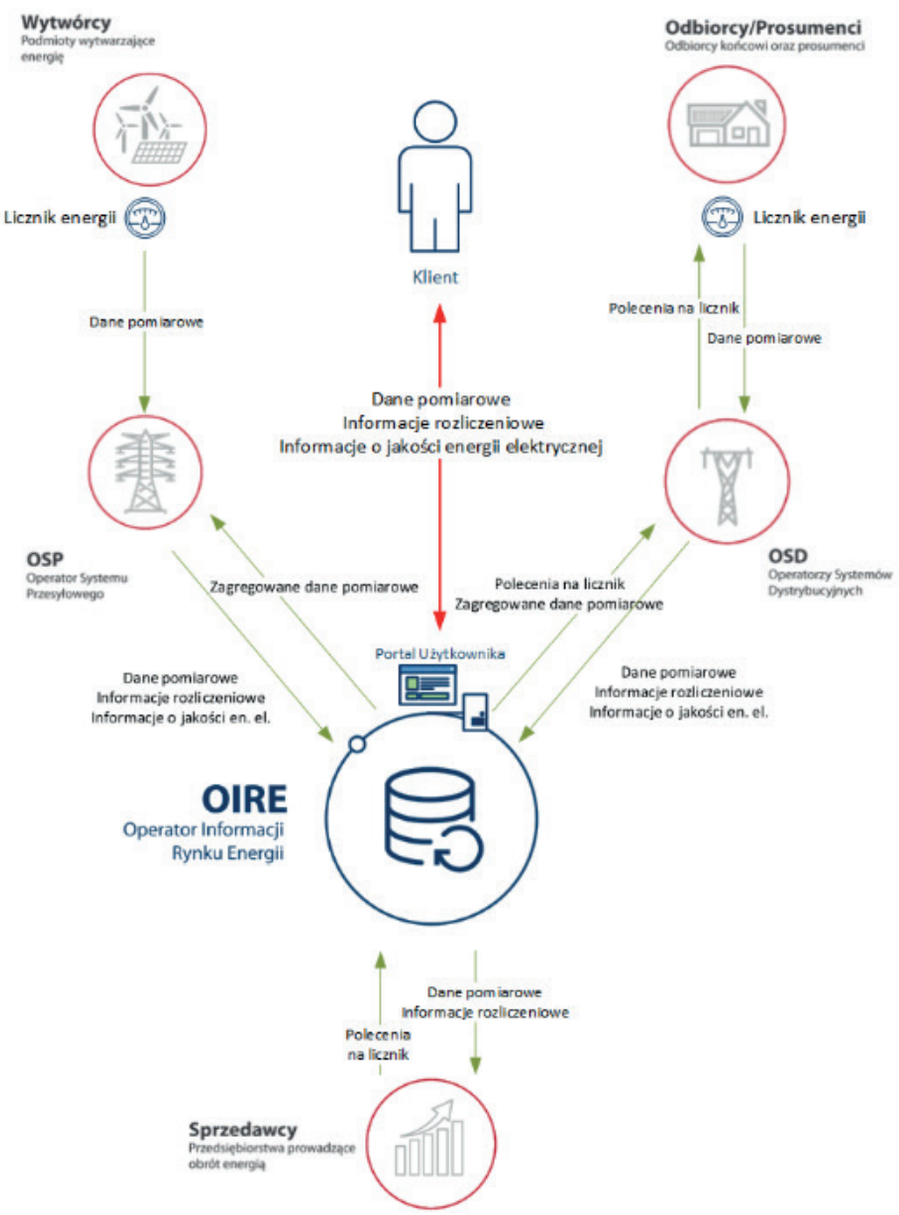
Rysunek 16 – Model wymiany informacji z OIRE.



Źródło: *https://www.pse.pl*

Jak już zostało wspomniane, nowelizacja ustawy Prawo energetyczne nakłada na operatorów systemów elektroenergetycznych obowiązek instalacji liczników zdalnego odczytu, dane pomiarowe będą przekazywane do Centralnego Systemu Informacji Rynku Energii po uprzednim pozyskaniu ich z liczników zdalnego odczytu przez Operatora Systemu Dystrybucyjnego oraz Operatora Systemu Przesyłowego. Pozyskane dane CSIRE będzie przechowywać, a także udostępniać dane pomiarowe uprawnionym podmiotom, np. sprzedawcom energii elektrycznej. Z kolei odbiorcy energii elektrycznej będą mieli dostęp do swoich danych za pośrednictwem dedykowanego portalu. Ponadto, za pośrednictwem Centralnego Systemu Informacji Rynku Energii podmioty uprawnione będą miały możliwość przekazywania poleceń na licznik zdalnego odczytu, np. polecenia włączenia trybu przedpłatowego[160].

Rysunek 17 – Schemat przepływu danych pomiarowych.



Źródło: *https://www.pse.pl*

[160] Prezentacja Polskich Sieci Elektroenergetycznych S.A., *Operator Informacji Rynku Energii oraz Centralny System Informacji Rynku Energii.*

Podsumowując, perspektywa wprowadzenia systemowych rozwiązań, których nieodłącznym elementem będzie system inteligentnego opomiarowania niesie za sobą konieczność rozpoczęcia procesu planowania wdrażania tego rodzaju rozwiązań, mając na uwadze podejście *security by design* oraz inne zalecane działania o charakterze organizacyjnym zawarte w całości niniejszego dokumentu. Szczególnie ważne mogą być aspekty związane z zarządzaniem ryzykiem, cyklem życia systemów informacyjnych, testowaniem systemów i komponentów, audytami bezpieczeństwa systemów informacyjnych oraz ich monitorowaniem, a także zachowaniem ciągłości działania. Samo wdrożenie systemu inteligentnego opomiarowania, jako element budowy inteligentnych sieci elektroenergetycznych, jest działaniem wpływającym pozytywnie na wiele aspektów, m.in. na zarządzanie energią elektryczną, przyczyniając się do ograniczenia emisji CO_2. Co prawda, wiele przedsiębiorstw stosuje już tego rodzaju systemy, jednak nowe regulacje Prawa energetycznego, wprowadzając systemowe rozwiązanie oraz zaznaczając obowiązkowość jego wdrożenia w określonym horyzoncie czasowym, przyczynią się do intensyfikacji procesów wdrożeniowych.

Przy prowadzonej analizie ryzyka organizacja powinna wziąć pod uwagę zagrożenia związane z sieciami inteligentnymi.

Podstawowym elementem zwiększania bezpieczeństwa sieci inteligentnych jest zbudowanie świadomości samych zagrożeń, które mogą wystąpić przy korzystaniu z tego rodzaju rozwiązań. Już samo podłączenie infrastruktury operatora usługi kluczowej do sieci telekomunikacyjnych zwiększa ryzyko wystąpienia zagrożenia cyberbezpieczeństwa, np. poprzez uzyskanie dostępu do sieci wewnętrznej przez atakującego. Prowadząc analizę ryzyka, powinno się uwzględniać fakt, że powstanie wiele potencjalnych punktów wejścia do wewnętrznej infrastruktury operatora, a także to, że działania inne niż cyberataki, np. złośliwe oprogramowanie, błędy użytkowników, także mogą wpłynąć na proces świadczenia usługi.

W celu zapewnienia minimalnych środków wpływających na bezpieczeństwo rozwiązań sieci inteligentnych, zaleca się podjęcie działań zmierzających do usprawnienia lub do zaimplementowania rozwiązań tego typu[161].

Rysunek 18 – Wdrażanie Smart Grid powinno być uporządkowane i zaplanowane.

Zaleca się dokonanie inwentaryzacji zasobów i urządzeń działających w sieci w celu kompleksowego przygotowania strategii cyberbezpieczeństwa (patrz rozdział 6.3).

Sieci OT są często rozwijane przez długi czas. Zdarzają się sytuacje, w których organizacja nie wie jakie urządzenia są podłączone do wspólnej sieci. W celu kompleksowego podejścia do bezpieczeństwa, zaleca się dokonanie weryfikacji wszystkich urządzeń znajdujących się w sieci, tego w jaki sposób i do jakich urządzeń się komunikują[162].

Należy zwrócić uwagę na rozwiązanie do inwentaryzacji zasobów (patrz rozdział 6.3).

Rozwiązanie, które zostanie użyte do wykrywania zasobów powinno być odpowiednie do wykorzystywanych protokołów sieciowych[163].

[161] *Securing Critical Infrastructure: A Guide to Smart Grid Security*, CISCO, s. 4.
[162] *Ibidem*.
[163] *Securing Critical Infrastructure: A Guide to Smart Grid Security*, CISCO, s. 4.

Segmentacja sieci jako alternatywny sposób na gotowości na wypadek zagrożeń (patrz rozdział 11.1).

Zapory sieciowe i inne rozwiązania zaprojektowane i wdrożone w celu segmentacji sieci przemysłowej, które zapobiegną rozprzestrzenianiu się ataków w całym środowisku, mają wpływ przy kolejnej inwentaryzacji zasobów, co z kolei może przełożyć się na inne metody segmentacja sieci[164].

Wykrywanie zagrożeń w czasie rzeczywistym (patrz rozdział 13.2).

Zaleca się, aby organizacja wdrożyła rozwiązania monitorujące w czasie rzeczywistym zagrożenia dla sieci inteligentnych. Rekomenduje się zapewnienie funkcjonalności m.in. monitorowania anomalii wskazujących podejrzaną aktywność, wykrywania nietypowych dostępów i ruchów do sieci OT, identyfikacji zmiany konfiguracji[165].

Stworzenie SOC i integracja zastosowanych rozwiązań i działań i narzędziami używanymi przez SOC (patrz rozdział 13.1).

Zaleca się stworzenie w ramach organizacji komórki organizacyjnej SOC (Security Operations Center). Utworzony SOC powinien mieć możliwość całościowej oceny stanu cyberbezpieczeństwa organizacji, stąd rekomenduje się integrację kompetencji SOC dla IT, jak i OT w jednej komórce, poprzez współpracę specjalistów oraz integrację zastosowanych rozwiązań technicznych z narzędziami wykorzystywanymi w SOC. Holistyczne podejście do organizacji, bez widocznych podziałów na SOC IT i SOC OT, może przyczynić się co wzrostu efektowności działania[166].

Dowody kontroli:

- *udokumentowane zasady wykrywania i analizy zdarzeń, uwzględniające cel, zakres, role i obowiązki oraz koordynację pomiędzy wszystkimi powiązanymi podmiotami, w tym klientami,*
- *sprawozdania z ćwiczeń uświadamiających oraz szkoleń w zakresie wykrywania, rozumienia i zgłaszania zdarzeń naruszających bezpieczeństwo,*
- *wykaz wykrytych i eskalowanych poważnych zdarzeń z przeszłości, obejmujący wszystkie związane z nimi informacje (przyczyna, skutki, kolejność podjętych działań),*
- *systemy, narzędzia i procedury wykrywania i analizy zdarzeń, systemy, narzędzia i procedury wykrywania i analizy zdarzeń,*
- *aktualna dokumentacja zasad dotyczących detekcji zdarzeń oraz związanych z nimi procedur i systemów,*
- *informacje na temat przeglądów zasad detekcji zdarzeń oraz związanych z nimi procedur i systemów,*
- *wytyczne i procedury dla kierownictwa w celu realizacji i zasad reagowania na zdarzenia,*
- *informacje na temat przeprowadzonych w przeszłości ćwiczeń cybernetycznych, w tym daty ich przeprowadzenia,*
- *informacje dotyczące komunikacji z organem właściwym bądź CSIRT.*

[164] Ibidem.
[165] Ibidem.
[166] Ibidem.

13. Wytyczne sektorowe dotyczące zgłaszania incydentów

13.1. Zdolność w zakresie reagowania na incydenty

W obliczu rosnącego prawdopodobieństwa wystąpienia incydentów oraz ataków na małe i większe organizacje sektora energii, niezbędne jest przygotowanie zdolności organizacji do reagowania na incydenty w celu zabezpieczenia świadczenia przez nie usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej[167]. Przepisy dotyczące cyberbezpieczeństwa, m.in. UKSC, egzekwują wymóg zdolności reagowania na incydenty.

Reagowanie na incydenty wymaga dokładnego przygotowania, a także umiejętności identyfikowania, powstrzymywania i odzyskiwania danych po cyberatakach. Istnieją standardy i wytyczne dotyczące reagowania na incydenty, np. norma ISO 27035:2016, *SANS Incident Response in a Security Operation Center*[168] oraz NIST 800-61 Rev. 2 *Computer Security Incident Handling Guide*[169].

Norma ISO 27035 proponuje pięć faz procesu zarządzania incydentami:

1. Planowanie i przygotowanie,
2. Wykrywanie i raportowanie,
3. Ocena i decyzja,
4. Reakcja,
5. Wyciąganie wniosków.

Wytyczne NIST 800-61 Rev. 2 są jednym z najbardziej szczegółowych standardów publicznie dostępnych, które szczegółowo opisują proces reagowania na incydenty w zakresie bezpieczeństwa teleinformatycznego. Zgodnie z dokumentem NIST istnieją cztery główne etapy postępowania w przypadku reagowania na incydenty:

1. Przygotowanie,
2. Wykrywanie i analiza,
3. Ograniczanie, eliminacja i odbudowa,
4. Działania po incydencie.

[167] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560)

[168] SANS Institute, Information Security Reading Room, Incident Response in a Security Operation Center, 22 sierpnia 2020 r.

[169] NIST, SP 800-61 Rev. 2, Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology

Reakcja na incydenty wymaga holistycznego podejścia do analizy sytuacji i łagodzenia wrogich działań podejmowanych przeciwko aktywom organizacji. Analiza zagrożeń pomaga uświadomić sobie, jak ważne jest prowadzenie stałego dialogu i współpracy pomiędzy działami IT i OT, ekspertami ds. cyberbezpieczeństwa i bezpieczeństwa fizycznego, jednostkami rynkowymi i audytorami. W związku z tym, w celu wspierania aktywnego, wczesnego ostrzegania i szybkiego reagowania na zdarzenia krytyczne zaleca się utworzenie stałej i multidyscyplinarnej grupy zadaniowej w organizacji, która musi być w stanie wybrać odpowiednią strategię łagodzenia skutków zaistniałych incydentów, w celu zminimalizowania wpływu na ciągłość świadczenia usługi kluczowej.

Aby osiągnąć ten cel, multidyscyplinarna grupa zadaniowa powinna uwzględniać:

- ekspertów ds. operacyjnych linii biznesowych znający konsekwencje wyłączenia systemu bądź kanału komunikacyjnego,
- ekspertów IT/TLC znających specyfikację ciągłości działania infrastruktury organizacji, którzy są w kontakcie z dostawcami i innymi partnerami podczas poważnych incydentów,
- ekspertów ds. reagowania na incydenty, którzy zobowiązani są do podejmowania decyzji dotyczących działań określających poziom dotkliwości,
- ekspertów ds. komunikacji, którzy powinni ustalić strategię komunikacji wewnętrznej i zewnętrznej organizacji,
- analityków potrafiących zrozumieć schematy ataków i zachowania złośliwego oprogramowania, którzy powinni wskazać możliwe środki zaradcze.

Multidyscyplinarna grupa zadaniowa powinna być zorganizowana w systemie zmianowym i musi pozostawać w kontakcie z zespołem zarządzania kryzysowego lub zarządem organizacji, na wypadek, gdyby zdarzenie przerodziło się w kryzys. Organizacja powinna zapewnić środki celem zmotywowania i przeszkolenia wszystkich członków zespołu zadaniowego.

Security Operations Centre (SOC)

Zgodnie z art. 14 ust 1.UKSC, organizacje mają możliwość ustanowienia własnych zespołów SOC lub zawarcia umowy z zewnętrznym podmiotem świadczącym tego rodzaju usługi, w tym np. podmiotem w ramach grupy kapitałowej. Decyzja o sposobie realizacji obowiązku OUK w zakresie posiadania struktur odpowiedzialnych za cyberbezpieczeństwo powinna być poprzedzona analizą ryzyka. Każde z tych rozwiązań cechuje się zaletami, ale także wadami, które organizacja powinna uwzględnić. Przedsiębiorstwo powinno dokonać wyboru kierując się zapewnieniem największej możliwej efektywności działania SOC, nie traktując kryterium finansowego jako przewodniego.

Zaleca się, aby organizacja przy wyborze konkretnego rozwiązania, wzięła pod uwagę takie kwestie jak:

1. Bezpieczeństwo zbieranych i przetwarzanych danych oraz ewentualne ryzyko związane z dostępem do danych podmiotu zewnętrznego.
2. Możliwości utrzymania i rozwijania umiejętności ekspertów pracujących w SOC m.in. w zakresie nowych technologii, standardów i procesów.
3. Kwestie związane z rekrutacją specjalistów i ewentualne związane z tym trudności.
4. Możliwości zaangażowania się w proces doskonalenia wewnętrznych struktur, który powinien skutkować osiągnięciem przez wewnętrzny SOC odpowiedniego poziomu dojrzałości.
5. Zapewnienie dyżurów 24 godziny na dobę, 7 dni w tygodniu.

Zalety ustanowienia wewnętrznego SOC obejmują między innymi:

1. Szybkość reakcji oraz procesu komunikacji w przypadku wystąpienia zagrożenia.
2. Możliwość poznania charakterystyki funkcjonowania organizacji oraz wypracowanie odpowiednich mechanizmów i procedur.
3. Wdrażane lub zastosowanie rozwiązań uwzględniających i dostosowanych do potrzeb danej organizacji.
4. Prawdopodobieństwo, w przypadku świadczenia usług SOC przez podmiot zewnętrzny, braku możliwości reakcji w odpowiednim czasie, w sytuacji ataku na kilka podmiotów obsługiwanych przez tego samego usługodawcę, np. w przypadku ataku na kilka spółek z tego samego sektora.

Innym modelem jest model hybrydowy SOC, w którym w godzinach pracy działa własny zespół, a po godzinach jest obsługiwany przez kontrahentów lub działają one równolegle.

Rekomenduje się powołanie zintegrowanego Security Operations Center (ISOC) do holistycznego monitorowania i tworzenia efektywnej świadomości sytuacyjnej. ISOC rozszerza zakres obowiązków i możliwości SOC poprzez integrację dziedzin technologii operacyjnej (OT), bezpieczeństwa fizycznego i technologii informacyjnej (IT) w jednym, centralnym ośrodku monitorowania mającym na celu budowanie świadomości sytuacyjnej, koordynowania działań w zakresie reagowania na incydenty oraz optymalizacji zasobów.

Computer Security Incident Response Team (CSIRT)[170]

Podobnie jak w przypadku SOC, organizacja może utworzyć zespół reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), wewnętrzny lub zlecony na zewnątrz. Jego funkcje najlepiej opisano w dokumencie pn. *Computer Security Incident Response Team Services Network*, który został opublikowany przez organizację FIRST[171]. Różnica między SOC a CSIRT polega na tym, że zespół CSIRT działa głównie na poziomie strategicznym i operacyjnym, a nie na poziomie technicznym. Skupia się głównie na analizie zagrożeń, wpływie incydentów bezpieczeństwa na biznes, wymianie informacji, współpracy i zapobieganiu. Ponadto, podczas gdy personel SOC składa się z pracowników ściśle przypisanych do tej jednostki, zespół CSIRT może być zespołem doraźnym, który składa się z pracowników z różnych jednostek.

Źródła detekcji i narzędzia

Konieczne jest wdrożenie pasywnych narzędzi monitorujących systemy informacyjne w celu wykrywania anomalii, które mogą wskazywać na cyberatak i przewidywać zagrożenia. Ustanowienie bazowej komunikacji w ramach infrastruktury OT umożliwia łatwiejsze wykrywanie nowych, innych połączeń. Wiele źródeł danych z różnych wdrożeń zabezpieczeń oferuje zestaw alertów, które należy przeanalizować, aby znaleźć krytyczne zagrożenia i powiązać informacje należące do tego samego zagrożenia lub incydentu. Pozwala to na zbudowanie kontekstu na podstawie danych celem ułatwienia podejmowania decyzji i ustalania priorytetów działań. Alerty można kategoryzować w oparciu o ich źródło wykrywania, takie jak sieciowe lub hostowe systemy wykrywania włamań, raporty od ludzi i inne dzienniki. Poniżej zostały opisane tego typu narzędzia:

[170] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Poland
[171] https://www.first.org/

1. Systemy IDS (ang. Intrusion Detection System)

Narzędzia do monitorowania i wykrywania włamań zwykle koncentrują się na określonych wektorach zagrożeń i podejściach analitycznych. Dlatego wdrożenie kilku różnych technik monitorowania i wykrywania może zapewnić szerszy opis sytuacji. Przydatnym źródłem są wytyczne ENISA dotyczące zależności systemów ICS – SCADA od sieci komunikacyjnych[172].

Systemy IDS zawierają podejścia oparte na sygnaturach, które wykrywają znane zagrożenia. Systemy IDS posiadają także podejście oparte na anomaliach, ponieważ mogą nauczyć się podstawowej komunikacji sieciowej lub zachowania hosta i dzięki temu wykryć odchylenia. Podejście oparte na anomalii zwiększa także prawdopodobieństwo fałszywych alarmów, tj. podniesienia ostrzeżenia o czymś, co nie jest prawdziwym, złośliwym działaniem.

Rozwiązania dotyczące bezpieczeństwa wdrażane z poziomu hosta bądź punktu końcowego, z reguły nie mają zastosowania do wielu urządzeń OT, np. PLC czy RTU z powodu problemów, takich jak ograniczone zasoby i różnorodność systemów operacyjnych. Rozwiązania te są istotne dla urządzeń IT, np. stacji roboczych, ale nie zapewniają pełnych możliwości wykrywania, dlatego środowiska OT wymagają rozwiązań do monitorowania sieci. Rozwiązania do monitorowania sieci dedykowane OT są zazwyczaj w pełni pasywne, tj. nie wprowadzają żadnego ruchu w sieci, aby nie zakłócać krytycznych procesów. Istnieją również nowsze rozwiązania, które są selektywnie aktywne, tzn. mogą wysyłać określone zapytania, które są precyzyjnie dostrojone do określonych urządzeń OT, co pozwala narzędziom uzyskać więcej informacji z urządzeń, takich jak określone wersje oprogramowania układowego i informacje SNMP (ang. *Simple Network Management Protocol*), bez ingerencji w ich normalne zachowanie.

2. Logi

Dzienniki logów są najczęstszym źródłem informacji wspomagających wykrywanie ataków. Mogą pochodzić z różnych urządzeń i systemów, jak np. systemów operacyjnych, urządzeń sieciowych czy usług uwierzytelniania, i są one gromadzone przez serwery dzienników. Protokół komunikacyjny, który jest zwykle używany do takiego gromadzenia, to *syslog*. Można jednak użyć również innych protokołów. Zazwyczaj dzienniki zawierają informacje, takie jak źródło, sygnatura czasowa, krótki opis i ważność. Dużym wyzwaniem przy zbieraniu danych o logach jest to, że generują dużo danych ogólnych, w tym tzw. prawdziwe negatywy i fałszywe pozytywy.

W związku z powyższym logi muszą być agregowane i skorelowane. Rekomenduje się do tego narzędzie SIEM.

3. System SIEM (ang. *Security Incident and Event Management*)

System SIEM to oprogramowanie przeznaczone do agregowania i analizowania informacji, zarówno z punktów końcowych, jak i z narzędzi do monitorowania sieci. Istnieją różne podejścia do tworzenia takich platform dla przedsiębiorstw energetycznych. Jednym jest posiadanie całkowicie oddzielnych instalacji dla sieci IT i OT, drugim jest posiadanie jednej instancji. SIEM mogą być również podłączone do fizycznych systemów bezpieczeństwa i ostrzegać np. o włamaniach.

[172] W szczególności sekcja „3.3.2 Grupy bezpieczeństwa i narzędzia dla systemów SCADA", https://www.enisa.europa.eu/publications/ics-scada-dependencies

Dowody kontroli:

– *wdrożona i utrzymywana procedura bądź regulamin konfiguracji systemów, tabele konfiguracji systemów, harmonogram i plan cykli przeglądu konfiguracji systemów,*

– *dokumentacja dotycząca sposobu wdrożenia rozdzielenia krytycznych systemów informacyjnych i danych,*

– *dokumentacja formalna dotycząca przemysłowych systemów sterowania (ICS),*

– *sprawozdania z monitorowania kluczowych sieci i systemów informacyjnych,*

– *udokumentowana polityka w zakresie procedur monitorowania, w tym minimalne wymogi dotyczące monitorowania,*

– *dowód wdrożenia narzędzi służących do monitorowania systemów,*

– *udokumentowane testy krytycznych systemów informacyjnych zrealizowane w przeszłości, harmonogram i plan przeglądów konfiguracji bezpieczeństwa.*

13.2. Zarządzanie zagrożeniami

Zarządzenie zagrożeniami cyberbezpieczeństwa umożliwia wczesną ich identyfikację, orientację sytuacyjną opartą na zebranych danych, a także ułatwia podejmowanie decyzji oraz podejmowanie działań ograniczających te zagrożenia.

Zarządzanie zagrożeniami obejmuje:

- manualne i zautomatyzowane gromadzenie danych oraz analizę zagrożeń,
- kompleksową metodykę monitorowania w czasie rzeczywistym, w tym zastosowanie zaawansowanych technik, jak modelowanie behawioralne,
- korzystanie z zaawansowanych analiz w celu optymalizacji danych, generowania informacji o bezpieczeństwie i zapewniania świadomości sytuacyjnej,
- technologię i wykwalifikowany personel wykorzystujący świadomość sytuacyjną w celu podejmowania odpowiednich działań oraz szybkich decyzji.

Zbieranie danych o zagrożeniach

Analiza zagrożeń to zdobywanie wiedzy opartej na dowodach, uwzględniająca kontekst, mechanizmy, wskaźniki, wnioski i porady, które można zastosować w odniesieniu do istniejącego lub pojawiającego się zagrożenia. Tę wiedzę powinno się wykorzystać przy podejmowaniu decyzji dotyczących reagowania organizacji na dane zagrożenie.

Organizacja powinna zbierać dane dotyczące zagrożeń z wielu różnych źródeł, począwszy od informacji dostępnych publicznie, do platform wymiany wiedzy o zagrożeniach, takich jak MISP[173] (ang. *Malware Information Sharing Platform*). Organizacja może mieć wiele różnych zewnętrznych źródeł informacji, płatnych lub bezpłatnych. Poza MISP do najbardziej kluczowych można zaliczyć także

[173] https://www.misp-project.org/

CRIT (ang. *Collaborative Research Into Threats*) oraz zespoły tworzone przez CISA i zespoły ISAC, które są dedykowane głównie sektorowi energii. Źródłem danych o zagrożeniach mogą być źródła techniczne pochodzące bezpośrednio od producentów oprogramowania i systemów, platformy wymiany wiedzy o zagrożeniach, a także organizacje krajowe i międzynarodowe, które w swojej działalności zajmują się analizą zagrożeń i wykrytych podatności. Dane mogą być również gromadzone przy wykorzystaniu źródeł wewnętrznych, takich jak dzienniki zdarzeń sieciowych i rejestry poprzednich odpowiedzi na incydenty czy zdarzenia.

Oprócz samych źródeł informacji ważna jest również struktura gromadzonych danych do ich przetwarzania i analizy na późniejszym etapie. Dane o zagrożeniach są zwykle traktowane jako wskaźniki kompromitacji IoC (ang. *Indicators of Compromise*), czyli dane takie jak złośliwe adresy IP, domeny i hashe plików, informacje o podatnościach, kod, tekst wiadomości źródłowych czy inne, dodatkowe informacje pochodzące z mediów społecznościowych. Centralnym punktem gromadzenia, przechowywania i analizowania takich danych w organizacji może być rozwiązanie typu SIEM.

W związku z powyższym rekomenduje się stosowanie zarówno zewnętrznej, jak i wewnętrznej analizy zagrożeń przeprowadzonej w oparciu o dane zgromadzone w infrastrukturze organizacji.

Gromadzone informacje powinny obejmować następujące kategorie:

- adresy MAC/IP,
- informacje pochodzące od producenta,
- typ i rola urządzenia,
- numer modelu,
- wersja oprogramowania software/firmware,
- skonfigurowane i aktywne usługi,
- szczegóły diagnostyczne i prognostyczne na poziomie urządzenia,
- dane o wydajności,
- dzienniki zdarzeń.

Zbieranie informacji o zdarzeniach w systemach ICS (ang. *Industrial Control Systems*) może być przeprowadzone różnymi metodami. Większość z tych metod jest pasywna i dlatego ma minimalny wpływ na system ICS. Na przykład monitorowanie portu przełącznika sieciowego dostarcza cennych informacji o komunikacji sieciowej takiego systemu. Oprócz zbierania informacji o zdarzeniach z przełączników sieciowych, cenne informacje o pracy sieci przemysłowej można uzyskać również z urządzeń nadzorczych. Takimi urządzeniami w systemach ICS są systemy HMI, SCADA oraz Historian.

