TLP WHITE

Dojrzałość w obszarze cyberbezpieczeństwa sektora transportu w Polsce

Raport 2022

NASK

Ministerstwo Infrastruktury

EY
Building a better working world

Spis treści

O raporcie

Ministerstwo Infrastruktury

Szanowni Państwo,

rozwój technologii oraz wykorzystanie narzędzi teleinformatycznych w każdym aspekcie codziennego życia nie ominął także sektora transportu. W krajobrazie polskiego przewoźnictwa, które obejmuje zarówno kolejnictwo, lotnictwo, transport wodny oraz drogowy, bardzo istotna jest także cyberprzestrzeń. Pełniąc rolę organu właściwego ds. cyberbezpieczeństwa w sektorze transportu wierzę, że ten raport będzie dla Państwa dużą wartością. Wyniki badania dojrzałości wskazują na postępy, jakie poczynił sektor transportu. Niewątpliwie, wykorzystanie technologii cyfrowej znacząco wpływa na wszystkie podsektory transportu, a zagrożenia teleinformatyczne i związane z nimi ryzyka oddziałują na systemy transportowe. Pokazuje to chociażby liczba cyberataków na inteligentne systemy mobilności, która wzrosła znacząco na całym świecie. Nie bez znaczenia pozostaje także pandemia COVID-19, która całkowicie zakłóciła postrzeganie i planowanie organizacji wokół ryzyka strategicznego, operacyjnego, technologicznego i finansowego.

Efektem współpracy Ministerstwa Infrastruktury, NASK PIB oraz EY Polska jest niniejszy Raport, przedstawiający zrealizowane cele oraz udoskonalenia, jakie zostały wypracowane w ramach rozwijania wyższego poziomu dojrzałości i odporności cyberbezpieczeństwa w sektorze transportu. Składamy go w Państwa ręce z nadzieją, że zawarte w nim dane oraz zalecenia przyczynią się do ułatwienia wdrażania najlepszych praktyk w zakresie bezpieczeństwa, które są zgodne z obowiązującymi standardami i wytycznymi.

Andrzej Adamczyk
Minister Infrastruktury

NASK

Szanowni Państwo,

Nowelizacja ustawy o KSC, a także propozycja Dyrektywy NIS2 wprowadzają szereg wyzwań dla podmiotów krajowego systemu cyberbezpieczeństwa we wszystkich sektorach. Warto zawczasu przygotować się na nadchodzące zmiany poprzez ocenę aktualnego poziomu dojrzałości organizacji w obszarze cyberbezpieczeństwa. NASK PIB aktywnie angażuje się w inicjatywy, które wspierają rozwój odporności na zagrożenia w cyberprzestrzeni. Wierzymy, że raport, który trzymacie Państwo w rękach będzie pomocą nie tylko dla badanych Operatorów Usług Kluczowych z sektora transportu, ale także dla innych podmiotów, które mogą zostać objęte nowymi przepisami. Pozwoli zastanowić się nad kierunkami dalszych działań i tym samym wyjść naprzeciw zbliżającym się regulacjom.

Krzysztof Silicki
Zastępca Dyrektora NASK, Dyrektor ds. Cyberbezpieczeństwa i Innowacji

Sektor transportu to jeden z istotniejszych sektorów dla Polskiej gospodarki. Postępująca cyfryzacja i rozwój przemysłu 4.0 sprawia, że staje się on coraz bardziej podatny na zagrożenia teleinformatyczne. Na przykładzie Rotterdamu w 2017 roku, w czasie ataku ransomware NotPetya, widzieliśmy jak można zdestabilizować ekosystem portu, a przez to także całą gospodarkę państwa. W 2020 roku widzieliśmy natomiast atak malware na szwajcarskie przedsiębiorstwo kolejowe Stadler – systemy firmy zostały zainfekowane malware, który umożliwił ściągnięcie wrażliwych danych. Po tym jak firma odmówiła zapłaty okupu, przestępcy opublikowali online wykradzione dane i wewnętrzne dokumenty. Przykłady można by mnożyć.

Dlatego, wspólnie z Ministerstwem Infrastruktury i NASK Państwowym Instytutem Badawczym postanowiliśmy zbadać dojrzałość sektora transportu w Polsce w zakresie cyberbezpieczeństwa. Od czasu przyjęcia w 2016 roku Dyrektywy NIS, a potem jej implementacji – Ustawy o krajowym systemie cyberbezpieczeństwa (2018 rok), sektor ten, jako sektor kluczowy, objęty jest szczególnym nadzorem państwa w zakresie cyberbezpieczeństwa. Nie ma jednak wątpliwości, że nowa wersja Dyrektywy (tzw. NIS2) oraz gwałtowny rozwój technologii stawia przed nim nowe wyzwania. Naszym celem było zebranie informacji na temat tych wyzwań i przygotowanie rekomendacji, które mogą pomóc w budowie dojrzałości teleinformatycznej zarówno transportu kolejowego, jak i wodnego oraz lotniczego.

Piotr Ciepiela,
Globalny Lider Bezpieczeństwa Architektury i Nowoczesnych Technologii, Partner EY

Wstęp

W drugim kwartale 2022 r. Ministerstwo Infrastruktury, NASK PIB oraz EY Polska przeprowadzili wspólne badanie dojrzałości sektora transportu w obszarze cyberbezpieczeństwa. Do badania zaproszonych zostało 25 podmiotów – wszyscy operatorzy usług kluczowych (OUK) wyznaczeni przez Ministerstwo Infrastruktury w sektorze transportu w Polsce. Celem przeprowadzonego badania było zbadanie poziomu dojrzałości sektora w obszarze cyberbezpieczeństwa, w kontekście wdrażania w sektorze zapisów Ustawy o krajowym systemie cyberbezpieczeństwa, a także przygotowania do nowelizacji jej zapisów i przyjętej w 2022 roku Europejskiej Dyrektywy NIS2. Ankieta została podzielona na 4 główne sekcje: Organizacja, Narzędzia, Procesy oraz Zespół. Pytania zawarte w każdej z tych sekcji pozwalają zweryfikować obecny stan dojrzałości OUK w obszarach, do których się odnoszą. Dodatkowo, na końcu ankiety zamieszczono pytania otwarte na temat wyzwań związanych z implementacją Ustawy o krajowym systemie cyberbezpieczeństwa i tych związanych z zapisami Dyrektywy NIS2. Udział w badaniu był dobrowolny. Ankieta została rozesłana przez Ministerstwo Infrastruktury, które zanonimizowało wyniki przed ich analizą. Raport oparty jest o wyniki ankiet z dwudziestu czterech OUK (dwa z sektora kolejowego, dziesięć z sektora wodnego oraz dwanaście z sektora lotniczego). Raport podzielony jest na rozdziały odpowiadające poszczególnym podsektorom. Każdy rozdział składa się z opisu specyfiki danego podsektora i analizy badań.

Raport został sporządzony w dwóch wersjach: TLP Amber oraz TLP White. Wersja raportu TLP Amber dedykowana jest operatorom usług kluczowych, organom właściwym ds. cyberbezpieczeństwa oraz administracji państwowej. Zawiera szczegółowe wyniki badań (również z sekcji Narzędzia), a także wnioski oraz sugerowane działania do podjęcia. Wersja raportu TLP White nie zawiera poufnych informacji i jest przeznaczona dla szerokiego grona odbiorców.

Zapraszamy do lektury!

Ustawa o KSC i NIS2 – jakie wyzwania stoją przed sektorami kluczowymi

EY

Ustawa KSC i NIS2 – jakie wyzwania stoją przed sektorami kluczowymi

Przyjęcie Dyrektywy NIS[1] w 2016 roku i późniejsza jej implementacja do porządku prawnego w Polsce: Ustawa o krajowym systemie cyberbezpieczeństwa postawiły przed sektorami kluczowymi nowe wyzwania związane z cyberbezpieczeństwem. Ponadto ustalony został w tym zakresie wyraźny nadzór państwa - organy właściwe ds. cyberbezpieczeństwa i CSIRT krajowe. Nowelizacja ustawy oraz tzw. Dyrektywa NIS2 zwiększają nie tylko obowiązki operatorów, ale także rozszerzają zakres podmiotów, które będą musiały tym obowiązkom sprostać.

Ustawa o krajowym systemie cyberbezpieczeństwa (KSC) i nowelizacja

Według Ustawy o krajowym systemie cyberbezpieczeństwa, operatorzy usług kluczowych to firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Usługa kluczowa jest zależna od systemów informatycznych[2]. Ustawa wskazuje sektory, w których identyfikowani są operatorzy usług kluczowych. Są to sektor energetyczny, transportowy, bankowy i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej. Dokładna lista usług kluczowych została zawarta w rozporządzeniu wykonawczym do ustawy[3]. Identyfikacji operatorów usług kluczowych dokonują organy właściwe, które wydają w tym zakresie decyzję administracyjną, a podstawą do wydania decyzji są następujące kryteria:

- podmiot świadczy usługę kluczową w jednym z sektorów,
- świadczenie usługi zależy od systemów informacyjnych,
- wystąpienie incydentu miałoby istotny skutek zakłócający dla świadczenia usługi kluczowej.

Ocena istotności skutku zależy od progów istotności skutku zakłócającego, które zostały wyznaczone przez Radę Ministrów z uwzględnieniem przede wszystkim:

- liczby użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot,
- zależności innych sektorów od usługi świadczonej przez ten podmiot,
- wpływu, jaki mógłby mieć incydent, ze względu na jego skalę i czas trwania, na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne,
- udziału podmiotu świadczącego usługę kluczową w rynku,
- zasięgu geograficznego obszaru, którego mógłby dotyczyć incydent,
- zdolności podmiotu do utrzymywania wystarczającego poziomu świadczenia usługi kluczowej, przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia,
- innych czynników charakterystycznych dla danego sektora lub podsektora.

Operatorzy usług kluczowych zobowiązani są wdrożyć system zarządzania bezpieczeństwem w systemie informacyjnym, wykorzystywanym do świadczenia usługi kluczowej. W ramach zarządzania wymagane jest systematyczne szacowanie ryzyka i dostosowanie do niego środków bezpieczeństwa, takich jak bezpieczna eksploatacja systemu, bezpieczeństwo fizyczne systemu (w tym kontrola dostępu), bezpieczeństwo i ciągłość dostaw usług, które mają wpływ na świadczenie usługi kluczowej, utrzymanie planów działania umożliwiających ciągłość świadczenia usługi, ciągłe monitorowanie systemu zapewniającego świadczenie usługi.

Ponadto operator jest zobowiązany do stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego, w tym zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatności systemu. Operator jest także odpowiedzialny za opracowanie dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego, uaktualnianie jej i przechowywanie przez okres co najmniej 2 lat.

1 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 (Directive concerning measures for a high common level of security of network and information systems across the Union).

2 Operatorzy usług kluczowych (OUK) nie są więc tożsami z operatorami infrastruktury krytycznej (IK). Kwestie ochrony infrastruktury krytycznej regulowane są na mocy Ustawy z 27 kwietnia 2007 o zarządzaniu kryzysowym. Zawarta tam definicja określa IK jako systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Obecnie Rządowe Centrum Bezpieczeństwa prowadzi prace mające na celu przejście od modelu obiektowego do usługowego w dziedzinie ochrony IK.

3 Rozporządzenie w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.

W przypadku wystąpienia incydentu, operator zapewnia jego obsługę poprzez:

- klasyfikację incydentu na podstawie kryteriów określonych przez Radę Ministrów w drodze Rozporządzenia,
- w przypadku zakwalifikowania incydentu jako poważny – zgłoszenie do właściwego CSIRT nie później niż w ciągu 24 godzin od momentu wykrycia,
- współdziałanie z CSIRT w ramach obsługi incydentu wraz z zapewnieniem odpowiedniego dostępu do informacji,
- usunięcie podatności systemu.

Do realizacji zadań określonych w ustawie operator powołuje struktury wewnętrzne odpowiedzialne za cyberbezpieczeństwo, o czym informuje zarówno organ właściwy, jak i sektorowy zespół cyberbezpieczeństwa (jeśli został powołany). Możliwe jest także zawarcie umowy z podmiotem zewnętrznym, który świadczy usługi z zakresu cyberbezpieczeństwa. Ustawa dopuszcza więc outsourcing usług bezpieczeństwa. Informację na temat podpisania umowy z podmiotem zewnętrznym należy przekazać w analogiczny sposób wraz z danymi kontaktowymi podmiotu i zakresem świadczonej usługi w terminie 14 dni od daty zawarcia umowy.

Minister właściwy do spraw informatyzacji określił warunki organizacyjne i techniczne dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, a także dla wewnętrznych struktur operatorów w drodze Rozporządzenia.

Nadzór nad każdym z kluczowych sektorów gospodarki sprawuje organ właściwy ds. cyberbezpieczeństwa. 11 sektorów wymienionych w ustawie podlega kompetencji konkretnych ministrów działowych[4]. Oznacza to, że organami właściwymi są ministrowie właściwi dla konkretnych działów administracji, którzy na podstawie porozumienia mogą powierzyć realizację niektórych zadań jednostkom podległym lub nadzorowanym. Co za tym idzie: regulatorzy sektorowi (jeśli istnieją) mogą realizować te funkcje zamiast ministra właściwego.

Zadaniem organu właściwego ds. cyberbezpieczeństwa jest analiza podmiotów funkcjonujących w danym sektorze i wydawanie decyzji o uznaniu za operatora usługi kluczowej. Poza tym organ właściwy przygotowuje także rekomendacje działań, których zadaniem jest wzmocnienie poziomu cyberbezpieczeństwa sektora.

Do obowiązków organu należy też:

- wzywanie podmiotu do usunięcia podatności, które mogą lub mogły doprowadzić do poważnego incydentu,
- prowadzenie kontroli operatorów usług kluczowych,
- współpraca z innymi państwami UE za pośrednictwem Pojedynczego Punktu Kontaktowego,
- udział w ćwiczeniach oraz przetwarzanie danych osobowych niezbędnych do realizacji zadań.

Ustawa przewiduje powołanie sektorowych zespołów cyberbezpieczeństwa przez organy właściwe. Dużą zaletą działania takiego zespołu jest uwzględnienie specyfiki danego sektora, co pozwala dostosować wsparcie dla operatorów usług kluczowych.

Zespół nie tylko przyjmuje zgłoszenia o incydentach i pomaga w obsłudze, ale również analizuje ich skutki, wypracowuje wnioski oraz współpracuje z właściwym CSIRT. Może też wymieniać informacje o incydentach poważnych z innymi krajami Unii Europejskiej.

W nowelizacji ustawy następuje kilka znaczących zmian w tych zapisach. Przede wszystkim tzw. wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo będą teraz określane jako SOC (Security Operation Center), a minister właściwy ds. informatyzacji będzie prowadził ich rejestr. Oznacza to, że jeśli operator będzie zlecał realizowanie obowiązków ustawowych firmom zewnętrznym, musi mieć pewność, że SOC te znajdują się we właściwym rejestrze.

Drugą znaczącą zmianą jest obowiązek tworzenia sektorowych CSIRT. Do tej pory sektorowe zespoły cyberbezpieczeństwa były dobrowolne. Obecnie funkcjonuje tylko jeden - CSIRT KNF, który odpowiada za sektor finansowy. Teraz organy właściwe ds. cyberbezpieczeństwa będą miały obowiązek powoływania CSIRT-ów sektorowych, co dla takich sektorów jak transport, gdzie specyfika poszczególnych podsektorów jest odmienna, może być wyzwaniem (ustawa przewiduje tylko jeden CSIRT dla każdego sektora, nie uwzględniając specyfiki podsektorowej).

Kolejną nowością zapisaną w nowelizacji jest wprowadzenie do krajowego systemu cyberbezpieczeństwa ISAC – Centrów Wymiany i Analizy Informacji (*Information Sharing and Analysis Center*), których rejestr także prowadzić będzie minister właściwy ds. informatyzacji.

4 Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. 1997 nr 141 poz. 943) ustala łącznie 28 działów administracji rządowej w Polsce. Dokument opisuje ich zakres oraz właściwość ministrów kierujących danymi działami.

Bardzo ważnym elementem nowelizacji jest także implementacja do polskiego porządku prawnego Aktu o Cyberbezpieczeństwie, który wprowadza europejski schemat certyfikacji produktów i usług ICT. Jest to szczególnie istotne w kontekście zapisów Dyrektywy NIS2.

Dyrektywa NIS2 i związane z nią wyzwania

Największą zmianą wprowadzaną przez Dyrektywę NIS2 będzie tzw. samoidentyfikacja podmiotów. To nie organy właściwe określać będą kryteria, na podstawie których będą podlegały pod zapisy Dyrektywy. Obecnie, każdy podmiot operujący w danym sektorze i będący przynajmniej średnim przedsiębiorstwem będzie podlegał pod te zapisy. Państwa członkowskie mają natomiast stworzyć mechanizm, który pozwoli tym podmiotom na samonotyfikacje, czyli przekazanie administracji publicznej swoich danych kontaktowych i nazwy sektora w którym operują oraz określenia usług które świadczą. To podejście rezygnuje także z określania tzw. usług kluczowych i nakłada na operatorów konieczność szacowania ryzyka teleinformatycznego dla całej organizacji, co będzie przedmiotem kontroli. Oznacza to, że nie tylko więcej podmiotów w sektorze będzie podlegać pod zapisy Dyrektywy, ale także zapisy te obejmować będą wszystkie usługi, a nie tylko te określane dotąd jako kluczowe.

Kolejną dużą zmianą są wymagania dla operatów: poza szacowaniem ryzyka wprowadzony został obowiązek zapewniania bezpieczeństwa łańcucha dostaw, notyfikacji zagrożeń także do odbiorców usług, a nie tylko incydentów oraz zapewnienie szyfrowania. Są to duże wyzwania, do których warto zacząć się przygotowywać jak najszybciej.

Rozszerzeniu uległa także sama definicja incydentu poważnego (significant). W nowej Dyrektywie jest to incydent, który:

- spowodował lub może spowodować poważne problemy w działaniu, zakłócenie świadczenia usług lub straty finansowe dla zainteresowanego podmiotu,
- incydent miał lub może mieć wpływ na inne osoby fizyczne lub prawne przez znaczne straty materialne lub niematerialne.

Przełoży się to prawdopodobnie na o wiele szerszą definicje incydentu w prawie krajowym, i co za tym idzie, obowiązek zgłaszania większej ilości incydentów, jako tych poważnych.

Ważnym elementem Dyrektywy jest także powiązanie zagadnień związanych z zarządzaniem kryzysowym z cyberbezpieczeństwem, zarówno na poziomie EU, jak i na poziomie krajów członkowskich. Oznacza to, że poszczególni operatorzy będą musieli dobrze zmapować potencjalne incydenty poważne, które mogą mieć wpływ na ciągłość działania organizacji, a także powiązać ich potencjalne skutki z kwestiami związanymi z zarządzaniem kryzysowym w poszczególnych sektorach.

Dyrektywa wprowadza także zapisy, na podstawie których państwa członkowskie mają tworzyć warunki do integracji sektorowej i wymiany dobrych praktyk i doświadczeń. Nowelizacja UoKSC wychodzi już tym zapisom naprzeciw, wprowadzając ISAC do krajowego systemu cyberbezpieczeństwa.

Ostatnią istotną zmianą jest kwestia certyfikacji. Dyrektywa NIS2 pozwala na obowiązkową certyfikację produktów i usług ICT w sektorach nią objętych.

Kompetencje organu właściwego ds. cyberbezpieczeństwa i współpraca z sektorem

Wydział Bezpieczeństwa Teleinformatycznego, Ministerstwo Infrastruktury

Ustawa o krajowym systemie cyberbezpieczeństwa (Ustawa o KSC) z dnia 5 lipca 2018 r. wyznacza kilka sektorów kluczowych dla funkcjonowania Państwa, a nadzór nad nimi sprawują właściwi Ministrowie (odpowiedzialni za poszczególne działy gospodarki) i Przewodniczący Komisji Nadzoru Finansowego.

Organem właściwym do spraw cyberbezpieczeństwa dla sektora transportu jest Minister Infrastruktury, który realizuje wytyczne Strategii Cyberbezpieczeństwa, postanowienia Ustawy o KSC, a także szereg innych przedsięwzięć mających wpływ na kształt krajowego systemu cyberbezpieczeństwa w podległych sektorach. Działania te obejmują zarówno wyznaczanie operatorów usług kluczowych w sektorze transportu, podnoszenie poziomu odporności na cyberzagrożenia, zwiększenie poziomu ochrony informacji w sektorze, jak i promowanie wiedzy oraz dobrych praktyk.