Polling polega na wykorzystaniu bibliotek skanujących w celu uzyskania informacji o sieciach przemysłowych, których nie można łatwo wydobyć poprzez pasywny monitoring lub ze zdarzeń w punktach końcowych. Takie informacje są związane z rolą urządzenia lub informacjami diagnostycznymi. Metody skanowania obejmują wykorzystanie bibliotek, takich jak *Nmap* lub silniki odcisków pal-

ców[174], a metody *polling* opierają się na komunikatach dla sterowników PLC i RTU sformatowanych zgodnie z protokołami przemysłowymi. Operatorzy systemów ICS zwykle unikają tej praktyki, ponieważ skanowanie może powodować problemy z wydajnością urządzeń ICS, a nawet doprowadzić do wyłączenia niektórych urządzeń operacyjnych.

Idealną strategią gromadzenia wewnętrznej informacji o zagrożeniach jest użycie hybrydowej metody pasywnego monitorowania i aktywnego *pollingu*, w której większość informacji jest uzyskiwana pasywnie, a pozostałą część można uzyskać poprzez *polling* w taki sam sposób, jak robi to inżynierska stacja robocza.

Należy zwizualizować wszystkie zidentyfikowane zasoby, sieci i ich topologię. Aplikacje oraz wszystkie usługi i ich interakcje między sobą powinny być udokumentowane.

Analiza zagrożeń

Analiza zagrożeń to proces wydobywania informacji z danych, które zostały pozyskane celem znalezienia potencjalnych zagrożeń dla infrastruktury danej organizacji[175]. Celem tego procesu jest umożliwienie podejmowania opartych na faktach decyzji w zakresie reagowania na incydenty. Inwentaryzacja zasobów oraz zrozumienie dokładnych zależności procesów biznesowych od poszczególnych zasobów IT czy OT, są kluczowe w kontekście przeprowadzenia prawidłowej analizy zagrożeń. Celem tej analizy jest udostępnienie analitykom informacji, które pomogą im w łagodzeniu skutków potencjalnych incydentów.

Łączenie następujących danych określa kontekst potencjalnego zagrożenia:

- informacje dotyczące potencjalnych wrogów,
- IoC z źródeł informacji dotyczących zagrożeń/analizy złośliwego oprogramowania,
- IoC z własnej analizy SOC,
- wewnętrzna baza danych zasobów/infrastruktura sieciowa,
- stan podatności w zasobach IT/OT,
- monitorowanie bezpieczeństwa wewnętrznego.

Informacje zebrane w ramach przeprowadzonej analizy zagrożeń powinny zostać dostarczone właściwym odbiorcom w odpowiednim czasie. Najpopularniejszymi metodami rozpowszechniania informacji o zagrożeniach są e-maile, modyfikowalne dokumenty wewnątrzorganizacyjne typu *spreadsheet* czy briefingi dotyczące wykrytych zagrożeń. Przy raportowaniu w zakresie zagrożeń należy uwzględnić kompletną strukturę danych, która obejmuje w swoim zakresie wpływ zagrożeń na aktywa, wektory zagrożeń, zagrożone aktywa, rozmieszczenie geograficzne oraz klasyfikację zagrożeń zgodną z ustaloną ich taksonomią. Platforma do wymiany informacji w tym zakresie, np. MISP, może wspierać wszystkie działania związane z rozpowszechnianiem wiedzy o wykrytych zagrożeniach.

[174] https://github.com/kudelskisecurity/scannerl
[175] https://www.ee-isac.eu/

Po rozwiązaniu problemu dotyczącego wystąpienia incydentu w organizacji, cała zgromadzona dokumentacja w zakresie reagowania na incydent powinna zostać wzięta pod uwagę w kontekście analizy zagrożeń. Uzyskane informacje powinny być przekazane do SOC (bądź do jednostki mu odpowiadającej) w celu usprawnienia dalszych działań związanych z cyberbezpieczeństwem, takich jak monitorowanie i wykrywanie.

Informacje pozyskane w ramach procesu reagowania na incydenty mogą stanowić cenną wiedzę w kontekście analizy zagrożeń. Do takich informacji należą m.in źródłowe przyczyny incydentu i początkowe wektory ataków, które mogą ujawnić słabości. Ponadto, mogą pojawić się nowe IoC dla znanych już zagrożeń. Wymiana wiedzy może także następować w odwrotnym kierunku, tzn. informacje pozyskane w ramach analizy zagrożeń mogą okazać się wartościowe w kontekście reagowania na incydenty. Możemy do nich zaliczyć m.in. listę aktualnych podmiotów stanowiących zagrożenie, wiedzę pozyskaną na temat poszczególnych dostawców, organizacji, kompleksową wiedzę w zakresie inwentaryzacji aktywów, czy także informacje korelujące zdarzenie cyberbezpieczeństwa z podmiotem mogącym stanowić potencjalne zagrożenie.

W związku z powyższym rekomenduje się ścisłą współpracę pomiędzy komórką zajmującą się analizą zagrożeń w organizacji, a strukturami odpowiedzialnymi za reagowanie na incydenty teleinformatyczne.

Dowody kontroli:

– *dokumentacja nt. integracji danych z użytkowanych systemów informacyjnych ze źródłami danych nt. podatności typu MITRE, NIST CVE,*

– *systemy, narzędzia i procedury wykrywania i analizy zdarzeń, systemy, narzędzia i procedury wykrywania i analizy zdarzeń.*

13.3. Zarządzanie podatnościami

Środki bezpieczeństwa dotyczące procesu zarządzania podatnościami powinny obejmować określenie krytyczności narzędzi używanych w tym procesie, a także klasyfikację podatności pod względem ich krytyczności dla funkcjonowania organizacji. Należy przy tym również uwzględnić proces ujawniania podatności oraz nawiązanie współpracy komórek odpowiedzialnych za IT i OT w organizacji.

- *Należy ustanowić proces zarządzania podatnościami wewnątrz organizacji wraz z określeniem ich krytyczności na podstawie przeprowadzonej analizy ryzyka, obejmujący wykorzystanie zarówno automatycznych, jak i nieautomatycznych narzędzi.*
- *Usuwając podatności, należy rozpocząć od tych najbardziej krytycznych, biorąc pod uwagę istotność posiadanych aktywów i systemów.*
- *Należy ustanowić proces ujawniania podatności.*
- *Należy regularnie przeprowadzać testy penetracyjne nowych rozwiązań IoT w kontrolowanym środowisku bądź przed lub podczas fazy ich wdrażania, a także po ważnych aktualizacjach systemu.*
- *Należy zapewnić ścisłą współpracę komórek organizacyjnych odpowiedzialnych za OT i IT w przedsiębiorstwie oraz ich efektywną współpracę z właścicielami systemów, kadrą zarządzającą i innymi właściwymi podmiotami w ramach organizacji.*

Zgodnie z definicją zawartą w normie ISO 27002, podatność określana jest jako *słabość zasobu lub grupy aktywów, którą można wykorzystać poprzez jedno lub więcej zagrożeń*[176]. Zarządzanie podatnościami to proces identyfikowania, klasyfikowania, priorytetyzacji, naprawiania i łagodzenia takich podatności. Międzynarodowe normy, które w swojej właściwości dotyczą systemów zarządzania bezpieczeństwem informacji, tj. ISO 27001/2 czy IEC 62443, zalecają zarządzanie podatnościami oraz ich ocenę[177].

Podatności mogą występować w sieciach technologii informacyjnej (IT) lub sieciach technologii operacyjnej (OT). Większość sektorów jest zdominowana przez sieci IT, takie jak Internet, które są sieciami otwartymi. Z kolei sektor energii jest zdominowany przez sieci OT, które są sieciami zamkniętymi, przez co potencjalnie charakteryzują się mniejszą podatnością na ataki z zewnątrz. Jednakże, postępująca digitalizacja powoduje coraz częstsze interakcje systemów OT z innymi, otwartymi sieciami, tak jak odbywa się to w przypadku inteligentnych domów czy pojazdów elektrycznych, przez co naraża te systemy na cyberataki oraz czyni je bardziej podatnymi. Sektor energetyczny stoi przed szczególnym wyzwaniem, jakim jest zabezpieczenie słabych punktów systemów OT, które pierwotnie nie były zaprojektowane do łączenia się z otwartymi sieciami.

Rosnąca cyberprzestępczość i związane z nią zagrożenia często wymuszają na organizacjach skupienie większej uwagi na bezpieczeństwie informacji. Proces zarządzania podatnościami powinien być częścią działań organizacji mających na celu kontrolę ryzyk związanych z bezpieczeństwem informacji. Proces ten pozwoli uzyskać ciągły przegląd podatności w środowisku IT i OT danej organizacji, a także przegląd związanych z nimi ryzyk. Poprzez identyfikację podatności i ich ograniczanie, organizacja może zapobiec przedostawaniu się cyberprzestępców do swojej sieci[178].

Protokół SCAP (ang. *Security Content Automation Protocol*) został stworzony do automatyzacji procesów zarządzania podatnościami. SCAP identyfikuje wspólne podatności i zagrożenia CVE (ang. *Common Vulnerability Enumeration*) dla publicznie znanych podatności. Pozyskiwanie i mapowanie CVE do danych aktywów organizacji jest kluczowym krokiem w procesie zarządzania podatnościami.

Zbieranie informacji o podatnościach

Organizacja powinna pozyskiwać na bieżąco informacje o wszelkich podatnościach technicznych wykorzystywanych przez siebie systemów informacyjnych[179].

Informacje o podatnościach mogą być pozyskiwane z różnych publicznie dostępnych źródeł. Wśród nich należy wyróżnić m.in.:

- NIST CVE – repozytorium danych dotyczących zidentyfikowanych podatności prowadzone przez Narodowy Instytut Standaryzacji i Technologii (NIST) w Stanach Zjednoczonych,

[176] ISO/IEC 27002 *Information technology – Security techniques – Code of practice for information security management.*
[177] SANS Institute, *Implementing a Vulnerability Management Process*, Information Security Reading Room.
[178] A. Williams, M. Nicollet, *Improve IT Security With Vulnerability Management*, 2005.
[179] National Cybersecurity Authority, *Essential Cybersecurity Controls* (ECC-1:2018).

- CISA – w ramach CISA istnieje baza danych dotycząca podatności,
- MITRE – amerykańska organizacja non-profit, prowadząca CVE,
- Biuletyny bezpieczeństwa Microsoft,
- Informacje o podatnościach pochodzące bezpośrednio od producenta.

Ponadto, istnieje wiele dodatkowych źródeł informacji w tym zakresie, takich jak *zerodayinitiative.com*, *vulners.com*, *securiteam.com*, *cxsecurity.com* i *exploit-db.com*, które utrzymują zaktualizowane bazy danych dotyczące podatności związanych z OT.

Mapowanie podatności na aktywa

Wyżej wymienieni publikatorzy podatności, tj. NIST, CISA czy MITRE udostępniają możliwość pobierania informacji CVE w wielu formatach, w tym CSV, XML, JSON, text i HTML. Dane te są często aktualizowane, nawet w godzinnych odstępach, przez co powinny być regularnie synchronizowane z inwentarzem aktywów. Pobrane CVE można dopasować do zinwentaryzowanych zasobów przy użyciu identyfikatorów produktów CPE (ang. *Common Platform Enumeration*) w celu identyfikowania podatności. CPE zawiera nazwy dostawców, wersje i inne szczegóły służące do identyfikacji produktów. Podczas tworzenia inwentaryzacji aktywów ważne jest, aby upewnić się, że wszystkie CPE są prawidłowo skonfigurowane. Właściciele procesów zarządzania podatnościami są odpowiedzialni za aktualizowanie inwentarza aktywów, uwzględniając ujawnione podatności w zabezpieczeniach dla każdego wykorzystywanego przez siebie urządzenia OT i IT.

Wstępna priorytetyzacja podatności

CVSS, czyli *Common Vulnerability Scoring System*, generuje liczbowy wynik określający wagę danej podatności pod względem jej krytyczności, co powinno pomóc organizacjom w ocenie i określeniu priorytetu działań w kontekście zarządzania podatnościami. Wstępną ocenę ryzyka można powiązać z każdym aktywem na podstawie wagi podatności i krytyczności danego aktywa (krytyczna, wysoka, średnia lub niska). Ten wynik ryzyka i liczbę aktywów, na które dana podatność ma wpływ, należy wziąć pod uwagę przy ustalaniu priorytetów procesu łagodzenia (mitygacji).

Ocena ryzyka i ich potencjalny wpływ

Organizacja powinna ocenić stopień narażenia na podatności, o których zdobyła wiedzę, oraz podjąć odpowiednie środki celem przeciwdziałania związanemu z nimi ryzyku. Ponadto należy uwzględnić, że organizacja powinna korzystać wyłącznie z zaufanych metod i narzędzi do właściwej oceny podatności[180]*. Taka ocena podatności powinna być przeprowadzana regularnie*[181].

Należy przeprowadzić przegląd aktywów w celu określenia wagi każdej podatności pod względem jej krytyczności, a także jej wpływu na aktywo. Wynik CVSS nie obejmuje specyficznego kontekstu dla danego aktywa, lecz zapewnia ocenę środowiskową, która pozwala właścicielowi procesu dostosować wynik CVSS uwzględniając kontekst podatności w organizacji. Inwentarz aktywów powinien być aktualizowany w razie potrzeby za pomocą kontekstowych rankingów ważności podatności.

[180] National Cybersecurity Authority, *Critical Systems Cybersecurity Controls* (CSCC-1:2019).
[181] National Cybersecurity Authority, *Essential Cybersecurity Controls* (ECC-1:2018).

Priorytetyzacja działań zaradczych

Właściciele procesów zarządzania podatnościami powinni nadać priorytet działaniom zaradczym dla wykorzystywanych systemów informacyjnych, oprogramowania, urządzeń OT/IT, zgodnie z wagą skutków podatności. Plany zaradcze powinny zapewniać jasny harmonogram dla każdego działania, a inwentarz aktywów należy aktualizować, zwracając uwagę na konkretne ryzyka, na które narażone jest dane aktywo.

W związku z tym, należy zapewnić ścisłą współpracę komórek organizacyjnych odpowiedzialnych w przedsiębiorstwie za OT i IT oraz ich efektywną współpracę z właścicielami systemów, kadrą zarządzającą i innymi właściwymi podmiotami w ramach organizacji.

Strategia procesu łagodzenia (mitygacji)

Organizacja powinna zidentyfikować wszystkie możliwe opcje łagodzenia skutków dla systemów i urządzeń, których dotyczy problem związany z wykrytą podatnością i ocenić każdą opcję pod kątem jej potencjalnego wpływu na działanie aktywów[182].

Niektóre środki zaradcze mają bezpośredni związek z dostępnością aktywów. Na przykład aktualizacja oprogramowania *firmware* lub oprogramowania *software* często wymaga ponownego wdrożenia i uruchomienia aktywa. Większość podatności w zabezpieczeniach wymaga więcej niż jednej poprawki bezpieczeństwa, aby je złagodzić. Jeśli poprawka jest dostępna, może się okazać, że nie jest ona zatwierdzona przez samego producenta systemu, oprogramowania czy urządzenia, którego podatność dotyczy, lub może być niekompatybilna z innym oprogramowaniem (patrz rozdział 6.5).

W niektórych przypadkach podjęcie działań naprawczych nie jest możliwe z powodu braku poprawki lub braku odpowiedniego okna obsługi. W takich przypadkach należy ocenić alternatywne lub tymczasowe działania łagodzące (mitygujące). Jako warstwę segmentacji między sieciami IT i OT należy zawsze stosować zaporę ogniową. Zapory sieciowe z systemem IDS/IPS (ang. *Intrusion Detection System/Intrusion Prevention System*) mogą wykrywać i zapobiegać wykorzystywaniu znanych, zidentyfikowanych już podatności oraz zapewniać wirtualne wdrożenie poprawki bezpieczeństwa (ang. *virtual patching*), gdy rzeczywiste jej wdrożenie nie jest możliwe.

Wdrożenie procesu łagodzenia (mitygacji)

Właściciel procesu zarządzania podatnościami powinien wdrożyć środki zaradcze zgodnie z priorytetem świadczonych przez organizację usług i udostępniać informacje o stanie procesu łagodzenia (mitygacji) do wszystkich interesariuszy, w tym osobom odpowiedzialnym za zachowanie ciągłości świadczenia usług przy wykorzystaniu urządzeń, systemów czy oprogramowania, którego dotyczy podatność. Po wdrożeniu środków zaradczych, inwentaryzacja aktywów musi odzwierciedlać wszelkie wprowadzone zmiany, tzn. jeżeli oprogramowanie zostało zaktualizowane, kolejna wersja powinna zostać uwzględniona w inwentaryzacji. Jeśli podatność

[182] NIST, *Guide to Enterprise Patch Management Technologies*, https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final

zostanie zniwelowana bądź złagodzona, tymczasowo lub na stałe, informacje w tym zakresie powinny zostać zaktualizowane również w inwentarzu. W przypadku, gdy możliwe są tylko częściowe środki zaradcze, także należy to udokumentować.

Platforma n6[183]

Platforma n6 to stworzony przez CERT Polska (CSIRT NASK) system służący do gromadzenia, przetwarzania i przekazywania informacji o zdarzeniach bezpieczeństwa w sieci. W ciągu jednego roku przez platformę przetwarzane są dziesiątki milionów zdarzeń bezpieczeństwa z Polski i całego świata. n6 funkcjonuje w pełni automatycznie. Jej celem jest efektywne, niezawodne i szybkie dostarczenie dużych ilości informacji o zagrożeniach bezpieczeństwa właściwym podmiotom: właścicielom, administratorom i operatorom sieci. Dostęp do n6 jest bezpłatny i nie wymaga instalacji jakichkolwiek sond w sieci.

Źródłem danych systemu n6 jest wiele kanałów dystrybucyjnych dostarczających informacje o zdarzeniach bezpieczeństwa. Zdarzenia te wykrywane są w wyniku działań systemów wykorzystywanych przez różne podmioty zewnętrzne (takie jak inne CERTy, organizacje bezpieczeństwa, producentów oprogramowania, niezależnych ekspertów od bezpieczeństwa itp.) oraz systemów monitorowania obsługiwanych przez CERT Polska. Większość informacji aktualizowanych jest codziennie, niektóre częściej.

Dodatkowym źródłem informacji o sieciach klienta mogą być wyniki działań operacyjnych CERT Polska. Dotyczy to również działań operacyjnych innych podmiotów – dane otrzymane jednorazowo z zewnątrz, za zgodą źródła mogą być dodawane do systemu w celu redystrybucji.

n6 można porównać do sortowni incydentów, której sercem jest silnik n6 (n6 engine). Dzięki rozbudowanemu systemowi tagowania, incydenty mogą być przypisywane do konkretnych podmiotów, których dotyczą – np. na podstawie adresów IP i numerów AS (ang. *autonomous servers*). Dane są agregowane w skrojoną na miarę, specjalnie przygotowaną paczkę, która zachowuje oryginalny format źródła (każde źródło w oddzielnym pliku). Dodatkowo istnieje możliwość dostarczania innych informacji, takich jak np. dane o serwerach C&C (ang. *Command & Control*) nie znajdujących się w sieci klienta, ale które mogą zostać przez niego wykorzystane do wykrywania u siebie zainfekowanych komputerów.

W platformie przekazywane są informacje o źródłach ataku w postaci URL, domen, adresów IP lub nazw złośliwego oprogramowania, a także w zależności od dostępności informacje o danych specjalnych. Przykładowe zbiory danych znajdujące się w platformie n6: złośliwe adresy URL, złośliwe oprogramowanie i inne artefakty, zainfekowane hosty (boty), serwery C&C, skanowania DDoS, ataki bruteforce, uczestnictwo w sieci fast flux, phishing, spam, dane specjalne (w wyniku działań operacyjnych CERT Polska).

[183] https://n6.cert.pl/

Dowody kontroli:

– dane z systemów analitycznych typu SIEM, IDS, IPS, służących wykonywaniu zaawansowanych analiz na danych, wskaźniki kompromitacji IoC, czyli dane takie jak złośliwe adresy IP, domeny i hashe plików, informacje o podatnościach, kod, tekst wiadomości źródłowych czy inne, generowane informacje o bezpieczeństwie, raporty sytuacyjne.

13.4. Katalog incydentów

Każdy operator usługi kluczowej powinien klasyfikować incydenty według następujących kryteriów:

a) Źródło incydentu (szerzej opisane w punkcie 13.4.),

b) Skutki, jakie spowodowało wystąpienie danego incydentu (szerzej opisane w punkcie 13.4.1),

c) Skutki dla bezpieczeństwa państwa (szerzej opisane w punkcie 13.4.2).

Klasyfikacja incydentów powinna odbywać się poprzez przejście po kolei przez ustanowione kryteria, aby w jak najlepszym stopniu możliwe było prawidłowe zidentyfikowanie źródła oraz skali skutków, jakie spowodował dany incydent. Należy podkreślić, że poprzez pojęcie *incydent* należy rozumieć *zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo*[184]. W ustawie wyróżnia się trzy ich poziomy:

1) Incydent – zdarzenie obsługiwane przez operatora usługi kluczowej,
2) Incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej[185]. Klasyfikacja incydentu odbywa się na poziomie operatora usługi kluczowej, który ma obowiązek zgłoszenia tego typu incydentów do odpowiedniego CSIRT poziomu krajowego,
3) Incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV[186].

W momencie wystąpienia incydentu w danym podmiocie, operator usługi kluczowej zobowiązany jest rozpocząć działania zmierzające do zarządzania incydentem, czyli powinien on zapewnić obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu[187]. Jak widać, jest to szeroki wachlarz działań, które należy wykonać w celu ograniczenia jego skutków. W ramach zarządzania incydentem, OUK zapewnia jego obsługę, którą rozumie się jako czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu[188].

[184] Art. 2 pkt 5 UKSC.
[185] Art. 2 pkt 7 UKSC.
[186] Art. 2 pkt 6 UKSC.
[187] Art. 2 pkt 18 UKSC.
[188] Art. 2 pkt 10 UKSC.

Zaleca się opracowanie katalogu incydentów cyberbezpieczeństwa możliwych do wystąpienia w przedsiębiorstwie, charakterystycznych dla obszaru i zakresu działania spółki, a także dopasowanego do wewnętrznych uwarunkowań i specyfiki danego podmiotu.

Katalog incydentów powinien grupować możliwe do wystąpienia zdarzenia na podstawie weryfikowalnych i ustandaryzowanych kryteriów. Metodyka powinna określać wektor incydentu w korelacji z systemem informacyjnym, który może być zagrożony i definiować skutek oraz zasięg ewentualnego incydentu. Należy dążyć do tego, aby opracowana metodyka opierała się o słownik pojęć przedstawiony poniżej, co pozwoli na stworzenie spójnej nomenklatury pomocnej w procesie wymiany informacji i zgłaszania incydentów.

Rekomenduje się, by operator usługi kluczowej opracował katalog incydentów cyberbezpieczeństwa, który będzie uwzględniał m.in. obszar, zasięg i klasyfikację danego incydentu.

Operator usługi kluczowej powinien opracować katalog incydentów będący dokumentem kompleksowym i uwzględniającym uwarunkowania prawne oraz dobre praktyki. Ważne jest również, by katalog został stworzony w oparciu o taksonomię incydentów stosowaną przez większość operatorów usług kluczowych w sektorze. Jest to o tyle istotne, że dysponując wspólną klasyfikacją incydentów, operatorzy mogą w łatwiejszy sposób wymieniać się między sobą informacjami o potencjalnych zdarzeniach, a także lepiej komunikować się z CSIRT poziomu krajowego, CSIRT sektorowym i ISAC. Dzięki takiemu podejściu, każdy opisany w systematyce incydent może zostać dopasowany do odpowiedniego przepisu prawa krajowego, zwłaszcza w kontekście prowadzenia czynności dochodzeniowych przez organy ścigania.

Rekomenduje się, by katalog incydentów został opracowany w oparciu o wspólną taksonomię incydentów dla całego sektora energii.

W ramach prac Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii w związku z COVID-19, powołanego na podstawie zarządzenia Ministra Klimatu z dnia 19 maja 2020 r. *w sprawie powołania Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii w związku z COVID-19* (Dz. Urz. Min. Klim. z 2020 r., poz. 26)[189], opracowano *Słownik pojęć* ustalający wspólną taksonomię incydentów i zdarzeń dla operatorów usług kluczowych, który jest wykorzystywany do opracowania raportu sytuacyjnego. Słownik jest efektem współpracy i uzgodnień pomiędzy podmiotami działającymi w ramach różnych podsektorów. Należy podkreślić, że *Słownik pojęć* stanowi pewną podstawę i może zostać rozszerzony o elementy specyficzne dla danego podmiotu, jednakże zaleca się niemodyfikowanie zawartych w nim opisów i klasyfikacji.

[189] Zarządzenie Ministra Klimatu z dnia 19 maja 2020 r. w sprawie powołania Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii w związku z COVID-19, https://dziennikurzedowy.mos.gov.pl/dzienniki-urzedowe-z-2020-r/kwiecien-czerwiec/zarzadzenie/poz-26-zarzadzenie-ministra-klimatu-z-dnia-19-maja-2020-r-w-sprawie-powolania-zespolu-ds-mon/

Słownik pojęć

KLASYFIKACJA INCYDENTU	PRZYKŁADY INCYDENTU	OPIS
Obraźliwe treści (Abusive Content)	SPAM	Niechciane i niepożądane wiadomości e-mail, oznacza to, że odbiorca nie udzielił weryfikowalnego pozwolenia na wysłanie wiadomości. Wiadomość jest wysyłana jako część większego zbioru wiadomości, z których wszystkie mają funkcjonalnie porównywalną zawartość.
	Mowa nienawiści	Dyskredytacja lub dyskryminacja kogoś (np. prześladowanie w sieci, rasizm i groźby wobec jednej lub więcej osób).
	Przemoc, pornografia	Pornografia dziecięca, gloryfikacja przemocy itd.
Złośliwy kod (Malicious Code)	Wirus	Oprogramowanie, które jest umyślnie dołączane lub wprowadzane do systemu w szkodliwym celu. Interakcja użytkownika jest zwykle konieczna do aktywacji kodu.
	Worm	
	Trojan	
	Spyware/Ransomware	
	Dialer	
	Rootkit	
Zbieranie informacji (Information Gathering)	Scanning	Ataki wysyłające żądania do systemu w celu wykrycia słabych punktów. Obejmuje to także pewien rodzaj procesów testowania w celu zebrania informacji o hostach, usługach i kontach. Przykłady: zapytania DNS, ICMP, SMTP (EXPN, RCPT itp.), skanowanie portów.
	Sniffing	Obserwacja i rejestracja ruchu sieciowego (podsłuch).
	Social engineering	Zbieranie informacji od użytkowników w sposób nietechniczny (np. kłamstwa, zastraszenie, łapówki lub groźby).
Próby włamań (Intrusion Attempts)	Wykorzystanie znanych luk w zabezpieczeniach	Próba włamania się do systemu lub zakłócenia dowolnej usługi poprzez wykorzystanie luk w zabezpieczeniach przy użyciu standardowego identyfikatora, takiego jak numer CVE (np. przepełnienie bufora, backdoor, cross site scripting itp.).
	Próby logowania	Wiele prób logowania (odgadywanie/ łamanie haseł, brut force).
	Nowa sygnatura ataku	Próba użycia nieznanego exploita.
Włamania (Intrusions)	Skompromitowanie konta uprzywilejowanego	Udana kompromitacja systemu lub aplikacji (usługi). Przyczyną może być znana lub nowa luka, ale także nieautoryzowany dostęp lokalny. Obejmuje także bycie częścią botnetu.
	Skompromitowanie konta nieuprzywilejowanego	
	Kompromitacja aplikacji	
	Bot	

KLASYFIKACJA INCYDENTU	PRZYKŁADY INCYDENTU	OPIS
Dostępność (Availability)	Dos	W wyniku takiego ataku system otrzymuje masową ilość pakietów przez co operacje są opóźnione lub system ulega awarii. Przykładami DoS są ICMP i SYN floods, ataki typu teardrop i mail-bombing. DDoS często opiera się na atakach DoS pochodzących z botnetów, ale istnieją również inne scenariusze, takie jak ataki DNS. Jednak na dostępność mogą mieć wpływ również działania lokalne (zniszczenie, zakłócenie zasilania itp.) – lub spontaniczne awarie, błędy ludzkie, rażące zaniedbania.
	DDoS	
	Sabotaż	
	Awaria (bez złośliwości)	
Bezpieczeństwo treści informacyjnych (Information Content Security)	Nieautoryzowany dostęp do informacji	Oprócz lokalnego nadużycia danych i systemów, bezpieczeństwo informacji może być zagrożone przez udane złamanie zabezpieczeń konta lub aplikacji. Ponadto możliwe są ataki, które przechwytują i uzyskują dostęp do informacji podczas transmisji (podsłuch, podszywanie się lub przejęcie). Przyczyną może być także błąd człowieka/ konfiguracji/ oprogramowania.
	Nieautoryzowana modyfikacja treści	
Oszustwo (Fraud)	Nieautoryzowane użycie zasobów	Wykorzystywanie zasobów do nieautoryzowanych celów, w tym przedsięwzięć o charakterze zarobkowym (np. korzystanie z poczty elektronicznej w celu uczestniczenia w nielegalnych zyskach lub piramidach finansowych).
	Prawa autorskie	Oferowanie lub instalowanie kopii nielicencjonowanego oprogramowania komercyjnego lub innych materiałów chronionych prawem autorskim.
	Masquerade	Rodzaj ataków, w których jeden użytkownik nielegalnie przyjmuje tożsamość innego, aby z niego korzystać.
	Phishing	Udawanie innego podmiotu w celu przekonania użytkownika do ujawnienia prywatnego poświadczenia.
Podatności (Vulnerable)	Otwartość na nadużycia	Otwarte, niezabezpieczone zasoby, luki widoczne na podstawie skanów Nessus itp., nieaktualne sygnatury wirusów itp.
Inne (Other)	Wszystkie zdarzenia, które nie mieszczą się w żadnej z podanych kategorii, należy zaliczyć do tej klasy.	

Zaleca się, by opracowany katalog uwzględniał efekty kaskadowe wystąpienia danego incydentu spowodowane zależnością różnych systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej.

Nie ulega wątpliwości, iż systemy funkcjonujące w przedsiębiorstwie są ze sobą powiązane. W dobie postępującej informatyzacji, dużo większą część procesu technologicznego realizuje się za pomocą systemów informacyjnych. Z racji tego, operator usługi kluczowej powinien zidentyfikować systemy krytyczne, a także ich dalsze powiązania z innymi systemami. Jest to znaczące z tego powodu, że często wystąpienie incydentu w jednym z systemów ma dalsze konsekwencje w innych. Jeżeli istnieje taka możliwość, należy wziąć pod uwagę również efekty kaskadowe w kontekście rynku lokalnego oraz, w miarę posiadanej wiedzy, całego systemu energetycznego państwa, w tym skutki, jakie mógłby mieć incydent w danym systemie informacyjnym. Ponadto, zaleca się ocenę wpływu danego incydentu na odbiorców końcowych.

Rekomenduje się cykliczne aktualizowanie opracowanego katalogu incydentów.

Operator usługi kluczowej powinien na bieżąco analizować i monitorować informacje na temat nowych wektorów ataków, podatności, form ataków i informacji przekazywanych przez CSIRT poziomu

krajowego i CSIRT sektorowy, aby na bieżąco reagować na pojawiające się cyberzagrożenia. Na podstawie analizy trendów powinien być aktualizowany katalog incydentów, aby był on jak najlepiej dopasowany do obecnej sytuacji krajowej i międzynarodowej.

Do każdej z grup incydentów zawartych w katalogu incydentów organizacja powinna stworzyć procedury postępowania i udostępniać je pracownikom odpowiedzialnym za procedurę reakcji. Stosownie do możliwości organizacji, każda z grup incydentów powinna mieć określoną komórkę lub komórki organizacyjne, które będą zaangażowane w procesie reagowania na incydent.

Ważne jest, aby w ramach struktury danego podmiotu poszczególne komórki organizacyjne miały świadomość, w którym momencie wystąpienia incydentu powinny zostać zaangażowane i jakie działania powinny podjąć. Dzięki takiemu podejściu, możliwe będzie szybkie i efektywne reagowanie na sytuację kryzysową związaną z wystąpieniem incydentu.

13.4.1. Incydenty poważne

Z dotychczasowej praktyki wynika, że incydentem mogą być różne zdarzenia, jednakże, aby można je było uznać za incydent poważny bądź incydent krytyczny, to muszą spełnić odpowiednie przesłanki. Rada Ministrów uregulowała kwestię uznania danego incydentu za poważny poprzez określenie tych przesłanek w drodze rozporządzenia *w sprawie progów uznania incydentu za poważny*[190], odpowiednio do rodzajów zdarzenia w poszczególnych sektorach i podsektorach określonych z załączniku nr 1 do UKSC[191]. Na podstawie wskazanych w tym dokumencie progów odnoszących się do skutków, jakie dany incydent może spowodować, wymieniono:

- liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej,
- czas oddziaływania incydentu na świadczoną usługę kluczową,
- zasięg geograficzny obszaru, którego dotyczy incydent, innych czynników charakterystycznych dla danego podsektora, czyli takich okoliczności jak: śmierć człowieka, ciężki uszczerbek na zdrowiu, inny ciężki uszczerbek na zdrowiu więcej niż jednej osoby, straty finansowe przekraczające 250 tys. zł.

Operator usługi kluczowej klasyfikuje incydent jako poważny, a następnie nie później niż w ciągu 24 godzin od momentu jego wykrycia, zgłasza jego wystąpienie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. Progi uznania incydentu za poważny różnią się w zależności od świadczonej usługi kluczowej, dlatego poniższa tabela zawiera zagregowane dane z załącznika do rozporządzenia Rady Ministrów *w sprawie progów uznania incydentu za poważny*.

Zatem, w momencie wystąpienia incydentu, odpowiedzialność za odpowiednią klasyfikację incydentu jako poważny spoczywa na operatorze usługi kluczowej. Powinien on odpowiednio przeanalizować progi zawarte w stosownym rozporządzeniu dotyczące danej usługi kluczowej i na tej podstawie przekazać zgłoszenie do właściwego CSIRT poziomu krajowego.

[190] Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. *w sprawie progów uznania incydentu za poważny* (Dz. U. z 2018 r. poz. 2180).
[191] Art. 11 ust. 4 UKSC.

Tabela 3 – Progi uznania incydentu za poważny.

Rodzaj incydentu	Progi uznania incydentu za poważny:	Liczba użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej	Czas oddziaływania incydentu na świadczoną usługę kluczową	Zasięg geograficzny obszaru, którego dotyczy incydent	Inne czynniki charakterystyczne dla danego podsektora
Wydobywanie kopalin	**Incydent dotyczący wydobywania kopalin**	n/d	Przerwanie wydobycia na okres dłuższy niż 72 godziny	n/d	Incydent spowodował co najmniej jedną z wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) inny ciężki uszczerbek na zdrowiu więcej niż jednej osoby, d) straty finansowe przekraczające 250 tys. zł
Energia elektryczna	**Incydent dotyczący pokrycia zapotrzebowania o zasięgu lokalnym**	n/d	Utrata na co najmniej 3 minuty zasilania odbiorców w wysokości powyżej 10% rzeczywistego zapotrzebowania systemu w okresie poprzedzającym incydent;	n/d	n/d
	Incydent dotyczący pokrycia zapotrzebowania o zasięgu krajowym	n/d	Utrata, na co najmniej 3 minuty, zasilania odbiorców w wysokości powyżej 10% rzeczywistego zapotrzebowania systemu w okresie poprzedzającym incydent	n/d	n/d
	Incydent dotyczący sieci przesyłowej	n/d	n/d	n/d	Awaryjne, równoczesne wyłączenie co najmniej dwóch elementów sieci przesyłowej powodujące: a) istotne pogorszenie warunków pracy systemu lub b) ograniczające zdolności wymiany transgranicznej lub d) ogłoszenie przez Operatora Systemu Przesyłowego stanu zagrożenia systemu przesyłowego lub stanu zaniku zasilania lub stanu odbudowy systemu zgodnie z klasyfikacją stanów systemu określoną w art. 18 rozporządzenia Komisji (UE) 2017/1485 z dnia 2 sierpnia 2017 r. ustanawiającego wytyczne dotyczące pracy systemu przesyłowego energii elektrycznej (Dz. Urz. UE L 220 z 25.08.2017, str. 1)

	Incydent dotyczący modułów wytwarzania energii	n/d	Trwające powyżej 15 minut: a) równoczesne, nieplanowane wyłączenie co najmniej dwóch modułów wytwarzania energii w jednej elektrowni o sumarycznej mocy powyżej 400 MW brutto lub b) równoczesne, nieplanowane ograniczenie mocy lub wyłączenie modułów wytwarzania energii w łącznej wielkości mocy powyżej 1500 MW brutto	n/d	n/d
	Incydent dotyczący urządzeń i narzędzi wykorzystywanych do monitorowania i sterowania pracą systemu	n/d	Utrata jednego z następujących urządzeń lub narzędzi wykorzystywanych w czasie rzeczywistym, przy jednoczesnym braku dostępności urządzeń i narzędzi podstawowych i rezerwowych: a) środków łączności dyspozytorskiej, przez okres co najmniej 1 godziny lub b) systemów zdalnego sterowania urządzeniami stacyjnymi i źródłami wytwórczymi przez okres powyżej 15 minut, lub c) systemów monitorowania pracy systemu (w tym estymacji stanu systemu) przez okres powyżej 15 minut, lub d) narzędzi wykorzystywanych do oceny bezpieczeństwa pracy systemu przez okres powyżej 15 minut	n/d	n/d

	Incydent dotyczący urządzeń i narzędzi wykorzystywanych do monitorowania i sterowania pracą systemu	n/d	e) systemów monitorowania pracy systemu (w tym estymacji stanu systemu) przez okres powyżej 15 minut, lub f) narzędzi wykorzystywanych do oceny bezpieczeństwa pracy systemu przez okres powyżej 15 minut g) systemów klasy „smart metering" w przypadku braku możliwości pozyskania danych z co najmniej 30% planowanych do odczytu układów pomiarowych, przez okres powyżej 48 godzin	n/d	n/d
Ciepło	**Incydent dotyczący wytwarzania ciepła**	n/d	Przerwanie wytwarzania ciepła na okres dłuższy niż 24 godziny	n/d	Incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) inny ciężki uszczerbek na zdrowiu więcej niż jednej osoby, d) straty finansowe przekraczające 250 tys. zł
	Incydent dotyczący obrotu lub przesyłania, lub dystrybucji ciepła	n/d	Incydent doprowadził do przerwania przesyłania lub dystrybucji ciepła na dłużej niż 24 godziny;	n/d	Incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) inny ciężki uszczerbek na zdrowiu więcej niż jednej osoby, d) straty finansowe przekraczające 250 tys. zł
Ropa naftowa i gaz	**Incydent dotyczący przesyłu ropy naftowej i paliw ciekłych**	n/d	Incydent skutkuje niemożliwością terminowego i w ilościach nominowanych dostarczania i przesyłu ropy naftowej, przez okres dłuższy niż 20 godzin	n/d	Niekontrolowany wyciek ropy naftowej lub innych substancji niebezpiecznych do atmosfery lub gruntu

	Incydent dotyczący produkcji, wydobywania, wytwarzani paliw ciekłych, magazynowania ropy naftowej, przeładunku ropy naftowej, magazynowania paliw ciekłych, przeładunku paliw ciekłych, obrotu paliwami ciekłymi i obrotu paliwami ciekłymi z zagranicą, wytwarzania paliw syntetycznych	n/d	Incydent skutkuje zakłóceniem w produkcji lub rafinacji lub w funkcjonowaniu urządzeń przetwarzających lub magazynowaniu i przesyłaniu ropy naftowej, dłuższym niż 20 godzin	n/d	a) znacząca utrata integralności stacji, lub b) utrata ochrony stacji przeciwko efektom eksplozji, lub c) utrata stacji utrzymania w przypadku instalacji mobilnych, lub d) niekontrolowany wyciek ropy naftowej lub innych substancji niebezpiecznych do atmosfery lub gruntu
	Incydent dotyczący wytwarzania paliw gazowych, przesyłania paliw gazowych, dystrybucji paliw gazowych, obrotu paliwami gazowymi lub obrotu gazem ziemnym z zagranicą, magazynowania paliw gazowych, skraplania lub regazyfikacji LNG lub sprowadzania i wyładunku LNG	n/d	Incydent skutkuje niemożliwością prawidłowego dostarczania i przesyłu gazu ziemnego w okresie co najmniej 24 godzin lub zakłóceniem w produkcji lub w funkcjonowaniu urządzeń przetwarzających lub magazynowaniu lub przesyłaniu gazu ziemnego, przez okres dłuższy niż 20 godzin;	n/d	Nieplanowany wyciek gazu lub innych substancji niebezpiecznych, niezależnie od tego czy doszło do zapłonu, stanowiący bezpośrednie niebezpieczeństwo a) utraty życia lub spowodowania uszczerbku na zdrowiu lub b) wyrządzenia szkody w wielkich rozmiarach, lub c) niekontrolowane obniżenie lub wzrost ciśnienia w sieci gazowej, lub d) zatrzymanie pracy tłoczni gazu lub stacji gazowej, lub e) niekontrolowane zamknięcie lub otwarcie armatury na obiektach sieci gazowej
Dostawy i usługi dla sektora energii	**Incydent dotyczący dostaw systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenia usług na rzecz sektora energii**	n/d	a) incydent skutkuje zakłóceniem w produkcji paliw ciekłych lub rafinacji paliw ciekłych, lub w funkcjonowaniu urządzeń przetwarzających paliwa ciekłe, lub przeładunku paliw ciekłych, lub obrocie paliwami ciekłymi, lub obrocie paliwami ciekłymi z zagranicą, lub wytwarzaniu paliw syntetycznych, lub magazynowaniu i przesyłaniu ropy naftowej, w okresie dłuższym niż 4 godziny, lub	n/d	n/d

Dostawy i usługi dla sektora energii	**Incydent dotyczący dostaw systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenia usług na rzecz sektora energii**	n/d	b) incydent skutkuje przerwą w dostawie energii elektrycznej do systemu przesyłowego ropy naftowej przez okres powyżej 8 godzin, lub c) incydent skutkuje przerwą w dostawie energii elektrycznej do systemu magazynowego ropy naftowej przez okres powyżej 8 godzin, lub d) incydent skutkuje przerwą w świadczeniu usług w transporcie kolejowym i samochodowym (cysterny kolejowe i autocysterny) przez okres powyżej 24 godzin	n/d	n/d
	Incydent dotyczący utrzymywania rezerw strategicznych lub zapasów agencyjnych ropy naftowej, produktów naftowych i gazu ziemnego	n/d	Incydent skutkuje przerwaniem realizacji procesu udostępniania rezerw strategicznych lub uwalniania zapasów agencyjnych ropy naftowej, produktów naftowych i gazu ziemnego na czas dłuższy niż 4 godziny	n/d	n/d
	Incydent dotyczący postępowania z odpadami promieniotwórczymi	Minimum 200 użytkowników, od których odbiera się odpady promieniotwórcze	n/d	Terytorium całego kraju	Incydent skutkuje bezpośrednim niebezpieczeństwem spowodowania uszczerbku na zdrowiu lub długotrwałym skażeniem środowiska

13.4.2. Incydenty krytyczne

Po zgłoszeniu przez operatora usługi kluczowej do właściwego CSIRT poziomu krajowego informacji o wystąpieniu w danym podmiocie incydentu poważnego, CSIRT GOV, CSIRT NASK bądź CSIRT MON na podstawie przesłanych przez operatora informacji na temat danego incydentu, a także własnych analiz klasyfikuje te zdarzenie jako incydent krytyczny (art. 26 ust. 3 pkt 6 UKSC). CSIRT poziomu krajowego klasyfikuje dany incydent jako krytyczny w oparciu o jego skutki powodujące znaczną szkodę dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności

obywatelskich lub życia i zdrowia ludzi[192]. Należy zauważyć, iż incydenty krytyczne są zdarzeniami wywołującymi dużo poważniejsze skutki, a także niosą za sobą wiele zagrożeń, które mogą eskalować nawet na inne państwa członkowskie UE. Wówczas jest to incydent cybernetyczny na dużą skalę. Taki rodzaj incydentu niesie za sobą zakłócenia, z którymi państwo członkowskie nie jest w stanie sobie samodzielnie poradzić, bądź incydent ten dotyczy dwóch lub większej liczby państw członkowskich UE, a działania dążące do ograniczenia jego skutków wymagają koordynacji na poziomie unijnym[193].

W celu wskazania przykładów potencjalnych incydentów krytycznych w sektorze energii warto odnieść się do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/941 z dnia 5 czerwca 2019 r. *w sprawie gotowości na wypadek zagrożeń w sektorze energii elektrycznej i uchylające dyrektywę 2005/89/WE*. Na podstawie tego rozporządzenia państwa członkowskie są zobowiązane do opracowania regionalnych scenariuszy kryzysów elektroenergetycznych, które mogą wystąpić w danym kraju. Wśród przykładowych scenariuszy można wskazać również kryzysy spowodowane cyberatakiem na systemy informacyjne, których efekty mogą być bardzo dotkliwe dla obywateli, gospodarki czy całego państwa, jak np.:

- samoczynne lub deficytowe ograniczenia dla odbiorców powyżej [...] godzin w ciągu doby, łącznie [...] GWh niedostarczonej energii,
- krótkotrwałe i incydentalne przypadki niedostarczenia energii, trwające [...] minut do [...] godzin, o łącznym wolumenie niedostarczonej energii na poziomie [...] MWh,
- lokalny blackout do [...] godzin, łącznie [...] GWh niedostarczonej energii.

Ponadto, w celu wskazania potencjalnych obszarów incydentów krytycznych w sektorze gazu ziemnego, można analogicznie odnieść się do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/1938 z dnia 25 października 2017 r. *dotyczącego środków zapewniających bezpieczeństwo dostaw gazu ziemnego i uchylającego rozporządzenie (UE) nr 994/2010*. Art. 11 ustanawia trzy stany kryzysowe, w tym stan nadzwyczajny, jeżeli występuje nadzwyczajnie wysokie zapotrzebowanie na gaz, znaczne zakłócenie dostaw gazu lub inne znaczne pogorszenie się sytuacji w zakresie dostaw gazu oraz jeżeli wdrożono wszystkie stosowne środki rynkowe, lecz mimo to dostawy gazu są niewystarczające do zaspokojenia pozostałego zapotrzebowania na gaz tak, że konieczne jest wprowadzenie dodatkowych środków nierynkowych. W przypadku stanu nadzwyczajnego podmiot, którego dotknęło zdarzenie przekazuje do organu właściwego:

- dzienne prognozy zapotrzebowania na gaz i prognoz dostaw gazu na kolejne trzy dni, w milionach metrów sześciennych dziennie (mcm/d),
- dzienne przepływy gazu we wszystkich transgranicznych punktach wejścia i wyjścia, a także we wszystkich punktach przyłączenie do sieci zakładu produkcyjnego, magazynu lub terminalu LNG, w milionach metrów sześciennych dziennie (mcm/d),
- wyrażony w dniach okres, przez który przewiduje się dostawę gazu do klientów chronionych.

Wyżej wskazane zdarzenia mogą stać się podstawą wystąpienia incydentu krytycznego.

[192] Art. 2 pkt 6 UKSC.

[193] Załącznik do Zalecenia Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz. U. L 239 z 19.9.2017).

Dowody kontroli:

– *dokumentacja postępowania z incydentami naruszenia BI w tym rejestr incydentów naruszenia BI,*

– *procedury zgłaszania i postępowania z incydentami,*

– *dokumentacja wykonywania ww. procedur.*

13.5. Zarządzanie incydentem cyberbezpieczeństwa

Ustawa z dnia 5 lipca 2019 r. *o krajowym systemie cyberbezpieczeństwa* reguluje kwestię zarządzania incydentem u operatorów usług kluczowych. W art. 8 UKSC czytamy, że *operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniający: […] zarządzanie incydentem*. Kolejne artykuły UKSC regulują kwestie uznania incydentu za poważny (szerzej opisane w rozdziale 13.4.1), a także pozostałe obowiązki operatora usługi kluczowej. Zgodnie z art. 11 UKSC, operator usługi kluczowej w ramach zarządzania incydentem ma zapewnić dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSRIT GOV w zakresie niezbędnym do realizacji jego zadań. Ponadto, to na operatorze usługi kluczowej spoczywa obowiązek klasyfikacji incydentu jako poważny na postawie progów uznania incydentu za poważny (patrz rozdział 13.4.1), a następnie po dokonaniu takiej klasyfikacji niezwłocznie, jednakże nie później niż w ciągu 24h, zgłasza wystąpienie incydentu poważnego do właściwego CSIRT poziomu krajowego. Operator usługi kluczowej w czasie obsługi incydentu poważnego bądź krytycznego, współdziała z CSIRT GOV, CSIRT NASK lub CSIRT MON, w tym przekazuje niezbędne dane. Ponadto, operator usługi kluczowej usuwa podatności, o których jest mowa w art. 32 ust. 2 UKSC, a także informuje organ właściwy ds. cyberbezpieczeństwa dla sektora energii o ich usunięciu. Należy pamiętać, że incydent zostaje uznany za krytyczny na podstawie klasyfikacji dokonanej przez właściwy CSIRT MON, CSIRT NASK lub CSIRRT GOV (patrz rozdział 13.4.2).

Należy pamiętać, że odpowiedzialność za obsługę incydentu i zachowanie ciągłości świadczenia usługi kluczowej spoczywa na operatorze usługi kluczowej.

Zaleca się by operatorzy usług kluczowych przygotowując plany zarządzania incydentem uwzględnili odpowiednie fazy tego procesu.
Zgodnie z normą ISO 27035:16 proces zarządzania incydentem składa się 5 faz:

1. Planowanie i przygotowanie
2. Detekcja i raportowanie
3. Ocena i podjęcie decyzji
4. Obsługa incydentu
5. Wyciągnięcie wniosków

Rysunek 19 – Fazy zarządzania incydentem wg ISO 27035:16.

Źródło: *Opracowanie własne.*

Jak widać, te 5 faz następuje po sobie i są one konieczne do zrealizowania, aby skutecznie obsłużyć dany incydent cyberbezpieczeństwa. Jeżeli chodzi o fazę planowania i przygotowania, to wymaga ona połączenia środków zapobiegawczych z organizacyjnymi oraz odpowiednim podejściem planistycznym. W ramach środków zapobiegawczych można wymienić takie elementy, jak np. określenie ryzyka wystąpienia różnych scenariuszy incydentów i ich wpływu na świadczenie usługi kluczowej, włączając w to ataki typu APT (ang. *Advanced Persistent Threat*)[194].

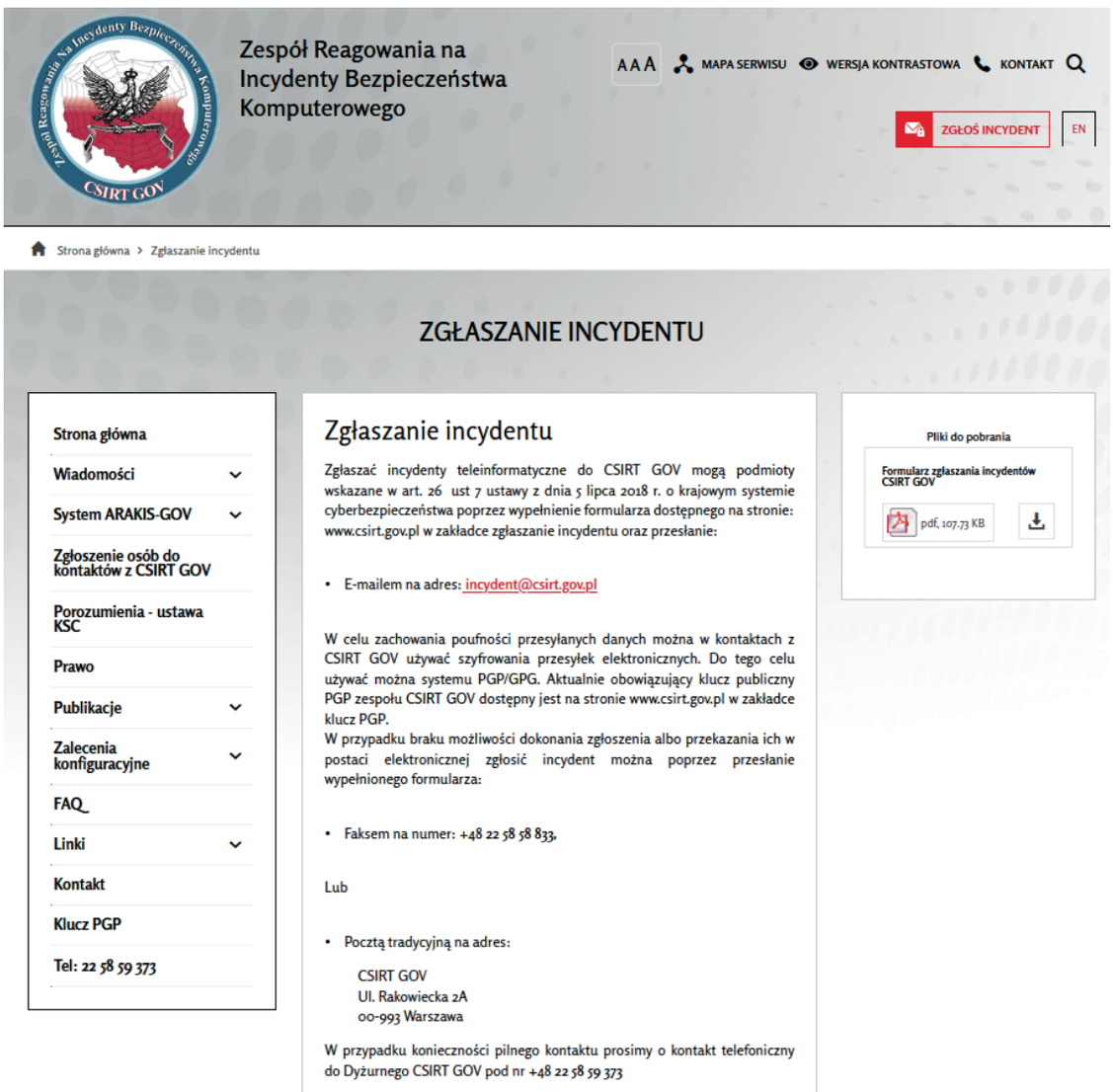
Rekomenduje się, by operator usługi kluczowej zgłaszał incydent poważny do właściwego CSIRT poziomu krajowego poprzez odpowiedni formularz opublikowany na stronie internetowej, a także powinien postępować w tym zakresie zgodnie z instrukcją wskazaną przez dany CSIRT krajowy.

Każdy CSIRT dysponuje stroną internetową, na której znajduje się formularz poprzez który należy zgłosić wystąpienie incydentu poważnego u operatora usługi kluczowej. Dla CSIRT GOV jest to zakładka „Zgłoś incydent" na stronie www.csirt.gov.pl (rysunek poniżej). W zakładce znajdują się informacje o tym jak należy zgłosić incydent, a także za pomocą jakich środków komunikacyjnych można to zrobić (e-mail, faks, poczta). Ponadto, wskazane jest, że w celu zachowania poufności, operator usługi kluczowej może w kontaktach z CSIRT GOV używać szyfrowania przesyłek elektronicznych używając systemu PGP/GPG[195]. Należy pamiętać, że wystąpienie incydentu poważnego zgłaszają do CSIRT GOV operatorzy usług kluczowych, którzy są jednocześnie operatorem infrastruktury krytycznej.

[194] *Cyber Security Incident Response. An EE-ISAC White Paper*, EE-ISAC, 2020, [PDF] s. 6-15, https://www.ee-isac.eu/comp/uploads/2020/12/EE-ISAC-Incident--Response-White-Paper-1.pdf [dostęp: 10.06.2021].

[195] *Zgłaszanie incydentu*, CSIRT GOV, https://csirt.gov.pl/cer/zglaszanie-incydentu/16,Zglaszanie-incydentu.html [dostęp: 27.05.2021].

Rysunek 20 – Zrzut ekranu ze strony CSIRT GOV.