W ramach wdrożenia przepisów o krajowym systemie cyberbezpieczeństwa w 2019 r., w Ministerstwie Infrastruktury, powstał Wydział Bezpieczeństwa Teleinformatycznego. Priorytetem Wydziału jest prowadzenie spraw związanych z obowiązkami organu właściwego do spraw cyberbezpieczeństwa dla sektora transportu. W październiku 2020 r. nastąpiło przejęcie przez Ministerstwo Infrastruktury nadzoru nad podsektorem transportu wodnego, nad którym do tej pory nadzór sprawowało Ministerstwo Gospodarki Morskiej i Żeglugi Śródlądowej. Co za tym idzie: w listopadzie 2020 r. Wydział przejął także zadania organu właściwego dla sektora zaopatrzenia w wodę pitną i jej dystrybucji. Obecnie, Ministrowi Infrastruktury podlega łącznie 31 operatorów usług kluczowych. Z czego 25 to operatorzy z sektora transportu (podsektory kolejowy, lotniczy i morski), a 6 operatorzy z sektora zaopatrzenia w wodę pitną i jej dystrybucję.

Rola organu właściwego ds. cyberbezpieczeństwa

Rolą ministra właściwego ds. transportu w krajowym systemie cyberbezpieczeństwa jest **prowadzenie bieżącej analizy podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej** lub niespełnienia warunków kwalifikujących podmiot jako operatora usługi kluczowej poprzez analizę dostępnych materiałów, a także współpracę z departamentami merytorycznymi w celu identyfikacji podmiotów lotniczych, kolejowych, drogowych i wodnych. Minister Infrastruktury pełni nadzór nad wyznaczonymi operatorami usług kluczowych w sektorze transportu pod kątem realizacji przez nich obowiązków określonych w Ustawie o KSC. Jednocześnie, mając na celu zbudowanie wysokiego poziomu cyberbezpieczeństwa w sektorze oraz pełniąc rolę organu właściwego do spraw cyberbezpieczeństwa, Ministerstwo Infrastruktury współpracuje z sektorem transportu i wspiera operatorów usług kluczowych przez różne inicjatywy:

- spotkania z operatorami usług kluczowych,
- wsparcie w budowie sektorowych ISAC'ów,
- wydawanie rekomendacji,
- kontakty robocze w ramach krajowego systemu cyberbezpieczeństwa,
- współpraca z ISSA Polska i innymi organami właściwymi w celu wypracowania jednolitego szablonu sprawozdania z audytu oraz wiele innych.

Przykładem takiej inicjatywy jest zorganizowanie już w 2019 r. (w czasie gdy Ustawa o KSC obowiązywała dopiero rok i realizacja jej zapisów mogła stanowić pewną trudność) pierwszego spotkania z operatorami usług kluczowych zatytułowanego „Forum wymiany doświadczeń", na którym udzieliliśmy odpowiedzi na wiele pytań, a także omówiliśmy wyzwania z jakimi przyszło zmierzyć się operatorom usług kluczowych. Systematyczne spotkania oraz regularny kontakt pomiędzy organem właściwym a wyznaczonymi podmiotami niewątpliwie pomaga sprostaniu nowym wyzwaniom, służy przekazywaniu wyjaśnień, a także niezbędnych uwag.

Wyznaczanie operatorów usług kluczowych i nadzór nad nimi

Minister właściwy ds. transportu przekazuje wnioski do ministra właściwego ds. informatyzacji o wpisanie do wykazu OUK lub o jego wykreślenie z tego wykazu, a także składa wnioski o zmianę danych w wykazie OUK. Wyznaczenie na operatora usług kluczowych odbywa się

w trybie wydania decyzji administracyjnej. W związku z przyjęciem Dyrektywy NIS2, zakres podmiotów objętych ustawą ulegnie zmianie – więcej operatorów będzie podlegało pod wymogi ustawowe.

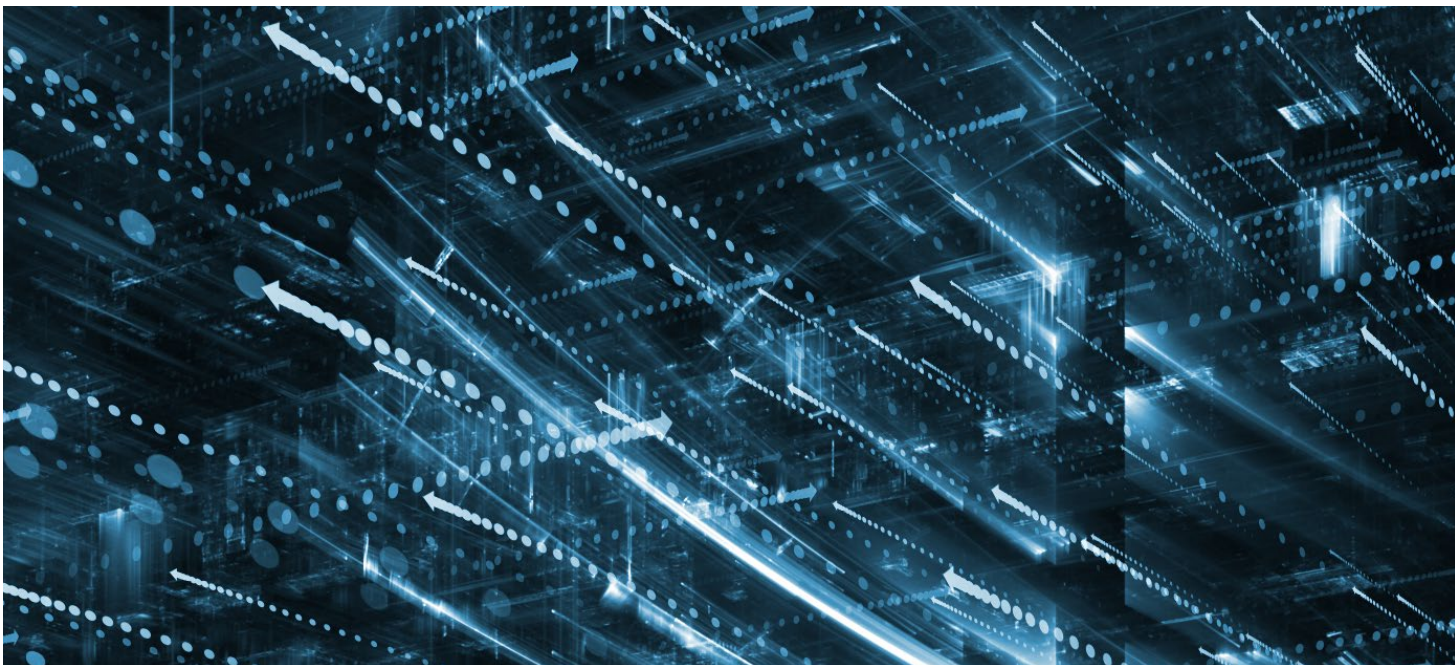
Minister Infrastruktury monitoruje także stosowanie przepisów ustawy o krajowym systemie cyberbezpieczeństwa przez operatorów usług kluczowych. Takie działanie jest realizowane na przykład poprzez analizę audytów bezpieczeństwa informacji prowadzonych przez operatorów usług kluczowych lub w postaci kontroli operatora usługi kluczowej. Pomimo obostrzeń covidowych, Ministerstwo Infrastruktury podjęło starania w kierunku przeprowadzenia kontroli operatorów usług kluczowych – w ubiegłym roku zrealizowano 5 kontroli, co przełożyło się na wykonanie planu kontroli OUK w 100%.

Ponadto we współpracy z tzw. CSIRT poziomu krajowego (CSIRT NASK, CSIRT GOV i CSIRT MON), a także z sektorowymi zespołami cyberbezpieczeństwa, Ministerstwo przygotowuje oraz rekomenduje do działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytycznych sektorowych dotyczących zgłaszania incydentów. Przykładem takiego działania są rekomendacje dla operatorów usług kluczowych dotyczące obowiązku zamieszczania treści na stronach internetowych z zakresu spełnienia wymagań art. 9 ust. 1 pkt 2 Ustawy o KSC. Rekomendacje te przekazaliśmy operatorom wypracowanymi kanałami komunikacji – do osób wyznaczonych przez OUK odpowiedzialnych za kontakty z podmiotami krajowego systemu cyberbezpieczeństwa.

Inne działania MI w zakresie cyberbezpieczeństwa

Ministerstwo Infrastruktury poza spełnianiem zadań wynikających z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, realizuje również czynności wpływające na poziom cyberbezpieczeństwa samego urzędu Ministerstwa. Dodatkowo bierze udział w licznych inicjatywach m.in.: badaniu dojrzałości sektora transportu w obszarze cyberbezpieczeństwa, przy współpracy z Naukową i Akademicką Siecią Komputerową (NASK) oraz firmą EY Polska - specjalizującą się w tematyce cyberbezpieczeństwa. Wyniki ankiet, które zostały uzupełnione przez operatorów usług kluczowych z sektora transportu, a także wkłady poszczególnych podmiotów przyczyniły się do opracowania przedmiotowego raportu.

Stała współpraca Ministerstwa Infrastruktury z operatorami usług kluczowych oraz NASK, przyczyniła się do objęcia patronatem honorowym i zawarcia porozumienia, które skutkowało utworzeniem Centrum Wymiany i Analizy Informacji – ISAC (z ang. *ISAC – Information Sharing and Analysis Center*) w podsektorze kolejowym, które stanowi centrum wymiany wiedzy oraz doświadczeń dotyczących incydentów cyberbezpieczeństwa. Podpisanie porozumienia ISAC było ważnym krokiem w kierunku wzmocnienia cyberbezpieczeństwa w podsektorze kolejowym, który jest jedną ze strategicznych gałęzi gospodarki. Wartością dodaną dla podmiotów współpracujących



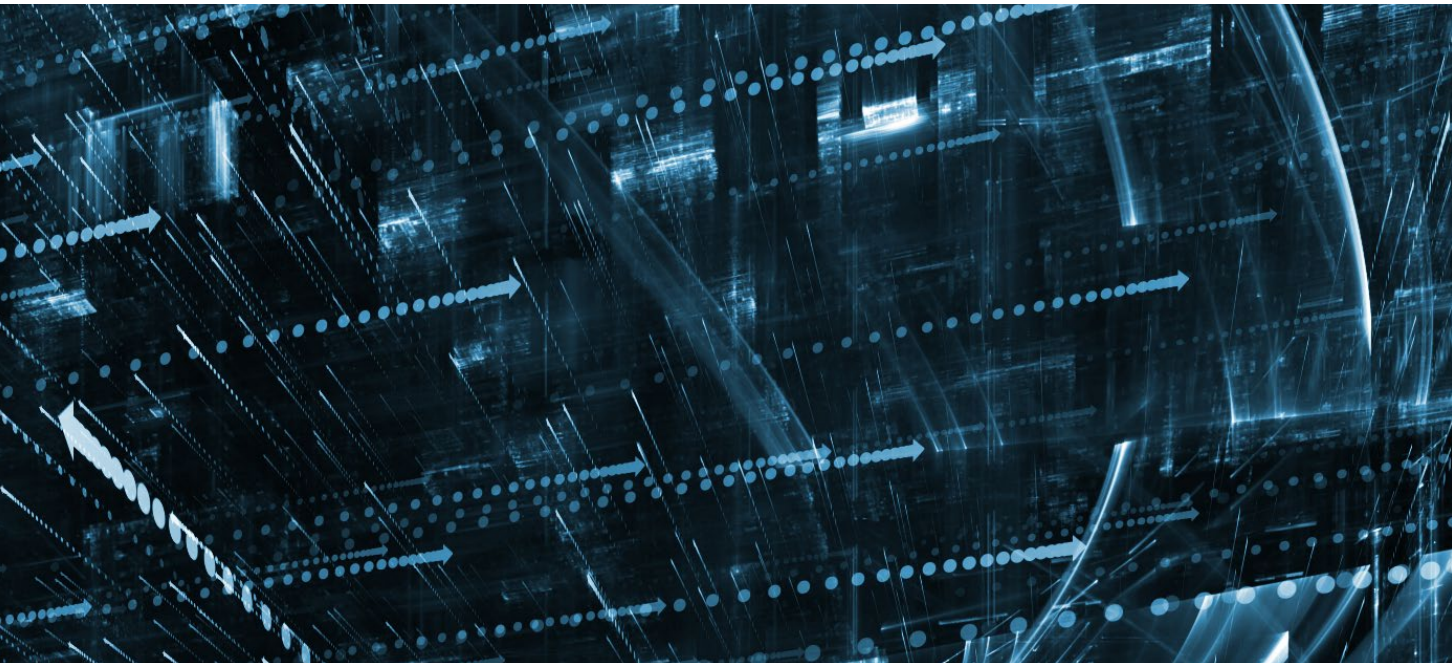
w ramach ISAC-Kolej jest m.in. wypracowanie spójnych standardów, dobrych praktyk, polityk i procedur w tym zakresie oraz usprawnienie współpracy z krajowymi oraz międzynarodowymi zespołami cyberbezpieczeństwa. W ramach budowania efektywnego systemu partnerstwa publiczno-prywatnego opartego na zaufaniu i wspólnej odpowiedzialności za cyberbezpieczeństwo, Ministerstwo podejmuje działania na rzecz utworzenia następnych ISAC w sektorze transportu.

Rozbudowując system wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym, Ministerstwo Infrastruktury podpisało porozumienie na korzystanie z Systemu S46, wspierającego szacowanie ryzyka na poziomie krajowym. Głównymi celami Systemu S46 jest współpraca podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, zgłaszanie i obsługa incydentów, szacowanie ryzyka na poziomie krajowym oraz ostrzeganie o zagrożeniach cyberbezpieczeństwa. Uczestnikami korzystającymi ze specjalnie przygotowanej platformy są m.in. podmioty publiczne, dostawcy usług cyfrowych, operatorzy usług kluczowych, sektorowe zespoły cyberbezpieczeństwa i podmioty świadczące usługi cyberbezpieczeństwa. Dzięki spójnej sieci powiązań i analizie ryzyka, podmioty są w stanie obserwować ryzyko w krajowej cyberprzestrzeni, ocenić istniejące zagrożenia i ich potencjalne skutki, a także reagować na incydenty cybernetyczne na szczeblu krajowym w czasie zbliżonym do rzeczywistego.

Nowelizacja KSC – wyzwania dla sektora transportu

Obecnie trwają prace nad nowelizacją Ustawy o KSC, co doprowadzi do utworzenia CSIRT-ów sektorowych dla każdego z poszczególnych sektorów. Oznacza to, że w przypadku utworzenia takiego CSIRT-u sektorowego w sektorze transportu, świadczone przez powołany w jego strukturach CSIRT usługi obejmowałyby cały sektor transportu, w którego skład wchodzą cztery podsektory: lotniczy, kolejowy, wodny oraz drogowy.

Ministerstwo stale monitoruje infrastrukturę teleinformatyczną, analizuje oraz przekazuje informacje na temat rozpoznanych podatności i zagrożeń w sieci, zwiększając zdolność do zwalczania cyberprzestępczości. Bezpieczeństwo sieci teleinformatycznych jest współcześnie niezwykle ważnym zagadnieniem zarówno z punktu widzenia poszczególnych organizacji, ale także stanowi istotny obszar współpracy.



Kompetencje CSIRT krajowego i współpraca z sektorem

CSIRT NASK, Państwowy Instytut Badawczy NASK (NASK PIB)

Państwowy Instytut Badawczy NASK (NASK PIB) działa na rzecz podnoszenia poziomu bezpieczeństwa teleinformatycznego w Polsce od wielu lat. W 1996 r. powstał pierwszy w Polsce zespół reagowania na incydenty komputerowe - CERT Polska. Do głównych zadań zespołu należy obsługa incydentów bezpieczeństwa i współpraca w tym obszarze z jednostkami z całego świata. CERT Polska należy do grona doświadczonych podmiotów i może się pochwalić członkostwem w międzynarodowym forum zrzeszającym zespoły reagujące – FIRST, a także członkostwem w europejskiej grupie roboczej TF-CSIRT ze statusem "Certified by Trusted Introducer"[1].

Przyjęcie Ustawy o krajowym systemie cyberbezpieczeństwa nałożyło na NASK PIB nowe obowiązki. Na mocy ustawy powołano CSIRT NASK, jeden z trzech CSIRT-ów poziomu krajowego, obok CSIRT MON i CSIRT GOV. W ramach constituency CSIRT NASK znaleźli się operatorzy usług kluczowych, dostawcy usług cyfrowych, jednostki samorządu terytorialnego, a także osoby fizyczne (tzw. CERT ostatniej szansy[6]). Do zadań CSIRT NASK należy monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym; szacowanie ryzyka w skali kraju; przekazywanie informacji na temat incydentów i ryzyk innym podmiotom krajowego systemu cyberbezpieczeństwa; wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa oraz reagowanie na zgłoszone incydenty.

CSIRT NASK współpracuje z organami właściwymi, ministrem właściwym ds. informatyzacji oraz pełnomocnikiem ds. cyberbezpieczeństwa. Ponadto zapewnia zaplecze analityczne oraz badawczo-rozwojowe dla krajowego systemu cyberbezpieczeństwa. Od 2017 r. prowadzi portal informacyjny CyberPolicy (https://cyberpolicy.nask.pl/), który stanowi kompendium wiedzy na temat cyberbezpieczeństwa, zawiera informacje na temat zmian legislacyjnych, zbiory dobrych praktyk, a także aktualności. W ramach obowiązków ustawowych realizuje także zadania z obszaru budowania świadomości w obszarze cyberbezpieczeństwa. Prowadzi szkolenia dla pracowników JST w kampanii #CyberbezpiecznySamorząd kierowanej przez KPRM[7]. Organizuje również prelekcje z zakresu podstawowych aspektów cyberbezpieczeństwa, najczęstszych zagrożeń i cyberhigieny w ramach projektu Cyfrowa Gmina, a także szkoli przedstawicieli administracji publicznej (szkolenia indywidualne). Wspiera także podmioty krajowego systemu cyberbezpieczeństwa jako operator systemu S46[8], który zapewnia szacowanie ryzyka usług zależnych od systemów teleinformatycznych, na poziomie kraju. Do S46 podłączone są trzy CSIRT-y poziomu krajowego, wszystkie organy właściwe, pełnomocnik rządu ds. cyberbezpieczeństwa oraz pierwsi operatorzy usług kluczowych. W 2022 r. rozpoczęło się podłączanie pozostałych operatorów (operatorów usług kluczowych, dostawców usług cyfrowych i realizujących zadania publiczne jednostek samorządu terytorialnego).

Współpraca z organami właściwymi w 2020 roku przyniosła owoce w postaci powołania ISAC - Kolej, pierwszego w Polsce Centrum Wymiany i Analizy Informacji. Porozumienie zostało zawarte pomiędzy spółkami Grupy PKP: PKP S.A., PKP Intercity S.A., PKP CARGO S.A., PKP Informatyka Sp. z o.o., PKP Linia Hutnicza Szerokotorowa Sp. z o.o., PKP Szybka Kolej Miejska w Trójmieście Sp. z o.o., a także PKP Polskie Linie Kolejowe S.A., Instytut Kolejnictwa oraz NASK PIB[9]. Celem powołania ISAC była wymiana wiedzy oraz doświadczeń z zakresu incydentów dotyczących cyberbezpieczeństwa, a tym samym zwiększenie poziomu bezpieczeństwa w podsektorze kolejowym. Działalność ISAC-Kolej okazała się szczególnie cenna w czasie pandemii (zagrożenia związane z pracą zdalną), a także wojny na Ukrainie i wprowadzenia w Polsce stopnia alarmowego dotyczącego zagrożeń w cyberprzestrzeni CHARLIE-CRP.

5 Raport CERT Polska 2021r.: https://cert.pl/uploads/docs/Raport_CP_2021.pdf

6 CERT ostatniej szansy – CERT of the last resort. Zgodnie z nomenklaturą ENISA, zawartą w dokumencie Deployment of Baseline Capabilities of National/ Governmental CERTs oznacza to, że w przypadku, kiedy jakiś podmiot nie jest w stanie uzyskać bezpośredniego kontaktu lub oczekiwanej pomocy od podmiotu, który jest zaangażowany w incydent bezpośrednio, zgłaszający przekazuje zapytanie do CSIRT „ostatniej szansy".