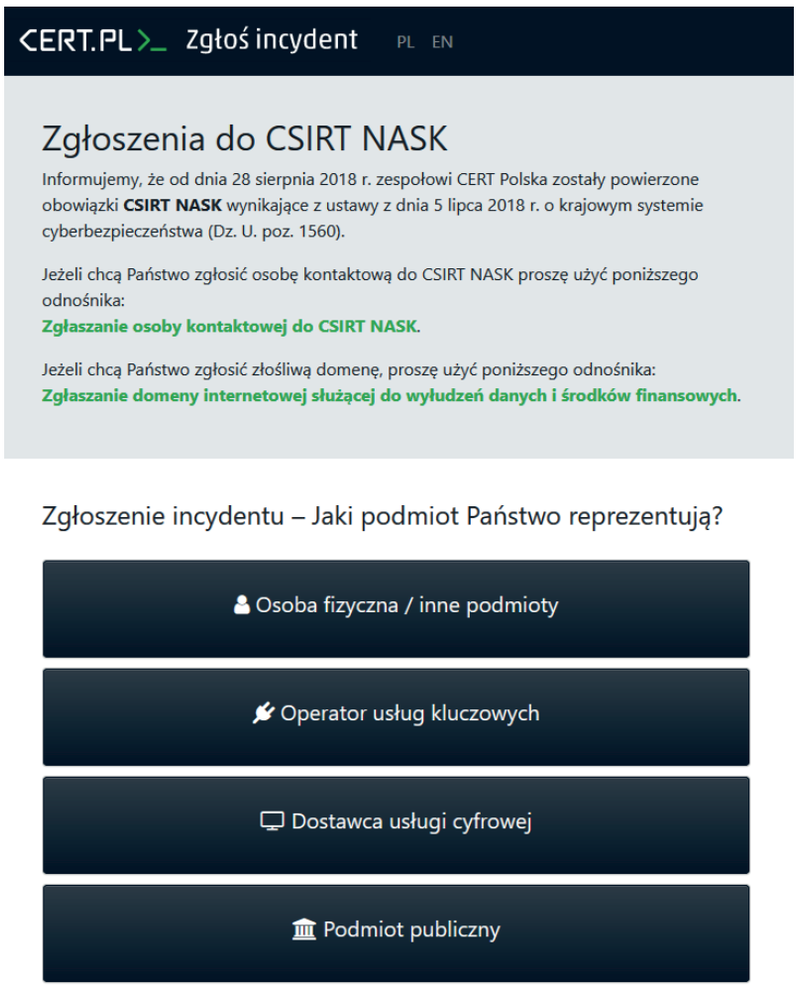


Źródło: *Zgłaszanie incydentu, CSIRT GOV, https://csirt.gov.pl/cer/zglaszanie-incydentu/16,Zglaszanie-incydentu.html [dostęp: 27.05.2021].*

Drugim CSIRT poziomu krajowego, do którego operatorzy usług kluczowych, nie będący operatorami infrastruktury krytycznej, mogą zgłaszać incydenty poważne to CSIRT NASK. Formularz zgłoszenia incydentu do CSIRT NASK znajduje się na stronie www.incydent.cert.pl[196].

[196] Zgłoszenie do CSIRT NASK, CSIRT NASK, https://incydent.cert.pl/ [dostęp: 27.05.2021].

Rysunek 21 – Zrzut ekranu ze strony CSIRT NASK.



Źródło: *Zgłoszenie do CSIRT NASK, CSIRT NASK, https://incydent.cert.pl/ [dostęp: 27.05.2021].*

Zaleca się, by operatorzy usług kluczowych powiadamiali o wystąpieniu incydentu oraz innych zdarzeń mających wpływ na ciągłość świadczenia usługi kluczowej organ właściwy do spraw cyberbezpieczeństwa dla sektora energii w celu wsparcia działań zmierzających do nadzorowania systemu cyberbezpieczeństwa w sektorze energii.

Ministerstwo Klimatu i Środowisko, jako organ właściwy ds. cyberbezpieczeństwa dla sektora energii, powinno zostać poinformowane o nieprzewidzianych zdarzeniach w celu monitorowania systemu cyberbezpieczeństwa sektora energii pod kątem pojawienia się innych podobnych zdarzeń, bądź eskalacji danego zdarzenia/incydentu na inne podmioty. Przyczyni się to również do szybszego przekazywania informacji o wystąpieniu zagrożenia do innych operatorów usług kluczowych w sektorze energii. Narzędzia służące do zgłaszania tego typu zdarzeń na dzień wydania rekomendacji to system S46, do którego również podłączony jest organ właściwy ds. cyberbezpieczeństwa dla sektora energii, a także komunikacja w ramach Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii w związku z COVID-19. W sytuacji, gdy operator usługi kluczowej uzna to za zasadne, może również przesłać odpowiednie informacje bezpośrednio do organu właściwego ds. cyberbezpieczeństwa dla sektora energii.

Organizacja powinna poddać analizie każdą istotną awarię związaną z realizowaną usługą kluczową, co do której istnieje podejrzenie, iż mogła mieć miejsce w związku z incydentem w zakresie cyberbezpieczeństwa.

Operator usługi kluczowej powinien poddać analizie każdą istotną awarię związaną z realizowaną usługą kluczową, do momentu wykluczenia jej przyczyny jako powiązanej z cyberbezpieczeństwem.

Koordynacja sytuacji kryzysowych powinna również zawierać współpracę pomiędzy osobami odpowiedzialnymi za zarządzanie kryzysowe w danym podmiocie[197] z wyznaczonymi osobami do kontaktu w ramach krajowego systemu cyberbezpieczeństwa. Powinien być to ważny element każdej procedury dotyczącej zarządzania zdarzeniami, ponieważ dopóki nie zostanie wykluczona przyczyna związana z cyberbezpieczeństwem, dopóty nie można wyeliminować takiego scenariusza. W rezultacie, osoby wyznaczone do kontaktu w ramach krajowego systemu cyberbezpieczeństwa powinny być włączone w prace sztabów kryzysowych w związku ze zdarzeniami kryzysowymi, które wystąpiły w podmiocie, aby w miarę potrzeb przekazywać na bieżąco odpowiednie informacje do CSIRT poziomu krajowego oraz do wiadomości organu właściwego.

W celu przygotowania odpowiednich procedur związanych z zarządzaniem kryzysowym, operatorzy usług kluczowych powinni zapoznać się z krajowymi i unijnymi aktami prawnymi regulującymi tę tematykę[198].

Rekomenduje się, aby w przypadku wykrycia nietypowego zdarzenia mogącego mieć związek z bezpieczeństwem systemów informacyjnych służących do świadczenia usługi kluczowej, lub innych systemów w których zdarzenie może wpłynąć na usługę kluczową, organizacja niezwłocznie podejmowała działania zmierzające do zbadania zdarzenia.

Operator usługi kluczowej powinien traktować każde nietypowe zdarzenie, którego oddziaływanie może mieć pośredni lub bezpośredni wpływ na systemy informacyjne, jako potencjalny incydent bezpieczeństwa systemu informacyjnego. Podejście to powinno być prezentowane do czasu kategorycznego wykluczenia.

Powinno się zobligować pracowników, wykonawców i podmioty zewnętrzne, które mają dostęp do wewnętrznego środowiska IT lub OT operatora usługi kluczowej, do zgłoszenia i raportowania o każdej zaobserwowanej lub podejrzanej anomalii lub zdarzeniu mogącym świadczyć o lukach bezpieczeństwa.

---

[197] Zgodnie z art. 6 ust. 5a ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (t.j. Dz.U. z 2020 r. poz. 1856) „operatorzy infrastruktury krytycznej" wyznaczają osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej oraz z art. 5 ustawy z dnia 18 marca 2010 r. *o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych* (t.j. Dz.U. z 2020 r. poz. 2173) „operator infrastruktury krytycznej" powołuje, zgodnie z procedurą zawartą w art. 5 ust. 1, pełnomocnika do spraw ochrony infrastruktury krytycznej. W danym podmiocie będącym „operatorem infrastruktury krytycznej" ta sama osoba może jednocześnie pełnić wskazane wyżej funkcje.

[198] Chodzi tu między innymi o przepisy ustawy z dnia 10 kwietnia 1997 r. *Prawo Energetyczne* (t.j. Dz.U. z 2021 r. poz. 716) wraz z rozporządzeniem Rady Ministrów z dnia 23 lipca 2007 r. *w sprawie szczegółowych zasad i trybu wprowadzania ograniczeń w sprzedaży paliw stałych oraz w dostarczaniu i poborze energii elektrycznej lub ciepła* (Dz.U. z 2007 r. nr 133 poz. 924), a także rozporządzenie Ministra Gospodarki z dnia 15 stycznia 2007 r. *w sprawie szczegółowych warunków funkcjonowania systemów ciepłowniczych* (Dz.U. z 2007 nr 16 r. poz. 92). Dodatkowo, kwestie te reguluje także ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Na poziomie unijnym obowiązują przepisy zawarte w Rozporządzeniu Komisji (UE) 2017/2196 z dnia 24 listopada 2017r. *ustanawiającego kodeks sieci dotyczący zagrożenia i stanu odbudowy systemów elektroenergetycznych* (NC ER), Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/941 z dnia 5 czerwca 2019 r. *w sprawie gotowości na wypadek zagrożeń w sektorze energii elektrycznej i uchylającego dyrektywę 2005/89/WE*, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1938 z dnia 25 października 2017 r. *dotyczące środków zapewniających bezpieczeństwo dostaw gazu ziemnego i uchylające rozporządzenie (UE) nr 994/2010* i inne.

Takie samo podejście do nietypowych zdarzeń powinni prezentować wszyscy, którzy mają dostęp do środowiska IT lub OT operatora usługi kluczowej. Jest to ważne, ponieważ z doświadczeń płynących z niektórych ataków, systemy bezpieczeństwa nie zawsze są w stanie wykryć pewne próby ataków, a zaobserwowane anomalie systemowe bądź nietypowe zachowania urządzeń mogą być dużo łatwiej zauważone przez personel obsługujący dany system czy oprzyrządowanie.

Operator usługi kluczowej powinien mieć opracowane procedury regulujące kwestie wykrywania i analizowania przypadków naruszenia zasad bezpieczeństwa, reagowania na incydenty, uczenia się na incydentach, w celu doskonalenia wdrożonych systemów zabezpieczeń.

Posiadając odpowiednio opracowane procedury postępowania na wypadek wystąpienia incydentów, operator usługi kluczowej jest w stanie niezwłocznie podjąć odpowiednie działania zmierzające do jego wykrycia, a w razie jego wystąpienia, do zastosowania odpowiednich algorytmów postępowania. Mając dobrze opracowane procedury, każda osoba zaangażowana w zarządzanie incydentem wie jaki jest zakres jej odpowiedzialności, a także jakie ma podjąć działania na wypadek różnych, nieprzewidzianych sytuacji. Tym samym procedury dotyczące wykrywania i analizowania przypadków naruszenia zasad bezpieczeństwa, reagowania na incydenty, powinny być przejrzyste i jasno identyfikować poszczególne role oraz zakres ich zadań w przypadku wystąpienia incydentu. Jeżeli operator odpowiednio obsłuży pojawiające się incydenty bezpieczeństwa, wówczas ogranicza się związane z tym ryzyka i konsekwencje[199].

Operator usługi kluczowej powinien opracować procedurę zgłaszania incydentów w ramach swojej organizacji, a także zapoznać z nią swoich pracowników i personel partnerów zewnętrznych, który realizuje zadania u danego operatora.

Procedura zgłaszania incydentów powinna zawierać m.in. formularz zgłoszenia incydentu, wskazany zespół do którego takie zgłoszenie trafi, sposób postępowania w przypadku wystąpienia incydentu (dokładnie opisanie co pracownik powinien zrobić z danym zdarzeniem), zasady poinformowania zgłaszającego o wyniku podjętych działań w danej sprawie itd. Warto rozważyć również uwzględnienie w takim dokumencie tzw. alarmu działania pod przymusem, aby pracownik, który jest zmuszony do wykonania jakiś czynności niezgodnych z wewnętrzną polityką mógł niezauważenie poinformować o działaniu pod przymusem[200].

Rekomenduje się by operatorzy usług kluczowych mieli opracowane odpowiednie procedury, w których będą przypisane role do poszczególnych stanowisk/komórek organizacyjnych, a także zakres odpowiedzialności. Ponadto, podmioty powinny wdrożyć mechanizmy monitorowania, analizowania i reagowania na incydenty[201].

Dysponowanie odpowiednimi procedurami i mechanizmami, w których każde stanowisko i komórka organizacyjna zaangażowana w obsługę incydentu wie co ma robić i jaki jest jej zakres kompetencji, przyczyni się do sprawnego zarządzania sytuacją kryzysową. Procedury te powinny być również dostoswane do specyfiki danego przedsiębiorstwa, a nawet rodzaju zdarzenia i typu incydentu. Powinny również zostać opracowane dokumenty ustalające moment przejścia, np. na tryb awaryjny

[199] J. Krawiec, G. Ożarek, *System zarządzania bezpieczeństwem informacji w praktyce. Zabezpieczenia.*, Polski Komitet Normalizacyjny, Warszawa 2014, s. 88.
[200] J. Krawiec, G. Ożarek, *System zarządzania bezpieczeństwem informacji w praktyce. Zabezpieczenia.*, Polski Komitet Normalizacyjny, Warszawa 2014, s. 89.
[201] Ibidem, s. 89-90.

funkcjonowania systemów, a nawet na sterowanie ręczne. W rezultacie, operatorzy powinni dysponować planami ciągłości działania (szerzej opisane w rozdziale 9).

W czasie obsługi incydentu zaleca się bieżące gromadzenie materiału dowodowego i analizowanie znalezionych artefaktów.

Zebranie materiału dowodowego jest o tyle ważne, że może dać odpowiedź na wiele pytań pojawiających się w czasie incydentu – kto zaatakował, dlaczego, w jaki sposób, jakie luki zostały wykorzystane itd. Ponadto, pozwoli na przekazanie materiału do CSIRT poziomu krajowego, który również będzie mógł przeprowadzić analizę we własnym zakresie. Co więcej, możliwe będzie ustalenie czy podobne incydenty miały miejsce w innych sektorach bądź państwach.

W ramach procedur zarządzania incydentem, powinny również zostać ustalone sposoby komunikacji z CSIRTami poziomu krajowego, organem właściwym ds. cyberbezpieczeństwa, organami ścigania i innymi podmiotami, ważnymi z punktu widzenia danego operatora usługi kluczowej.

W momencie wystąpienia incydentu warto mieć wcześniej ustalone sposoby komunikacji na wypadek niedostępności powszechnych środków komunikacji. Ponadto, warto mieć ustalone konkretne numery telefonów oraz dane przedstawicieli poszczególnych instytucji, aby można było łatwo zweryfikować czy informacja wysłana przez operatora usługi kluczowej dociera do właściwej osoby, a nie np. do cyberprzestępcy. Incydenty charakteryzują się często dużą dynamiką zmian, więc obsługa incydentu wymaga niejednokrotnie ciągłego kontaktu z CSIRTami poziomu krajowego i innymi podmiotami. Zatem, ustanowienie efektywnych kanałów komunikacji wydaje się być ważnym aspektem zarządzania incydentem. CSIRT poziomu krajowego może zaoferować operatorowi wsparcie techniczne, pomoc w oszacowaniu potencjalnego wpływu na usługę kluczową, obywateli, społeczeństwo, gospodarkę itd., wspomóc ograniczenie wpływu incydentu na inne podmioty (np. operatorów usług kluczowych z powiązanych sektorów czy podsektorów), w tym pozostałe CSIRT poziomu krajowego. Zatem, pierwsze informacje o wystąpieniu zdarzenia, powinny zostać przekazane w sposób zwięzły, ponieważ często na początkowym etapie zdarzenia operator może nie posiadać dużej ilości informacji[202]. Jeżeli operator od razu dysponuje większą wiedzą, to zaleca się szersze opisanie zdarzenia.

Zgodnie z UKSC, operator usługi kluczowej ma obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, a w przypadku zmiany jej danych lub zmiany osoby kontaktowej także niezwłoczne zaktualizowanie jej danych.

Operator usługi kluczowej wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (art. 9 ust. 1 pkt 1 UKSC), a następnie w ciągu 14 dni od dnia jej wyznaczenia przekazuje jej dane do organu właściwego ds. cyberbezpieczeństwa w sektorze energii, właściwego CSIRT poziomu krajowego, i w momencie jego powołania, do sektorowego zespołu cyberbezpieczeństwa. Operator może wyznaczyć więcej osób do kontaktu w ramach krajowego systemu cyberbezpieczeństwa. Wówczas, powinien przekazać dane tych osób do wskazanych wyżej podmiotów. Zgłoszenie takie powinno zawierać imię, nazwisko, numer telefonu oraz adres poczty elektronicznej. W przypadku zmiany osób wyznaczonych do kontaktu

[202] *Guidelines on notification of Operators of Essential Services incidents. Formats and procedures., NIS Cooperation Group*, CG Publication 05/2018, Lipiec 2018, [PDF] s. 11-12, ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677 [dostęp: 09.06.2021].

w ramach krajowego systemu cyberbezpieczeństwa bądź ich danych, operator ma obowiązek przekazać odpowiednią informację do wspomnianych podmiotów w terminie 14 dni od dnia ich zmiany. Jest to ważna czynność, ponieważ w przypadku wystąpienia incydentu, osoba taka jest głównym punktem kontaktowym, przekazującym odpowiednie dane do CSIRT poziomu krajowego (w przypadku wystąpienia incydentu poważnego – patrz rozdział 13.4.1), a także do wiadomości organu właściwego. Ponadto, osoba wskazana do kontaktów w ramach krajowego systemu cyberbezpieczeństwa otrzymuje również od organu właściwego informacje na temat zagrożeń, podatności, dobrych praktyk itd., przekazane od Pojedynczego Punktu Kontaktowego, ENISA, sieć CSIRT i innych partnerów. Z racji tego, posiadanie aktualnych danych przez organy właściwe, CSIRT poziomu krajowego i sektorowy zespół cyberbezpieczeństwa jest kluczowe w celu odpowiedniego zarządzania incydentem, a także wymiany informacji.

Zaleca się, by po opanowaniu incydentu uruchomić przygotowane wcześniej procedury odtworzenia po awarii.

Po zażegnaniu sytuacji kryzysowej konieczne jest powrócenie do codziennego działania systemów. Tematyka związana z odbudową została opisana w rozdziale 9.3 Rekomendacji.

Rekomenduje się regularne sprawdzanie opracowanych procedur poprzez organizację wewnętrznych ćwiczeń.

Przeprowadzanie regularnych ćwiczeń w zakresie reagowania na incydenty pozwala zweryfikować poziom znajomości mechanizmów przez poszczególnych pracowników i komórki organizacyjne. Tym samym, w momencie wystąpienia prawdziwego incydentu, osoby zaangażowane w obsługę incydentu wiedzą od razu jakie działania mają podjąć, bez konieczności szczegółowego czytania instrukcji, co niejednokrotnie może wydłużyć czas obsługi incydentu.

Operatorom usług kluczowych rekomenduje się podłączenie do systemu teleinformatycznego S46 w celu posiadania pełniejszej wiedzy na temat zagrożeń, incydentów i powiązań międzysektorowych.

System teleinformatyczny S46 został utworzony zgodnie z art. 46 ust. 1 UKSC. Za rozwój i utrzymanie systemu odpowiada minister właściwy ds. informatyzacji[203]. Głównym celem S46 jest wspieranie współpracy podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa, zgłaszanie i obsługa incydentów, szacowanie ryzyka na poziomie krajowym oraz ostrzeganie o zagrożeniach cyberbezpieczeństwa. System ten opiera się na ustaleniu poziomu zależności pomiędzy operatorami usług kluczowych z różnych sektorów, a następnie zbudowanie sieci powiązań. Umożliwi to szacowanie ryzyka na poziomie krajowym, a także pozwoli na pełne zrozumienie ewentualnych efektów kaskadowych incydentów w ramach krajowego systemu cyberbezpieczeństwa.

[203] *Rozwój systemu teleinformatycznego S46*, https://www.nask.pl/pl/projekty-dofinansowane/projekty-realizowane-ze/3957,Rozwoj-systemu-teleinformatycznego-S46.html

14. Tabela poziomów dojrzałości organizacji

Poniższa tabela przedstawia prosty model określający cztery poziomy dojrzałości organizacji pod kątem cyberbezpieczeństwa, oparty na dziesięciu kategoriach środków zaradczych wskazanych przez ENISA[204], które obejmują przedłożone rekomendacje sektorowe na rzecz wzmocnienia cyberbezpieczeństwa w sektorze energetycznym

Wartości wskazane w poniższej tabeli oznaczają:

0 – brak stosowania środka zaradczego,

1 – niski poziom dojrzałości organizacji,

2 – średni poziom dojrzałości organizacji,

3 – wysoki poziom dojrzałości organizacji.

Tabela 4 – Przypisanie środków zaradczych do poziomów dojrzałości.

Kategorie środków zaradczych	Stosowanie środków zaradczych w odniesieniu do poziomów dojrzałości				
		0	1	2	3
Zarządzanie ryzykiem	4.1 Polityka Bezpieczeństwa Informacji		X	X	X
	4.2 Organizacja bezpieczeństwa informacji		X	X	X
	4.3 Metodyka zarządzania ryzykiem, szacowanie ryzyka			X	X
	4.4 Plan postępowania z ryzykiem				X
Zarządzanie stroną trzecią	5.1 Umowy z podmiotami trzecimi			X	X
	5.2 Monitorowanie usług świadczonych przez strony trzecie, weryfikacja rozwiązań w oparciu o uzgodnione kryteria				X
	5.3 Korzystanie z usług chmurowych				X
Cykl życia systemów informacyjnych	6.1 Analiza i specyfikacja wymagań bezpieczeństwa		X	X	X
	6.2 Cykl życia systemów informacyjnych		X	X	X
	6.3 Zarządzanie aktywami		X	X	X
	6.4 Utrzymanie systemów informacyjnych			X	X
	6.5 Aktualizacja oprogramowania		X	X	X

[204] Dziesięć kategorii środków zaradczych wskazanych w ENISA, *Appropriate Security Measures for Smart Grids. Guidelines to Assess the Sophistication of Security Measures Implementation*, 2012, s. 6.

	6.6 Zarządzanie licencjami			X	X
	6.7 Testowanie systemów i komponentów		X	X	X
Bezpieczeństwo osobowe, podnoszenie świadomości, szkolenia	7.1 Program podnoszenia kompetencji z zakresu cyberbezpieczeństwa		X	X	X
	7.2 Podnoszenie kompetencji i kwalifikacji		X	X	X
	7.3 Weryfikacja personelu, zmiany kadrowe				X
Audyty bezpieczeństwa systemów informacyjnych	8.1 Audyty bezpieczeństwa systemów informacyjnych		X	X	X
	8.2 Metodyki audytu systemów informacyjnych			X	X
Zachowanie ciągłości działania i odbudowa	9.1 Ciągłość świadczenia usług kluczowych		X	X	X
	9.2 Wymagania dla komunikacji i wymiany informacji związanych z ciągłością działania		X	X	X
	9.3 Odbudowa, plan odbudowy po katastrofie (DRP)				X
Bezpieczeństwo fizyczne	10.1 Bezpieczeństwo fizyczne		X	X	X
	10.2 Bezpieczeństwo fizyczne stron trzecich				X
Bezpieczeństwo sieci łączności elektronicznej	11.1 Segmentacja sieci, protokoły, szyfrowanie		X	X	X
	11.2 Monitorowanie sieci teleinformatycznych		X	X	X
Bezpieczeństwo systemów informacyjnych	12.1 Ochrona danych		X	X	X
	12.2 Zarządzanie uprawnieniami		X	X	X
	12.3 Kontrola dostępu do danych			X	X
	12.4 Dostęp zdalny i urządzenia mobilne			X	X
	12.5 Bezpieczeństwo systemów automatyki przemysłowej, sieci inteligentnych				X
Wytyczne sektorowe dotyczące zgłaszania incydentów	13.1 Zdolność w zakresie reagowania na incydenty		X	X	X
	13.2 Zarządzanie zagrożeniami		X	X	X
	13.3 Zarządzanie podatnościami			X	X
	13.4 Katalog incydentów			X	X
	13.4.1 Incydenty poważne		X	X	X
	13.4.2 Incydenty krytyczne				X
	13.5 Zarządzanie incydentem cyberbezpieczeństwa		X	X	X

Źródło*: opracowanie własne na podstawie ECOFYS, „Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector – final report", 2018, s. 167-168.*

15. Załączniki

Załącznik nr 1
Wzór formularza weryfikacji dojrzałości cyberbezpieczeństwa organizacji

Poniżej znajduje się poglądowo uzupełniony formularz weryfikacji dojrzałości organizacji pod kątem cyberbezpieczeństwa:

Formularz weryfikacji dojrzałości organizacji pod kątem cyberbezpieczeństwa							
Nazwa organizacji:	XYZ						
Sektor:	Energia						
Podsektor/ podsektory:	Energia elektryczna						
AKTYWNOŚĆ	**KATEGORIA**	**PODKATEGORIA**	**STOPIEŃ WDROŻENIA (1-5)**	**ŚREDNI WYNIK KATEGORII (1-5)**	**ŚREDNI WYNIK AKTYWNOŚCI**	**CAŁKOWITY WYNIK (108-540)**	**RELATYWNY POZIOM DOJRZAŁOŚCI**
IDENTYFIKACJA (ID)	**Zarządzanie aktywami (ID.ZA)** - Dane, personel, urządzenia, systemy i obiekty, które umożliwiają organizacji osiągnięcie celów biznesowych, są identyfikowane i zarządzane zgodnie z ich znaczeniem dla celów organizacyjnych i strategii ryzyka organizacji.	**ID.ZA-1** - Urządzenia fizyczne i systemy w organizacji są inwentaryzowane.	3	3,17	**3,31**	**340**	**ŚREDNI**
		ID.ZA-2 - Platformy software i aplikacje w organizacji są inwentaryzowane.	2				
		ID.ZA-3 - Komunikacja w organizacji oraz przepływy danych są mapowane.	5				
		ID.ZA-4 - Zewnętrzne systemy informacyjne są skatalogowane.	4				
		ID.ZA-5 - Zasoby (np. sprzęt, urządzenia, dane, czas, personel i oprogramowanie) są traktowane priorytetowo zgodnie z ich klasyfikacją, krytycznością i wartością biznesową.	2				
		ID.ZA-6 - Role i odpowiedzialność w zakresie cyberbezpieczeństwa są określone dla wszystkich pracowników oraz podmiotów zewnętrznych (np. dostawców, klientów, partnerów).	3				
	Otoczenie biznesowe (ID.OB) - Misja, cele, interesariusze i działania organizacji są rozumiane i priorytetyzowane – informacje te są wykorzystywane do informowania o rolach, obowiązkach i decyzjach dotyczących zarządzania ryzykiem w zakresie cyberbezpieczeństwa.	**ID.OB-1** - Rola organizacji w łańcuchu dostaw jest określona i komunikowana.	1	3,40			
		ID.OB-2 - Miejsce organizacji w jej sektorze przemysłowym jest zidentyfikowane i komunikowane.	4				
		ID.OB-3 - Priorytety misji, celów i działań organizacji są ustalane i komunikowane.	4				
		ID.OB-4 - Zależności i krytyczne funkcje dla świadczenia usług kluczowych są określone.	3				
		ID.OB-5 - Wymagania dotyczące odporności dla świadczenia usług kluczowych, są ustanawiane dla wszystkich warunków funkcjonowania organizacji (np. w trakcie ataku, w trakcie odbudowy czy normalnego funkcjonowania).	5				

IDENTYFIKACJA (ID)	**Zarządzanie (ID.Z)** - Zasady, procedury i procesy zarządzania i monitorowania wymogów w zakresie regulacyjnym, prawnym, ryzyka, ochrony środowiska i operacyjnym w organizacji są zrozumiałe i informują o zarządzaniu ryzykiem cyberbezpieczeństwa.	**ID.Z-1** - Polityka cyberbezpieczeństwa organizacji jest ustanowiona i przekazywana.	2	2,75	**3,31**	**340**	**ŚREDNI**
		ID.Z-2 - Role i obowiązki w zakresie cyberbezpieczeństwa są koordynowane i dostosowane do ról wewnętrznych oraz partnerów zewnętrznych.	4				
		ID.Z-3 - Wymogi prawne i regulacyjne dotyczące cyberbezpieczeństwa, w tym obowiązki w zakresie prywatności i swobód obywatelskich, są rozumiane i zarządzane.	3				
		ID.Z-4 - Zarządzanie w organizacji oraz zarządzanie ryzykiem odnoszą się do zagrożeń związanych z cyberbezpieczeństwem.	2				
	Szacowanie ryzyka (ID.SR) - Organizacja rozumie ryzyko cyberbezpieczeństwa dla działalności organizacyjnej (w tym misji, funkcji, wizerunku lub reputacji), zasobów organizacyjnych i osób.	**ID.SR-1** - Podatności w zasobach są identyfikowane i dokumentowane.	5	3,83			
		ID.SR-2 - Informacje o zagrożeniach cyberbezpieczeństwa są pozyskiwane ze źródeł wymiany informacji.	4				
		ID.SR-3 - Zagrożenia, zarówno wewnętrzne, jak i zewnętrzne, są identyfikowane i dokumentowane.	3				
		ID.SR-4 - Potencjalne skutki biznesowe i prawdopodobieństwo wystąpienia zostały zidentyfikowane.	4				
		ID.SR-5 - Zagrożenia, podatności, prawdopodobieństwo wystąpienia i skutki są używane do określania ryzyka.	2				
		ID.SR-6 - Odpowiedzi na ryzyko są identyfikowane i priorytetyzowane.	5				
	Strategia zarządzania ryzykiem (ID.ZR) - Priorytety, ograniczenia, tolerancja ryzyk i założenia organizacji są określone i wspierają decyzje dotyczące ryzyka operacyjnego.	**ID.ZR-1** - Procesy zarządzania ryzykiem są ustanawiane, zarządzane i uzgadniane przez zainteresowane strony.	2	3,00			
		ID.ZR-2 - Tolerancja ryzyka w organizacji jest określona i wyraźnie wyrażona.	4				
		ID.ZR-3 - Organizacja określa tolerancję ryzyka na podstawie jej roli w infrastrukturze kluczowej oraz analizie ryzyka sektorowego.	3				

IDENTYFIKACJA (ID)	**Zarządzanie ryzykiem łańcucha dostaw (ID.ŁD)** - Priorytety, ograniczenia, tolerancja ryzyk i założenia organizacji są określone i wykorzystywane do wspierania decyzji o ryzyku związanych z zarządzaniem ryzykiem łańcucha dostaw. Organizacja ustanowiła i wdrożyła procesy identyfikacji, szacowania i zarządzania ryzykiem łańcucha dostaw.	**ID.ŁD-1** - Procesy zarządzania ryzykiem cyberbezpieczeństwa w łańcuchu dostaw są identyfikowane, ustanawiane, oceniane, zarządzane i uzgadniane przez zainteresowane podmioty.	5	3,40	**3,31**	**340**	**ŚREDNI**
		ID.ŁD-2 - Partnerzy zewnętrzni i dostawcy w zakresie systemów informacyjnych, komponentów i usług są identyfikowani, priorytetyzowani i oceniani za pomocą procesu oceny ryzyka cyberbezpieczeństwa w łańcuchu dostaw.	2				
		ID.ŁD-3 - Umowy z dostawcami i partnerami zewnętrznymi są wykorzystywane do wdrażania odpowiednich środków dla osiągnięcia celów programu cyberbezpieczeństwa organizacji oraz Planu Zarządzania Ryzykiem Cyberbezpieczeństwa w Łańcuchu Dostaw.	4				
		ID.ŁD-4 - Dostawcy i partnerzy zewnętrzni są stale oceniani przy użyciu audytów, wyników testów lub innych form oceny w celu potwierdzenia, że wywiązują się ze swoich zobowiązań umownych.	3				
		ID.ŁD-5 - Planowanie i testowanie reagowania oraz odzyskiwania jest realizowane wraz z dostawcami, również zewnętrznymi.	3				
OCHRONA (OCH)	**Zarządzanie tożsamościami, uwierzytelnianie i kontrola dostępu (OCH.KD)** - Dostęp do zasobów fizycznych i logicznych oraz powiązanych obiektów jest ograniczony do autoryzowanych użytkowników, procesów i urządzeń oraz jest zarządzany zgodnie z ocenianym ryzykiem nieautoryzowanego dostępu do autoryzowanych działań i transakcji.	**OCH.KD-1** - Tożsamości i poświadczenia są wystawiane, zarządzane, weryfikowane, odwoływane i audytowane dla autoryzowanych urządzeń, użytkowników oraz procesów.	2	3,29	**3,13**		
		OCH.KD-2 - Fizyczny dostęp do zasobów jest zarządzany i chroniony.	3				
		OCH.KD-3 - Dostęp zdalny jest zarządzany.	4				
		OCH.KD-4 - Uprawnienia dostępu i autoryzacja są zarządzane z uwzględnieniem zasady najniższych uprawnień i rozdzielenia obowiązków.	5				
		OCH.KD-5 - Integralność sieci jest chroniona (np. poprzez segregację sieci czy jej segmentację).	2				
		OCH.KD-6 - Tożsamości są sprawdzane i powiązywane z poświadczeniami oraz potwierdzane w interakcjach.	2				
		OCH.KD-7 - Użytkownicy, urządzenia i inne zasoby są uwierzytelniane (np. jednoskładnikowo, wieloskładnikowo) współmierne do ryzyka działania (np. ryzyk dla bezpieczeństwa i prywatności osób fizycznych oraz innych ryzyk organizacyjnych).	5				

OCHRONA (OCH)	**Świadomość i podnoszenie kompetencji (OCH. PK)** - Personel i partnerzy organizacji są edukowani w zakresie podnoszenia świadomości dotyczącej cyberbezpieczeństwa i są szkoleni w kontekście wykonywania zadań i obowiązków związanych z cyberbezpieczeństwem, zgodnie z odpowiednimi politykami, procedurami i umowami.	**OCH.PK-1** - Wszyscy użytkownicy są informowani i szkoleni.	3	3,00	**3,13**	**340**	**ŚREDNI**
		OCH.PK-2 - Użytkownicy ze zwiększonymi uprawnieniami rozumieją swoje role i obowiązki.	4				
		OCH.PK-3 - Podmioty zewnętrzne (np. dostawcy, klienci, partnerzy) rozumieją swoje role i obowiązki.	1				
		OCH.PK-4 - Kadra kierownicza wyższego szczebla rozumie swoje role i obowiązki.	5				
		OCH.PK-5 - Personel cyberbezpieczeństwa oraz bezpieczeństwa fizycznego rozumie swoje role i obowiązki.	2				
	Bezpieczeństwo danych (OCH. BD) - Informacje i rejestry (dane) są zarządzane zgodne ze strategią ryzyka organizacji w celu ochrony poufności, integralności i dostępności informacji.	**OCH.BD-1** - Dane w spoczynku są chronione.	4	3,50			
		OCH.BD-2 - Przesyłane dane są chronione.	3				
		OCH.BD-3 - Zasoby są formalnie zarządzane podczas usuwania, przenoszenia i dysponowania.	4				
		OCH.BD-4 - Utrzymywana jest odpowiednia zdolność do zapewnienia dostępności.	3				
		OCH.BD-5 - Wdrożono mechanizmy ochrony przed wyciekami danych.	2				
		OCH.BD-6 - Mechanizmy sprawdzania integralności są używane do weryfikacji oprogramowania, firmware oraz integralności informacji.	5				
		OCH.BD-7 - Środowisko(-a) rozwoju i testowania jest oddzielone od środowiska produkcyjnego.	4				
		OCH.BD-8 - Mechanizmy sprawdzania integralności służą do weryfikacji integralności sprzętu.	3				

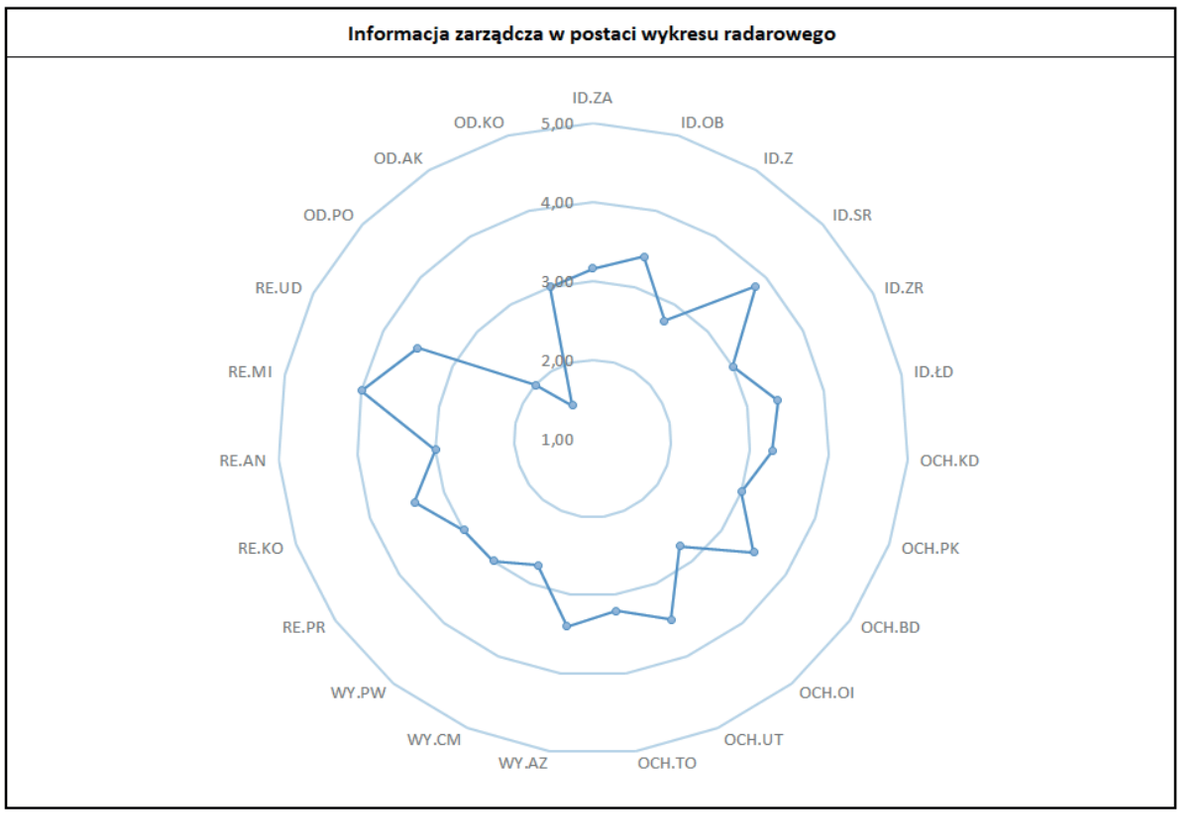
OCHRONA (OCH)	**Procedury i procesy ochrony informacji (OCH.OI)** - Polityki bezpieczeństwa (dotyczące celu, zakresu, ról, obowiązków, zaangażowania kierownictwa i koordynacji między jednostkami organizacyjnymi), procesy i procedury są utrzymywane i używane do zarządzania ochroną systemów informacyjnych oraz zasobów.	**OCH.OI-1** - Podstawowa konfiguracja systemów informacyjnych/przemysłowych systemów sterowania jest tworzona i utrzymywana z zastosowaniem zasad bezpieczeństwa (np. zasady najmniejszej funkcjonalności).	2	2,75	**3,13**	**340**	**ŚREDNI**
		OCH.OI-2 - Wdrożony jest cykl życia rozwoju systemów, w celu zarządzania systemami.	4				
		OCH.OI-3 - Stosowane są procesy kontroli zmiany konfiguracji.	2				
		OCH.OI-4 - Kopie zapasowe informacji są sporządzane, utrzymywane i testowane.	5				
		OCH.OI-5 - Warunki wynikające z polityk i regulacji dotyczących fizycznego środowiska operacyjnego dla aktywów organizacji są spełnione.	1				
		OCH.OI-6 - Dane są niszczone zgodnie z funkcjonującymi politykami.	1				
		OCH.OI-7 - Procesy ochrony są usprawniane.	2				
		OCH.OI-8 - Informacje na temat skuteczności technologii ochrony są przekazywane.	2				
		OCH.OI-9 - Organizacja posiada i zarządza planami reagowania (w zakresie reagowania na incydenty i ciągłości działania) oraz planami odtwarzania (w zakresie odtwarzania po incydencie i po awarii).	3				
		OCH.OI-10 - Plany reagowania i odtwarzania są testowane.	4				
		OCH.OI-11 - Cyberbezpieczeństwo jest stosowane w praktykach w zakresie zasobów ludzkich (np. dotyczących zarządzania kontami byłych pracowników, monitorowania personelu).	5				
		OCH.OI-12 - Opracowano i wdrożono plan zarządzania podatnościami.	2				
	Utrzymanie (OCH.UT) - Utrzymanie i naprawa elementów przemysłowych systemów sterowania oraz systemów informacyjnych jest realizowana zgodnie z politykami i procedurami.	**OCH.UT-1** - Konserwacja i naprawa zasobów organizacji jest wykonywana i odpowiednio rejestrowana za pomocą zatwierdzonych i kontrolowanych narzędzi.	4	3,50			
		OCH.UT-2 - Zdalna obsługa zasobów organizacji jest zatwierdzana, rejestrowana i wykonywana w sposób zapobiegający nieautoryzowanemu dostępowi.	3				

OCHRONA (OCH)	**Technologia ochronna (OCH.TO)** - Techniczne rozwiązania bezpieczeństwa są zarządzane w celu zapewnienia bezpieczeństwa i odporności systemów i zasobów, zgodnie z odpowiednimi politykami, procedurami i umowami.	**OCH.TO-1** - Zapisy logów/ inspekcji są określone, dokumentowane, wdrażane i sprawdzane zgodnie z politykami.	3	3,20	**3,13**	**340**	**ŚREDNI**
		OCH.TO-2 - Nośniki wymienne są chronione, a ich stosowanie ograniczone zgodnie z politykami.	4				
		OCH.TO-3 - Zasada najmniejszej funkcjonalności jest wdrożona poprzez odpowiednią konfigurację systemów tak, by posiadały tylko niezbędne możliwości.	2				
		OCH.TO-4 - Sieci komunikacyjne i sterowania są chronione.	4				
		OCH.TO-5 - Odpowiednie mechanizmy (jak np. failsafe, równoważenie obciążenia, hot swap) są wdrażane w celu osiągnięcia wymagań dotyczących odporności w normalnych i niekorzystnych sytuacjach.	3				
WYKRYWANIE (WY)	**Anomalie i zdarzenia (WY.AZ)** - Nietypowa aktywność jest wykrywana, a potencjalny wpływ zdarzenia jest zrozumiany.	**WY.AZ-1** - Poziom bazowy operacji sieciowych oraz spodziewanych przepływów danych dla użytkowników i systemów jest określony i zarządzany.	2	3,40	**3,00**		
		WY.AZ-2 - Wykryte zdarzenia są analizowane aby zrozumieć cele i metody ataku.	5				
		WY.AZ-3 - Dane o zdarzeniach są pozyskiwane oraz korelowane z wielu źródeł i czujników.	3				
		WY.AZ-4 - Wpływ zdarzeń jest określany.	4				
		WY.AZ-5 - Progi alarmowe incydentów są ustalone.	3				
	Ciągłe monitorowanie bezpieczeństwa (WY.CM) - System informacyjny i zasoby są monitorowane by identyfikować zdarzenia związane z cyberbezpieczeństwem i weryfikować skuteczność środków ochronnych.	**WY.CM-1** - Sieć jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa.	2	2,75			
		WY.CM-2 - Środowisko fizyczne jest monitorowane w celu wykrycia potencjalnych zdarzeń cyberbezpieczeństwa.	3				
		WY.CM-3 - Aktywność personelu jest monitorowana w celu wykrycia potencjalnych zdarzeń związanych z cyberbezpieczeństwem.	4				
		WY.CM-4 - Złośliwy kod jest wykrywany.	3				
		WY.CM-5 - Nieautoryzowany kod mobilny jest wykrywany (np. ActiveX, JavaScript).	2				
		WY.CM-6 - Aktywność zewnętrznego dostawcy usług jest monitorowana w celu wykrywania potencjalnych zdarzeń cyberbezpieczeństwa.	1				
		WY.CM-7 - Przeprowadza się monitorowanie pod kątem nieautoryzowanego personelu, połączeń, urządzeń i oprogramowania.	4				
		WY.CM-8 - Przeprowadza się skanowanie podatności.	3				

WYKRYWANIE (WY)	**Procesy wykrywania (WY.PW)** - Procesy i procedury wykrywania są utrzymywane i testowane w celu zapewnienia świadomości w zakresie nietypowych zdarzeń.	**WY.PW-1** - Role i obowiązki w zakresie wykrywania są dobrze zdefiniowane, w celu zapewnienia rozliczalności.	2	3,00	**3,00**	**340**	**ŚREDNI**
		WY.PW-2 - Działania związane z wykrywaniem spełniają wszystkie obowiązujące wymagania.	4				
		WY.PW-3 - Procesy wykrywania są testowane.	3				
		WY.PW-4 - Informacje o wykrywaniu zdarzeń są przekazywane.	2				
		WY.PW-5 - Procesy wykrywania są stale udoskonalane.	4				
REAGOWANIE (RE)	**Planowanie reagowania (RE.PR)** - Procesy i procedury reagowania są realizowane i utrzymywane by zapewnić reagowanie na wykryte incydenty cyberbezpieczeństwa.	**RE.PR-1** - Plan reagowania jest realizowany w trakcie lub po incydencie.	3	3,00	**3,38**		
	Komunikacja (RE.KO) - Działania w zakresie reagowania są koordynowane z podmiotami wewnętrznymi i zewnętrznymi (np. wsparcie zewnętrzne ze strony organów ścigania).	**RE.KO-1** - Personel zna swoje role i kolejność operacji, na wypadek konieczności reagowania.	2	3,40			
		RE.KO-2 - Incydenty są zgłaszane zgodnie z ustalonymi kryteriami.	3				
		RE.KO-3 - Informacje są udostępniane zgodnie z planami reagowania.	4				
		RE.KO-4 - Koordynacja z zainteresowanymi stronami jest prowadzona w sposób zgodny z planami reagowania.	4				
		RE.KO-5 - Dobrowolna wymiana informacji z zewnętrznymi podmiotami jest prowadzona w celu osiągnięcia szerszej świadomości sytuacyjnej w zakresie cyberbezpieczeństwa.	4				
	Analiza (RE.AN) - Przeprowadza się analizy w celu zapewnienia skutecznej reakcji i wspierania działań naprawczych.	**RE.AN-1** - Powiadomienia z systemów wykrywania są badane.	3	3,00			
		RE.AN-2 - Wpływ incydentu jest rozumiany.	2				
		RE.AN-3 - Stosowane są działania związane z informatyką śledczą.	3				
		RE.AN-4 - Zdarzenia są klasyfikowane zgodnie z planami reagowania.	4				
		RE.AN-5 - Procesy są ustanawiane w celu otrzymywania, analizowania i reagowania na podatności ujawnione dla organizacji ze źródeł wewnętrznych i zewnętrznych (np. wewnętrznych testów, biuletynów bezpieczeństwa czy badaczy bezpieczeństwa).	3				

REAGOWANIE (RE)	**Mitygacja (RE.MI)** - Wykonuje się działania w celu zapobiegania rozwojowi zdarzenia, złagodzenia jego skutków i zakończenia obsługi incydentu.	**RE.MI-1** - Incydenty są opanowywane.	2	4,00	**3,38**	**340**	**ŚREDNI**
		RE.MI-2 - Incydenty są mitygowane.	5				
		RE.MI-3 - Nowo zidentyfikowane podatności są mitygowane lub dokumentuje się akceptację ryzyka związanego z nimi.	5				
	Udoskonalanie (RE.UD) - Działania w zakresie reagowania organizacji są udoskonalane poprzez uwzględnianie wniosków wyciągniętych z bieżących i poprzednich działań związanych z wykrywaniem i reagowaniem.	**RE.UD-1** - Plany reagowania uwzględniają wyciągnięte wnioski.	3	3,50			
		RE.UD-2 - Strategie reagowania są aktualizowane.	4				
ODTWARZANIE (OD)	**Planowanie odtwarzania (OD.PO)** - Procesy i procedury odtwarzania są realizowane i utrzymywane w celu zapewnienia przywrócenia systemów lub zasobów dotkniętych incydentem cyberbezpieczeństwa.	**OD.PO-1** - Plan odtwarzania jest realizowany w trakcie lub po incydencie cyberbezpieczeństwa.	2	2,00	**2,33**		
	Aktualizacja (OD.AK) - Planowanie i procesy związane z odtwarzaniem są udoskonalane poprzez wzięcie pod uwagę dotychczasowych doświadczeń, na rzecz przyszłych działań.	**OD.AK-1** - Plany odtwarzania zawierają wyciągnięte dotychczas wnioski.	1	1,50			
		OD.AK-2 - Strategie odtwarzania są aktualizowane.	2				
	Komunikacja (OD.KO) - Działania odtwórcze są koordynowane z podmiotami wewnętrznymi i zewnętrznymi (np. centrami koordynującymi, dostawcami usług internetowych, poszkodowanymi, innymi CSIRT i dostawcami).	**OD.KO-1** - Public relations są zarządzane.	3	3,00			
		OD.KO-2 - Reputacja organizacji po wystąpieniu incydentu jest odzyskiwana.	2				
		OD.KO-3 - Działania naprawcze są przekazywane podmiotom wewnętrznym i zewnętrznym, a także zespołom wykonawczym i zarządzającym.	4				

Wykres radarowy wizualizujący powyższe dane:



Objaśnienie zastosowanej skali punktowej stopni wdrożenia:

Objaśnienie skali punktowej stosowanej w formularzu		
Stopień wdrożenia	Skala	Objaśnienie
1	Niski	Brak świadomości, brak wiedzy.
2		Realizowane ad-hoc, procesy są niesformalizowane, słabo kontrolowane, słaba powtarzalność.
3	Średni	Procesy są zarządzane, udokumentowane, realizowane przez większość czasu. Realizacja może być niekonsekwentna.
4		Procesy są ustandaryzowane, dobrze ustanowione, konsekwentnie realizowane, powtarzalne, okresowo przeglądane i aktualizowane.
5	Wysoki	Procesy są weryfikowane pod kątem udoskonaleń w trybie ciągłym. Mogą być uznane za najlepsze w swojej klasie lub jako wiodące praktyki.

Załącznik nr 2
Przykładowa lista szkoleń dla pracowników operatorów usług kluczowych

	Przykładowe tematy szkoleń dla pracowników operatorów usług kluczowych
1	Sieci i systemy informacyjne w energetyce i przemyśle
	1.1 Wstęp do automatyki przemysłowej; 1.2 Systematyka systemów informacyjnych w przemyśle; 1.3 Komponenty automatyki przemysłowej; 1.4 Przewodowe i bezprzewodowe sieci przemysłowe.
2	Ataki
	2.1 Cele ataków; 2.2 Źródła ataków; 2.3 Projektowanie sieci OT a bezpieczeństwo (vs. cele biznesowe); 2.4 Automatyka vs. Bezpieczeństwo; 2.5 Rozumiem, jak pracuje sieć; 2.6 Rola socjotechniki w atakach; 2.7 Analiza zdarzeń – OSINT; 2.8 Bezpieczeństwo systemów a zagrożenia; 2.9 Zwalczanie cyberataków na sieci OT; 2.10 Główne wektory ataków – obrona; 2.11 Cyberataki na infrastrukturę krytyczną – praktyczne ćwiczenia i warsztaty.
3	Rozpoznanie
	3.1 Poznanie środowiska IT i OT kluczem do oceny bezpieczeństwa; 3.2 Protokoły i urządzenia w sieci przemysłowej; 3.3 Metody rozpoznawania topologii i inwentaryzacji urządzeń; 3.4 Rozwiązania w zakresie monitoringu sieci; 3.5 Implementacja systemów monitorowania w zależności od topologii sieci i potrzeb – zalecenia projektowe; 3.6 Inwentaryzacja oraz monitoring urządzeń znajdujących się na publicznych adresach IP; 3.7 *Threat Hunting* – analiza taktyk i technik wykorzystywanych przez grupy APT oraz przełożenie ich na własne systemy bezpieczeństwa; 3.8 Wykorzystanie narzędzi do pasywnej identyfikacji i inwentaryzacji aktyw*ów – wektory ataków*; 3.9 Zarządzanie siecią OT w chmurze – przyszłość czy zagrożenie?
4	Segmentacja
	4.1 Kontrola dostępu i ochrona przed zagrożeniami w sieciach przemysłowych: – kontrola dostępu per użytkownik, – kontrola dostępu per urządzenie, – dostęp zdalny, – optymalne podejście do nadawania dostępu wykonawcom, – strefa zdemilitaryzowana (ang. DMZ); 4.2 Macro i Micro segmentacja w sieciach przemysłowych: – segmentacja w obszarze strefy, – segmentacja na poziomie urządzenia końcowego, 4.3 Separacja sieci przemysłowych od sieci IT (np. urządzenia typu firewall w warstwach L1/L2/L3)); 4.4 Wykorzystanie standardu ISA/IEC 62443.

5	Wykrywanie
	5.1. Podatności w sieciach przemysłowych; 5.2. Rozwiązania w zakresie wykrywania ataków na sieci przemysłowe i narzędzia rejestrowania zdarzeń: – sygnaturowe wykrywanie zagrożeń, – niesygnaturowe wykrywanie zagrożeń (wykrywanie anomalii), – wykorzystanie narzędzi do monitoringu sieci OT pod kątem identyfikacji zagrożeń – alertowanie;
6	Reagowanie
	6.1 Współpraca między IT a OT; 6.2 Integracja sieci OT z SOC / SIEM / SOAR; 6.3 Pomoc zewnętrzna – usługi oparte na chmurze obliczeniowej; 6.4 Ulepszanie – poprawki, rekomendacje; 6.5 Monitorowanie sieci; 6.6 Wykorzystanie sztucznej inteligencji w ochronie systemów informacyjnych; 6.7 Standardy; 6.8 Narzędzia typu IPS/IDS i ich wykorzystanie w praktyce; 6.9 Koncepcja ochrony „Defence-In-Depth"; 6.10 Analiza poincydentalna.
7	7.1 Szacowania krytyczności współzależności pomiędzy systemami odpowiedzialnymi za procesy w kontekście ewentualnego cyberataku ; 7.2 Rola łańcucha dostaw w szacowaniu ryzyka dla systemów infrastruktury OT; 7.3 Laboratoria badawcze urządzeń OT (np. PLC); 7.4 Ćwiczenia – wirtualna elektrownia.
8	8.1 Metody i możliwości szyfrowania komunikacji; łączność specjalna; 8.2 Dostęp zdalny w ramach umów serwisowych dla firm zewnętrznych.
9	Szkolenie dot. finansowania cyberbezpieczeństwa: 9.1 Finansowanie z krajowych programów operacyjnych; 9.2 Krajowy Plan Odbudowy; 9.3 Program Cyfrowa Europa; 9.4 Centra Kompetencji.
10	10.1 Zarządzanie rozwojem architektury systemów informacyjnych w związku z nowymi procesami inwestycyjnymi; 11.1 Projektowanie i budowa sieci łączności i sterowania.
11	Tworzenie procedur w małych organizacjach dot. bezpieczeństwa. Procesowe podejście do bezpieczeństwa – ciągła praca nad bezpieczeństwem (aktualizacja, zarządzanie, wyznaczanie ról, szacowanie ryzyka itd.).
12	SOC – dobre praktyki: 12.1 Procedowanie umów na usługi typu SOC; 12.2 Modele outsourcingu; 12.3 Priorytetyzacja zdarzeń z różnych podmiotów; 12.4 Dobre praktyki budowania SOC wewnątrz organizacji.
13	Zamówienia publiczne – procedura opracowania specyfikacji istotnych warunków zamówienia z uwzględnieniem kwestii cyberbezpieczeństwa; Dobre praktyki w zakresie cyberbezpieczeństwa, które mogą zostać zastosowane na etapie procesu zakupowego rozwiązań automatyki przemysłowej (ICS).

14	Nowoczesne rozwiązania technologiczne z portfolio podmiotu (tematy zaproponowane przez podmioty prowadzące szkolenia)
15	Zarządzanie kryzysowe a cyberbezpieczeństwo: – integracja zarządzania kryzysem cyberbezpieczeństwa z zarządzaniem kryzysowym w podmiocie, – plan ciągłości działania, – plan odbudowy po incydencie.
16	16.1 IOT i IIOT – szanse i zagrożenia w OT; 16.2 Rozwiązania wykorzystywane do identyfikacji i monitorowania IoT.
17	Skuteczne zgłaszanie incydentów poważnych w rozumieniu UKSC: – definiowanie incydentów przez OUK, – kanały komunikacji, – wymagane dokumenty.
18	18.1 Zarządzanie zmianą w systemach przemysłowych OT z punktu widzenia krytyczności podatności w komponentach systemu; 18.2 Organizacja zespołów odpowiedzialnych za cyberbezpieczeństwo; 18.3 Współpraca zespołów IT, OT i cyberbezpieczeństwa w organizacji w odniesieniu do stosowania mechanizmów bezpieczeństwa i transferu wiedzy w zakresie swoich kompetencji; 18.4 Budowanie kompetencji poprzez szkolenie kadry w oparciu o certyfikaty (CISSP, CEH, …); 18.5 Zastosowanie Honeypot w OT.
19	19.1 Jak przeprowadzić testy penetracyjne w sieciach OT?; 19.2 Badanie wydajności sieci – testy obciążeniowe.
20	Konwergencja sieci IT i OT

Załącznik nr 3
Formularz audytowy opracowany przez ENISA

Obszar SZBI	Podobszar SZBI	Wymaganie bezpieczeństwa	Opis	Pytania	Dowody
Bezpieczeństwo	Zarządzanie incydentami	Raportowanie incydentów	Operator tworzy, wdraża i aktualizuje procedury zgłaszania incydentów.	Czy istnieje wykaz incydentów, mających miejsce w przeszłości?	Istnienie raportów związanych z wykrywaniem i przekazywaniem incydentów bezpieczeństwa w przeszłości.
				Czy polityka i procedury związane z reagowaniem na incydenty są regularnie i odpowiednio aktualizowane?	Aktualna dokumentacja polityki wykrywania incydentów oraz powiązanych procedur i systemów
				Czy przeprowadzane są przeglądy polityki wykrywania incydentów oraz związanych z nią procedur i systemów?	Dowody dokonywania przeglądów polityki wykrywania incydentów oraz powiązanych procedur i systemów.
				Czy organizacja regularnie przeprowadza ćwiczenia z zakresu cyberbezpieczeństwa?	Dowody przeprowadzonych w przeszłości ćwiczeń z zakresu cyberbezpieczeństwa, zawierające daty ich przeprowadzenia.
Bezpieczeństwo	Zarządzanie incydentami	Zgłaszanie incydentów właściwym jednostkom	Operator wdraża usługę, która umożliwia mu przyjmowanie do wiadomości bez zbędnej zwłoki informacji dotyczących incydentów, słabych punktów, zagrożeń i odpowiednich odwzorowań, wysyłanych przez właściwy organ krajowy (aktualny wykaz systemów informacyjnych, połączenia systemu z sieciami osób trzecich itp.)	Czy operator wdraża usługę, która umożliwia mu bezzwłoczne przyjmowanie informacji dotyczących incydentów, podatności, zagrożeń i mapowań incydentów, wysyłanych przez właściwy organ krajowy?	Dowody w postaci dzienników komunikacji z krajowymi organami ds. cyberbezpieczeństwa i/lub CSIRT.