7 W 2021 r. w ramach kampanii #CyberbezpiecznySamorząd przeszkolono ok. 2300 osób, w trzech kategoriach (w zależności od reprezentowanej grupy JST).

8 S46 to system informatyczny, który na podstawie ustawy o KSC wspiera podmioty krajowego systemu cyberbezpieczeństwa i zapewnia szacowanie ryzyka usług, zależnych od systemów teleinformatycznych, na poziomie kraju.

9 https://cyberpolicy.nask.pl/aktualnosci/powolano-isac-kolej/

Wyzwania związane z NIS2

Zbliżające się zmiany prawne, wynikające z nowelizacji Ustawy o krajowym systemie cyberbezpieczeństwa, a także Dyrektywy NIS2, będą miały istotny wpływ na zakres działalności CSIRT NASK. Z pewnością zmieni się *constituency* CSIRT-u, a więc liczba podmiotów, które będą zobligowane do raportowania incydentów. Wynika to z rozszerzenia zakresu NIS2 o podmioty z sektorów i podsektorów, które dotychczas nie były objęte Dyrektywą, a także wprowadzenie konieczności zarządzenia ryzykiem w łańcuchu dostaw (również w sektorze transportu). Wiele z tych przedsiębiorstw dotychczas nie podlegało żadnym zobowiązaniom z obszaru cyberbezpieczeństwa i będą potrzebowały wsparcia CSIRT-ów w dostosowaniu się do nowych przepisów. Podobnie jak nowe organy właściwe i organy właściwe, które dostaną pod swoją pieczę nowych operatorów. Zwiększy to zapotrzebowanie na szkolenia, kampanie edukacyjne, a w późniejszym etapie również konieczność bezpośrednich spotkań, wypracowania zasad komunikacji, opracowywania rekomendacji dla poszczególnych sektorów. Niezbędne będzie również wsparcie w budowaniu Sektorowych Zespołów Cyberbezpieczeństwa, które staną się obowiązkowe, a także dalsze prace na rzecz powstawania Centrów Wymiany i Analizy Informacji ISAC. Projekt NIS2 wprowadza również obowiązek przyjęcia polityki mającej na celu promowanie i ułatwianie skoordynowanego ujawniania podatności (*coordinated vulnerability disclosure, CVD*) przez Państwa Członkowskie. Jeden z CSIRT-ów poziomu krajowego zostanie wyznaczony jako tzw. „zaufany pośrednik" dla CVD na poziomie krajowym. CSIRT NASK musi liczyć się z możliwością przyjęcia niektórych z powyższych zobowiązań, a tym samym wizją rozbudowy zarówno zaplecza kadrowego, jak i operacyjnego. W tym zadaniu niezwykle cenne będą dotychczasowe doświadczenia budowania współpracy z organami właściwymi, członkostwo w ISAC – Kolej, prowadzenie szkoleń i prelekcji na konferencjach branżowych. Dostosowanie do nowych regulacji będzie wyzwaniem, na które warto przygotować się z wyprzedzeniem. Inicjatywy takie jak badanie dojrzałości sektora transportu wychodzą naprzeciw czekających nas zmian. Mamy nadzieję, że podobne badanie zostanie przeprowadzone również w pozostałych sektorach i posłuży jako narzędzie do oceny kierunku, w którym należy podążać na drodze do zwiększenia poziomu cyberbezpieczeństwa w Polsce.

Transport kolejowy

Transport kolejowy odgrywa znaczącą rolę nie tylko w Polsce, ale również w Europie.

Według danych Eurostatu[10] w 2020 r. w UE funkcjonowało 216 000 km czynnych linii kolejowych, które transportowały 472 miliardy pasażerokilometrów i 430 miliardy tonokilometrów[11]. W Polsce analogiczne dane zbiera Urząd Transportu Kolejowego, który w 2020 roku zarejestrował przewóz 12,5 miliarda pasażerokilometrów[12] i 52 miliardy tonokilometrów[13]. 2021 rok został wybrany przez KE Europejskim Rokiem Kolei. Inicjatywa miała na celu podkreślenie korzyści płynących z kolei jako zrównoważonego, inteligentnego i bezpiecznego środka transportu, aby wspierać realizację celów Europejskiego Zielonego Ładu w dziedzinie transportu[14].

Kolej należy również do jednego z najbezpieczniejszych środków transportu, pod względem ilości wypadków. Jednak transformacja cyfrowa, rozbudowa systemów teleinformatycznych i jednoczesna rosnąca ilość połączeń sprawiają, że cyberbezpieczeństwo ma dla sektora fundamentalne znaczenie. Zagrożenia i podatności teleinformatyczne to jedno z większych wyzwań dla współczesnej kolei.

W raporcie „Railway cybersecurity. Security measures in the Railway Transport Sector", Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) zaznacza, że do 2020 roku podsektor transportu kolejowego nie był bezpośrednim celem ataków cyberprzestępców. Niemniej jednak w latach 2015 – 2020, w różnych krajach europejskich, miało miejsce kilka incydentów, które zwracają uwagę na podatność sektora. Najnowsze dotyczyły:

- Wycieku danych z sieci Wi-Fi pasażerów w brytyjskich kolejach – wyciek dotyczył adresów e-mail i informacji na temat podróży ok. 10 000 pasażerów, którzy korzystali z otwartej sieci Wi-Fi[15].
- Ataku malware na szwajcarskie przedsiębiorstwo kolejowe Stadler – systemy firmy zostały zainfekowane malware, który umożliwił ściągnięcie wrażliwych danych. Po tym jak firma odmówiła zapłaty okupu, przestępcy opublikowali online wykradzione dane i wewnętrzne dokumenty[16].
- Ataku ransomware na hiszpańską firmę zarządzającą koleją – firma ADIF została zaatakowana ransomware, który umożliwił wykradzenie gigabajtów danych personalnych i biznesowych[17].

Na 8 incydentów wymienionych w raporcie ENISA, 3 miały miejsce w 2020 roku, co może sugerować zwiększanie zagrożenia.

Dyrektywa NIS i związane z nią wyzwania dla podsektora kolei

Przełomowym momentem w podejściu do cyberbezpieczeństwa w podsektorze kolejowym było uwzględnienie go w Dyrektywie NIS z 2016 r. W Aneksie II Dyrektywy wymieniono sektory i podsektory, w których państwa członkowskie mogą identyfikować operatorów usług kluczowych. Jednak każde państwo, na etapie transpozycji Dyrektywy do porządków krajowych, samodzielnie tworzy listę usług, które traktuje jako kluczowe. W przypadku podsektora kolejowego, jedynie Cypr, Łotwa, Malta i Niderlandy nie zidentyfikowały usług kluczowych. W pozostałych państwach członkowskich został on włączony w zakres obowiązywania Dyrektywy[18]. Wykaz usług uznanych za kluczowe różni się przy tym znacząco pomiędzy państwami. Przykładowo we Francji wyodrębniono bardzo szczegółowy i kompleksowy zbiór usług kluczowych (utrzymanie infrastruktury, utrzymanie taboru kolejowego, kontrola ruchu

10 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Railway_passenger_transport_statistics_-_quarterly_and_annual_data#In_2020.2C_rail_passenger_transport_almost_halved_in_the_EU_compared_to_2019

11 Pasażerokilometr: jednostka miary w transporcie pasażerskim. Jeden pasażerokilometr odnosi się do transportu jednego pasażera na odległości jednego kilometra. Tonokilometr: jednostka miary w transporcie towarowym. Jeden tonokilometr odnosi się do transportu jednej tony towaru na odległości jednego kilometra.

12 https://utk.gov.pl/pl/raporty-i-analizy/analizy-i-monitoring/statystyka-przewozow-pa/16649,Dane-eksploatacyjne-w-2020-rMonthly-statistics-2020.html

13 https://utk.gov.pl/pl/raporty-i-analizy/analizy-i-monitoring/statystyka-przewozow-to/16644,Dane-eksploatacyjne-w-2020-rMonthly-Statistics-2020.html

14 Zgodnie z informacjami promocyjnymi publikowanymi w ramach Europejskiego roku transportu kolejowego, kolej jest najbardziej ekologicznym środkiem transportu. W większości zelektryfikowana, produkuje znacznie mniej CO2 niż transport drogowy, czy lotniczy. Jest odpowiedzialna za jedynie 0,4% emisji gazów cieplarnianych, a także na przestrzeni lat konsekwentnie redukuje emisję i zapotrzebowanie energetyczne, zwiększając wykorzystanie odnawialnych źródeł energii. https://europa.eu/year-of-rail/why-rail_en

15 https://www.bbc.com/news/technology-51682280

16 https://www.stadlerrail.com/media/pdf/2020_0507_media%20release_cyber-attack_en.pdf

17 https://www.railjournal.com/technology/adif-hit-by-cyberattack/

18 Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady oceniające spójność podejść przyjętych przez państwa członkowskie w procesie identyfikacji operatorów usług kluczowych zgodnie z art. 23 ust. 1 Dyrektywy (UE) 2016/1148 w sprawie bezpieczeństwa sieci i informacji. 28.20.2019r. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52019DC0546&from=EN

kolejowego i zarządzanie ruchem kolejowym, przewóz towarów i materiałów niebezpiecznych, przewóz pasażerów, metro, tramwaje i inne przewozy lekkimi pojazdami szynowymi, przewozy kolejowe), podczas gdy w Polsce zidentyfikowanych usług jest znacznie mniej (**przygotowanie rozkładów jazdy pociągów, transport kolejowy towarów, transport kolejowy pasażerów**).

Wdrożenie Dyrektywy NIS w podsektorze kolejowym ocenił raport ENISA z 2020 r. Wśród największych wyzwań zgłaszanych przez operatorów znalazły się:

- znalezienie równowagi pomiędzy wymaganiami operacyjnymi, konkurencyjnością biznesu i cyberbezpieczeństwem. Jednocześnie trwająca transformacja cyfrowa wymusza przywiązywanie coraz większej wagi do kwestii cyberbezpieczeństwa,
- uzależnienie od dostawców, którzy reprezentują różne standardy techniczne, zwłaszcza w zakresie technologii operacyjnych i cyberbezpieczeństwa,
- przestarzałe systemy OT - systemy o długiej żywotności, które z biegiem czasu nie nadążają nad rosnącymi wymaganiami w zakresie cyberbezpieczeństwa. Dodatkowo systemy te zwykle są zlokalizowane po całej sieci kolejowej (stacje i tory), co utrudnia ich kontrolę i obsługę,
- niska świadomość zagrożeń cyberbezpieczeństwa wśród kadry,
- brak spójności w przepisach dotyczących cyberbezpieczeństwa, które wynikają z różnych regulacji.

Obecnie podsektor kolejowy czekają nowe wyzwania, związane ze zbliżającym się przyjęciem Dyrektywy NIS2.

Europejskie inicjatywy w obszarze cyberbezpieczeństwa transportu kolejowego

Na poziomie UE podejmowane są liczne inicjatywy związane ze wzmacnianiem poziomu cyberbezpieczeństwa w transporcie kolejowym. Najważniejsze z nich to:

- **Europejski ISAC kolejowy** (***The European Railway-ISAC***) https://er.isacs.eu/ - Centrum Wymiany Analiz i Informacji dla sektora kolejowego. Inicjatywa skupia ekspertów ds. informacji i cyberbezpieczeństwa, którzy koncentrują się na bezpieczeństwie przemysłowych systemów sterowania i infrastrukturze IT w kolei. ISAC jest formą partnerstwa publiczno-prywatnego, wciąż zwiększa liczbę organizacji, które chciałyby wymieniać się wiedza na temat zagrożeń w podsektorze transportu kolejowego.
- **CENELEC Specyfikacja Techniczna 50701** - Grupa Robocza 26 Europejskiego Komitetu Normalizacyjnego Elektrotechniki (The Working Group 26 of the European Committee for Electrotechnical Standardisation, CENELEC), która opracowała Specyfikację Techniczną 50701 dotyczącą sposobu zarządzania cyberbezpieczeństwem dla operatorów i dostawców produktów w podsektorze kolejowym. W oparciu o powyższą specyfikację w lutym 2022 r. ENISA opublikowała ogólnodostępne wytyczne „Zoning and conduits for railways".
- **Projekt 4SECURERAIL**[19] – projekt miał miejsce w latach 2019-2021, a jego celem było opracowanie propozycji utworzenia europejskiego zespołu reagowania na incydenty związane z bezpieczeństwem komputerowym, umożliwiającego natychmiastowe udostępnianie zidentyfikowanych zagrożeń zainteresowanym partnerom. W ramach projektu opracowano model CSIRT dla europejskiego sektora kolejowego.

19 https://www.4securail.eu/

Cyberbezpieczeństwo w transporcie kolejowym w Polsce

Podsektor kolejowy w Polsce w 2020 r. obsługiwał niemal 20 tysięcy kilometrów linii kolejowych, a gęstość sieci wynosi 6,2 km/100 km2, podczas gdy średnia w UE wynosi 4,8 km. Ponad połowa szlaków jest zelektryfikowana[20].

Wśród firm działających na rynku kolejowym możemy wymienić przede wszystkim przewoźników i zarządców infrastruktury. Pod koniec 2020 r. 30 podmiotów posiadało aktywną licencję na wykonywanie przewozów kolejowych osób i 109 na przewóz towarów. Obecnie niemal wszystkie firmy wykorzystują w swojej działalności rozwiązania cyfrowe. Jednak, zgodnie z zapisami Ustawy o krajowym systemie cyberbezpieczeństwa, rolę operatorów usług kluczowych pełnią jedynie te podmioty, które świadczą usługi kluczowe, opisane w tabeli poniżej. Organ właściwy ds. cyberbezpieczeństwa wyznaczył trzech operatorów w podsektorze transportu kolejowego.

Usługa	Opis
Konstrukcja rozkładu jazdy pociągów	Spełnienie co najmniej dwóch z czterech kryteriów głównych: ▸ Zależność co najmniej dwóch z niżej wymienionych sektorów lub podsektorów od usługi świadczonej przez dany podmiot: sektor energia, podsektor energia elektryczna, sektor energia, podsektor ropa naftowa, sektor energia, podsektor ciepło. ▸ Wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne: 1) strata finansowa z tytułu niezrealizowania przewozu: wynosząca 500 tys. złotych dziennie, 2) brak możliwości uruchomienia pociągów: w liczbie 5 tys. sztuk dziennie, 3) brak możliwości realizacji dostaw paliw kopalnych (węgiel), płynnych (paliwa) powyżej 12 godzin, 4) brak możliwości realizacji przejazdów pociągów pasażerskich (transport publiczny) powyżej 12 godzin. ▸ Udział w rynku zarządców infrastruktury kolejowej: powyżej 50% długości eksploatowanych linii kolejowych (wg aktualnych danych publikowanych przez Prezesa Urzędu Transportu Kolejowego). ▸ Liczba składanych przez przewoźników wniosków o konstrukcję rozkładu jazdy – nie mniej niż 800 tys. rocznie.
Transport kolejowy pasażerski	Spełnienie co najmniej jednego z kryteriów: ▸ Udział przewoźnika w rynku wynoszący powyżej 25%, liczony wg wykonanej pracy przewozowej lub liczby pasażerów (na podstawie danych publikowanych przez Prezesa Urzędu Transportu Kolejowego). ▸ Świadczenie usługi na obszarze co najmniej 9 województw.
Transport kolejowy towarów	Udział przewoźnika w rynku wynoszący powyżej 25%, liczony wg wykonanej pracy przewozowej lub przewiezionej masy towarów (na podstawie danych publikowanych przez Prezesa Urzędu Transportu Kolejowego).

20 https://dane.utk.gov.pl/sts/sprawozdania-roczne/sprawozdania-z-funkcjon/17668,Sprawozdanie-z-funkcjonowania-rynku-transportu-kolejowego-2020.html

W Polsce organ właściwy zidentyfikował (wydanie decyzji administracyjnej) obecnie podmioty w podsektorze kolejowym. Są one zobligowane do wypełnienia obowiązków ustawowych. Liczba ta zmieni się po wejściu w życie przepisów Dyrektywy NIS2, która nałoży obowiązek wdrożenia przepisów dla wszystkich zarządców infrastruktury kolejowej i przewoźników (o ile nie są mikroprzedsiębiorstwami).

Liczba incydentów w sektorze transportu w Polsce wciąż jest niewielka. Dane z raportów rocznych CERT Polska pokazują, że w ostatnich 3 latach (2019-2021) nie przekraczała 1% wszystkich zgłoszonych incydentów. W 2020 r. CERT Polska zarejestrował 3 incydenty w podsektorze kolejowym, a w 2021 r. – 55[21]. Sytuacja w niewielkim stopniu uległa zmianie w 2022 r. w związku z wojną na Ukrainie. 18 i 28 kwietnia miały miejsce ataki na stronę pkp.pl. Były to działania o charakterze ofensywnym. Przeprowadziła je prorosyjska grupa przestępcza KillNet lub powiązane z nią grupy haktywistyczne. Jako powód podawano niezadowolenie z poparcia, jakie Polska okazała narodowi Ukraińskiemu. Serie ataków wymierzono nie tylko w sektor transportu, ale także w instytucje sądownictwa, Straż Graniczną, czy Narodowy Bank Polski[22]. Dowodzi to istotności samego sektora transportu, a szczególnie transportu kolejowego.

Niewielka aktywność przestępców nie świadczy jednak o wysokim poziomie cyberbezpieczeństwa przedsiębiorstw podsektora kolejowego. W 2020 r. zespół CERT Polska w ramach przeszukiwania polskiego Internetu pod kątem dostępnych urządzeń infrastruktury przemysłowej, zlokalizował podatność w systemach informacji pasażerskiej na kolei, która mogła zostać wykorzystana przez osoby niepowołane[23]. Dlatego też wskazane jest prowadzenie regularnych przeglądów i inwentaryzacji wykorzystywanych systemów telemetrycznych, zmianę domyślnych haseł dostępowych, poprawne wystawianie certyfikatów SSL, a także odpowiednią izolację usług od internetu i prowadzenie działań budujących świadomość wśród pracowników. W tym ostatnim punkcie z pomocą przychodzi ISAC - Kolej, który opracował wytyczne dotyczące cyberbezpieczeństwa dla pracowników kolei. Kampanię przygotowano na podstawie udostępnionego przez Komisję Europejską dokumentu „Transport cybersecurity toolkit"[24].

ISAC - Kolej – prekursor Centrum Wymiany i Analizy Informacji w Polsce

W 2020 r., w ramach samoorganizacji sektora, przy współpracy z PIB NASK i Ministerstwem Infrastruktury, powołano Centrum Wymiany i Analiz Informacji podsektora transportu kolejowego (ISAC-Kolej). Jest to pierwszy ISAC w Polsce. Organizacja służy budowaniu współpracy w obszarze cyberbezpieczeństwa w podsektorze transportu kolejowego. ISAC-Kolej jest niezależny od administracji państwowej, a także innych organizacji politycznych i zawodowych. W ramach ISAC odbywają się regularne spotkania, których celem jest wymiana informacji na temat aktualnych zagrożeń, podatności i sposobów minimalizacji ryzyka, a także opracowywanie wytycznych i poradników dla sektora. Założycielami organizacji były spółki kolejowe PKP, PKP PLK, PKP IC, PKP Cargo, PKP LHS, PKP SKM, PKP Informatyka Kolejowa, a także Instytut Kolejnictwa oraz NASK PIB. Jednak do ISAC - Kolej mogą dołączyć wszyscy zarządcy infrastruktury i przewoźnicy kolejowi.

21 Dane CERT Polska.

22 Raport „Grupy haktywistyczne. Agresja rosyjska przeciwko Ukrainie". Maj 2022.

23 https://cert.pl/uploads/docs/Raport_CP_2020.pdf#page=35

24 https://utk.gov.pl/pl/aktualnosci/17658,Poradnik-cyberbezpieczenstwa-dla-pracownikow-kolei.html

Działalność ISAC – Kolej

Zagrożenia teleinformatyczne rzadko dotyczą tylko jednego podmiotu w danym sektorze gospodarki, szczególnie gdy jest to sektor ważny i strategiczny z punktu widzenia bezpieczeństwa Państwa czy gospodarki narodowej. Dlatego tylko dobra współpraca i właściwa wymiana wiedzy z tego zakresu może przyczynić się do sukcesywnego podnoszenia poziomu cyberbezpieczeństwa danej branży. Ta właśnie idea przyświecała formalnemu powołaniu w dniu 06.11.2020 r. ISAC - Kolej (Information Sharing and Analysis Center) rozumianego jako Centrum Wymiany i Analizy Informacji w obszarze cyberbezpieczeństwa dla podsektora transportu kolejowego (kierując się sektorami i podsektorami określonymi w przepisach Ustawy o krajowym systemie cyberbezpieczeństwa), stworzonego dla podmiotów branży kolejowej, podmiotów publicznych zajmujących się sprawami cyberbezpieczeństwa oraz podmiotów zajmujących się sprawami bezpieczeństwa ruchu kolejowego.

ISAC – Kolej, zgodnie z wytycznymi NASK – PIB, jest formą partnerstwa publiczno-prywatnego rozumianego jako długookresowe porozumienie przedstawicieli sektora prywatnego i publicznego. W chwili obecnej ISAC – Kolej tworzy dziewięć niezależnych podmiotów działających w podsektorze kolejowym w oparciu o zapisy Ustawy o transporcie kolejowym oraz państwowe instytuty badawcze.

I chociaż ISAC – Kolej nie ma osobowości prawnej, nie jest spółką celową czy stowarzyszeniem, nie posiada zaplanowanego wielomilionowego budżetu na funkcjonowanie, to przez niespełna 2 lata jego funkcjonowania „non-profit" udało się stworzyć, bazując na zaufaniu, współpracy i przede wszystkim zaangażowaniu, zupełnie przyzwoitą platformę współpracy w obszarze cyberbezpieczeństwa dla podsektora transportu kolejowego. Pomimo, że praktycznie cały rok zajęło samo tworzenie ISAC – Kolej licząc czas od momentu podjęcia się inicjatywy jego powołania aż do jego formalnego powstania, to z perspektywy czasu uważam, że przedsięwzięcie to każdego dnia przyczynia się do podnoszenia poziomu cyberbezpieczeństwa w podmiotach tworzących to partnerstwo. Potwierdza to teorię, że wystarczy kilku specjalistów z zakresu cyberbezpieczeństwa z różnych podmiotów tego samego sektora gospodarki, którzy zaczną wymieniać się informacjami oraz doświadczeniem z obszaru zabezpieczeń przed zagrożeniami, by zminimalizować ryzyka płynące z cyberprzestrzeni. Podejmowanie działań przez daną firmę lub instytucję w obszarze zabezpieczeń przed zagrożeniami samodzielnie i niezależnie na zasadzie „sami wiemy i potrafimy najlepiej dbać o swoje bezpieczeństwo" nie zawsze wystarcza. ISAC – Kolej stanowi bardzo dobrą formę gromadzenia wiedzy na temat aktualnych zagrożeń i ryzyka, głównie dlatego, że składa się ze specjalistów, którzy znają specyfikę podsektora kolejowego pracując w nim niekiedy kilkanaście lat i mają najbardziej aktualne informacje na temat zagrożeń.

ISAC – Kolej działa w oparciu o zawarte „Porozumienia w sprawie utworzenia ISAC – Kolej" oraz przyjęty przez wszystkich „Regulaminu Centrum Wymiany Analizy Informacji podsektora transportu kolejowego ISAC-Kolej".

Zadaniami, które każdego dnia realizuje ISAC – Kolej to:

- wymiana wiedzy o możliwych ryzykach, występujących incydentach i sposobach ich skutecznej obsługi,
- budowanie doświadczenia i potencjału w zakresie wymiany informacji o ryzykach, incydentach oraz ich zapobieganiu w obszarze cyberbezpieczeństwa,
- platforma wymiany dobrych praktyk i budowanie zdolności reagowania na zagrożenia cybernetyczne w ramach podsektora kolejowego.

- gromadzenie i pogłębianie wiedzy na temat podsektora kolejowego ze źródeł krajowych i zagranicznych,
- wypracowanie standardów w zakresie cyberbezpieczeństwa w podsektorze kolejowym,
- edukacja w zakresie cyberbezpieczeństwa pracowników podmiotów zrzeszonych w ISAC – Kolej,
- nawiązywanie współpracy międzynarodowej z analogicznymi podmiotami z podsektora kolejowego,
- stały monitoring aktualnego stanu cyberbezpieczeństwa w podsektorze kolejowym,
- ścisła współpraca z właściwymi organami administracji publicznej (rządowej i samorządowej) w zakresie cyberbezpieczeństwa,
- przekazywanie organom administracji publicznej (w tym organom nadzoru i organom właścicielskim) informacji o zagrożeniach i incydentach cyberbezpieczeństwa w podsektorze kolejowym,
- udział w tworzeniu standardów dla podsektora kolejowego i regulacji prawnych, które wspierają działania oraz przyczyniają się do zwiększenia poziomu bezpieczeństwa teleinformatycznego,
- ścisła współpraca z właściwymi Zespołami Reagowania na Incydenty (CERT - Computer Emergency Response Team) i Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT (ang. Computer Security Incident Response Team)
- przekazywanie jasnego sygnału klientom podmiotów zrzeszonych w ISAC – Kolej, że podsektor kolejowy współpracuje ze sobą w zakresie cyberbezpieczeństwa, które przekłada się na wzmocnienie bezpieczeństwa w usługach świadczonych dla klientów spoza podsektora,
- tworzenie warunków rozwoju podsektora kolejowego oraz przyczynianie się do jego rozwoju w obszarze cyberbezpieczeństwa,
- realizacja przedsięwzięć na rzecz podmiotów zrzeszonych w ISAC – Kolej oraz podnoszenie innowacyjności w obszarze cyberbezpieczeństwa podsektora kolejowego,
- wspieranie podmiotów zrzeszonych w ISAC-Kolej a uznanych za operatorów usług kluczowych w wykonywaniu obowiązków określonych w przepisach o krajowym systemie cyberbezpieczeństwa.

Usankcjonowanie możliwości tworzenia ISAC-ów oraz korzyści płynące z funkcjonowania tego rodzaju organizacji jako ważnych z punktu widzenia gromadzenia informacji o zagrożeniach i podatnościach w danym sektorze gospodarki dostrzegł również ustawodawca wprowadzając stosowane zmiany do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa. Z założenia ISAC ma zadanie wspierać podmioty krajowego systemu cyberbezpieczeństwa współpracując z właściwymi CSIRT-ami poziomu krajowego jak i CSIRT-ami sektorowymi. Oznacza to, że ISAC, jak niekiedy jest mylnie pozycjonowany, nie stanowi preludium do przekształcenia go docelowo w CSIRT sektorowy. To niezależne struktury krajowego systemu cyberbezpieczeństwa, które powinny działać niezależnie w danym sektorze wzajemnie ze sobą współpracując a nie konkurując.

Dotychczasowe inicjatywy i działania jakie zrealizował oraz każdego dnia prowadzi ISAC – Kolej to:

- cykliczne spotkania przedstawicieli tworzących ISAC – Kolej i omawianie najważniejszych spraw dotyczących obszaru cyberbezpieczeństwa podsektora transportu kolejowego,
- opracowanie i przekazanie uwag za cały podsektor kolejowy do projektu Dyrektywy NIS2,
- przyjęcie wytycznych dla pracowników podsektora kolejowego dotyczących cyberbezpieczeństwa, opartych na dokumencie „Transport cybersecurity toolkit",

- podpisanie Porozumienia o współpracy z zakresu cyberbezpieczeństwa z Urzędem Transportu Kolejowego – regulatorem rynku dla podsektora transportu kolejowego w Polsce,
- uzyskanie zgody Rządowego Centrum Bezpieczeństwa oraz CSIRT GOV na przekazywanie informacji o zagrożeniach poza podmioty uznane za operatorów infrastruktury krytycznej w ramach podmiotów tworzących ISAC – Kolej,
- informowanie o incydentach oraz wsparcie w ich obsłudze podmiotów nie tworzących ISAC – Kolej, a działających w podsektorze kolejowym lub działającym na jego rzecz (np. wykonawców, partnerów, itp.),
- stworzenie listy dystrybucyjnej za pomocą której codziennie wysyłane są członkom ISAC – Kolej m.in. raporty dotyczące złośliwego ruchu sieciowego, informacje o podatnościach, ostrzeżenia o zagrożeniach, informacje o incydentach czy informacje na temat aktualnych wskaźników ryzyka (IoC),
- stworzenie i przekazywanie członkom ISAC – Kolej cyklicznego biuletynu informacyjnego dotyczącego cyberbezpieczeństwa,
- utworzenie w Komunikatorze PKP Polskie Linie Kolejowe S.A. – aplikacji mobilnej dla systemu Android i iOS służącym do powiadamiania o wypadkach i wydarzeniach na kolei grupy „Cyberbezpieczeństwo" – za pomocą aplikacji wyznaczone osoby mogą otrzymywać wiadomości i ostrzeżenia dotyczące bieżących zagrożeń cybernetycznych.

Wyżej wymienione działania podejmowane każdego dnia przez ISAC – Kolej, pomimo że czas rozpoczęcia działań przypadł najpierw w kryzysie pandemii (wyzwania związane z pracą zdalną), a obecnie poprzez konflikt zbrojny w Ukrainie i związany z tym wprowadzony od 21.02.2022 r. stopień alarmowy dotyczący zagrożeń w cyberprzestrzeni CHARLIE-CRP, w mojej opinii znacząco przyczyniają się do podnoszenia poziomu bezpieczeństwa cybernetycznego na polskiej kolei. Stąd oczywistym jest, że nie wszystkie zamierzenia i plany, z różnych względów, udało się ISAC – Kolej wdrożyć. Jednak jak w każdej rozpoczętej działalności początki są zazwyczaj trudne, a bezpieczeństwo cybernetyczne wymaga mierzenia się z wyzwaniami praktycznie każdego dnia. Stąd przed ISAC – Kolej jeszcze długa droga w kierunku osiągnięcia pełnej dojrzałości.

Pozytywnym sygnałem płynącym z rynku, że ISAC – Kolej spełnia swoją rolę jest to, że inne sektory i branże zwracają się z prośbą o podzielenie się doświadczeniem z zakresu jego funkcjonowania. Dlatego zapraszam do kontaktu, gdyż ISAC – Kolej jest organizacją otwartą na współpracę i wymianę informacji oraz dobrych praktyk z obszaru cyberbezpieczeństwa.

Grzegorz Kuta
Dyrektor Biura Bezpieczeństwa Informacji i Spraw Obronnych
PKP PLK

Analiza wyników badań

W podsektorze transportu kolejowego na dzień przeprowadzania badania wyznaczono 3 operatorów usług kluczowych. W badaniu wzięło udział 2 z nich. Poniżej przedstawione zostały wyniki poszczególnych sekcji.

Organizacja

Dwóch operatorów podsektora kolejowego, którzy nadesłali odpowiedzi na pytania badawcze to duże przedsiębiorstwa, zatrudniające powyżej 250 pracowników. W obu organizacjach wskazano osobę kontaktową do odpowiedniego CSIRT-u.

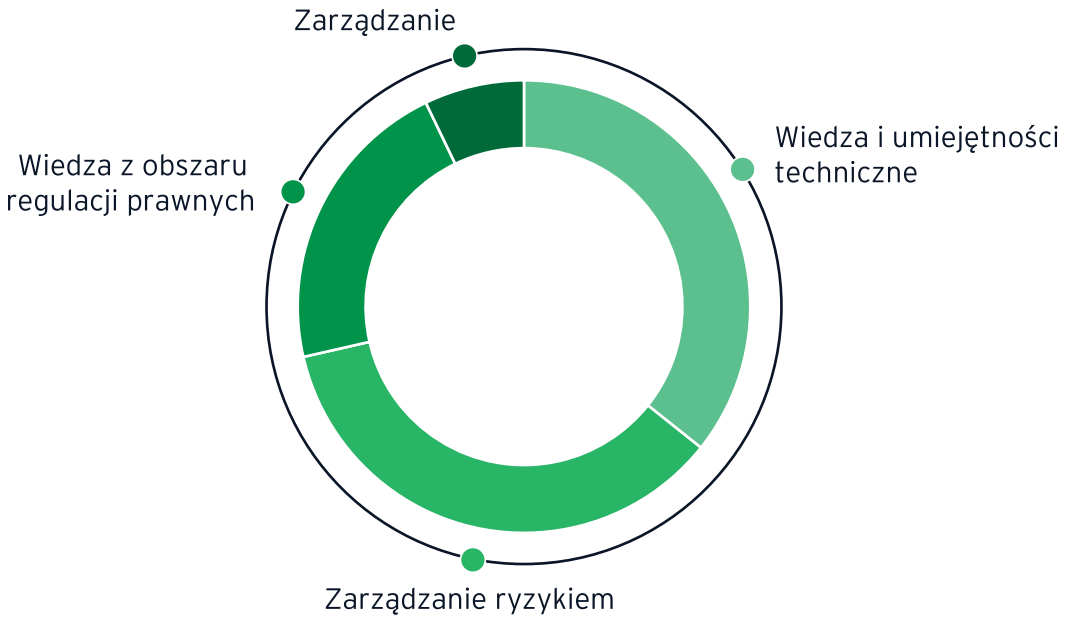
Operatorzy zgodnie zaznaczyli, że ich organizacje przeznaczają w budżecie środki finansowe na cyberbezpieczeństwo. W obu przypadkach są to środki ulokowane w ramach funduszy dla działu IT.

Procesy

Dla obu operatorów szacowanie ryzyka dla systemów teleinformatycznych jest częścią korporacyjnego zarządzania ryzykiem. Obie organizacje prowadzą szacowanie ryzyka dla systemów zdefiniowanych w organizacji jako usługi kluczowe. W obu OUK zidentyfikowano odbiorców usług zależnych od systemów teleinformatycznych, ale tylko jeden z nich zmapował procesy i ich zależność od systemów informatycznych. Oba OUK posiadają także wewnętrzne polityki cyberbezpieczeństwa w zakresie IT oraz OT.

Oba OUK zadeklarowały, że realizują wszystkie zadania wymienione w Ustawie o krajowym systemie cyberbezpieczeństwa[25].

Kompetencje zespołów odpowiedzialnych za cyberbezpieczeństwo



25 Wymienione w Ustawie o krajowym systemie cyberbezpieczeństwa zadania operatorów usług kluczowych: 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym: a) utrzymanie i bezpieczną eksploatację systemu informacyjnego, b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej, d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym; 3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej; 4) zarządzanie incydentami; 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym: a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, b) dbałość o aktualizację oprogramowania, c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym, d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa; 6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa, wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa; zapewnia użytkownikowi usługi kluczowej dostęp do wiedzy pozwalającej na zrozumienie zagrożeń; cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej; przekazuje organowi właściwemu do spraw cyberbezpieczeństwa dane, o których mowa w art. 7 ust. 2 pkt 8 i 9, nie później niż w terminie 3 miesięcy od zmiany tych danych."

Badani operatorzy opracowali plany/procedury reagowania na incydenty, a także przywracania działania po zaistniałym incydencie. Zaznaczyli także, że procedury te są regularnie sprawdzane i kontrolowane. Odbywa się to w ramach zewnętrznych audytów, wewnętrznych audytów i zewnętrznych ocen bezpieczeństwa.

Zespół

U obu operatorów usług kluczowych w podsektorze kolejowym zostały zdefiniowane odpowiednie role i obszary odpowiedzialności związane z cyberbezpieczeństwem. Obie organizacje deklarują posiadanie dedykowanego zespołu w tym obszarze.

Personel zajmujący się zagadnieniami związanymi z cyberbezpieczeństwem w obu OUK jest interdyscyplinarny. Powyższy wykres przedstawia zakres kompetencji w zespołach.

Pracownicy odpowiedzialni za obszar cyberbezpieczeństwa w obu organizacjach są szkoleni. Szkolenia te obejmują następujące obszary wiedzy:

- Zarządzanie ryzykiem.
- Zarządzanie incydentami.
- Zarządzanie ciągłością działania.
- Audyt bezpieczeństwa.
- System BPM.
- Szkolenia z obsługi środków kontroli bezpieczeństwa.
- Administracja systemami bezpieczeństwa.

Ponadto obie organizacje deklarują włączenie aspektów cyberbezpieczeństwa do obowiązkowych szkoleń w organizacji np. szkoleń wdrażających nowych pracowników.

Oba OUK współpracują z innymi podmiotami w zakresie przekazywania informacji dotyczących cyberbezpieczeństwa. Odbywa się to w sposób sformalizowany.

Jako największe wyzwanie przy obecnym wdrażaniu ustawy podmioty identyfikują prawo zamówień publicznych, natomiast w kontekście Dyrektywy NIS2 bezpieczeństwo łańcucha dostaw i potencjalną, obowiązkową certyfikację.

Transport lotniczy

Transport lotniczy to jeden z podsektorów, które szczególnie ucierpiały z powodu restrykcji związanych z COVID-19.

Przed pandemią liczba pasażerów w europejskim transporcie lotniczym przekroczyła 1 mld osób, przy czym największą liczbę pasażerów obsłużyły Niemcy, Hiszpania, Francja i Włochy (łącznie 58% europejskich pasażerów). Warto wspomnieć, że prawie połowę transportu lotniczego obejmowały loty poza UE[26]. Natomiast w roku 2020 liczba pasażerów w Europie zmniejszyła się o 73,3% w porównaniu do 2019 r. Spadki zostały odnotowane we wszystkich krajach członkowskich, przy czym największe w Słowenii (-83,3%), Słowacji (-82,4%) i Chorwacji (-81,9%). Najmniejszą różnicę zaobserwowano w Luxemburgu, a i tak wyniosła ona 67,3%. Sytuacja poprawiła się dopiero w drugim półroczu 2021 r.[27], co zostało również zauważone na polskich lotniskach. Według statystyk Urzędu Lotnictwa Cywilnego (ULC) trzeci kwartał 2021 r. przyniósł ożywienie rynku lotniczego, spowodowane wyższą liczbą połączeń w letnich rozkładach lotów, niską liczbą zakażeń COVID-19, postępującym programem szczepień i możliwością korzystania z unijnych certyfikatów COVID. W trzech pierwszych kwartałach 2021 r. polskie porty lotnicze obsłużyły 12,9 mln pasażerów (nadal o 65% mniej w porównaniu z 2019 r., ale już o 3,8% więcej względem roku 2020 r.), z czego 9,1 mln w samym trzecim kwartale[28]. Łącznie ilość obsłużonych pasażerów w 2021 r. przekroczyła 19,5 mln na 15 polskich lotniskach[29]. Najwięcej pasażerów obsłużyło lotnisko Chopina w Warszawie, Kraków-Balice oraz Gdańsk im. L. Wałęsy[30]. Wzrosty odnotowały również przewozy towarowe. W pierwszych trzech kwartałach 2021 r. przewieziono 94,7 tys. ton cargo, z czego najwięcej przewiózł PLL LOT, DHL i UPS[31].

Incydenty cyberbezpieczeństwa w podsektorze lotniczym

Z każdym rokiem podsektor lotniczy w coraz większym stopniu korzysta z rozwiązań informatycznych, które można znaleźć w całym łańcuchu dostaw, od technologii stosowanej w nowych samolotach, połączenia WI-FI i pokładowych systemów informacyjno-rozrywkowych dla pasażerów, po oprogramowanie wykorzystywane do zarządzania, wykorzystywane na lotniskach i przez linie lotnicze (kontrola bezpieczeństwa, rezerwacje biletów lotniczych). Rozwiązania te są podatne na zagrożenia cyberbezpieczeństwa, w szczególności, gdy próbowano je zintegrować z przestarzałymi systemami informatycznymi, których nie projektowano z myślą o takim ryzyku. Coraz częściej podsektor korzysta również z automatyzacji, co stwarza pole dla nowych zagrożeń. Coraz więcej interesariuszy lotnictwa zaczyna również włączać do swoich systemów wyższe poziomy automatyzacji, a to tworzy zupełnie nowy obszar dla potencjalnych podatności[32]. Dane Eurocontrol pokazują, że liczba cyberataków w lotnictwie systematycznie rośnie od 2018 r.[33] Przedstawiciele izraelskiego lotniska Ben Gurion w 2019 roku poinformowali, że codziennie blokują 3 miliony prób włamania do systemów (spowodowane przez boty). Jednak prawdziwym przełomem okazał się rok 2020 i COVID-19. Pandemiczne restrykcje spowodowały nie tylko ograniczenia w ruchu lotniczym, ale również wzrost zainteresowania przestępców podsektorem lotnictwa. Sprzyjały temu zamieszanie i pośpiech, z jakim linie lotnicze na całym świecie wdrażały zmiany w swoich systemach, próbując dostosować się do sytuacji. W 2020 r. zespół EATM-CERT (European Air Traffic Management Computer Emergency Response Team) zaobserwował wzrost liczby zgłoszonych incydentów o 530% w porównaniu do 2019 r. Najwięcej incydentów dotyczyło kradzieży danych (36%), a także fałszywych stron internetowych (35%). Na kolejnych pozycjach znalazł się phishing (16%), a także malware (5%) i ransomware (5%). Większość ataków celowała w linie lotnicze (61%), a pozostałe w porty i przedsiębiorstwa. 39% organizacji, które stały się ofiarami ataków oceniła ich wpływ na wykonywane usługi jako średni lub wysoki[34].