Bezpieczeństwo	Wykrywanie incydentów	Logowanie do systemów	Operator ustanawia w każdym systemie informacyjnym system rejestrowania danych w celu rejestrowania zdarzeń związanych co najmniej z uwierzytelnianiem użytkowników, zarządzaniem kontami i prawami dostępu, modyfikacjami zasad bezpieczeństwa oraz funkcjonowaniem systemów informacyjnych.	Czy istnieje mechanizm śledzenia i dokumentowania incydentów związanych z bezpieczeństwem informacji w ramach procesu monitorowania incydentów?	Wykaz incydentów poważnych wykrytych i przekazywanych w przeszłości, zawierający powiązane informacje (przyczyna, wpływ, kolejność podjętych działań).
				Czy systemy zostały skonfigurowane w taki sposób, aby możliwe było automatyczne rejestrowanie i przekazywanie incydentów do odpowiednich osób?	Wykaz systemów, narzędzi i procedur służących do wykrywania i analizy incydentów.
Bezpieczeństwo	Wykrywanie incydentów	Korelacja i analiza zalogowań do systemów	Operator tworzy system korelacji i analizy zalogowań, który analizuje zdarzenia rejestrowane przez system logowania zainstalowany na każdym z systemów informacyjnych w celu wykrycia zdarzeń mających wpływ na bezpieczeństwo systemów informacyjnych.	Czy badane są incydenty związane z bezpieczeństwem informacji; czy tworzone są odpowiednie raporty przekazywane do kierownictwa organizacji?	Aktualna dokumentacja polityki wykrywania incydentów oraz powiązanych procedur i systemów
				Czy polityka wraz z procedurami związanymi z wykrywaniem incydentów jest aktualizowana w regularnych odstępach czasu?	Dowody dokonywania przeglądów polityki wykrywania incydentów oraz powiązanych procedur i systemów.
				Czy przeprowadzacie Państwo ćwiczenia z zakresu bezpieczeństwa informacji?	Dowody przeprowadzenia w przeszłości powiązanych ćwiczeń z zakresu cyberbezpieczeństwa, w tym daty ich przeprowadzenia.
Bezpieczeństwo	Wykrywanie incydentów	Wykrywanie incydentów	Operator konfiguruje system wykrywania zdarzeń bezpieczeństwa, który analizuje pliki i protokoły, przepływy danych w celu wyszukania zdarzeń mogących mieć wpływ na bezpieczeństwo systemów informacyjnych.	Czy istnieje polityka i związane z nią procedury wykrywania i analizy incydentów?	Udokumentowana polityka wykrywania i analizy incydentów, określająca cel, zakres, role i obowiązki oraz koordynację działań wszystkich powiązanych podmiotów.
				Czy istnieje mechanizm zapewniający, że personel jest dostępny i odpowiednio przeszkolony w celu wykrycia, zrozumienia i zgłoszenia zdarzenia naruszającego bezpieczeństwo?	Sprawozdania z ćwiczeń uświadamiających i szkoleniowych.

Bezpieczeństwo	Zarządzanie incydentami	Reagowanie na incydenty związane z bezpieczeństwem systemów informacyjnych	Operator tworzy wdraża i aktualizuje procedurę obsługi, reagowania i analizowania incydentów, które mają wpływ na funkcjonowanie lub bezpieczeństwo systemów informacyjnych	Czy istnieje polityka bezpieczeństwa wraz z powiązanymi procesami lub systemami, dotycząca reagowania na incydenty?	Udokumentowana polityka wykrywania i analizy incydentów, określająca cel, zakres, role i obowiązki oraz koordynację działań wszystkich powiązanych podmiotów, w tym klientów.
				Czy istnieje mechanizm zapewniający, że personel reagujący na incydenty jest dostępny i odpowiednio przeszkolony do zarządzania i obsługi incydentów?	Zapisy sesji szkoleniowych dotyczących reagowania na incydenty dla odpowiedniego personelu
				Czy polityka i procedury reagowania na incydenty są poddawane przeglądowi po wystąpieniu incydentu?	Systemy, narzędzia i procedury do wykrywania i analizy incydentów.
				Czy istnieją procesy obsługi incydentów zgodne z normami branżowymi i dobrymi praktykami?	Zobowiązanie kierownictwa do przestrzegania polityki, wytycznych i procedur reagowania na incydenty.

Zarządzanie	Zarządzanie bezpieczeństwem systemów informacyjnych i zarządzanie ryzykiem	Bezpieczeństwo zasobów ludzkich/ kadr	W ramach ustanowionej polityki bezpieczeństwa systemów informacyjnych opracowano program podnoszenia świadomości w zakresie bezpieczeństwa systemów informacyjnych dla wszystkich pracowników oraz program szkoleń w zakresie bezpieczeństwa dla pracowników, których obowiązki związane są z systemami informacyjnymi.	Czy referencje zawodowe kluczowych pracowników (administratorów systemu, pracowników ochrony, strażników itp.) są potwierdzone?	Dokumentacja dotycząca weryfikacji referencji zawodowych kluczowego personelu.
				Czy kluczowemu personelowi zapewniono materiały szkoleniowe dotyczące kwestii bezpieczeństwa?	Dokumenty potwierdzające uczestnictwo personelu w szkoleniu (np. , data i program szkolenia, podpisana lista uczestników podczas warsztatów uświadamiających itp.)
				Czy kluczowy personel został formalnie wyznaczony do pełnienia niezbędnych funkcji związanych z bezpieczeństwem?	Lista osób uprawnionych do pełnienia funkcji związanych z bezpieczeństwem oraz opis odpowiedzialności i zadań dla ról w tym zakresie. Opisy stanowisk podpisane przez kluczowych pracowników, szkolenia z zakresu pełnionych ról.
				Czy polityki/procedury dotyczące bezpieczeństwa zasobów ludzkich są regularnie przeglądane i aktualizowane?	Komentarze lub dzienniki zmian polityki/procedur. Przegląd wersji polityk/procedur z uwzględnieniem zmian, które miały miejsce.

Zarządzanie	Zarządzanie bezpieczeństwem systemów informacyjnych i zarządzanie ryzykiem	Wskaźniki bezpieczeństwa systemów informacyjnych	Operator ocenia zgodność systemów informacyjnych z przyjętą polityką bezpieczeństwa. Ocena ta odbywa się przy pomocy przyjętych metod i wskaźników. Wskaźniki mogą odnosić się do wyników organizacji zarządzania ryzykiem, utrzymywania zasobów w bezpiecznych warunkach, praw dostępu użytkowników, uwierzytelniania dostępu do zasobów oraz administrowania zasobami.	Czy w systemach wspierających podstawowe usługi wdrożono system kluczowych wskaźników, aby móc w każdej chwili ocenić ich skuteczność?	Wdrożony system kluczowych wskaźników dla oceny bezpieczeństwa systemów informacyjnych
				Czy wprowadzono politykę/procedury dotyczące wdrażania wskaźników bezpieczeństwa w celu testowania systemów wspierających podstawowe usługi?	Polityka/procedury testowania krytycznych systemów informacyjnych, zawierające informacje kiedy należy przeprowadzać testy, plany testów, przypadki testowe, szablony raportów z testów, pożądane wartości kluczowych wskaźników.
				Czy dokonano oceny skuteczności polityki/procedur w zakresie testów bezpieczeństwa?	Lista raportów dotyczących oceny bezpieczeństwa i testów bezpieczeństwa.
Zarządzanie	Zarządzanie bezpieczeństwem systemów informacyjnych i zarządzanie ryzykiem	Analiza ryzyka związanego z bezpieczeństwem systemów informacyjnych	Operator przeprowadza i regularnie aktualizuje analizę ryzyka, identyfikując swoje krytyczne systemy informacyjne oraz określa główne zagrożenia dla tych systemów.	Czy kluczowy personel jest świadomy głównych zagrożeń dla bezpieczeństwa informacji i odpowiednich środków zaradczych?	Dowody uczestnictwa personelu w szkoleniu (np. przyjęte zaproszenie, data i program szkolenia, podpisana lista obecności podczas warsztatów uświadamiających itp.)
				Czy istnieje mechanizm zapewniający, że wszyscy pracownicy ochrony stosują metodyki i narzędzia zarządzania ryzykiem?	Wytyczne dla personelu dotyczące oceny ryzyka oraz udokumentowane dowody aktualizacji/ przeglądów metodyk i narzędzi zarządzania ryzykiem.
				Czy metodyki i/lub narzędzia zarządzania ryzykiem są poddawane okresowym przeglądom, uwzględniającym zmiany i incydenty, które miały miejsce w przeszłości?	Dokumentacja procesu przeglądu i aktualizacji metodyk i/ lub narzędzi zarządzania ryzykiem. Harmonogram i ogólny plan cyklu przeglądu.

Zarządzanie	Zarządzanie bezpieczeństwem systemów informacyjnych i zarządzanie ryzykiem	Audyt bezpieczeństwa systemów informacyjnych	Operator ustanawia i aktualizuje politykę i procedury przeprowadzania ocen i audytów bezpieczeństwa systemów informacyjnych w odniesieniu do aktywów krytycznych.	Czy istnieje zaktualizowana polityka i/lub procedura przeprowadzania ocen i audytów bezpieczeństwa systemów informatycznych oraz aktywów wspierających podstawowe usługi?	Polityka i/lub procedury audytu bezpieczeństwa informacji, formalnie udokumentowane i regularnie aktualizowane.
Zarządzanie	Zarządzanie stroną trzecią	Monitorowanie usług świadczonych przez strony trzecie	Operator monitoruje powiązania z wewnętrznymi i zewnętrznymi interesariuszami, w tym m. in. dostawcami, w szczególności tymi, którzy mają dostęp do krytycznych aktywów operatora lub nimi zarządzają.	Czy umowy ze stronami trzecimi są odpowiednio udokumentowane i wymienione w wykazie?	Wykaz umów ze stronami trzecimi
Zarządzanie	Zarządzanie bezpieczeństwem systemów informacyjnych i zarządzanie ryzykiem	Licencje w zakresie bezpieczeństwa systemów informacyjnych	W oparciu o analizę ryzyka i zgodnie z procesem licencjonowania, o którym mowa w polityce bezpieczeństwa, operator dokonuje licencjonowania zidentyfikowanego w analizie ryzyka systemu informacyjnego, w tym między innymi spisu i architektury komponentów administracyjnych systemu informacyjnego.	Czy systemy wspierające podstawowe usługi są regularnie poddawane skanowaniu bezpieczeństwa i czy zostały one włączone do ram zarządzania ryzykiem w organizacji?	Raporty z poprzednich skanowań i testów bezpieczeństwa.
				Czy istnieje polityka/procedury dotyczące przeprowadzania ocen bezpieczeństwa i testów bezpieczeństwa?	Udokumentowana polityka/procedury dotyczące ocen bezpieczeństwa i testów bezpieczeństwa, które obejmują co najmniej: które aktywa powinny być oceniane, w jakich okolicznościach, rodzaj ocen i testów bezpieczeństwa, częstotliwość, zatwierdzone strony (wewnętrzne lub zewnętrzne), poziomy poufności dla wyników ocen i testów oraz cele ocen i testów bezpieczeństwa.
				Czy dokonano oceny skuteczności polityki/procedur w zakresie testów bezpieczeństwa?	Udokumentowana ocena skuteczności polityki/procedur w zakresie testów bezpieczeństwa

Zarządzanie	Zarządzanie bezpieczeństwem systemów informacyjnych i zarządzanie ryzykiem	Polityka bezpieczeństwa systemu informatycznego	W oparciu o analizę ryzyka operator ustanawia, aktualizuje i wdraża politykę bezpieczeństwa systemu informacyjnego, zatwierdzoną przez kierownictwo wyższego szczebla.	Czy istnieje polityka bezpieczeństwa informacji oraz system zarządzania bezpieczeństwem informacji ?	Aktualna udokumentowana polityka bezpieczeństwa informacji (opatrzona datą i podpisem).
				Czy istnieją jakieś certyfikaty dotyczące określonych standardów zarządzania ryzykiem bezpieczeństwa?	Certyfikacja zgodności z normami zarządzania ryzykiem w zakresie bezpieczeństwa informacji (np. ISO 27001), w tym oświadczenie o zakresie.
				Czy procesy dotyczące bezpieczeństwa informacji są poddawane przeglądowi w regularnych odstępach czasu, z uwzględnieniem naruszeń i incydentów, które miały wpływ na innych istotnych operatorów?	Dokumentacja przeglądu procesów bezpieczeństwa informacji, zakres przeglądu.
Zarządzanie	Zarządzanie stroną trzecią	Umowy ze stroną trzecią	Operator ustanawia politykę w zakresie relacji ze stronami trzecimi w celu złagodzenia zidentyfikowanych potencjalnych zagrożeń. Dotyczy to w szczególności, ale nie tylko, interfejsów między systemem informacyjnym a stronami trzecimi.	Czy wymogi bezpieczeństwa są uwzględnione w umowach ze stronami trzecimi?	Wymogi bezpieczeństwa określone w umowach ze stronami trzecimi dostarczającymi produkty i usługi informatyczne, procesy biznesowe zlecane na zewnątrz, centra pomocy technicznej itp.
				Czy wprowadzono politykę bezpieczeństwa dla stron trzecich?	Dokumentacja polityki bezpieczeństwa dla stron trzecich
				Czy polityka bezpieczeństwa dla stron trzecich jest poddawana przeglądowi po incydentach lub zmianach?	Udokumentowane komentarze lub dzienniki zmian polityki.
				Czy istnieją jakieś ryzyko związane z osobami trzecimi i ich usługami, które nie są wskazane/zmitygowane?	„Polityka/procedura oceny/zarządzania ryzykiem dostawcy wdrożona i utrzymywana.
				Czy dokonuje się okresowego przeglądu i aktualizacji polityki bezpieczeństwa stron trzecich, biorąc pod uwagę wcześniejsze incydenty, zmiany itp.	Dokumentacja procesu przeglądu polityki w zakresie stosunków ze stronami trzecimi

Ochrona	Zarządzanie tożsamością i dostępem	Uwierzytelnienia	W celu identyfikacji operator konfiguruje unikatowe konta dla użytkowników lub dla zautomatyzowanych procesów, które muszą uzyskać dostęp do zasobów swojego SIC. Nieużywane lub nie są już potrzebne konta mają zostać dezaktywowane. Należy ustanowić regularny proces przeglądu.	Czy istnieją mechanizmy kontroli dostępu do sieci i systemów informatycznych, pozwalające na korzystanie z nich wyłącznie przez osoby upoważnione?	Polityka kontroli dostępu zawierająca opis ról, grup, praw dostępu, procedury przyznawania i odbierania prawa dostępu do systemów informatycznych.
				Czy niepotrzebne konta są dezaktywowane?	Definicja reguły usuwania nieużywanych już kont po krótkim okresie czasu.
				Czy istnieje mechanizm monitorowania dostępu do sieci i systemów informatycznych oraz zatwierdzania wyjątków i rejestrowania naruszeń dostępu?	Matryce związane z kontrolą dostępu (np. matryca kontroli podziału obowiązków, kontrola zdalnego dostępu itp.)
Ochrona	Utrzymanie bezpieczeństwa IT	Procedura zarządzania bezpieczeństwem IT	Operator opracowuje i wdraża procedurę utrzymania bezpieczeństwa zgodnie z jego polityką bezpieczeństwa. W tym celu procedura definiuje warunki umożliwiające utrzymanie minimalnego poziomu zabezpieczeń dla zasobów systemów informacyjnych.	Czy ustanowiono procedurę utrzymania bezpieczeństwa zgodnie z polityką bezpieczeństwa?	Procedura utrzymania bezpieczeństwa odpowiednio udokumentowana i zatwierdzona przez kierownictwo wyższego szczebla.
				Czy określono warunki umożliwiające osiągnięcie minimalnego poziomu bezpieczeństwa dla systemów wspierających zasoby usług podstawowych?	Jasno określony minimalny proces utrzymania zabezpieczeń.
				Czy zasoby oprogramowania i sprzętu są regularnie utrzymywane i aktualizowane?	Formalnie udokumentowane wymagania dotyczące oprogramowania i sprzętu w celu zapewnienia kompatybilności. Zarządzanie aktywami oprogramowania/ sprzętu formalnie udokumentowane i zabezpieczone.
Ochrona	Struktura/ architektura bezpieczeństwa IT	Rozdzielenie systemu	Operator oddziela swoje systemy w celu ograniczenia rozprzestrzeniania się incydentów związanych z bezpieczeństwem informatycznym w obrębie swoich systemów lub podsystemów.	Czy systemy informatyczne są odpowiednio rozdzielone w celu zminimalizowania potencjalnych konsekwencji w przypadku wystąpienia ryzyka?	Dokumentacja dotycząca sposobu wdrożenia podziału systemu na systemy informacyjne i dane.

Ochrona	Struktura/ architektura bezpieczeństwa IT	Kryptografia	W swojej Polityce bezpieczeństwa operator ustanawia i wdraża politykę i procedury związane z kryptografią w celu zapewnienia odpowiedniego i skutecznego wykorzystania kryptografii do ochrony poufności, autentyczności lub integralności informacji w swoim systemie informacyjnym.	Czy istnieją mechanizmy kryptograficzne chroniące poufność i integralność informacji przechowywanych w firmie lub poza jej granicami (obiekty cyfrowe)?	Istnienie odpowiednich zabezpieczeń kryptograficznych.
				Czy zaimplementowano mechanizmy kryptograficzne, takie jak podpisy cyfrowe i hasze w celu wykrywania nieautoryzowanych zmian w krytycznych danych w stanie spoczynku?	Stosowane są zabezpieczenia chroniące poufność klucza prywatnego .
Ochrona	Utrzymanie bezpieczeństwa IT	Przemysłowe systemy sterowania		Czy operator, w stosownych przypadkach, uwzględnia szczególne wymogi bezpieczeństwa dotyczące przemysłowych systemów sterowania?	Formalnie udokumentowane wymagania dla przemysłowych systemów sterowania
Ochrona	Administrowanie bezpieczeństwem IT	Konta administratorów	Operator tworzy specjalne konta dla administracji, które będą używane tylko przez administratorów wykonujących operacje administracyjne (instalacja, konfiguracja, zarządzanie, konserwacja, itp.) w jego systemach informacyjnych. Konta te są przechowywane w aktualnym wykazie.	Czy operator tworzy specjalne konta administracyjne, które będą używane tylko przez administratorów wykonujących określone operacje (np. instalację, konfigurację, zarządzanie, konserwację itp.) na systemy wspierające podstawowe usługi?	Dostosowane i udokumentowane konta administracyjne z określonymi prawami dostępu przyznanymi odpowiednim pracownikom.
				Czy konta administratorów służą wyłącznie do łączenia się z systemami informatycznymi administracji?	Udokumentowany proces zarządzania systemem kont administratorów. Dostępne są logi aktywności konta administratora.

Ochrona	Bezpieczeństwo fizyczne i środowiskowe	Bezpieczeństwo fizyczne i środowiskowe	Operator zapobiega nieuprawnionemu fizycznemu dostępowi, uszkodzeniu i zakłóceniu działania informacji i urządzeń przetwarzających informacje organizacji.	Czy zapobiega się nieupoważnionemu fizycznemu dostępowi do obiektów i infrastruktury oraz czy wdrożono kontrole środowiskowe, mające na celu ochronę przed nieupoważnionym dostępem (np. włamanie, pożar, zalanie itp.)?	Podstawowe wdrożenie fizycznych środków bezpieczeństwa i kontroli środowiska, takich jak zamki w drzwiach i szafkach, alarm przeciwwłamaniowy, alarmy przeciwpożarowe, gaśnice itp
				Czy do pomieszczeń, w których znajdują się systemy informatyczne, ma dostęp tylko ograniczona liczba uprawnionych pracowników z uprawnieniami i odpowiednimi poświadczeniami autoryzacji?	Lista pracowników z autoryzowanym dostępem i poświadczeniami autoryzacji
				Czy wdrożono politykę w zakresie fizycznych i środowiskowych środków bezpieczeństwa?	Udokumentowana polityka w zakresie środków bezpieczeństwa fizycznego i kontroli środowiska, w tym opis obiektów i systemów objętych zakresem.
Ochrona	Zarządzanie tożsamością i dostępem	Prawo dostępu	Zgodnie z zasadami określonymi w polityce bezpieczeństwa systemów, operator przyznaje prawa dostępu użytkownikowi lub zautomatyzowanemu procesowi tylko wtedy, gdy dostęp ten jest absolutnie niezbędny użytkownikowi do wykonania jego zadania lub zautomatyzowanemu procesowi do wykonania jego operacji technicznych.	Czy prawa dostępu są przyznawane w sposób ustrukturyzowany i monitorowany? Czy są one przyznawane automatycznie w stosownych przypadkach?	Sekcja praw dostępu zawarta w polityce/ procedurach kontroli dostępu.
				Czy operator definiuje prawa dostępu do wielu funkcjonalności zasobu?	Rejestr mapujący prawa dostępu do odpowiednich zasobów i/lub procesów ujętych w polityce kontroli dostępu.

Ochrona	Administrowanie bezpieczeństwem IT	Filtrowanie ruchów	Operator filtruje strumienie krążące w jego Krytycznych Systemach Informacyjnych. Operator zakazuje zatem przepływów , które nie są potrzebne do funkcjonowania jego systemów i które mogą ułatwić atak.	Czy istnieje mechanizm monitorowania systemów wspierających podstawowe usługi?	Monitorowanie raportów krytycznych sieci i systemów informatycznych.
				Czy istnieje polityka monitorowania ruchu systemów wspierających podstawowe usługi?	Udokumentowana polityka w zakresie procedur monitorowania, w tym minimalne wymogi w zakresie monitorowania.
				Czy istnieją narzędzia wspierające monitorowanie ruchu w systemach wspierających podstawowe usługi?	Dowód na istnienie narzędzi do monitorowania systemów.
Ochrona	Administrowanie bezpieczeństwem IT	System administrowania informacją	Zasoby sprzętowe i programowe wykorzystywane do celów administracyjnych są zarządzane i konfigurowane przez operatora lub, w stosownych przypadkach, przez usługodawcę, którego operator upoważnił do wykonywania czynności administracyjnych.	Czy zasoby sprzętowe i programowe, wykorzystywane są do celów administracyjnych?	Szczegółowa inwentaryzacja zasobów sprzętowych i programowych wykorzystywanych na potrzeby administracji systemów.
				Czy systemy informacyjne administracji są wykorzystywane wyłącznie do celów administracyjnych i nie są mieszane z innymi operacjami?	Systemy informatyczne administracji odizolowane i odseparowane od reszty infrastruktury w celu zwiększenia odporności.
				Czy ww. zasoby są zarządzane i konfigurowane przez uprawnionego operatora?	Odpowiedzialny wyspecjalizowany personel do zarządzania i konfiguracji wyżej wymienionych zasobów.
Ochrona	Administrowanie bezpieczeństwem IT	Konfiguracja systemu	Operator instaluje tylko te usługi i funkcjonalności lub podłącza urządzenia, które są niezbędne do funkcjonowania i bezpieczeństwa jego systemów informacyjnych	Czy sieci i systemy obsługujące podstawowe usługi są skonfigurowane z myślą o bezpieczeństwie informacji?	Zasady konfiguracji systemu. Tabele konfiguracji systemu. Harmonogram i planowanie cykli przeglądu konfiguracji systemu
				Czy skuteczność konfiguracji zabezpieczeń w celu ochrony integralności systemów jest oceniana i poddawana przeglądowi?	Udokumentowane dotychczasowe ćwiczenia/testy krytycznych systemów informatycznych. Harmonogram i plan przeglądów konfiguracji zabezpieczeń.

Odporność	Ciągłość działania	Zarządzanie odbudową po katastrofie	Zgodnie z polityką bezpieczeństwa, operator określa cele i wytyczne strategiczne dotyczące zarządzania odzyskiwaniem danych po katastrofie w przypadku poważnego incydentu związanego z bezpieczeństwem IT.	Czy organizacja jest przygotowana do odbudowy i przywrócenia usług dotkniętych katastrofami?	Wdrożone środki na wypadek katastrof, takie jak awaryjne lokalizacje w innych regionach, kopie zapasowe krytycznych danych w innych lokalizacjach itp.
				Czy istnieje procedura odbudowy po katastrofie?	Formalnie udokumentowana polityka/procedury odzyskiwania danych po katastrofie, w tym wykaz klęsk żywiołowych lub poważnych katastrof, które mogą mieć wpływ na usługi, oraz wykaz zdolności do odzyskiwania danych po katastrofie (dostępnych wewnętrznie lub zapewnianych przez strony trzecie).
				Czy personel został przeszkolony do działań związanych z odbudową po katastrofie?	Ewidencja indywidualnych działań szkoleniowych.
Odporność	Zarządzanie kryzysowe	Zarządzanie kryzysowe	Operator definiuje w swojej polityce bezpieczeństwa organizację zarządzania kryzysowego w przypadku incydentów związanych z bezpieczeństwem IT i ciągłości działań organizacji.	Czy istnieje polityka zarządzania kryzysowego w zakresie reagowania na incydenty związane z bezpieczeństwem IT?	Formalnie udokumentowana polityka zarządzania kryzysowego, która obejmuje co najmniej kluczowe systemy informacyjne, zasoby informacyjne, role i obowiązki w przypadku incydentu związanego z bezpieczeństwem IT.

Odporność	Ciągłość działania	Zarządzanie ciągłością działania	Zgodnie z Polityką bezpieczeństwa operator definiuje strategiczne cele i wytyczne dotyczące zarządzania ciągłością działania w przypadku wystąpienia incydentu bezpieczeństwa IT.	Czy wdrożono strategię ciągłości biznesowej dla krytycznych usług świadczonych przez organizację?	Formalnie udokumentowana strategia ciągłości usług, w tym cele dotyczące czasu odzyskiwania kluczowych usług i procesów.
				Czy w organizacji wdrożono plany awaryjne dla systemów wspierających podstawowe usługi?	Plany awaryjne dla systemów krytycznych, w tym jasne kroki i procedury dla typowych zagrożeń, mechanizmów aktywacji, etapy i cele czasowe odzyskiwania.
				Czy wszyscy pracownicy zaangażowani w działania związane z zapewnieniem ciągłości działania są odpowiednio przeszkoleni w zakresie ról i obowiązków związanych z systemem informatycznym?	Zapisy indywidualnych zajęć treningowych, jak również raporty powysiłkowe.
Odporność	Zarządzanie kryzysowe	Proces zarządzania kryzysowego	Operator definiuje w Polityce bezpieczeństwa procesy zarządzania kryzysowego, które organizacja będzie realizować w przypadku wystąpienia incydentów bezpieczeństwa IT oraz ciągłości działania organizacji.	Czy operator definiuje w swojej polityce bezpieczeństwa procesy zarządzania kryzysowego, które organizacja wdroży w przypadku incydentów związanych z bezpieczeństwem IT?	Formalnie udokumentowana procedura zarządzania kryzysowego

Załącznik nr 4
Zbiór rekomendowanych działań mających na celu wzmocnienie cyberbezpieczeństwa polskiego sektora energii

4. Zarządzanie ryzykiem

4.1. Polityka bezpieczeństwa informacji

4.1.1. Polityka bezpieczeństwa informacji powinna zawierać spisane cele, strategie oraz działania, które w jasny i ustrukturyzowany sposób określają, jak należy zarządzać zgromadzonymi danymi, jak je chronić i rozpowszechniać. Dokument powinien ułatwiać dokładne zrozumienie celu istnienia procedur bezpieczeństwa i ma za zadanie podnosić świadomość pracowników organizacji na temat zagrożeń bezpieczeństwa i związanego z nimi ryzyka.