26 Dane na 2018r. Eurostat: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Passenger_transport_statistics/pl&oldid=511153#Pasa.C5.BCerowie_w_transporcie_lotniczym

27 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Air_transport_statistics

28 https://ulc.gov.pl/_download/statystyki/analiza_3_kwartal_2021.pdf

29 https://www.ulc.gov.pl/_download/statystyki/wg_portow_lotniczych_4kw2021.pdf

30 https://ulc.gov.pl/_download/statystyki/analiza_3_kwartal_2021.pdf

31 https://ulc.gov.pl/_download/statystyki/analiza_3_kwartal_2021.pdf

32 Aviation is facing a rising wave of cyber-attacks in the wake of COVID, Stephenson Harwood LLP - Paul Phillips, Johnny Champion and Patrick Bettle; https://www.lexology.com/library/detail.aspx?g=4c9f8862-73c4-4255-9f71-d99c19e12e4c

33 https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-3-cybersecurity-aviation.pdf

34 https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf

Zagrożenia i incydenty w podsektorze lotnictwa

Lock-down, który miał miejsce w wielu krajach, dla linii lotniczych oznaczał konieczność modyfikowania siatki połączeń, masowych zwrotów pieniędzy za odwołane loty, wprowadzenia rozwiązań typu vouchery, kupony i zmiana zasad w programach lojalnościowych. Scenariusze tych zachowań wykorzystali przestępcy. W 2020 r. EATM-CERT zidentyfikował 335 fałszywych stron internetowych, z czego 280 podszywało się pod IATA i stowarzyszenie Airlines for Europe (A4E), a ich pojawienie się w Internecie zbiegało się w czasie z lock-downem, ogłaszanym w kolejnych państwach. Łącznie szacuje się koszt oszustw na fałszywych stronach internetowych na ok. 1 mld dolarów rocznie.

Kolejnym popularnym incydentem w podsektorze lotniczym jest kradzież danych (danych osobowych pasażerów, numerów kart kredytowych, dane podawane do płatności online). W 2018 r. ofiarą ataku padło British Airways i easyJet. W 2021 r. przestępcy wykradli dane firmy SITA, jednego z największych dostawców rozwiązań IT w lotnictwie, który obsługuje rezerwacje 90% światowych linii lotniczych. Coraz częściej mają miejsce ataki ransomware. W 2020 r. zgłoszono 62 incydenty tego typu, co oznacza, że średnio co tydzień podsektor lotniczy boryka się z zagrożeniem ransomware.

Ransomware może powodować duże straty i przeprowadzony z powodzeniem stanowi zagrożenie dla prowadzenia działalności lotnisk i linii lotniczych. Kwoty średniego okupu systematycznie wzrastają z ok. 5 mld dolarów w 2017 r. do ok. 20 mld dolarów w 2021 r., a w jednym, rekordowym przypadku przestępcy zażądali 50 mld dolarów za odblokowanie zaszyfrowanych plików.

Przykłady ostatnich (i największych) cyberataków w podsektorze lotniczym

- **SpiceJet (maj 2022)** – atak ransomware na indyjskie linie lotnicze, który spowodował zatrzymanie na lotniskach setek pasażerów na terenie Indii. SpiceJet nie poinformował, które systemy zostały zaszyfrowane i jakie straty spowodowano. W ciągu paru godzin linia lotnicza odzyskała zdolność operacyjną.
- **SunWing Airlines Inc. (kwiecień 2022)** – celem ataku było oprogramowanie software, dostarczane przez firmę z zewnątrz. Oprogramowanie obsługiwało check-in i on-boarding pasażerów i w efekcie jego awarii wprowadzono manualną odprawę. Przywrócenie sprawności systemu zajęło 4 dni i spowodowało liczne opóźnienia, odwołania lotów i utrudnienia dla pasażerów[35].
- **Russian CAA (marzec 2022)** – udany atak na Rosyjską Federalną Agencję Transportu. Hakerzy wykasowali z serwerów agencji 65 terabajtów danych. Bezpośrednią przyczyną ataku była rosyjska inwazja na Ukrainę.
- **SITA (marzec 2021)** – jeden z największych w historii wycieków danych w podsektorze lotnictwa. Ofiarą ataku stała się firma SITA, dostawca rozwiązań z obszaru IT dla linii lotniczych i lotnisk. Wśród bazy klientów SITA posiada 90% światowych linii lotniczych (w tym Air India, Finnair, Japan Airlines, Jeju Air, Lufthansa, Malaysia Airlines, Singapore Airlines and Cathay Pacific). Liczbę wykradzionych rekordów szacuje się na 9,4 mln (w tym dane osobowe pasażerów), jednak dotąd nie została ona oficjalnie potwierdzona.
- **VT San Antonio Aerospace (2020)** – atak ransomware, w wyniku którego zaszyfrowano systemy przedsiębiorstwa oferującego usługi konserwacyjne, remontowe i naprawcze dla linii lotniczych na całym świecie. W ciągu trzech dni udało się przywrócić system do funkcjonalności, jednak w tym czasie ponad 1 terabajt danych został skradziony.
- **easyJet (2020)** – szwajcarska linia lotnicza utraciła z powodu cyberataku dane kart kredytowych ponad 2 tys. klientów. Przedsiębiorstwo poinformowało poszkodowanych o kradzieży ich danych dopiero po 4 miesiącach, w wyniku czego został wystosowany pozew zbiorowy o odszkodowanie opiewające na kwotę 18 miliardów funtów.
- **Albany International Airport (2019)** – albańskie lotnisko ucierpiało w wyniku ataku ransomware. Przestępcy za odszyfrowanie systemów zażądali pięciocyfrowej sumy, która została zapłacona w bitcoinach. Atak nie wpłynął na funkcjonowanie lotniska, a kwota okupu została zwrócona przez ubezpieczyciela.
- **Air New Zealand (2019)** – atak phishing na dwóch pracowników linii lotniczej, który pozwolił przestępcom uzyskać dostęp do systemu obsługującego rozkład lotów, a także danych pasażerów.

35 https://www.infosecurity-magazine.com/news/cyberattackers-hit-sunwing-airlines/

- **British Airways (2018)** – atak, którego skutkiem była kradzież danych ponad 400 tys. klientów linii lotniczej (wraz z danymi paszportowymi i informacjami dot. kart kredytowych). Późniejsze śledztwo wykazało, że przedsiębiorstwo nie wprowadziło odpowiednich zabezpieczeń, w związku z czym otrzymało grzywnę w wysokości 20 milionów funtów.
- **Air Canada (2018)** – w wyniku zhakowania aplikacji mobilnej wyciekły dane paszportowe pasażerów.
- **Cathay Pacific (2018)** – ponad 9,4 miliona rekordów danych pasażerów zostało skradzionych w wyniku cyberataku, który przeprowadzono na systemy linii lotniczych z Hongkongu. Okazało się, że system operacyjny nie był aktualizowany, a dane przechowywane w ramach back-upu nie chroniło żadne hasło. Cathay Pacific zapłacił grzywnę w wysokości 500 tys. funtów.
- **Bristol Airport (2018)** – ransomware zaszyfrował elektroniczną informację o lotach na lotnisku w Bristolu. Lotnisko nie zapłaciło okupu i do czasu odzyskania kontroli nad systemem, ręcznie uzupełniało informację na temat lotów.

Cyberataki w podsektorze lotniczym nie ominęły także Polski. W 2015 r. miał miejsce atak DDoS na Polskie Linie Lotnicze LOT, w efekcie którego odwołano 10 lotów, a 15 uległo opóźnieniu. Awaria na systemy informatyczne spowodowała uziemienie na lotniskach ok. 1400 pasażerów[36]. Zespół CERT Polska co roku rejestruje incydenty w podsektorze lotniczym, a liczby te utrzymują się na podobnym poziomie (6 incydentów w 2020 r., 9 incydentów w 2021 r., 8 incydentów w 2022 r.[37]).

Cyberbezpieczeństwo w podsektorze lotniczym

Cyberprzestępczość w lotnictwie, ze względu na jego wyjątkowy, globalny charakter i łańcuchy dostaw, często składające się z międzynarodowych przedsiębiorstw, musi być zwalczana globalnie. Civil Aviation Organization (ICAO), wyspecjalizowana agencja ONZ, odpowiedzialna za lotnictwo, w 2019 r. opublikowała globalną Strategię Cyberbezpieczeństwa w Lotnictwie. W dokumencie zauważono ciągły wzrost cyberzagrożeń w lotnictwie, wynikający z wdrażania nowoczesnych technologii.

W Unii Europejskiej w listopadzie 2015 r. Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (*European Union Aviation Safety Agency, EASA*) opracowała mapę drogową/harmonogram działań dla cyberbezpieczeństwa. Głównym celem tej inicjatywy było zaangażowanie wszystkich interesariuszy w podsektorze by włączyć aspekty cyber do ówczesnego pojęcia bezpieczeństwa. Działania te doprowadziły do powstania w 2016 r. Europejskiej Platformy Współpracy Strategicznej[38] (European Strategic Cooperation Platform, ESCP), która służy do komunikacji i budowania współpracy na rzecz cyberbezpieczeństwa. Sukcesem tej współpracy było opracowanie i przyjęcie w 2019 r. europejskiej Strategii Cyberbezpieczeństwa w Lotnictwie[39], w której oficjalnie przyznano, że systemy i zasoby w lotnictwie są zagrożone cyberatakami i konieczne jest podjęcie wspólnych działań na rzecz budowania cyberbezpieczeństwa w przyszłości. W Strategii określono 4 mierzalne cele na drodze poprawy cyberodporności i 4 cele na drodze budowy bezpiecznych i nieustannie ulepszanych systemów lotniczych.

4 cele na drodze poprawy odporności teleinformatycznej:

1	Zapewnienie ciągłości działania – możliwe dzięki zabezpieczeniom rozłożonym w łańcuchach funkcjonalnych, odpowiednich do poziomu ryzyka.
2	Systemy operacyjne wyposażone w wielowarstwowe środki ochrony.
3	Systemy operacyjne, które zapewnią ciągłość podstawowych funkcji, nawet w czasie awarii.
4	Wykorzystanie transorganizacyjnego charakteru systemów lotniczych i wykorzystanie go do budowy współpracy.

36 https://avlab.pl/podsumowanie-cyberatakow-na-branze-lotnicza/

37 Dane zebrane w sierpniu 2022 r.

38 https://www.easa.europa.eu/community/content/european-strategic-coordination-platform-escp

39 https://www.easa.europa.eu/downloads/103075/en

4 cele na drodze do budowy bezpiecznych systemów:

1	Systemy projektowane w sposób, który uniemożliwia użytkownikom niezamierzonego używania funkcji.
2	Zabezpieczanie systemów przed utratą atrybutów bezpieczeństwa już na etapie projektowania.
3	Zapewnienie bezpieczeństwa systemów w całym cyklu życia.
4	Regularna ocena poziomu ochrony systemu.

Kolejnym działaniem EASA było wspieranie powstania w 2017 r. europejskiego ISACa dla sektora lotniczego – ECCSA[40]. Wśród 12 podmiotów założycielskich znalazły się: Airbus, Air France/KLM, Brussels Airport, Urząd Lotnictwa Cywilnego w Polsce, ENAV S.p.A., EUROCONTROL, Finnair, Frankfurt Airport, Leonardo S.p.A., Lufthansa Group, NAV Portugal i Thales Group. Od 2019 r. ECCSA jest otwarta na przyjmowanie innych organizacji ze społeczności lotniczej, a także inne firmy (np. dostawców produktów lub usług dla lotnictwa), które mogą przyczynić się do podniesienia sektorowego poziomu cyberbezpieczeństwa.

W 2022 r. EASA uruchomiła portal społecznościowy, który zawiera szczegółowe informacje na temat przepisów, norm i inicjatyw z obszaru cyberbezpieczeństwa w lotnictwie. Portal przeznaczony jest dla profesjonalistów i ma służyć również dzieleniu się informacjami i budowaniu współpracy[41].

Dyrektywa NIS

Podsektor transportu lotniczego został wpisany w zakres Dyrektywy NIS, z wyszczególnieniem 3 rodzajów podmiotów: przewoźników lotniczych, zarządzających portami lotniczymi i operatorów zarządzających ruchem lotniczym zapewniających służbę kontroli ruchu lotniczego[42]. Dokładne kryteria, na podstawie których wyznaczono operatorów usług kluczowych różnią się w zależności od państwa[43]. W niektórych krajach głównym kryterium określającym operatorów usług kluczowych jest liczba obsługiwanych pasażerów (np. w Niemczech operatorem zostało każde przedsiębiorstwo lotnicze, które świadczy usługi dla minimum 500 tys. obywateli w skali roku.) W innych skupiono się na rodzaju świadczonych usług, zależności od systemów, czy zagrożenia wystąpieniem incydentu (np. we Francji operatorzy usług kluczowych to przedsiębiorstwa, które świadczą usługi typu check-in, boarding, transport pasażerów, zależne od systemów informatycznych i zagrożone wystąpieniem incydentu).

Polska

W Polsce Dyrektywę NIS implementuje Ustawa o krajowym systemie cyberbezpieczeństwa z 2018 r. Operatorzy usług kluczowych zostali wyznaczeni na podstawie Rozporządzenia w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych z 11 września 2018 r. W Polsce ustawodawca zdefiniował 6 usług kluczowych w podsektorze lotniczym, dla których opisano szczegółowe kryteria zawarte w rozporządzeniu:

- Transport lotniczy pasażerski.
- Transport lotniczy towarów.
- Działalność usługowa wspomagająca transport lotniczy przez zarządzającego lotniskiem.
- Działalność usługowa wspomagająca transport lotniczy przez przedsiębiorcę, posiadającego status zarejestrowanego agenta.
- Działalność usługowa wspomagająca transport lotniczy przez przedsiębiorcę posiadającego status agenta obsługi naziemnej.
- Działalność usługowa wspomagająca transport lotniczy przez instytucję zapewniającą służby żeglugi powietrznej.

40 https://www.easa.europa.eu/eccsa

41 https://www.easa.europa.eu/newsroom-and-events/news/cybersecurity-aviation-community-launched

42 Szczegółowa definicja podmiotów wchodzących w zakres Dyrektywy została zawarta w załączniku II.

43 https://www.nortonrosefulbright.com/en/knowledge/publications/fc813c25/cybersecurity-law-in-the-aviation-sector

Poniższa tabela opisuje kryteria uznania każdej z usług za kluczową

Usługa kluczowa	Kryteria
Transport lotniczy pasażerski	Liczba użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot: przewóz minimum 500 tys. pasażerów rocznie określany: na podstawie uśrednionych danych statystycznych za 3 lata poprzedzające wydanie decyzji o uznaniu za operatora usługi kluczowej lub w przypadku podmiotów działających na rynku krócej niż 3 lata, na podstawie danych statystycznych za 2 pełne lata lub 1 pełny rok poprzedzający wydanie decyzji.
Transport lotniczy towarów	Udział podmiotu świadczącego usługę kluczową w rynku: wynoszący minimum 25% udział realizowanych lotów transportu towarów w skali rynku krajowego obliczony: na podstawie uśrednionych danych statystycznych za 3 lata poprzedzające wydanie decyzji o uznaniu za operatora usługi kluczowej lub w przypadku podmiotów działających na rynku krócej niż 3 lata, na podstawie danych statystycznych za 2 pełne lata lub 1 pełny rok poprzedzający wydanie decyzji.
Działalność usługowa wspomagająca transport lotniczy przez zarządzającego lotniskiem	Obsługa minimum 500 tys. pasażerów rocznie określana: na podstawie uśrednionych danych statystycznych za 3 lata poprzedzające wydanie decyzji o uznaniu za operatora usługi kluczowej lub w przypadku podmiotów działających na rynku krócej niż 3 lata, na podstawie danych statystycznych za 2 pełne lata lub 1 pełny rok poprzedzający wydanie decyzji lub w przypadku nowych podmiotów, których przewidywany zakres działania spełni wymogi progu uznania za operatora usługi kluczowej, na podstawie planu generalnego, o którym mowa w art. 55 ust. 6 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.
Działalność usługowa wspomagająca transport lotniczy przez przedsiębiorcę, posiadającego status zarejestrowanego agenta	Realizowanie przez podmiot kontroli bezpieczeństwa ładunku lub poczty lotniczej wraz z nadawaniem skontrolowanym ładunkom statusów SPX, SCO oraz SHR w myśl rozporządzenia wykonawczego Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiającego szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego, lub świadczenie usługi elektronicznego przekazu informacji o statusie ochrony nadanym przesyłce, przekazywanej drogą lotniczą do punktu docelowego.
Działalność usługowa wspomagająca transport lotniczy przez przedsiębiorcę posiadającego status agenta obsługi naziemnej	Prawidłowe działanie innych usług kluczowych w porcie lotniczym zależy od usług świadczonych przez agenta obsługi naziemnej, przy jednoczesnym braku możliwości jej świadczenia przez inny podmiot.
Działalność usługowa wspomagająca transport lotniczy przez instytucję zapewniającą służby żeglugi powietrznej	Spełnienie co najmniej dwóch z poniższych kryteriów: ▸ Zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent: świadczenie usługi na terytorium całego kraju. ▸ Brak alternatywy dla świadczonej usługi i możliwości jej realizowania przez inną służbę w przypadku wystąpienia incydentu. ▸ Usługa zapewniana jest dla więcej niż 10 tys. lotów rocznie, niezależnie od maksymalnej masy startowej i liczby miejsc pasażerskich w statku powietrznym, przy lotach liczonych jako suma startów i lądowań oraz obliczanych jako średnia z ubiegłych 3 lat.

Na tej podstawie kryteriów z rozporządzenia Ministerstwo Infrastruktury decyzją administracyjną **wskazało 12 operatorów usług kluczowych w podsektorze lotniczym (wszystkie podmioty wzięły udział w niniejszym badaniu)**.

Wyniki badań

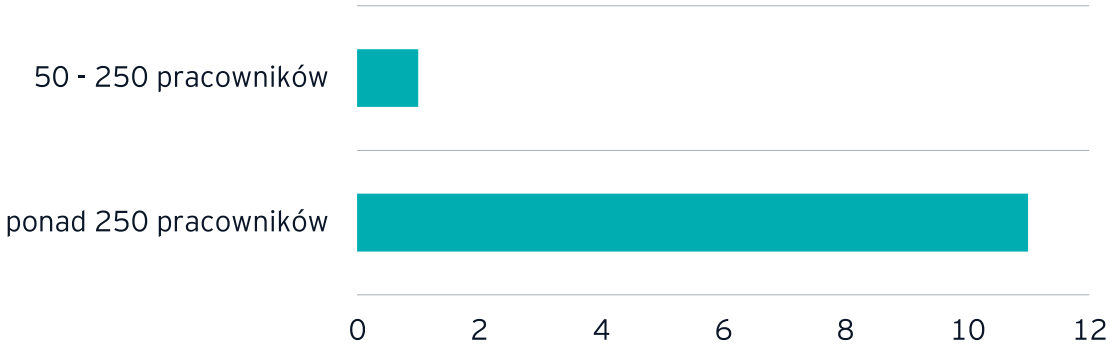
W badaniu wzięło udział 12 operatorów usług kluczowych z podsektora transportu lotniczego. Poniżej przedstawione zostały wyniki poszczególnych sekcji.

Organizacja

Funkcjonowanie organizacji jest podstawą do rozważania wielu kwestii, również tych związanych z obszarem cyberbezpieczeństwa w danej firmie.

Badane podmioty to przeważnie przedsiębiorstwa duże, gdzie liczba pracowników jest większa niż 250 osób (9 odpowiedzi). Następnie wskazano średnie przedsiębiorstwa o wielkości w przedziale 50 < 250 pracowników (3 odpowiedzi). Nie ma wśród badanych OUK przedsiębiorstw mniejszych.