4.1.2. Polityka bezpieczeństwa informacji powinna być dokumentem spisanym, który jest zrozumiały i dostępny dla każdego pracownika organizacji oraz osób korzystających z jej zasobów informacyjnych. Partnerzy biznesowi powinni być zapoznawani z wybranymi i podstawowymi zasadami polityki bezpieczeństwa w zakresie wymaganym co do stopnia i zakresu korzystania przez nich z zasobów teleinformatycznych danej organizacji.

4.1.3. Ponadto polityka bezpieczeństwa informacji powinna zawierać ogólne, ale spójne założenia reguł i procedur dotyczących bezpieczeństwa dla danego obszaru. Szczegółowe zasady dotyczące zabezpieczeń, instrukcje reagowania na incydenty bezpieczeństwa czy opis sposobu korzystania z danych bądź przydzielania uprawnień dostępu powinny być opisane w oddzielnych dokumentach zawierających przyjęte w organizacji standardy i procedury postępowania.

4.1.4. Projektując mechanizmy ochrony informacji, należy uwzględnić mechanizmy identyfikacji, autentykacji i zapewnienia autentyczności zarówno na poziomie fizycznym, jak i poziomie systemów IT/OT. Dodatkowo należy wziąć pod uwagę procedury związane ze śledzeniem zdarzeń w systemie, które obejmują same mechanizmy, a także programy czy procedury stosowane do śledzenia zmian w tychże systemach.

4.1.5 Dokument określający politykę bezpieczeństwa informacji organizacji powinien obejmować również kwestie przetwarzania danych osobowych oraz zarządzania nimi zgodnie z wytycznymi RODO. Polityka bezpieczeństwa informacji powinna uwzględniać rekomendacje na podstawie zaleceń poaudytowych. Należy jasno zdefiniować zasady przydzielania uprawnień dostępu do poszczególnych klas informacji oraz ustalić schemat obiegu informacji w organizacji.

4.1.6. Polityka bezpieczeństwa informacji musi obejmować wszystkie urządzenia wykorzystywane w procesie przetwarzania danych. Powinna zawierać również informacje dotyczące zasad edukacji pracowników w zakresie bezpieczeństwa i weryfikacji przestrzegania standardów organizacji w zakresie bezpieczeństwa. Ponadto w ramach systemu bezpieczeństwa informacji powinna być podnoszona wiedza pracowników organizacji poprzez cykliczną dystrybucję biuletynów informacyjnych.

4.2. Organizacja bezpieczeństwa informacji

4.2.1. Organizacja powinna przypisać odpowiednie role poszczególnym pracownikom i tym samym odpowiedzialność za bezpieczeństwo informacji.

4.2.2. Należy dokładnie określić obowiązki i odpowiedzialności pracowników tak, aby nie pozostawały ze sobą w konflikcie. Ma to na celu ograniczenie modyfikacji i nadużycia aktywów organizacji.

4.2.3. Organizacja powinna wyznaczyć pracownika do kontaktu z podmiotami wchodzącymi w skład Krajowego Systemu Cyberbezpieczeństwa, w tym z organem właściwym ds. cyberbezpieczeństwa w sektorze energii, a także z właściwym zespołem reagowania na incydenty bezpieczeństwa komputerowego CSIRT poziomu krajowego, tj. CSIRT GOV bądź CSIRT NASK, zgodnie z zasadami określonymi w ustawie o krajowym systemie cyberbezpieczeństwa.

4.2.4. Ponadto organizacja powinna utrzymywać stosowane kontakty z innymi podmiotami z obszaru cyberbezpieczeństwa, które stanowią doskonałe źródło informacji, m.in. o zagrożeniach, podatnościach, wskaźnikach kompromitacji IoC, technologiach, a także wiedzę specjalistyczną w zakresie budowania i wzmacniania struktur cyberbezpieczeństwa w organizacji.

4.2.5. Należy także uwzględnić bezpieczeństwo informacji w zarządzaniu projektami, niezależnie od rodzaju projektu.

4.2.6. Należy wdrożyć politykę związaną ze świadczeniem pracy zdalnej oraz wdrożyć wspierające ją zabezpieczenia celem ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania pracy zdalnej.

4.2.7. Organizacja powinna opracować i wdrożyć politykę stosowania urządzeń mobilnych, a także wdrożyć wspierające ją zabezpieczenia w celu zarządzania ryzykami, które wynikają z użytkowania tych urządzeń.

4.3. Metodyka zarządzania ryzykiem, szacowanie ryzyka

4.3.1. Organizacja powinna zarządzać ryzykiem wystąpienia incydentu cyberbezpieczeństwa w kontekście systemów informacyjnych służących do świadczenia usługi kluczowej. Proces ten jest złożony ze skoordynowanych działań w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka wystąpienia incydentu.

4.3.2. Obowiązkiem operatora jest „prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem". *Rekomenduje się jednak, by operator usługi kluczowej przeprowadzał ten proces nie rzadziej, niż co 12 miesięcy.*

4.4. Plan postępowania z ryzykiem

4.4.1. Organizacja w ramach procesu zarządzania ryzykiem i reagowania na nie, powinna ustanowić plan postępowania z ryzykiem, w szczególności dla ryzyka na poziomie wyższym niż akceptowalny.

5. Zarządzanie stroną trzecią

5.1. Umowy z podmiotami trzecimi

5.1.1. Zaleca się by operator usługi kluczowej uwzględnił w swojej analizie ryzyka element dotyczący ryzyka prawnego wynikającego z zawieranych umów z podmiotami zewnętrznymi i dostawcami usług/sprzętu.

5.1.2. Operator usługi kluczowej powinien opracować i stosować procedury zarządzania dostępem stron trzecich.

5.1.3. Rekomenduje się by operator usługi kluczowej opracował procedury monitorowania opracowywanych opisów zamówień publicznych i umów pod kątem ich rzetelności i bezstronności.

5.1.4. Zaleca się by operator usługi kluczowej zawierał w umowach dotyczących systemów automatyki przemysłowej zapisy chroniące aktywa tych systemów.

5.1.5. Rekomenduje się by w umowach w podmiotami trzecimi znalazły się zapisy regulujące kwestię aktualizacji oprogramowania oraz zapewnienia implementacji odpowiednich „łatek bezpieczeństwa" do systemów zakupionych od danego podmiotu.

5.1.6. Organizacja powinna posiadać wdrożone procedury związane z zachowaniem bezpieczeństwa informacji przy współpracy z podmiotami zewnętrznymi, które obejmowałyby produkty, procesy czy usługi. W zawieranych umowach z podmiotami zewnętrznymi powinny znajdować się odpowiednie zapisy w tym zakresie.

5.1.7. Powinno się skłonić dostawców usług do bieżącego informowania o bezpieczeństwie przeprowadzanych procesów i usług, a także do informowania o postępach prowadzonych działań. Należy opracować wymagania bezpieczeństwa w zakresie współpracy z dostawcami i usługodawcami.

5.1.8. Zaleca się by operator usługi kluczowej w ramach zawieranych umów z podmiotami zewnętrznymi uwzględnił mechanizmy sankcyjne.

5.1.9. Umowy dotyczące oprogramowania systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej zawierane z podmiotami zewnętrznymi powinny zawierać odpowiednie zapisy mające na celu zwiększenie bezpieczeństwa tych systemów.

5.2. Monitorowanie usług świadczonych przez strony trzecie, weryfikacja rozwiązań w oparciu o uzgodnione kryteria

5.2.1. Rekomendowane jest by zapisy w umowach oraz już sama realizacja umów opierała się, m.in. na przeprowadzonym wcześniej szacowaniu ryzyka w organizacji. Analiza ryzyka powinna także pomóc w zidentyfikowaniu obszarów, które powinny być w umowach uwzględnione, a które dotąd były pomijane.

5.2.2. Wykonana analiza ryzyka powinna objąć uwarunkowania zdarzeń losowych, sił wyższych (np. epidemii), gdzie firma trzecia świadcząca usługę nie jest w stanie zapewnić świadczenia usługi na wystarczająco wysokim poziomie.

5.2.3. Rekomendowane jest monitorowanie wskazanych w umowie ram czasowych realizacji umowy, np. wdrażania usługi, oraz wskazanie kryteriów do monitorowania i oceny realizacji umowy.

5.2.4. Rekomendowane jest wprowadzenie w organizacji i w umowach ze stronami trzecimi regulacji zobowiązujących pracowników oraz zobowiązujących kontrahentów do zgłaszania

wszelkich zaobserwowanych lub możliwych do wystąpienia słabości związanych z bezpieczeństwem informacji w systemach lub usługach.

5.2.5. Rekomenduje się wdrożenie wewnątrz organizacji procedur dot. monitorowania i audytowania dostawców usług i uwzględnienie tego w zapisach umów z dostawcami.

5.2.6. Zaleca się by operatorzy usług kluczowych w zakresie zawieranych kontraktów ze stroną trzecią stosowali umowy o gwarantowanym poziomie świadczenia usług (SLA – ang. *Service Level Agreement*) w celu ustalenia odpowiednich kryteriów monitorowania usługi świadczonej przez dostawcę.

5.3. Korzystanie z usług chmurowych

5.3.1. W celu ograniczenia ryzyka powiązanego z atakiem na chmurę, należy stosować zasadę wiedzy zerowej (ang. *zero-knowledge*) i zabezpieczyć wszystkie dane, zarówno te, które są przechowywane w chmurze, jak i te, które są w stanie transmisji. Należy planować wdrażanie funkcji związanych z bezpieczeństwem już na bardzo wczesnym etapie tworzenia czy implementowania danego rozwiązania.

5.3.2. Należy zadbać o to, aby w umowach z dostawcami usług chmurowych uwzględnić, w szczególności, aspekty bezpieczeństwa i dostępności tych usług, a także przepisy prawa krajowego i unijnego oraz wewnętrzne regulacje danej organizacji.

5.3.3. W przypadku użytkowania aplikacji opartych na chmurze oraz systemów scentralizowanych, należy unikać pojedynczych systemowych punktów awarii (ang. *single points of failure*).

6. Cykl życia systemów informacyjnych

6.1. Analiza i specyfikacja wymagań bezpieczeństwa

6.1.1. Organizacja powinna uwzględnić aspekty bezpieczeństwa na wszystkich etapach życia systemów informacyjnych oraz oprogramowania, a także dostosować architekturę do wymagań prawnych.

6.1.2. Należy dokonać standaryzacji wymagań względem poziomu bezpieczeństwa systemów, a także zwiększać jego poziom poprzez modernizację i inwestycję w nowe rozwiązania.

6.1.3. Operatorzy sieci energetycznych powinni ustanowić kryteria projektowe i architekturę na potrzeby odpornej sieci, co można osiągnąć poprzez: wprowadzenie w każdym obiekcie środków ochrony w głąb (ang. *Defence-In-Depth*) dostosowanych do krytyczności danego obiektu, identyfikację węzłów krytycznych, zarówno pod względem zdolności wytwórczych, jak i wpływu na klienta.

6.1.4. Funkcje krytyczne sieci powinny być zaprojektowane w taki sposób, aby poprzez rozważenie redundancji, odporności na wahania fazy i ochrony przed kaskadowymi wyłączeniami mocy ograniczyć ryzyko, które może wywołać efekty kaskadowe,

6.1.5. Operatorzy sieci energetycznych powinni prowadzić współpracę z innymi właściwymi operatorami i dostawcami technologii w celu zapobiegania efektom kaskadowym poprzez zastosowanie odpowiednich środków i usług,

6.1.6. Operatorzy sieci energetycznych powinni projektować i budować sieci łączności i sterowania w celu ograniczenia skutków wszelkich błędów fizycznych i logicznych do ograniczonych części sieci oraz zapewnienia odpowiednich i szybkich środków łagodzących.

6.1.7. Organizacja powinna stworzyć jednolity model postępowania w fazie zamawiania nowych rozwiązań, uściślając modele współpracy z dostawcami oraz minimalne wymagania jakie powinny być spełnione.

6.1.8. W celu uniknięcia niepotrzebnego gromadzenia danych wrażliwych organizacja powinna określić zakres i cel przetwarzania tych danych, w tym danych osobowych we wczesnych etapach prac projektowych.

6.1.9. Należy przyjąć zasadę gromadzenia wrażliwych danych tylko w sytuacji, gdy jest to niezbędne z punktu widzenia danego procesu.

6.1.10. W miarę możliwości, należy wyznaczyć konkretną lokalizację przechowywania danych, a także określić, między którymi podmiotami jakie dane będą udostępniane, ponadto należy zapewnić dostęp do danych wyłącznie upoważnionemu personelowi.

6.1.11. Organizacja powinna wziąć pod uwagę konieczność modyfikacji dostępu do danych względem pracownika, który zmienił stanowisko lub zakończył świadczenie pracy dla organizacji.

6.1.12. Organizacja powinna przeprowadzić analizę oceny skutków przetwarzania danych w konkretnych urządzeniach związanych ze świadczeniem usługi kluczowej. Działanie to może być zintegrowane z procesem zarządzania ryzykiem organizacji.

6.1.13. Należy zabezpieczyć dane poprzez mechanizmy zwiększające ich bezpieczeństwo, np. szyfrowanie w procesie przekazywania danych, czy pseudonimizacja w procesie ich przechowywania.

6.1.14. Organizacja powinna uwzględniać zasadę *privacy by design* w kontekście wrażliwych danych już na etapie procedury przetargowej na konkretne rozwiązanie.

6.2. Cykl życia systemów informacyjnych

6.2.1. Określenie wymagań bezpieczeństwa już na etapie zamówienia jest metodą, która w sposób efektywny i wydajny pozwoli na implementację minimalnych wymagań, a także pozwoli na zaoszczędzenie kosztów, które organizacja mogłaby ponieść w przypadku konieczności modyfikacji mechanizmów bezpieczeństwa w późniejszych cyklach życia systemu.

6.3. Zarządzanie aktywami

6.3.1. Organizacja powinna zarządzać aktywami w zakresie świadczonej usługi kluczowej. Czynności te powinny być realizowane przy użyciu odpowiednich rozwiązań organizacyjnych oraz zautomatyzowanych rozwiązań technicznych.

6.4. Utrzymanie systemów informacyjnych

6.4.1. Rekomendowane jest przeprowadzenie szacowania bezpieczeństwa systemów informacyjnych pod kątem bezpiecznej eksploatacji systemu, uwzględniającej zagrożenia wynikające np. z wieku systemu, ograniczonej liczby osób posiadających wiedzę o systemie.

6.4.2. Rekomendowane jest gromadzenie wiedzy o systemie i jej zabezpieczanie.

6.4.3. Rekomendowane jest zawieranie w umowach ze stronami trzecimi klauzul dotyczących szczegółów w zakresie zapewnienia obsługi systemu jak i ciągłości wiedzy dot. systemu.

6.4.4. Rekomendowana jest realizacja wdrożonych zapisów procedur/instrukcji dot. bezpieczeństwa systemu informacyjnego w organizacji.

6.4.5. Rekomendowane jest regularne przeprowadzanie testów systemów informacyjnych.

6.4.6. Przy projektowaniu nowego systemu informacyjnego wskazane jest uwzględnienie elementów dotyczących utrzymywania systemu w późniejszym okresie czasu.

6.5. Aktualizacja oprogramowania

6.5.1. Operator usługi kluczowej powinien wdrożyć w swojej organizacji proces aktualizacji oprogramowania.

6.5.2. Zaleca się by operator usługi kluczowej opracował i utrzymywał aktualny katalog oprogramowania zawierający informacje na temat posiadanych zasobów.

6.5.3. Zaleca się regularne przeprowadzanie aktualizacji oprogramowania z uwzględnieniem analiz podatności i zaleceń producenta, a także poziomu krytyczności poszczególnych aktualizacji.

6.5.4. Rekomenduje się bieżące obserwowanie informacji o wydawanych przez producentów oprogramowania łatkach bezpieczeństwa, w celu poprawienia bezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej. Zaleca się przygotowanie i wdrożenie procedury instalacji poprawek bezpieczeństwa.

6.5.5. Zaleca się by w przypadku braku opracowania przez producenta poprawek bezpieczeństwa eliminujących daną podatność, operator usługi kluczowej przeprowadził analizę ryzyka i podjął odpowiednie działania nakierowane na zminimalizowanie ryzyka wystąpienia incydentu.

6.6. Zarządzanie licencjami

6.6.1. Rekomenduje się by operator usługi kluczowej dokonał inwentaryzacji posiadanego przez siebie licencjonowanego oprogramowania.

6.6.2. W przypadku zakupu oprogramowania, operator powinien uwzględnić rzeczywiste zapotrzebowanie i zdefiniować wymagania techniczne.

6.6.3. Rekomenduje się by operator usługi kluczowej posiadał system zarządzania licencjami oprogramowania.

6.7. Testowanie systemów i komponentów

6.7.1. Organizacja powinna testować systemy i komponenty dotyczące systemów informacyjnych, od których zależy świadczenie usługi kluczowej.

7. Bezpieczeństwo osobowe, podnoszenie świadomości, szkolenia

7.1. Program podnoszenia kompetencji z zakresu cyberbezpieczeństwa

7.1.1. Zaleca się, żeby operator usługi kluczowej opracował odpowiednio dopasowany do swoich potrzeb program podnoszenia kompetencji z zakresu cyberbezpieczeństwa wśród swoich pracowników.

7.2. Podnoszenie kompetencji i kwalifikacji

7.2.1. W pakiecie szkoleń podstawowych, dedykowanych nowo przyjętym pracownikom, organizacja powinna uwzględnić szkolenia z zakresu cyberbezpieczeństwa.

7.2.2. Organizacja powinna zapewnić kompleksowe podejście do szkoleń i działań mających na celu podniesienie świadomości cyberbezpieczeństwa swoich pracowników niezależnie od komórki organizacyjnej w jakiej pracują.

7.2.3. Proces podnoszenia świadomości z zakresu cyberbezpieczeństwa wśród użytkowników systemów informacyjnych powinien być procesem ciągłym, aby utrwalać ich wiedzę i przypominać informacje na temat cyberzagrożeń i podstawowych zasad bezpieczeństwa.

7.2.4. Pracownicy w których zakresie obowiązków wymagana jest zaawansowana wiedza z zakresu cyberbezpieczeństwa, powinni mieć zapewniony dostęp do cyklicznych szkoleń i odpowiednich ścieżek rozwoju.

7.2.5. Zaleca się uczestnictwo w międzynarodowych forach współpracy w zakresie bezpieczeństwa, które powstały w celu umożliwienia dyskusji, współpracy i wymiany informacji w ramach grupy zaangażowanych podmiotów, w celu poprawienia świadomości zagrożeń.

7.2.5. Rekomenduje się by operatorzy usług kluczowych brali aktywny udział w organizowanych krajowych ćwiczeniach cyberbezpieczeństwa, jak również, w ramach możliwości, w tych organizowanych na poziomie międzynarodowym.

7.2.7. Organizacja powinna dokumentować przeprowadzanie szkoleń dla pracowników.

7.3. Weryfikacja personelu, zmiany kadrowe

7.3.1. W celu zabezpieczenia interesów organizacji podczas procesu zmiany zatrudnienia przez pracownika lub jego zakończenia, powinno określić się i przedstawić pracownikowi jakie zakresy odpowiedzialności w zakresie bezpieczeństwa informacji będą aktualne po zmianie statusu zatrudnienia. Powinno zwrócić się szczególną uwagę na konieczny zwrot aktywów informacyjnych przez pracowników w momencie zakończenia zatrudnienia.

7.3.2.. Ponadto, organizacja powinna prowadzić ocenę ryzyka zakłócenia jej funkcjonowania z powodu nielegalnego wykorzystania informacji przez pracowników. Wyniki takiej analizy mogą przyczynić się do zmian procedury zatrudniania na bardziej dostosowaną do prawdopodobieństwa wystąpienia zdarzenia niepożądanego.

8. Audyty bezpieczeństwa systemów informacyjnych

8.1. Audyty bezpieczeństwa systemów informacyjnych

8.1.1. Zaleca się, aby operator usługi kluczowej określił w ramach ogólnej polityki bezpieczeństwa informacji zasady prowadzenia programów audytów bezpieczeństwa systemów informacyjnych względem personelu i krytycznych aktywów informacyjnych, w tym cele audytów, polityki, odpowiedzialności i procedury.

8.1.2. Zaleca się, aby operator usługi kluczowej uwzględnił w programowaniu audytu bądź w programach audytu wyniki szacowania ryzyka bezpieczeństwa systemów informacyjnych, w tym szacowanie ryzyka wystąpienia incydentu.

8.1.3. Zaleca się, aby operator usługi kluczowej uwzględnił w programach audytu – w zależności od poziomu dojrzałości operatora – wymagania regulacyjne wynikające z UKSC, przepisów Prawa energetycznego, Zalecenia Komisji Europejskiej 2019/553 z dnia 3 kwietnia 2019 r. w sprawie cyberbezpieczeństwa w sektorze energetycznym.

8.1.4. Rekomenduje się, aby operatorzy usług kluczowych, będący operatorami systemów przesyłowych, dystrybucyjnych, Jednostki Wytwórcze Centralnie Dysponowane z podsektora energii elektrycznej, a także operatorzy systemów przesyłowych, dystrybucyjnych i obejmujące inne elementu procesu technologicznego w sektorach gazu, ropy i paliw, a także niektóre duże zakłady przemysłowe przeprowadzali audyt przez wewnętrzne struktury podmiotu bądź podmiot z grupy kapitałowej, w skład której wchodzi operator usługi kluczowej, zewnętrzny podmiot (tzw. audyt strony trzeciej), pod warunkiem bycia akredytowaną jednostką oceniającą zgodność bądź podmiot posiadający świadectwo bezpieczeństwa przemysłowego, o którym mowa w ustawie z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych*.

8.1.5. Rekomenduje się, aby kwalifikacje audytora były określone w programie audytów w ramach organizacji.

8.1.6. Rekomenduje się, aby operator usługi kluczowej opracował, w oparciu o ocenę ryzyka, listę usług kluczowych i systemów informacyjnych podlegających audytowi, uwzględniając realizowane procesy w ramach świadczenia usługi kluczowej, poziom odporności systemów i usług; istniejącą architekturę bezpieczeństwa, procedury wprowadzania zmian i utrzymania; a także przeszłe zdarzenia i incydenty.

8.1.7. Rekomenduje się, aby operator usługi kluczowej przeprowadził audyt uwzględniający elementy/zależności łańcucha dostaw, a także zmiany konfiguracji systemów informacyjnych – dotyczy tylko organizacji o najwyższym poziomie dojrzałości.

8.1.8. Rekomenduje się, aby operatorzy usług kluczowych określili w polityce bezpieczeństwa informacji bądź w programie audytu zasady i warunki korzystania z informatycznych narzędzi audytowych, a także zapewnili ochronę dostępu do tych narzędzi celem zapobieżenia ewentualnym nadużyciom i ujawnieniu danych audytowych.

8.1.9. Rekomenduje się, aby operatorzy usług kluczowych stosowali rozwiązania potwierdzające niezaprzeczalność zebranych w czasie audytu danych, takie jak podpisy elektroniczne, znaczniki czasu, uwierzytelnienie w systemach.

8.1.10. Rekomenduje się, aby dokumentacja wyników audytu składała się z raportu z audytu zawierającego specyfikację celu audytu, opis realizacji przedsięwzięcia audytowego, podsumowanie wyników dla kadry kierowniczej (często wyodrębniane jako osobny dokument), specyfikację punktów sprawdzeń wraz z wynikami, zalecenia poaudytowe, a także z wyników badań technicznych (tzw. dowody audytowe): przeglądy konfiguracji, analiza wyników testów penetracyjnych przeprowadzonych przez organizację bądź inny podmiot na zlecenie organizacji, itp.

8.1.1. Rekomenduje się, aby operator usługi kluczowej określił jednocześnie w ogólnej polityce bezpieczeństwa informacji zasady implementacji na poziomie organizacji zaleceń poaudytowych.

8.2. Metodyki audytu systemów informacyjnych

8.2.1. Istnieje kilka dostępnych metodyk przeprowadzenie audytu bezpieczeństwa informacji, stworzonych i proponowanych do zastosowania przez organizacje/instytucje zarówno polskie, jak i europejskie tj.: ISO, ISA, Urząd Dozoru Technicznego, ENISA (Agencja UE ds. Cyberbezpieczeństwa) czy ISSA Polska.

Przykładowe metodyki przeprowadzenia audytu bezpieczeństwa informacji przez operatora usługi kluczowej to:

– ISO 27001,

– ISA/IEC 62443,

– UDT Framework,

– ISSA Polska/IIA Polska,

– ENISA Framework.

9. Zachowanie ciągłości działania i odbudowa

9.1. Ciągłość świadczenia usług kluczowych

9.1.1. Powinno się opracować plan ciągłości działania obejmujący m.in. opracowane procedury ciągłości działania wraz ze zdefiniowaniem zakresów odpowiedzialności, uzgodnienie akceptowalnego poziomu strat, warunki jakie muszą wystąpić do zainicjowania planów (w z podziałem na konkretne procesy), opracowanie procedur odtworzenia procesów kluczowych, opracowanie procesu szkolenia personelu w zakresie procedur kryzysowych, testowanie planów ciągłości działania wraz z harmonogramem.

9.1.2. Organizacja powinna zidentyfikować kluczowe systemy informacyjne służące do świadczenia usług kluczowych, a także systemy informacyjne o charakterze wspomagającym, w których ewentualne zdarzenie może wpłynąć na te krytyczne. Ponadto zaleca się, aby identyfikacja wskazywała również na dane przekazywane w konkretnym systemie.

9.1.3. Należy także zidentyfikować krytyczne procesy technologiczne oraz biznesowe, a także określić ich wpływ na ciągłość działania przedsiębiorstwa. Ponadto, zaleca się dokonanie priorytetyzacji realizowanych usług, z uwzględnieniem usługi kluczowej jako tej krytycznej. Dodatkowo, powinno się określić parametry istotne dla ciągłości działania danego przedsiębiorstwa, takie jak Cel Czasu Odbudowy (ang. *recovery time objective*, RTO), Cel Punktu Odbudowy (ang. *recovery point objective*, RPO), maksymalny akceptowalny czas braku dostaw (ang. *maximum tolerable outage*, MTO) oraz Minimalny Cel Ciągłości Działania (ang. *minimum business continuity objective*, MBCO).

9.1.4. Zaleca się stworzenie oraz rozwijanie procedur mających na celu wykrywanie i monitorowanie ewentualnych zdarzeń cyberbezpieczeństwa, a także procedur pozwalających na usystematyzowanie innych działań związanych z reakcją na zdarzenie, np. usystematyzowanie procesu komunikacji wewnętrznej, scenariuszy awaryjnych. Organizacja powinna także dokonać niezbędnych modernizacji sprzętowych, oprogramowania lub dokonać zakupu nowych rozwiązań wspomagających zachowanie ciągłości działania.

9.1.5. Powinno się dokonać oszacowania czasu na jaki system informacyjny służący do świadczenia usługi kluczowej może być niedostępny, tak, aby ta niedostępność nie niosła za sobą istotnych konsekwencji (z ewentualnym uwzględnieniem konkretnych funkcji danego systemu).

9.1.6. Organizacja powinna zadbać o mechanizmy podnoszenia świadomości pracowników o funkcjonujących mechanizmach ciągłości działania, zagrożeniach, ewentualnych zadaniach pracowników podczas incydentu, a także, wkładu pracowników w efektywne zapewnienie ciągłości działania.

9.1.7. Kierownictwo organizacji powinno wyznaczyć osoby odpowiedzialne za zidentyfikowane procesy kluczowe, a także osoby odpowiedzialne za realizowanie zadań mających na celu zapewnienie ciągłości działania. Ponadto, kierownictwo swoim działaniem powinno powodować usprawnianie procesu zarządzania ciągłością działania.

9.1.8. Zaleca się wcześniejsze przygotowanie wymagań dla komunikacji i wymiany informacji związanej z ciągłością działania, wskazujących na najważniejsze aspekty związane m.in. ze stronami komunikacji.

9.1.9. Przygotowane procedury i mechanizmy ciągłości działania (np. plany ciągłości działania), w celu bieżącego utrzymania ich aktualności i przydatności, powinny być cyklicznie testowane i weryfikowane, a także ulepszane.