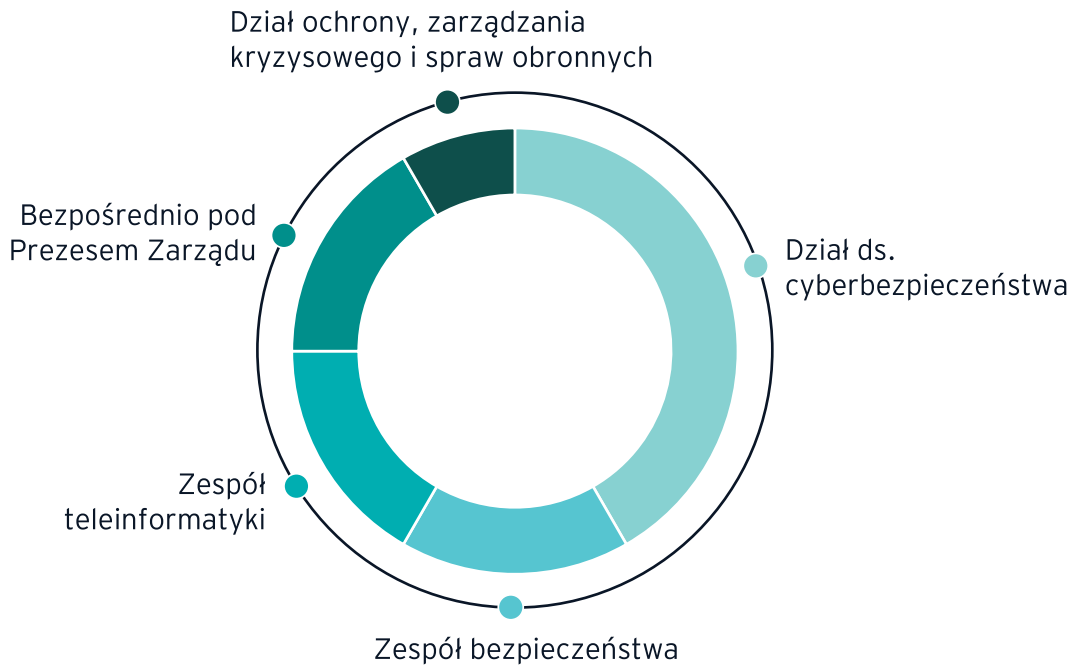
Wielkość OUK w podsektorze transportu lotniczego



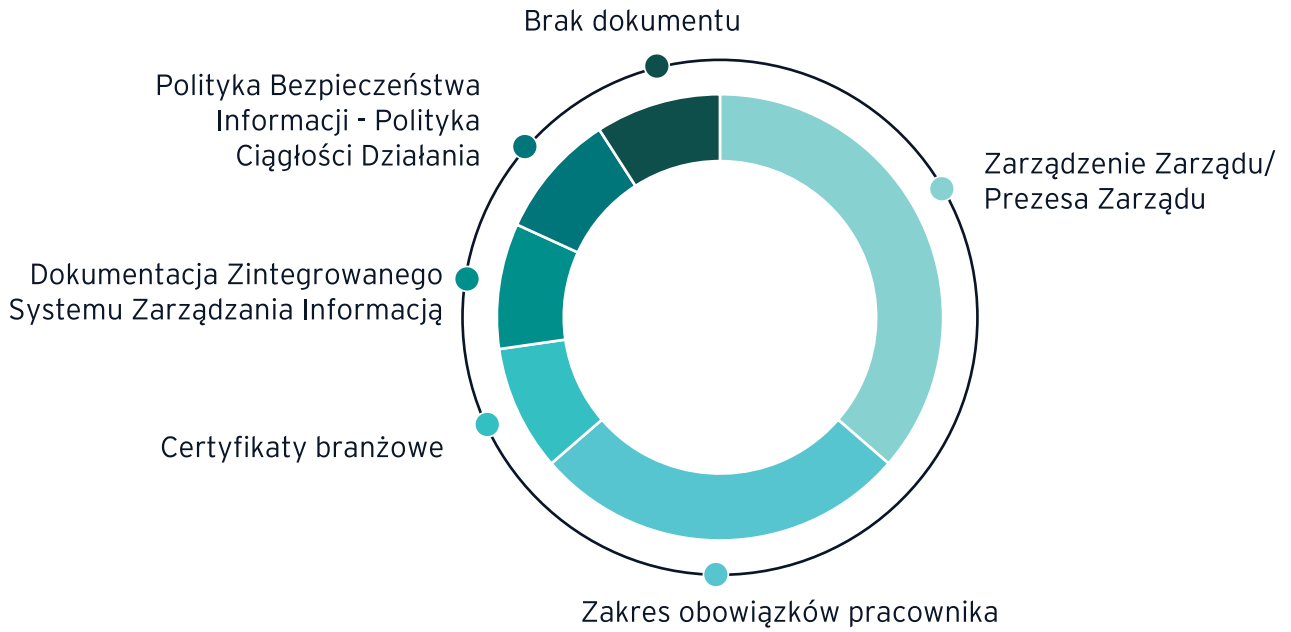
Wszyscy OUK (operatorzy usług kluczowych) z podsektora transportu lotniczego zadeklarowali, że wskazały osobę kontaktową do odpowiedniego CSIRT-u. Wyznaczenie osoby kontaktowej jest obowiązkowe i wynika z UoKSC.

Na poniższych wykresach przedstawione jest umiejscowienie osoby kontaktowej w strukturze organizacji oraz dokumenty, które określają jej kompetencje.

Umiejscowienie osoby kontaktowej u OUK



Dokumenty określające kompetencje osoby kontaktowej ds. cyberbezpieczeństwa



Procesy

Ponad połowa OUK z podsektora lotniczego deklaruje, że szacowanie ryzyka dla systemów teleinformatycznych jest częścią korporacyjnego zarządzania ryzykiem (7 odpowiedzi). Przeprowadzone jest one dla systemów zdefiniowanych w organizacji jako usługi kluczowe (transport lotniczy pasażerski, działalność usługowa wspomagająca transport lotniczy przez zarządzającego lotniskiem, działalność usługowa wspomagająca transport lotniczy przez przedsiębiorcę, posiadającego status zarejestrowanego agenta, działalność usługowa wspomagająca transport lotniczy przez przedsiębiorcę posiadającego status agenta obsługi naziemnej, działalność usługowa wspomagająca transport lotniczy przez instytucję zapewniającą służby żeglugi powietrznej).

Podmioty potwierdziły, że w ich organizacji zostały zmapowane procesy i ich zależności od systemów teleinformatycznych. Dziewięć OUK zidentyfikowało odbiorców usług zależnych od ich systemów teleinformatycznych. Wszystkie podmioty odpowiedziały twierdząco na pytanie o posiadanie wewnętrznych polityk cyberbezpieczeństwa w zakresie IT oraz OT. Jest to bardzo istotne w kontekście wymagań, które stawia przed operatorami Dyrektywa NIS2.

Wszystkie podmioty realizują zadania wynikające z ustawy[44], a część z nich wskazało na trudności w realizacji niektórych z nich:

A Prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem.

B Wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji.

C Przekazywanie organowi właściwemu do spraw cyberbezpieczeństwa danych, o których mowa w art. 7 ust. 2 pkt 8 i 9, nie później niż w terminie 3 miesięcy od zmiany tych danych.

D Bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej.

E Objęcie systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej, systemem monitorowania w trybie ciągłym.

F Zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej.

G Stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej.

H Stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym.

I Ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym.

J Niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa.

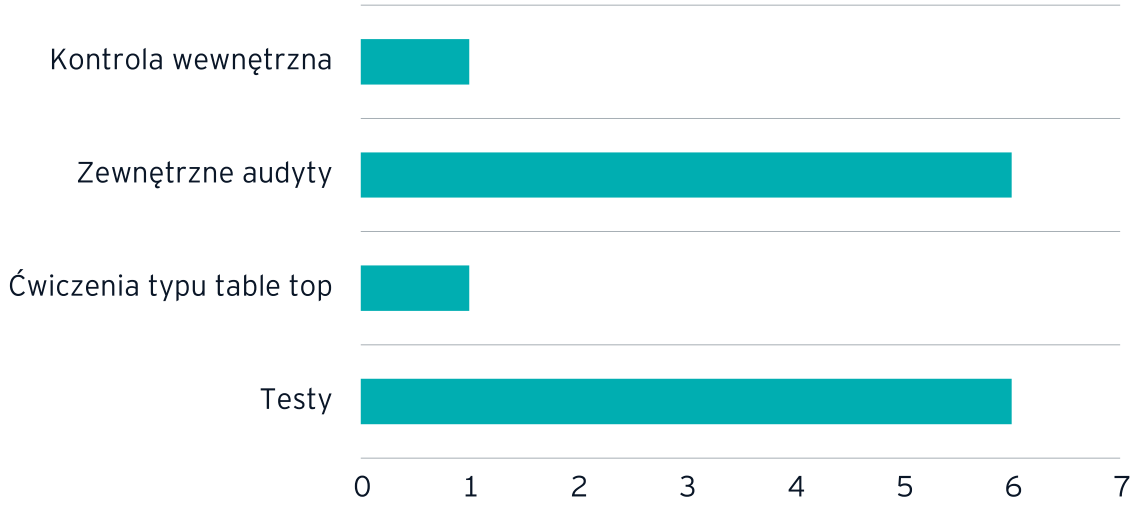
K Stosowanie skutecznych sposobów zabezpieczania się przed cyberzagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej.

OUK przekazują informacje o poziomie cyberbezpieczeństwa swojemu zarządowi. Odbywa się to poprzez roczne sprawozdania z działalności Działu Cyberbezpieczeństwa, podczas spotkań, raportów z audytu, poprzez wewnętrzną korespondencję firmową oraz za pomocą przeglądów zarządzania.

Większość OUK w podsektorze transportu lotniczego opracowują plany, bądź procedury reagowania na incydenty, w tym plany przywracania działania po zaistniałym incydencie. Dziewięć ankietowanych OUK zadeklarowało, że przeprowadza regularną kontrolę posiadanych przez siebie planów i procedur. Odbywa się to najczęściej poprzez testy i audyty zewnętrzne. O wiele rzadziej w toku wewnętrznej kontroli lub poprzez ćwiczenia. Poniższy wykres przedstawia szczegółowe dane w tym zakresie.

44 Wymienione w Ustawie o krajowym systemie cyberbezpieczeństwa zadania operatorów usług kluczowych: 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym: a) utrzymanie i bezpieczną eksploatację systemu informacyjnego, b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej, d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym; 3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej; 4) zarządzanie incydentami; 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym: a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, b) dbałość o aktualizację oprogramowania, c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym, d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa; 6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa; zapewnia użytkownikowi usługi kluczowej dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej; przekazuje organowi właściwemu do spraw cyberbezpieczeństwa dane, o których mowa w art. 7 ust. 2 pkt 8 i 9, nie później niż w terminie 3 miesięcy od zmiany tych danych.

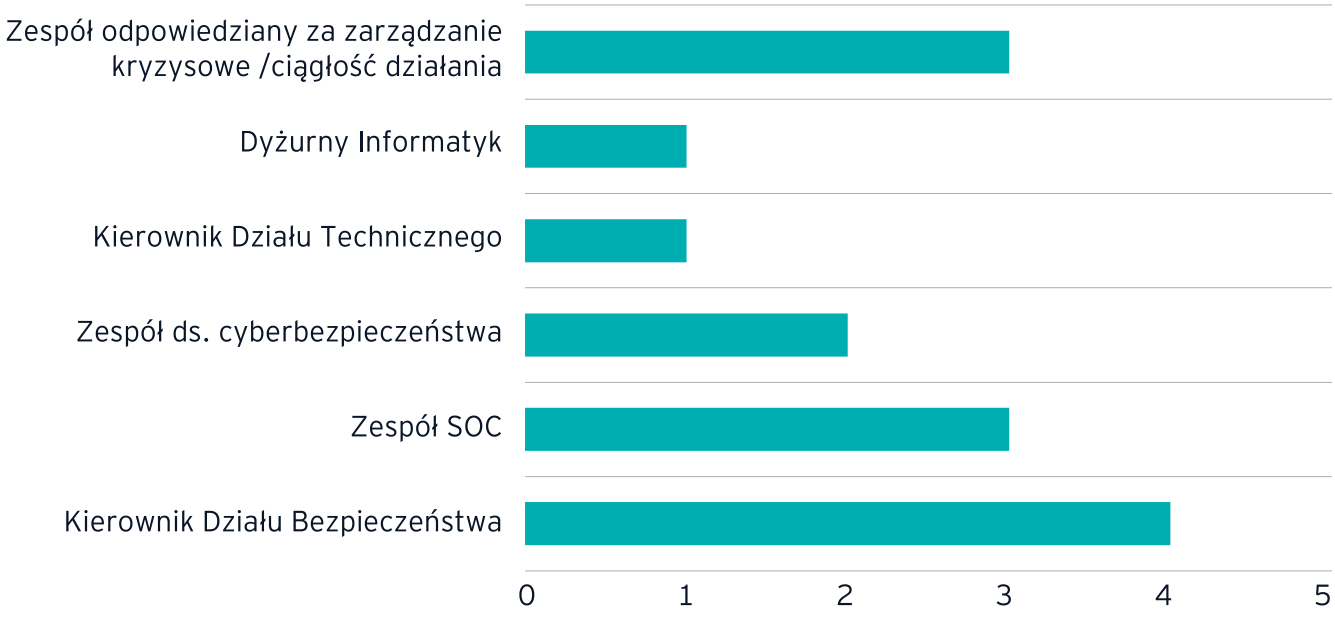
Testowanie procedur odpowiedzi na incydenty



Jednym z istotniejszych obowiązków ustawowych jest zgłaszanie do właściwego CSIRT-u poziomu krajowego incydentów poważnych[45], a co za tym idzie: właściwe zaklasyfikowanie tego incydentu, zgodnie z progami określonymi w Rozporządzeniu Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny.

Zadanie pełnione jest przez różne komórki w organizacjach u operatorów usług kluczowych. Ma to związek z procesem samej obsługi incydentu w organizacji. Poniższy wykres prezentuje, które komórki i osoby dokonują klasyfikacji incydentów jako poważne.

Komórki i osoby odpowiedzialne za klasyfikowanie incydentów poważnych



45 Według UoKSC incydent poważny to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej.

Pięć ankietowanych podmiotów wskazało, że posiada wewnętrzną (opracowaną na własne potrzeby) klasyfikację incydentów i zagrożeń. Niektóre kasyifikacje dotyczyły poziomu istotności incydentu, skutku incydentu czy też klasyfikacji incydentu w ramach wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO 27001.

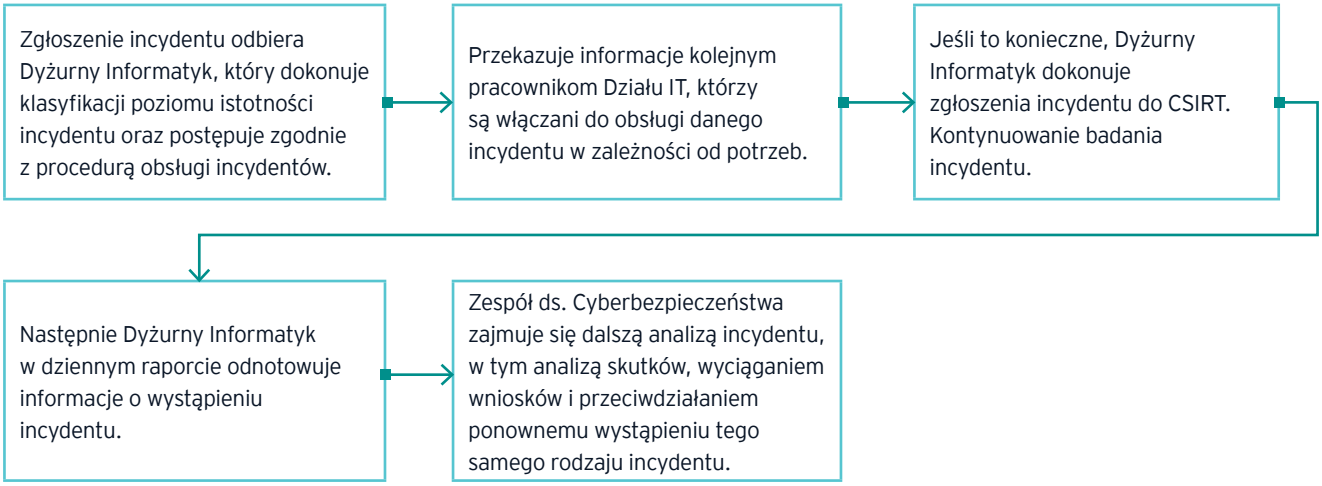
Aż 7 na 12 respondentów potwierdziło, że kryteria definiujące incydent jako poważny w Rozporządzeniu Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny są adekwatne.

Część podmiotów uważa, że kryteria powinny być zmienione. Główny argument związany jest z tym, że usługa w porcie lotniczym ma charakter dyskretny, a nie ciągły i dlatego przerwa dwugodzinna, zdefiniowana w rozporządzeniu, jest nieadekwatna. Zastrzeżenia budzi także klasyfikowanie incydentu jako poważny jedynie na podstawie czasu niedostępności usługi, ponieważ nie oddaje to obiektywnie skali wpływu incydentu na organizację. Dodatkowo OUK wskazali także, że warto rozważyć uwzględnienie wpływu na podmioty zależne oraz możliwość przywrócenia działalności biznesowej.

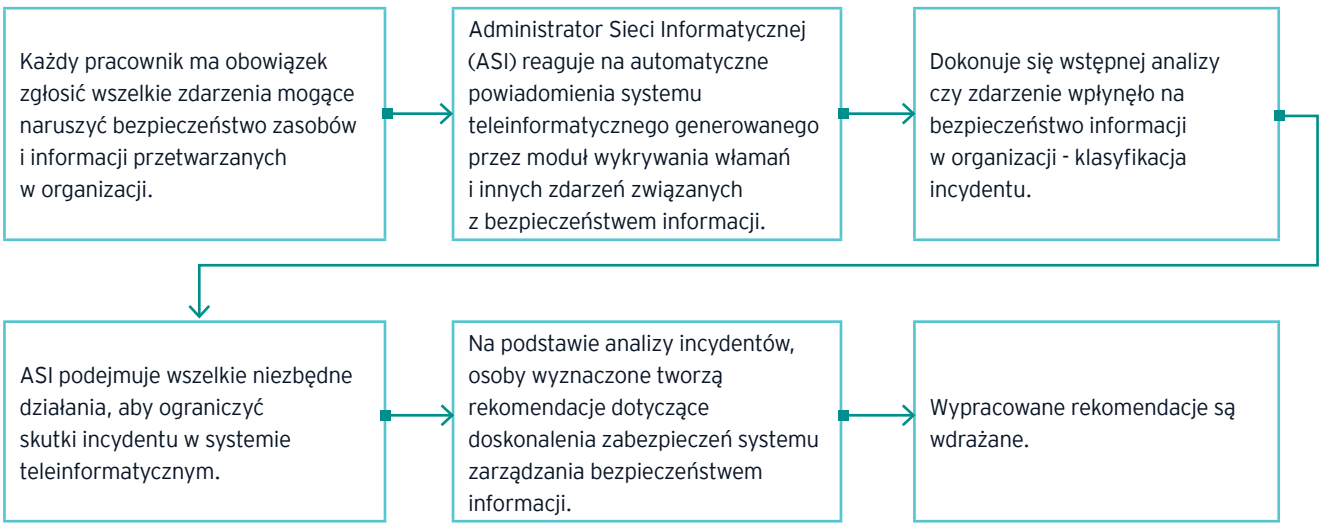
Proces raportowania i obsługi incydentu u OUK - studium przypadku

Procesy raportowania i obsługi incydentu różnią się w zależności od wielkości OUK oraz tego, czy dany podmiot ma wewnętrzny SOC, czy też wykupuje takie usługi na rynku. Jednak wszystkie podmioty uwzględniły w swoich procedurach konieczność zgłoszenia incydentu do CSIRT-u poziomu krajowego oraz klasyfikacje incydentu, zgodnie z ustawą UoKSC. Poniżej trzy studia przypadku.

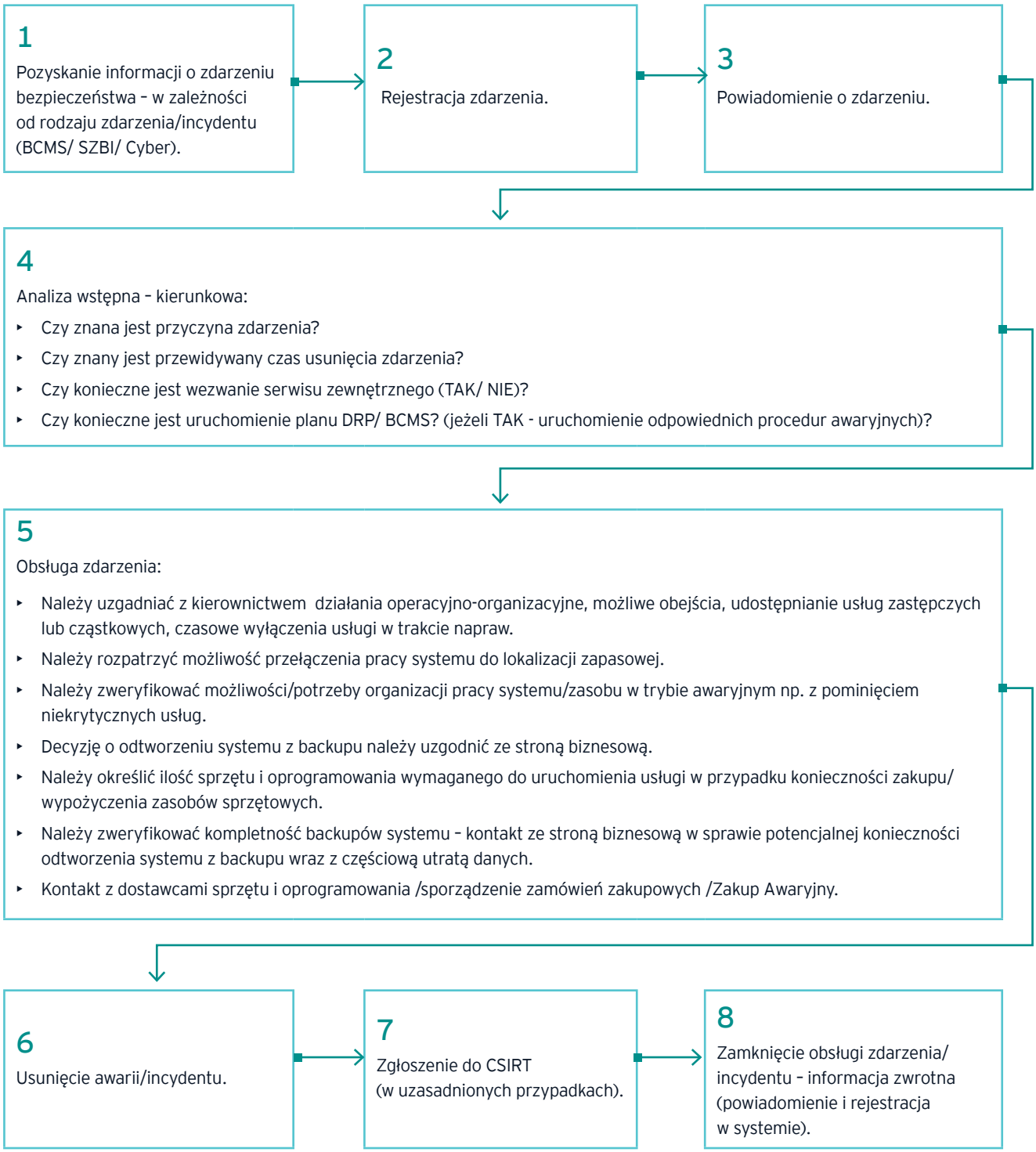
Studium 1



Studium 2



Studium 3


1
Pozyskanie informacji o zdarzeniu bezpieczeństwa – w zależności od rodzaju zdarzenia/incydentu (BCMS/ SZBI/ Cyber).
2
Rejestracja zdarzenia.
3
Powiadomienie o zdarzeniu.
4
Analiza wstępna – kierunkowa:
Czy znana jest przyczyna zdarzenia?
Czy znany jest przewidywany czas usunięcia zdarzenia?
Czy konieczne jest wezwanie serwisu zewnętrznego (TAK/ NIE)?
Czy konieczne jest uruchomienie planu DRP/ BCMS? (jeżeli TAK - uruchomienie odpowiednich procedur awaryjnych)?
5
Obsługa zdarzenia:
Należy uzgadniać z kierownictwem działania operacyjno-organizacyjne, możliwe obejścia, udostępnianie usług zastępczych lub cząstkowych, czasowe wyłączenia usługi w trakcie napraw.
Należy rozpatrzyć możliwość przełączenia pracy systemu do lokalizacji zapasowej.
Należy zweryfikować możliwości/potrzeby organizacji pracy systemu/zasobu w trybie awaryjnym np. z pominięciem niekrytycznych usług.
Decyzję o odtworzeniu systemu z backupu należy uzgodnić ze stroną biznesową.
Należy określić ilość sprzętu i oprogramowania wymaganego do uruchomienia usługi w przypadku konieczności zakupu/ wypożyczenia zasobów sprzętowych.
Należy zweryfikować kompletność backupów systemu – kontakt ze stroną biznesową w sprawie potencjalnej konieczności odtworzenia systemu z backupu wraz z częściową utratą danych.
Kontakt z dostawcami sprzętu i oprogramowania /sporządzenie zamówień zakupowych /Zakup Awaryjny.
6
Usunięcie awarii/incydentu.
7
Zgłoszenie do CSIRT (w uzasadnionych przypadkach).
8
Zamknięcie obsługi zdarzenia/ incydentu – informacja zwrotna (powiadomienie i rejestracja w systemie).

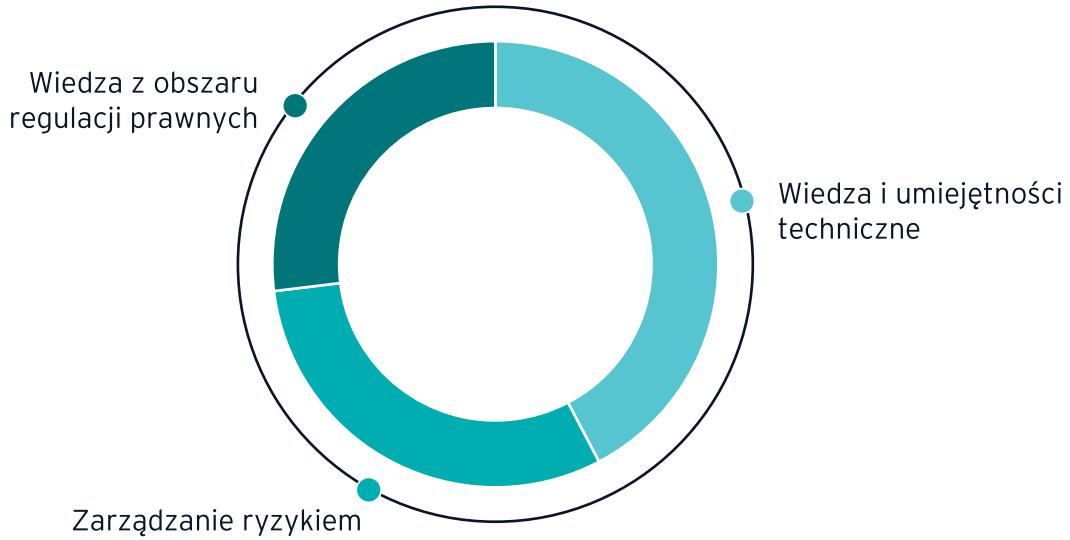
Zespół

Operatorzy usług kluczowych potwierdzili, że zdefiniowali odpowiednie role i obszary odpowiedzialności związane z cyberbezpieczeństwem.

Zdecydowana większość respondentów potwierdziła, że osoby zajmujące się bezpieczeństwem teleinformatycznym w ich organizacji posiadają wiedzę i umiejętności do realizacji wyznaczonych im ról i odpowiedzialności.

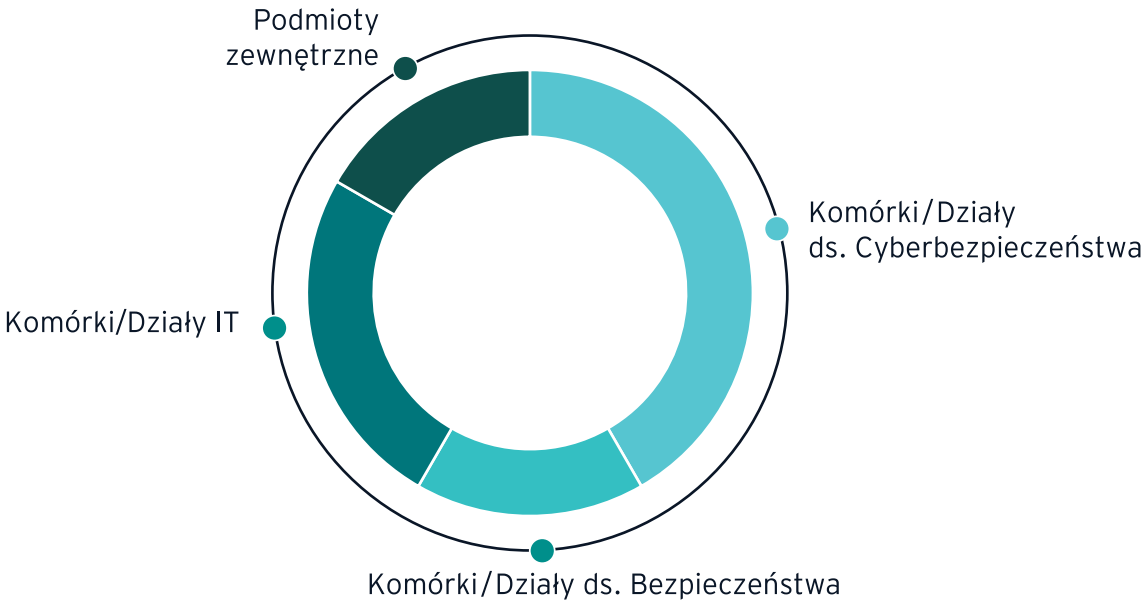
Większość podmiotów posiada dedykowany zespół do działań związanych z zarządzaniem cyberbezpieczeństwem. Są to zespoły interdyscyplinarne, gdzie obok specjalistów z wiedzą techniczną obecni są specjaliści z obszaru zarządzania ryzykiem oraz posiadający wiedzę na temat regulacji prawnych. Poniższy wykres przedstawia kompetencje tych zespołów.

Kompetencje zespołów odpowiedzialnych za cyberbezpieczeństwo



Zespoły zajmujące się cyberbezpieczeństwem to najczęściej odrębne komórki. W kilku przypadkach zespół ten znajduje się w strukturach działu bezpieczeństwa, bądź też działu IT.

Zespoły ds. cyberbezpieczeństwa w strukturze OUK



Operatorzy usług kluczowych wskazali, że szkolenia dla pracowników związanych z obszarem cyberbezpieczeństwa dotyczą następujących obszarów:

- Szkoleń kierunkowych w zakresie cyberbezpieczeństwa.
- Szkoleń z ochrony informacji.
- Bezpieczeństwa sieci.
- Obszaru white hacker.
- Ochrony obszarów IT i OT.
- Analizy zagrożeń.
- Krajowych regulacji prawnych z zakresu cyberbezpieczeństwa.
- Regulacji wewnętrznych firmy.
- Szkoleń technicznych z zakresu obsługi wykorzystywanej infrastruktury IT.
- Szkoleń technicznych.
- Wymagań standardów norm ISO (ISO 27001 i ISO 22301).
- Trendów związanych z nowymi technologiami.
- Szkoleń podnoszących świadomość pracowników z obszarów cyberbezpieczeństwa.
- Zapobiegania zdarzeniom i incydentom.

Ponadto część OUK z podsektora transportu lotniczego realizuje szkolenia z aspektów cyberbezpieczeństwa dla całej organizacji. Takie szkolenia odbywają się z najczęściej z częstotliwością raz na rok, lub raz na dwa lata.

Dwóch operatorów zdefiniowało łańcuch dostaw w zakresie cyberbezpieczeństwa. Pozostali wskazali, że jest to wyzwanie na przyszłość, w kontekście wymagań Dyrektywy NIS2.

W badaniu zapytano również operatorów usług kluczowych, jakie jest główne kryterium wyboru dostawców z obszaru cyberbezpieczeństwa. Respondenci odpowiedzieli następująco:

Cena (*9 odpowiedzi*)

Jakość usług (*6 odpowiedzi*)

Ocena dostawców (*1 odpowiedź*)

Jako największe wyzwania w procesie wdrażania Ustawy o krajowym systemie cyberbezpieczeństwa operatorzy usług kluczowych wymienili:

- Problemy z pozyskaniem odpowiedniego (i w odpowiedniej liczbie) personelu do zadań związanych cyberbezpieczeństwem.
- Szkolenia personelu odpowiedzialnego pod kątem cyberbezpieczeństwa.
- Rosnące koszty rozwiązań informatycznych i ich utrzymania na odpowiednim poziomie.
- Pogodzenie potrzeb biznesowych i cyberbezpieczeństwa.
- Zapewnienie zgodności prawnej z UoKSC w powiązaniu z przepisami z innych obszarów.
- Zbyt krótki czas na wdrożenie wymagań UoKSC.
- Brak czasu na przeprowadzenie procedur przetargowych w celu wyboru np. firmy doradczej czy wdrożeniowej.
- Przekonanie zarządzających o ważności zagadnień.
- Ograniczone zasoby finansowe.
- Wprowadzenie zmian w obszarze systemu zarządzania bezpieczeństwem informacji i systemu zarządzania ciągłością działania.
- Pozyskanie finansowania na wdrożenie pełnego zakresu wymagań UoKSC (m.in., SOC, dyżury 24/7, zbudowanie zespołu cyberbezpieczeństwa, modernizacja infrastruktury, wdrożenie zabezpieczeń o odpowiednich standardach).
- Nadmiar obowiązków.
- Wyzwania organizacyjne i technologiczne.
- Budowanie świadomości użytkowników systemów.

Jako największe wyzwania w kontekście wymagań Dyrektywy NIS2, OUK identyfikują:

- Pozyskanie odpowiedniego finansowania.
- Zapewnienie bezpiecznego łańcucha dostaw.
- Zbudowanie odpowiedniego wykwalifikowanego zespołu cyberbezpieczeństwa.
- Powiększenie zespołu SOC.
- Modernizacja infrastruktury.
- Wdrożenie zabezpieczeń o odpowiednich standardach.
- Znaczące koszty zakupu i implementacji produktów z zakresu cyberbezpieczeństwa zapewniających pełne spektrum funkcji ochrony systemów cyfrowych.

Transport wodny

Podsektor transportu wodnego jest niezwykle ważny dla europejskiej gospodarki jako środek transportu umożliwiający handel, import i eksport dóbr i towarów, zaopatrzenie w energię, a także przewóz pasażerów. Porty europejskie odgrywają kluczową rolę w handlu, rozwoju gospodarczym i tworzeniu miejsc pracy.

W Europie znajduje się ponad 1200 portów morskich, w 23 państwach członkowskich Unii Europejskiej. W 2010 roku obsługiwały one 52% europejskiego ruchu towarowego, podczas gdy dziesięć lat wcześniej było to zaledwie 45%[46]. W ciągu ostatnich 20 lat liczba kontenerów w portach europejskich wzrosła ponad czterokrotnie[47]. Ten ciągły wzrost zależności od transportu morskiego podkreśla jego żywotne znaczenie dla naszego społeczeństwa i gospodarki. Najbardziej ruchliwe porty kontenerowe w Europie znajdują się w Rotterdamie, Hamburgu i Antwerpii.

W Polsce do największych portów morskich należą: Port Gdańsk, Port Gdynia i Port Szczecin-Świnoujście. W 2021 roku przeładowano w nich łącznie 113,1 mln ton ładunków, co oznacza wzrost o prawie 9% w stosunku do poprzedniego roku, a także o 4,5% w porównaniu do roku 2019. Największy wzrost odnotował Port Gdańsk, który awansował na trzecią pozycję na Bałtyku, a biorąc pod uwagę przeładunek kontenerów, jest to największy port kontenerowy na Morzu Batyckim[48].

Transformacja cyfrowa transportu wodnego

Podobnie jak w pozostałych sektorach gospodarki, transport morski w celu optymalizacji swoich zadań, w coraz większym stopniu polega na technologiach informacyjno-komunikacyjnych (ICT). Są one wykorzystywane do m.in. do nawigacji, zarządzania towarami, komunikacji i kontroli ruchu. Porty zwiększają swoją konkurencyjność poprzez cyfryzowanie kolejnych operacji, a także inwestycje w nowe technologie – chmurę, Big Data, Internet rzeczy IoT. Dodatkowo globalny trend cyfryzacji oraz najnowsze polityki i regulacje wymagają od portów morskich stawienia czoła nowym wyzwaniom w zakresie technologii. Ma to wpływ na wyzwania w obszarze cyberbezpieczeństwa, zarówno w świecie technologii informatycznych (IT), jak i technologii operacyjnych (OT), które kiedyś dla podsektora transportu wodnego były czymś nieznanym. Koncepcja „smart ports" z jednej strony pozwala na wykorzystanie potencjału nowoczesnych technologii w transporcie morskim, a z drugiej wiąże się z koniecznością stawienia czoła zagrożeniom z obszaru cyberbezpieczeństwa. Wśród możliwych ryzyk znajdują się:

- Paraliż portu morskiego, uniemożliwienie świadczenia usług.
- Zagrożenie bezpieczeństwa pracowników i pasażerów.
- Kradzież danych, w szczególności tych poufnych, zawierających informacje krytyczne dla działalności portu.
- Kradzież dóbr, towarów, środków finansowych. Próba przemytu niedozwolonych towarów
- Uszkodzenia systemów odpowiedzialnych za usługi kluczowe.
- Utrata reputacji, konkurencyjności.
- Katastrofy ekologiczne[49].

Największe incydenty w podsektorze transportu wodnego

Transformacja cyfrowa portów morskich spowodowała, że stały się one celem ataków dla cyberprzestępców. Do największych incydentów w podsektorze możemy zaliczyć:

1

Cyberatak na port w Antwerpii - przestępcy w 2011 r. dokonali włamania na systemy IT kontrolujące transport i lokalizacje kontenerów, co zostało wykorzystane do przemytu narkotyków[50].

2

Atak ransoware NotPetya na firmę Maersk, w wyniku którego zdestabilizowany został port w Rotterdamie,

46 Raport ENISA Port Cybersecurity - Good practices for cybersecurity in the maritime sector: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

47 Dane Europejskiej Organizacji Portów Morskich: https://www.globaltrademag.com/european-ports/

48 https://polska-morska.pl/2022/02/14/polskie-porty-morskie-w-2021-roku/

49 Raport ENISA Port Cybersecurity - Good practices for cybersecurity in the maritime sector: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

50 https://www.bbc.com/news/world-europe-24539417

co przyczyniło się do dużych strat gospodarczych i finansowych[51].

3

Fala ataków ransomware na port w Barcelonie w 2018 roku[52].

4

Ataki ransomware na port w San Diego w 2018 roku[53].

W 2019 roku ENISA opublikowała raport „Port Cybersecurity - Good practices for cybersecurity in the maritime sector", podsumowujący wyniki badań przeprowadzonych w 13 europejskich portach, zlokalizowanych w 11 krajach członkowskich. Ankietowani, zapytani o największe wyzwania z obszaru cyberbezpieczeństwa, z jakimi mierzą się porty morskie wskazali:

- Niską świadomość w obszarze cyberbezpieczeństwa wśród pracowników portów morskich (w tym również brak „kultury" cyfrowej i przywiązanie do wykonywania zadań w sposób manualny).
- Brak szkoleń dla pracowników.
- Niedostatek zasobów finansowych i czasowych, które mogłyby być przeznaczone na rzecz rozwoju cyberbezpieczeństwa.
- Niedobór kompetencji i zasobów ludzkich w obszarze cyber.
- Złożoność ekosystemu portowego, konieczność uwzględnienia powiązanych ze sobą działań wielu interesariuszy.
- Konieczność znalezienia odpowiedniego kompromisu pomiędzy zwiększeniem efektywności z użyciem nowych technologii i cyberbezpieczeństwem.
- Przestarzałe systemy (szczególnie OT).
- Brak regulacji (jedynie dyrektywa NIS, a ona obejmuje wybrane podmioty w podsektorze).
- Trudność w nadążeniu nad ciągle zmieniającym się krajobrazem cyberzagrożeń.
- Skomplikowane systemy IT i OT, które są wykorzystywane w portach morskich.
- Wyzwania związane z łańcuchem dostaw.
- Nowe zagrożenia, które pojawiły się wraz z cyfryzacją portów morskich.