9.2. Wymagania dla komunikacji i wymiany informacji związanych z ciągłością działania

9.2.1. Rekomendowane jest, aby zawrzeć w procedurach/instrukcjach dotyczących komunikacji i wymiany informacji zasady obejmujące poniższe zagadnienia w zakresie utrzymania komunikacji:

- jednoznaczne wskazanie etapów działań i ich charakterystycznych cech (w miarę możliwości: zakresów działań, przedziałów czasowych, zdarzeń granicznych, ról głównych i pomocniczych),
- określenie jednoznacznego podziału ról i ich zakresów działań (w tym uwzględnienie zastępstw), na każdym zdefiniowanym etapie realizacji działań związanych z utrzymaniem ciągłości działania tak, by sposób i rodzaj komunikacji był jednoznaczny dla uczestników działań,
- ustalenie zastępowalności personelu w sytuacjach nieprzewidzianych takich jak brak komunikacji z osobą zastępującą w przypadku braku osoby zastępowanej,
- uwzględnienie rezerw personelu ponad standardową zastępowalność,
- uwzględnienie sytuacji przerwania komunikacji i wskazanie postępowania w takich przypadkach,
- opisanie sposobu komunikacji na poszczególnych etapach realizowania działań oraz zakresu komunikatów,
- wprowadzenie obowiązku zapoznania się wszystkich pracowników z procedurami dot. działań w zakresie utrzymania ciągłości, w tym komunikacji wraz z okresowym testowaniem znajomości procedur,
- regularne testowanie wszystkich kanałów komunikacji wskazanych do utrzymania ciągłości działania i potwierdzone sprawozdaniami,
- stworzenie co najmniej dwóch kanałów komunikacji w sytuacji kryzysowej (podstawowego i zastępczego) oraz rozpisania działań dot. zmiany kanału komunikacji,

– wskazanie w procedurach lub instrukcjach wykonawczych listy danych kontaktowych niezbędnych do realizacji działań (dane kontaktowe w zakresie podmiotu jak i dane kontaktowe służb zewnętrznych tj. straż pożarna, pogotowie) wraz z regularnym aktualizowaniem tej listy.

9.3. Odbudowa, plan odbudowy po katastrofie (DRP)

9.3.1. Organizacja powinna zdefiniować i utrzymywać parametry odbudowy systemów informacyjnych służących do świadczenia usługi kluczowej, zawarte w posiadanym planie odbudowy po katastrofie.

10. Bezpieczeństwo fizyczne

10.1. Bezpieczeństwo fizyczne

10.1.1. Zaleca się, aby organizacja przygotowała system bezpieczeństwa fizycznego określający m.in.:

- Ustalenie elementów, które podlegać będą ochronie,
- Minimalny poziom bezpieczeństwa dla różnych obszarów, np. obszaru zewnętrznego, ogólnodostępnych miejsc w siedzibie przedsiębiorstwa w przypadku dużej liczby pomieszczeń w których realizowane są procesy związane z usługą kluczową, a co za tym idzie, różnym oszacowanym ryzykiem zagrożeń, zaleca się wydzielenie stref ochronnych zróżnicowanych pod kątem poziomu zabezpieczeń. Zaleca się utworzenie strefy ograniczonego dostępu oraz strefy ściśle chronionej,
- Zróżnicowanie personelu pod względem kategorii, która jednocześnie wskazuje na poziomy dostępowe do różnych stref ochronnych lub pomieszczeń,
- Ustalenie zasadności zastosowania oraz wskazanie środków zabezpieczenia technicznego,
- Określenie procedur pracy systemu, również zasad pracy osób.

10.1.2. Zaleca się uwzględnienie w przeprowadzanej analizie ryzyka aspektów związanych z zagrożeniami mogącymi mieć wpływ na konieczność dostosowania pomieszczeń.

10.1.3. Zaleca się, aby organizacja w przeprowadzanej analizie ryzyka uwzględniła zagrożenia fizyczne związane z siedzibą przedsiębiorstwa. Analiza ryzyka powinna być przeprowadzona pod kątem konieczności zastosowania środków ochrony obwodowej.

10.2. Bezpieczeństwo fizyczne stron trzecich

10.1.1. W sytuacji konieczności skorzystania przez operatora usługi kluczowej z usługi doraźnej, świadczonej przez stronę trzecią, która wymaga udzielenia dostępu do obiektów przedsiębiorstwa będącego OUK, zaleca się:

– Zachowanie podwyższonej czujności podczas obecności pracowników wykonawcy na terenie należącym do operatora,

– Zaleca się uwzględnienie w przeprowadzanej analizie ryzyka sytuacji nielegalnego wykorzystania informacji pozyskanej przez osoby trzecie, a także sytuacji dostępu do pomieszczeń o podwyższonym standardzie zabezpieczeń.

– Rekomenduje się weryfikację statusu podwykonawcy danego działania m.in. pod kątem jego rozpoznawalności, spełniania odpowiednich standardów. Ponadto, w razie możliwości proponuje się pozyskanie personalnych rekomendacji oraz opinii na temat danej strony trzeciej wykonującej usługę doraźną.
– Zakres usługi powinien być jasno określony i zakomunikowany wszystkim pracownikom usługodawcy świadczącego usługę doraźną, którzy będą mieli dostęp do obiektów i pomieszczeń należących do operatora usługi kluczowej. Ponadto, powinno się zapewnić krótkie szkolenie informujące o procedurach i zasadach panujących na terenie organizacji. Po dokonaniu tych czynności powinno się określić ewentualny dostęp i wydać przepustki dla pracowników podwykonawcy.
– W sytuacji wykonywania prac, które ze względu na swój charakter lub ze względu na miejsce w jakim są prowadzone mogą spowodować zmaterializowanie się zagrożeń związanych z działaniem osób trzecich względem organizacji, operator usługi kluczowej powinien zapewnić stały nadzór wizyjny lub osobowy nad pracownikami podwykonawcy.
– Należy zwracać szczególną uwagę na niestandardowe zachowania pracowników strony trzeciej realizujących usługę na terenie przedsiębiorstwa.

11. Bezpieczeństwo sieci łączności elektronicznej

11.1. Segmentacja sieci, protokoły, szyfrowanie

11.1.1. Organizacja powinna stosować segmentację i separację sieci w zakresie systemów informacyjnych służących do świadczenia usługi kluczowej, o ile nie spowoduje to utrudnień lub zakłóceń w funkcjonowaniu tych systemów oraz sieci, a także samego świadczenia usługi kluczowej.

11.1.2. Organizacja powinna stosować szyfrowanie danych, informacji oraz komunikacji w zakresie świadczonej usługi kluczowej, a także uwzględnić ewentualność stosowania szyfrowania w środowiskach systemów informacyjnych służących do jej świadczenia, o ile nie spowoduje to utrudnień lub zakłóceń w funkcjonowaniu tych systemów, a także samego świadczenia usługi kluczowej.

11.2. Monitorowanie sieci łączności elektronicznej

11.2.1. W celu właściwego monitorowania prac sieci należy przeprowadzić inwentaryzację zasobów oraz urządzeń działających w sieciach.

11.2.2. W celu realizacji skutecznego monitorowania sieci należy określić krytyczność poszczególnych zasobów w sieci i oszacować dla nich ryzyka.

11.2.3. Rekomendowane jest monitorowanie zasobów oraz ruchu pomiędzy nimi, w tym zalecana jest automatyzacja monitoringu oraz scentralizowanie do jednego systemu zarządzającego.

11.2.4. Rekomendowane jest wydzielenie sieci wewnętrznej do realizacji zadań w zakresie monitorowania sieci.

11.2.5. Rekomendowane jest wdrożenie funkcjonalności umożliwiającej zbieranie i korelację zdarzeń w czasie rzeczywistym na podstawie zebranych informacji. System powinien także zbierać dane z wielu źródeł, a także uwzględniać dane przekazywane off-line uzyskane z odseparowanych sieci.

11.2.6. Rekomendowane jest zbudowanie wzorcowego obrazu sieci (ruchu) w prawidłowo działających sieciach, mające na celu m.in. zwiększenie możliwości wykrywania zdarzeń na podstawie anomalii względem wzorca.

11.2.7. Rekomendowane jest wdrożenie narzędzi do monitorowania które będzie miało możliwość reagowania na wykryte zdarzenia (alarm czy też działania defensywne w czasie rzeczywistym).

11.2.8. Rekomendowane jest aktualizowanie informacji dot. procesu monitorowania zasobów w sieci oraz aktualizacja danych po każdej zmianie w zidentyfikowanych do monitorowania obszarach.

11.2.9. W przypadku, gdy jest ograniczona możliwość monitorowania sieci ze względu np. na monitorowanie sieci odseparowanych fizycznie zalecane jest wykorzystanie innych metod zbierania informacji do uzupełnienia informacji dotyczących bezpieczeństwa zdarzeń w sieci w czasie rzeczywistym.

12. Bezpieczeństwo systemów informacyjnych

12.1. Ochrona danych

12.1.1. Rekomendowana jest identyfikacja danych dot. systemów IT/OT, szczególnie tych wrażliwych, na podstawie analizy ryzyka przeprowadzonej w organizacji uwzględniające oprócz wrażliwości z poziomu realizowanych zadań także przepisy prawa (m.in. RODO, dot. IK).

12.1.2. Rekomendowane jest stworzenie procedur/instrukcji dot. zasad postępowania z danymi w czasie ich przetwarzania, przechowywania, kopiowania czy też transmisji, a także zasad postępowania z nośnikami na których znajdują się dane (urządzenia w sieci, urządzenia końcowe, nośniki zewnętrzne, itp.).

12.1.3. Rekomendowane jest stworzenie procedur dotyczących kopii zapasowych.

12.1.4. Rekomendowane jest określenie zasad postępowania z zabezpieczeniami kryptograficznymi dla danych zgodnie z wynikami analizy oraz klasyfikacją danych wrażliwych w organizacji.

12.1.5. Rekomendowane jest udoskonalanie systemu w zakresie bezpieczeństwa danych we współpracy z pracownikami organizacji np. poprzez przeprowadzanie cyklicznych szkoleń lub też budowanie systemu wymiany informacji między kierownictwem a pracownikami w m.in. w celu uzyskiwania informacji o lukach bezpieczeństwa danych w działającym systemie.

12.2. Zarządzanie uprawnieniami

12.2.1. W zakresie zarządzania uprawnieniami rekomendowane jest wprowadzenie polityki dotyczącej nadawania, modyfikowania i odbierania uprawnień oraz nadzorowania tych działań.

12.2.2. Rekomendowane jest stworzenie procedur dotyczących nadawania/odbierania uprawnień, ich aktualizowania, regularnego ich przeglądu z równoczesnym wskazaniem osób/ról odpowiedzialnych za realizację tych zadań.

12.2.3. Rekomendowane jest by uprawnienia były nadawane zgodnie z zasadą minimalnego dostępu określonego przez zakres realizowanych zadań.

12.2.4. Rekomendowane jest wdrożenie rozwiązań dotyczących jednoznacznej identyfikacji użytkowników.

12.2.5. Dla kont administratorskich rekomendowane jest nadawanie uprawnień administratorom tylko w systemach im podlegających oraz ograniczeniu możliwości dostępu do danych przetwarzanych w systemach.

12.2.6. Rekomendowane jest wdrożenie zasady wielopoziomowego uwierzytelnienia dostępu, szczególnie do kont administratorskich.

12.2.7. Rekomendowane jest stworzenie procedur dotyczących zastępstw w sytuacjach zarówno planowanych jak i o charakterze nagłym zarówno dot. kont administratorskich jak i zwykłych użytkowników, wraz z rejestrowaniem takich zdarzeń, przeglądem rejestrów i ich odpowiednim przechowywaniem.

12.2.8. Rekomendowane jest prowadzenie rejestru prac w systemach oraz dokonywanych zmianach, ich regularny przegląd oraz odpowiednie zabezpieczenie przed utratą.

12.3. Kontrola dostępu do danych

12.3.1. Organizacja powinna stworzyć procedury (polityki) zarządzania uprawnieniami i dostępem do systemów dla pracowników organizacji, a także sposobu wnioskowania o dostęp oraz ustalonej ścieżki akceptacji.

12.3.2. Należy stworzyć procedurę zarządzania dostępem do systemów, dedykowanej dostawcom usług – stronom trzecim.

12.3.3. Organizacja powinna cyklicznie weryfikować prawa dostępu do systemów i sieci, zgodnie z przygotowanym harmonogramem. Powinno się także przeprowadzać doraźne weryfikacje przyznanych uprawnień. Dodatkowo, powinny zostać określone zasady odnośnie usuwania nieużywanych kont po krótkim okresie czasu.

12.3.4. W razie możliwości zaleca się skonfigurowanie, w systemach obsługujących usługę kluczową, dedykowanych kont administracyjnych z dostępem dla administratorów przeprowadzających konkretne operacje, np. konserwacje, instalacje. Ponadto, proces zarządzania kontami administracyjnymi powinien być udokumentowany, a także powinny być dostępne dzienniki aktywności kont administratorów. Zaleca się stworzenie dostosowanych i udokumentowanych kont administracyjnych z określonymi uprawnieniami dostępu przyznanymi właściwym pracownikom.

12.3.5. Należy unikać stosowania kont współdzielonych i zamiast nich stosować konta imienne dla administratorów oraz użytkowników.

12.3.6. W razie możliwości zaleca się wdrożenie narzędzi umożliwiających wspieranie procesów zarządzania dostępem fizycznym i logicznym oraz odpowiedniej separacji dostępów w zależności od poziomu uprawnień.

12.3.7. Powyższe procedury powinny określać również zasady dostępu do systemów w sposób zdalny.

12.3.8. Przydzielanie haseł do tworzonych kont, powinno funkcjonować jako formalny proces, który pozwoli na sprawowanie kontroli nad tą czynnością.

12.4. Dostęp zdalny i urządzenia mobilne

12.4.1. Zaleca się by dostęp do zasobów przedsiębiorstwa odbywał się poprzez szyfrowane kanały, a także by stosowane było uwierzytelnienie wieloskładnikowe.

12.4.2. W ramach pracy zdalnej zaleca się by pracownicy pracowali na sprzęcie firmowym wykorzystującym wirtualne sieci prywatne (ang. Virtual Private Network – VPN) oraz by był on odpowiednio zaopatrzony w niezbędne oprogramowanie (służące do pracy i chroniące dane urządzenie mobilne).

12.4.3. Zaleca się by operatorzy usług kluczowych zmieniali domyślne hasła i nazwy użytkowników skonfigurowane w poszczególnych urządzeniach, w tym w urządzeniach mobilnych. Rekomenduje się opracowanie stosownej polityki zarządzania hasłami – sposoby ich tworzenia, wymagania co do ich złożoności (np. ilość znaków, wielka litera, znak specjalny itd.), a także wymuszali na użytkownikach regularną zmianę haseł. Operator powinien zapoznać cały personel z wewnętrzną polityką zarządzania hasłami.

12.4.4. Rekomenduje się by operator usługi kluczowej dokonał segregacji dostępu zdalnego poprzez np. opracowanie zestawu zasad komunikacji zdalnej.

12.4.5. W celu kontroli dostępu zaleca się stworzenie tzw. „czarnych list", które zawierają informacje na temat adresów e-mail, IP czy domen, które nie powinny być dozwolone w ruchu przychodzącym do sieci danego przedsiębiorstwa.

12.4.6. Zaleca się unikać używania dzielonych kont przez różnych użytkowników do urządzeń i systemów w celu lepszego monitorowania aktywności poszczególnych osób, a także możliwości powiązania danego działania z konkretnym użytkownikiem.

12.4.7. Rekomenduje się by operator usługi kluczowej opracował stosowną politykę w zakresie udzielania dostępu zdalnego podmiotom zewnętrznym.

12.4.8. Zaleca się by urządzenia mobilne, na których pracuje personel były odpowiednio skonfigurowane i posiadały zainstalowane oprogramowanie chroniące, jak np. program antywirusowy, firewall itp.

12.4.9. Urządzenia mobilne po zakończeniu ich eksploatacji powinny być utylizowane z zachowaniem standardów bezpieczeństwa i ochrony polityki prywatności.

12.4.10. W ramach zdalnego dostępu do zasobów organizacji, ważne jest również zapewnienie bezpieczeństwa wideokonferencji (dla funkcji audio i wideo, a także przesyłanych plików i komunikatorów).

12.4.11. Zaleca się by w czasie pracy zdalnej, pracownicy mieli zapewniony odpowiedni poziom wsparcia technicznego (procedury, instrukcje, serwis itp.).

12.4.12. Operator usługi kluczowej powinien również zapewnić swój personel przebywający na pracy zdalnej, że przetwarzanie danych w kontekście telepracy (jak np. rejestr czasu pracy) jest zgodne z ramami prawnymi UE dotyczącymi ochrony danych osobowych.

12.4.13. Pracownicy przebywający na pracy zdalnej również powinni być poinformowani o zagrożeniach płynących z pracy zdalnej.

12.4.14. Pracownicy powinni dysponować narzędziami szyfrującymi w celu zachowania bezpiecznej komunikacji z podmiotami zewnętrznymi.

12.5. Bezpieczeństwo systemów automatyki przemysłowej, sieci inteligentnych

12.5.1. Rekomenduje się stworzenie polityki bezpieczeństwa systemów OT.

12.5.2. Organizacja powinna przeprowadzać testy bezpieczeństwa systemów OT.

12.5.3. Przy prowadzonej analizie ryzyka organizacja powinna wziąć pod uwagę zagrożenia związane z sieciami inteligentnymi.

12.5.4. Zaleca się dokonanie inwentaryzacji zasobów i urządzeń działających w sieci w celu kompleksowego przygotowania strategii cyberbezpieczeństwa.

13. Wytyczne sektorowe dotyczące zgłaszania incydentów

13.1. Zdolność w zakresie reagowania na incydenty

13.1.1. W celu wspierania aktywnego wczesnego ostrzegania i szybkiego reagowania na zdarzenia krytyczne zaleca się utworzenie stałej i multidyscyplinarnej grupy zadaniowej w organizacji, która musi być w stanie wybrać odpowiednią strategię łagodzenia skutków incydentów, gdy zajdzie taka potrzeba, w celu zminimalizowania wpływu na ciągłość usług i na biznes.

13.1.2. Multidyscyplinarna grupa zadaniowa powinna być zorganizowana w systemie zmianowym i musi pozostawać w kontakcie z zespołem zarządzania kryzysowego lub zarządem organizacji, na wypadek, gdyby zdarzenie przerodziło się w kryzys. Organizacja powinna zapewnić środki celem zmotywowania i przeszkolenia wspomnianego zespołu zadaniowego.

13.1.3. Konieczne jest wdrożenie pasywnych narzędzi monitorujących w celu wykrywania anomalii, które mogą wskazywać na cyberatak i przewidywać zagrożenia.

13.1.4. Logi muszą być agregowane i skorelowane. Rekomenduje się do tego narzędzie SIEM.

13.2. Zarządzanie zagrożeniami

13.2.1. Organizacja powinna zbierać dane dotyczące zagrożeń z wielu różnych źródeł, począwszy od informacji dostępnych publicznie, do platform wymiany wiedzy o zagrożeniach, takich jak MISP.

13.2.2. Rekomenduje się stosowanie zarówno zewnętrznej, jak i wewnętrznej analizy zagrożeń przeprowadzonej w oparciu o dane zgromadzone w infrastrukturze organizacji.

13.2.3. Należy zwizualizować wszystkie zidentyfikowane zasoby, sieci i ich topologię. Aplikacje oraz wszystkie usługi i ich interakcje między sobą powinny być udokumentowane.

13.2.4. Rekomenduje się ścisłą współpracę pomiędzy komórką zajmującą się analizą zagrożeń w organizacji, a strukturami odpowiedzialnymi za reagowanie na incydenty teleinformatyczne.

13.3. Zarządzanie podatnościami

13.3.1. Należy ustanowić proces zarządzania podatnościami wewnątrz organizacji wraz z określeniem ich krytyczności na podstawie przeprowadzonej analizy ryzyka, obejmujący wykorzystanie zarówno automatycznych, jak i nieautomatycznych narzędzi.

13.3.2. Usuwając podatności, należy rozpocząć od tych najbardziej krytycznych, biorąc pod uwagę istotność posiadanych aktywów i systemów.

13.3.3. Należy ustanowić proces ujawniania podatności.

13.3.4. Należy regularnie przeprowadzać testy penetracyjne nowych rozwiązań Internetu Rzeczy w kontrolowanym środowisku bądź przed lub podczas fazy ich wdrażania, a także po ważnych aktualizacjach systemu.

13.3.5. Należy zapewnić ścisłą współpracę komórek organizacyjnych odpowiedzialnych za OT i IT w przedsiębiorstwie oraz ich efektywną współpracę z właścicielami systemów, kadrą zarządzającą i innymi właściwymi podmiotami w ramach organizacji.

13.4. Katalog incydentów

13.4.1. Klasyfikacja incydentów powinna odbywać się poprzez przejście po kolei przez ustanowione kryteria, aby w jak najlepszym stopniu możliwe było prawidłowe zidentyfikowanie źródła oraz skali skutków, jakie spowodował dany incydent.

13.4.2. Zaleca się opracowanie katalogu incydentów cyberbezpieczeństwa możliwych do wystąpienia w przedsiębiorstwie, charakterystycznych dla obszaru i zakresu działania spółki, a także dopasowanego do wewnętrznych uwarunkowań i specyfiki danego podmiotu.

13.4.3. Rekomenduje się, by operator usługi kluczowej opracował katalog incydentów cyberbezpieczeństwa, który będzie uwzględniał m.in. obszar, zasięg i klasyfikację danego incydentu.

13.4.4. Rekomenduje się, by katalog incydentów został opracowany w oparciu o wspólną taksonomię incydentów dla całego sektora energii.

13.4.5. Zaleca się, by opracowany katalog uwzględniał efekty kaskadowe wystąpienia danego incydentu spowodowane zależnością różnych systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej.

13.4.6. Zaleca się cykliczne aktualizowanie opracowanego katalogu incydentów.

13.4.7. Do każdej z grup incydentów zawartych w katalogu incydentów organizacja powinna stworzyć procedury postępowania i udostępniać je pracownikom odpowiedzialnym za procedurę reakcji. Stosownie do możliwości organizacji, każda z grup incydentów powinna mieć określoną komórkę lub komórki organizacyjne, które będą zaangażowane w procesie reagowania na incydent.

13.5. Zarządzanie incydentem cyberbezpieczeństwa

13.5.1. Rekomenduje się, by operator usługi kluczowej zgłaszał incydent poważny do właściwego CSIRT poziomu krajowego poprzez odpowiedni formularz opublikowany na stronie internetowej, a także powinien postępować w tym zakresie zgodnie z instrukcją wskazaną przez dany CSIRT krajowy.

13.5.2. Zaleca się, by operatorzy usług kluczowych powiadamiali o wystąpieniu incydentu oraz innych zdarzeń mających wpływ na ciągłość świadczenia usługi kluczowej organ właściwy ds. cyberbezpieczeństwa dla sektora energii w celu wsparcia działań zmierzających do nadzorowania systemu cyberbezpieczeństwa w sektorze energii.

13.5.3. Organizacja powinna zgłaszać jako incydent każdą istotną awarię związaną z realizowaną usługą kluczową, co do której istnieje podejrzenie, iż mogła mieć miejsce w związku z incydentem w zakresie cyberbezpieczeństwa.

13.5.4. Rekomenduje się, aby w przypadku wykrycia nietypowego zdarzenia mogącego mieć związek z bezpieczeństwem systemów informacyjnych służących do świadczenia usługi kluczowej, lub innych systemów w których zdarzenie może wpłynąć na usługę kluczową, organizacja niezwłocznie podejmowała działania zmierzające do zbadania zdarzenia.

13.5.5. Powinno się zobligować pracowników, wykonawców i podmioty zewnętrzne, które mają dostęp do wewnętrznego środowiska IT lub OT operatora usługi kluczowej, do zgłoszenia i raportowania o każdej zaobserwowanej lub podejrzanej anomalii lub zdarzeniu mogącym świadczyć o lukach bezpieczeństwa.

13.5.6. Operator usługi kluczowej powinien mieć opracowane procedury regulujące kwestie wykrywania i analizowania przypadków naruszenia zasad bezpieczeństwa, reagowania na incydenty, uczenia się na incydentach, w celu doskonalenia wdrożonych systemów zabezpieczeń.

13.5.7. Operator usługi kluczowej powinien opracować procedurę zgłaszania incydentów w ramach swojej organizacji, a także zapoznać z nią swoich pracowników i personel partnerów zewnętrznych, który realizuje zadania u danego operatora.

13.5.8. Rekomenduje się by operatorzy usług kluczowych mieli opracowane odpowiednie procedury, w których będą przypisane role do poszczególnych stanowisk/komórek organizacyjnych, a także zakres odpowiedzialności. Ponadto, podmioty powinny wdrożyć mechanizmy monitorowania, analizowania i reagowania na incydenty.

13.5.9. W czasie obsługi incydentu zaleca się bieżące gromadzenie materiału dowodowego i analizowanie znalezionych artefaktów.

13.5.10. W ramach procedur zarządzania incydentem, powinny również zostać ustalone sposoby komunikacji z CSIRTami poziomu krajowego, organem właściwym ds. cyberbezpieczeństwa, organami ścigania i innymi podmiotami, ważnymi z punktu widzenia danego operatora usługi kluczowej.

13.5.11. Zaleca się, by po opanowaniu incydentu uruchomić przygotowane wcześniej procedury odtworzenia po awarii.

13.5.12. Rekomenduje się regularne sprawdzanie opracowanych procedur poprzez organizację wewnętrznych ćwiczeń.

13.5.13. Operatorom usług kluczowych rekomenduje się podłączenie do systemu teleinformatycznego S46 w celu posiadania pełniejszej wiedzy na temat zagrożeń, incydentów i powiązań międzysektorowych.

Załącznik nr 5
Macierz minimalnych rekomendowanych działań mających na celu wzmocnienie cyberbezpieczeństwa

Numer rekomendacji	Poziomy dojrzałości organizacji pod kątem cyberbezpieczeństwa			
	0 (brak)	1 (minimalny)	2 (średni)	3 (wysoki)
4.1.1.				
4.1.2.				
4.1.3.				
4.1.4.				
4.1.5.				
4.1.6.				
4.2.1.				
4.2.2.				
4.2.3.				
4.2.4.				
4.2.5.				
4.2.6.				
4.2.7.				
4.3.1.				
4.3.2.				
4.4.1.				
5.1.1.				
5.1.2.				
5.1.3.				
5.1.4.				
5.1.5.				
5.1.6.				
5.1.7.				
5.1.8.				
5.2.1.				
5.2.2.				
5.2.3.				
5.2.4.				
5.2.5.				
5.2.6.				
5.3.1.				
5.3.2.				
5.3.3.				
6.1.1.				
6.1.2.				
6.1.3.				
6.1.4.				
6.1.5.				
6.1.6.				

6.1.7.		
6.1.8.		
6.1.9.		
6.1.10.		
6.2.1.		
6.3.1.		
6.4.1.		
6.4.2.		
6.4.3.		
6.4.4.		
6.4.5.		
6.4.6.		
6.5.1.		
6.5.2.		
6.5.3.		
6.5.4.		
6.5.5.		
6.6.1.		
6.6.2.		
6.6.3.		
6.7.1.		
7.1.1.		
7.2.1.		
7.2.2.		
7.2.3.		
7.2.4.		
7.2.5.		
7.2.6.		
7.2.7.		
7.3.1.		
7.3.2.		
8.1.1.		
8.1.2.		
8.1.3.		
8.1.4.		
8.1.5.		
8.1.6.		
8.1.7.		
8.1.8.		
8.1.9.		
8.1.10.		
8.1.11.		
8.2.1.		
9.1.1.		
9.1.2.		
9.1.3.		
9.1.4.		

9.1.5.			
9.1.6.			
9.1.7.			
9.1.8.			
9.1.9.			
9.2.1.			
9.3.1.			
10.1.1.			
10.1.2.			
10.1.3.			
10.2.1.			
11.1.1.			
11.1.2.			
11.2.1.			
11.2.2.			
11.2.3.			
11.2.4.			
11.2.5.			
11.2.6.			
11.2.7.			
11.2.8.			
11.2.9.			
12.1.1.			
12.1.2.			
12.1.3.			
12.1.4.			
12.1.5.			
12.2.1.			
12.2.2.			
12.2.3.			
12.2.4.			
12.2.5.			
12.2.6.			
12.2.7.			
12.2.8.			
12.3.1.			
12.3.2.			
12.3.3.			
12.3.4.			
12.3.5.			
12.3.6.			
12.3.7.			
12.3.8.			
12.4.1.			
12.4.2.			
12.4.3.			
12.4.4.			

12.4.5.				
12.4.6.				
12.4.7.				
12.4.8.				
12.4.9.				
12.4.10.				
12.4.11.				
12.4.12.				
12.4.13.				
12.4.14.				
12.5.1.				
12.5.2.				
12.5.3.				
12.5.4.				
13.1.1.				
13.1.2.				
13.1.3.				
13.1.4.				
13.2.1.				
13.2.2.				
13.2.3.				
13.2.4.				
13.3.1.				
13.3.2.				
13.3.3.				
13.3.4.				
13.3.5.				
13.4.1.				
13.4.2.				
13.4.3.				
13.4.4.				
13.4.5.				
13.4.6.				
13.4.7.				
13.5.1.				
13.5.2.				
13.5.3.				
13.5.4.				
13.5.5.				
13.5.6.				
13.5.7.				
13.5.8.				
13.5.9.				
13.5.10.				
13.5.11.				
13.5.12.				
13.5.13.				