Sektor transportu wodnego a Ustawa o krajowym systemie cyberbezpieczeństwa

Zgodnie z Rozporządzeniem Rady Ministrów z dnia 11 września 2018 roku w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, w podsektorze transportu wodnego wyznaczono osiem usług kluczowych:

- Transport morski pasażerski.
- Transport morski towarów.
- Transport wodny śródlądowy pasażerski.
- Transport wodny śródlądowy towarów.
- Zarządzanie portem morskim.
- Obsługa transportu morskiego pasażerów i towarów.
- Działalność usługowa wspomagająca transport morski.
- Monitorowanie ruchu statków.

51 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

52 https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/

53 https://www.darktrace.com/en/blog/troubled-waters-cyber-attacks-on-san-diego-and-barcelonas-ports
https://www.portofsandiego.org/press-releases/general-press-releases/port-san-diego-releases-additional-information-cybersecurity

Poniższa tabela przedstawia dokładne kryteria uznania usługi za kluczową, zgodnie ze wspomnianym Rozporządzeniem.

Usługa	Kryteria
Transport morski pasażerski	Przewóz minimum 100 tys. pasażerów rocznie.
Transport morski towarów	Przewóz minimum 1 mln ton towarów rocznie.
Transport wodny śródlądowy pasażerski	Przewóz co najmniej 30% pasażerów transportu pasażerskiego żeglugi śródlądowej.
Transport wodny śródlądowy towarów	Realizowanie co najmniej 40% przewozów towarów rocznie w transporcie śródlądowym krajowym.
Zarządzanie portem morskim	Zarządzanie portem należącym do sieci bazowej TEN-T, o której mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 1315/2013 z dnia 11 grudnia 2013 r. w sprawie unijnych wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej i uchylającym decyzję nr 661/2010/UE (Dz. Urz. UE L 348/1 z 20.12.2013, str.1).
Obsługa transportu morskiego pasażerów i towarów	Obsługa minimum 100 tys. pasażerów przewożonych w transporcie morskim rocznie. Zależność innych sektorów: energii, transportu oraz podsektora transport kolejowy. Obsługa minimum 3 mln ton towarów przewożonych w transporcie morskim rocznie.
Działalność usługowa wspomagająca transport morski	Każdy podmiot wykonujący usługi, o których mowa w art. 1 ust. 2 lit. a, c, f oraz g rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/352 z dnia 15 lutego 2017 r. ustanawiające ramy w zakresie świadczenia usług portowych oraz wspólne zasady dotyczące przejrzystości finansowej portów (Dz. Urz. UE L 57/1 z 03.03.2017, str. 1).
Monitorowanie ruchu statków	Gromadzenie i dystrybucja informacji związanej z bezpieczeństwem ruchu morskiego na obszarze terytorialnego zakresu działania dyrektorów urzędów morskich określonym w przepisach wydanych na podstawie art. 40 ust. 1 i 2 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej.

Wyniki badania

Minister właściwy ds. transportu (obecnie Ministerstwo Infrastruktury – organ właściwy ds. cyberbezpieczeństwa) wyznaczył 10 operatorów usług kluczowych w podsektorze transportu wodnego. Wszyscy wzięli udział w badaniu.

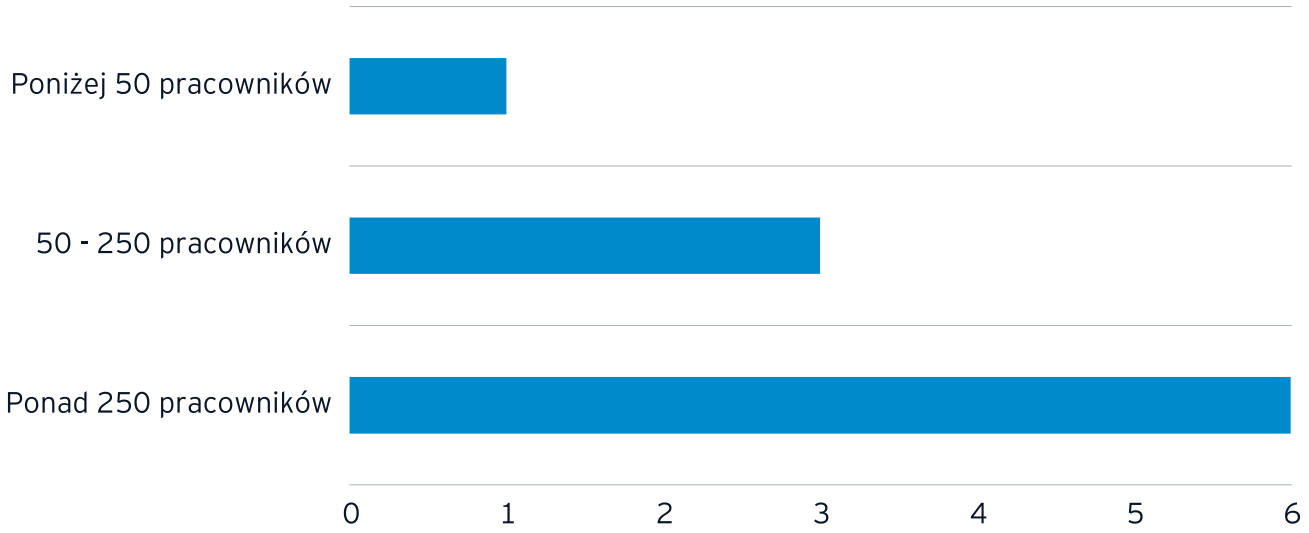
Warto przy tym zaznaczyć, że z uwagi na zmiany związane z Dyrektywą NIS2 zakres podmiotów objętych Ustawą będzie z pewnością szerszy. Może to być wyzwanie, zwłaszcza w kontekście bezpieczeństwa łańcucha dostaw.

Organizacja

W przeprowadzonym badaniu pojawiło się wiele pytań dotyczących parametrów funkcjonowania, a także struktury organizacji. W badaniu wzięło udział 10 operatorów usług kluczowych (OUK), czyli wszyscy wyznaczeni przez organ właściwy ds. cyberbezpieczeństwa na podstawie decyzji administracyjnej. Poniżej zostały zaprezentowane wyniki przeprowadzonego badania.

Badane przez nas podmioty to przeważnie przedsiębiorstwa duże, gdzie liczba pracowników jest większa niż 250 osób (6 odpowiedzi). Następnie wskazano średnie przedsiębiorstwa o wielkości w przedziale 50 < 250 pracowników (3 odpowiedzi). Jeden badany podmiot OUK z transportu wodnego ma mniej pracowników niż 50 osób, więc należy do mniejszych przedsiębiorstw.

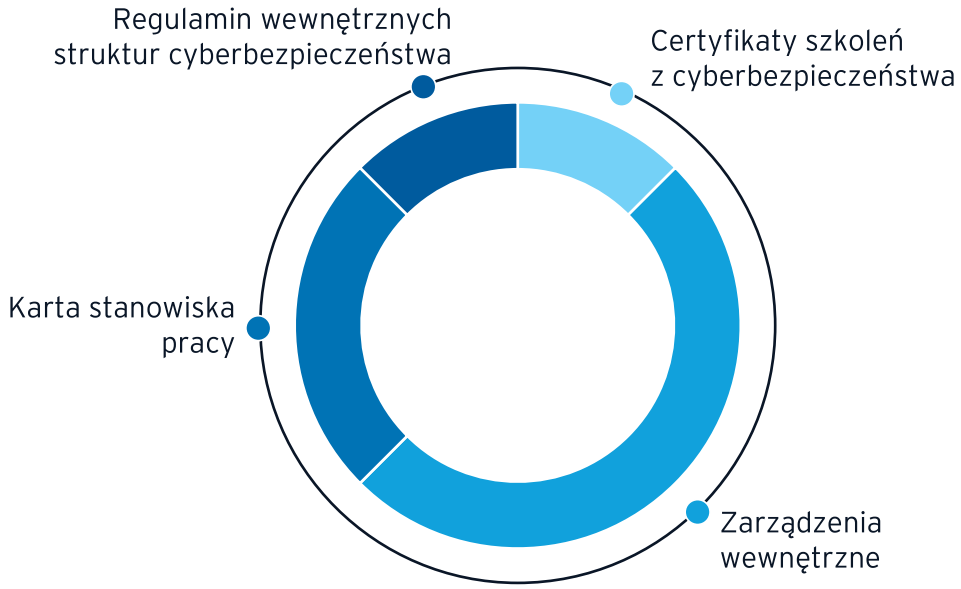
Wielkość OUK w podsektorze transportu wodnego



Na dzień przeprowadzania badania, dziewięć OUK z sektora transportu zadeklarowało, że wskazało osobę kontaktową do odpowiedniego CSIRT-u, z czego jeden podmiot zgłosił już dwie takie osoby. Wyznaczenie osoby kontaktowej jest obowiązkowe i wynika z UoKSC.

Najczęściej osoba kontaktowa ds. cyberbezpieczeństwa umiejscowiona jest w Dziale informatyki bądź komórce o podobnej nazwie (6 odpowiedzi). Kolejne umiejscowienie osoby kontaktowej to wewnętrzne struktury odpowiedzialne za bezpieczeństwo (2 odpowiedzi). W jednym przypadku osoba kontaktowa ds. cyberbezpieczeństwa podlega bezpośrednio Dyrektorowi, w innym natomiast znajduje się w pionie finansowym.

Dokumenty określające kompetencje osoby kontaktowej ds. cyberbezpieczeństwa



Operatorzy usług kluczowych zdefiniowali role osoby kontaktowej, ale w niewystarczającym stopniu zdefiniowali jej obowiązki i zależności z innymi rolami związanymi w organizacji z bezpieczeństwem. Rola ta jest przede wszystkim silnie połączona z działami IT, co w przypadku nowych obowiązków, wynikających z Dyrektywy NIS2 (bezpieczeństwo łańcucha dostaw, powiązanie cyberbezpieczeństwa i zarzadzania kryzysowego) może rodzić wyzwania.

Środki finansowe na cyberbezpieczeństwo są najczęściej

budżetowane w dziale w Dziale IT (9 odpowiedzi). W jednym podmiocie są one ulokowane w różnych komórkach w zależności od podejmowanych działań (m.in. budowlane, informatyczne, ochrona). Niektóre podmioty wskazywały na trudność w określeniu dokładnie wykorzystywanej kwoty na cyberbezpieczeństwo, gdyż są one składową budżetu Działu IT i nie są planowane jako osobne środki.

Procesy

W przypadku 9 podmiotów szacowanie ryzyka dla systemów teleinformatycznych jest częścią korporacyjnego zarządzania ryzykiem. Przeprowadzone jest ono dla systemów zdefiniowanych w organizacji jako usługi kluczowe (transport morski pasażerski, transport morski towarów, transport wodny śródlądowy pasażerski, transport wodny śródlądowy towarów, zarządzanie portem morskim, obsługa transportu morskiego pasażerów i towarów, działalność usługowa wspomagająca transport morski, monitorowanie ruchu statków).

Aż 8 podmiotów potwierdziło, że w ich organizacji zostały zmapowane procesy i ich zależności od systemów teleinformatycznych. Natomiast wszyscy ankietowani odpowiedzieli, że w ich organizacji zostali zidentyfikowani odbiorcy usług zależnych od ich systemów teleinformatycznych oraz, że posiadają swoje wewnętrzne polityki cyberbezpieczeństwa w zakresie IT oraz OT. Jest to bardzo istotne w kontekście wymagań, które stawia przed operatorami Dyrektywa NIS2.

Na pytanie „Które z zadań operatorów usług kluczowych wymienionych w Ustawie o krajowym systemie cyberbezpieczeństwa są realizowane (...)?"[54] sześć podmiotów odpowiedziało, że realizuje wszystkie zadania wymienione w Ustawie.

Jako największe wyzwania w procesie wdrażania Ustawy o krajowym systemie cyberbezpieczeństwa, operatorzy usług kluczowych wymienili:

- Prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem.
- Bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej.
- Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym.
- Cyberbezpieczeństwo i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej.
- Stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, dokładniej dbałość o aktualizację oprogramowania.

Operatorzy usług kluczowych podsektora transportu wodnego przekazują informacje o poziomie cyberbezpieczeństwa swojemu zarządowi. Najczęściej odbywa się to w formie sformalizowanego raportu, ale także drogą mailową lub poprzez pisma wewnętrzne, w szczególności w przypadku naruszenia bezpieczeństwa teleinformatycznego.

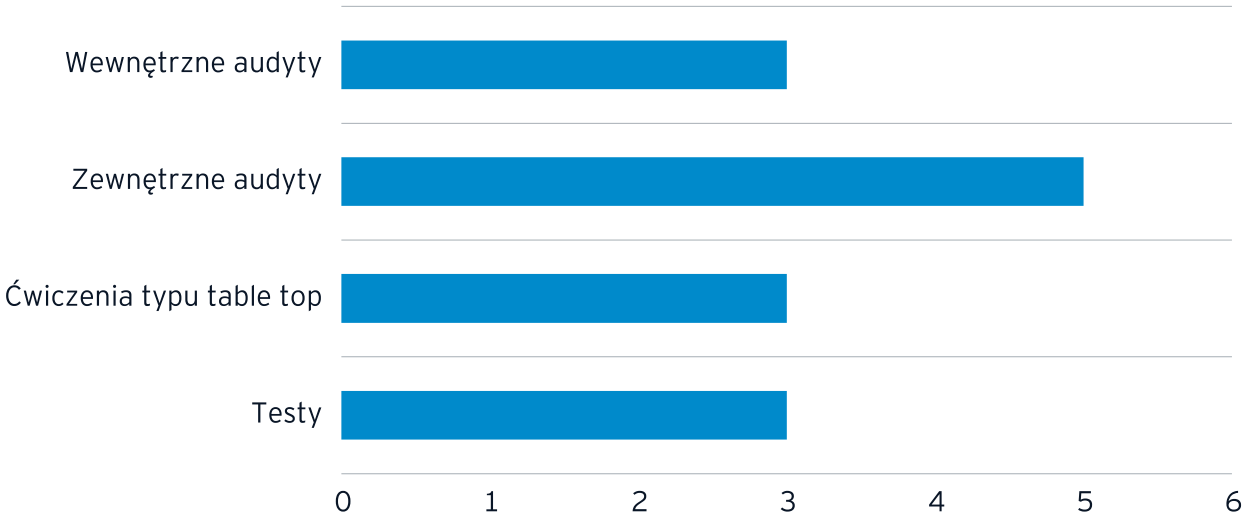
Wszystkie podmioty z podsektora transportu wodnego opracowały plany bądź procedury reagowania na incydenty. Podobnie w przypadku opracowania planów przywracania działania po zaistniałym incydencie, tu tylko 1 podmiot nie ma wciąż opracowanych dokumentów.

54 Wymienione w Ustawie o krajowym systemie cyberbezpieczeństwa zadania operatorów usług kluczowych: 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym: a) utrzymanie i bezpieczną eksploatację systemu informacyjnego, b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej, d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym; 3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej; 4) zarządzanie incydentami; 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym: a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, b) dbałość o aktualizację oprogramowania, c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym, d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa; 6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa, wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa; zapewnia użytkownikowi usługi kluczowej dostęp do wiedzy pozwalającej na zrozumienie zagrożeń; cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej; przekazuje organowi właściwemu do spraw cyberbezpieczeństwa dane, o których mowa w art. 7 ust. 2 pkt 8 i 9, nie później niż w terminie 3 miesięcy od zmiany tych danych.

Regularne kontrole tych procedur odbywają się najczęściej poprzez:

- Testy.
- Ćwiczenia typu table-top.
- Zewnętrzne audyty.
- Audyty wewnętrzne.

Testowanie procedur odpowiedzi na incydenty



Bardzo ważnym obowiązkiem ustawowym jest zgłaszanie do właściwego CSIRT poziomu krajowego incydentów poważnych.[55] W związku z tym niezwykle istotne jest właściwe zaklasyfikowanie tego incydentu, zgodnie z progami określonymi w Rozporządzeniu Rady Ministrów z 31 października 2018 r. w sprawie progów uznania incydentu za poważny. Zadanie jest pełnione przez różne komórki w organizacjach. Natomiast jeśli chodzi o to, kto najczęściej dokonuje klasyfikacji incydentu zgodnie z UoKSC (incydenty poważne), to respondenci wymienili takie jednostki:

- Zespół SOC (2 odpowiedzi).
- Zespół odpowiedzialny za zarządzanie kryzysowe/ciągłość działania (2 odpowiedzi).
- Zewnętrzny SOC (1 odpowiedź).
- Główny Informatyk (1 odpowiedź).
- Inspektor bezpieczeństwa informacji (1 odpowiedź).
- Kierownik działu bezpieczeństwa (1 odpowiedź).
- Specjalista ds. cyberbezpieczeństwa (1 odpowiedź).
- Powołany Oficer ds. Cyberbezpieczeństwa po konsultacjach z zespołem specjalistów (1 odpowiedź).

6 respondentów wskazało, że posiada wewnętrzną (opracowana na własne potrzeby) klasyfikacje incydentów i zagrożeń. Opracowane na własny użytek klasyfikacje bardzo się od siebie różnią. Niektóry OUK przyjęli kryterium priorytetu ważności (tj. niski, średni, wysoki), inni natomiast zakwalifikowali incydenty pod kątem obszaru działalności jakiego dotyczą (morze/ląd) oraz systemu/elementu infrastruktury którego dotykają. Duża część klasyfikacji to rozbudowana na własne potrzeby klasyfikacja zaproponowana przez vendora.

55 Według UoKSC incydent poważny to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej.

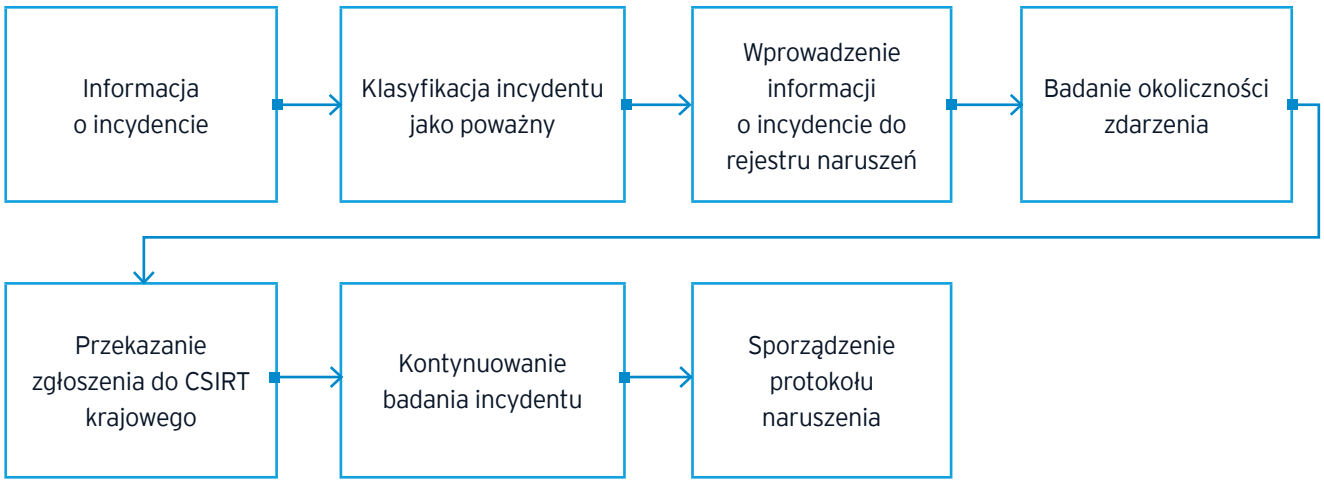
9 na 10 respondentów potwierdziło (1 ankietowany wstrzymał się od odpowiedzi), że kryteria definiujące incydent jako poważny w Rozporządzeniu Rady Ministrów w sprawie progów uznania incydentu za poważnyadekwatne[56], ponieważ:

- Kładą nacisk na kwestię najbardziej istotną - zagrożenie dla życia i zdrowia załóg/pasażerów.
- Próg czasowy dotyczący niemożności świadczenia usług kluczowych w trakcie cumowania został zdefiniowany zgodnie z realiami panującymi w branży (48h).

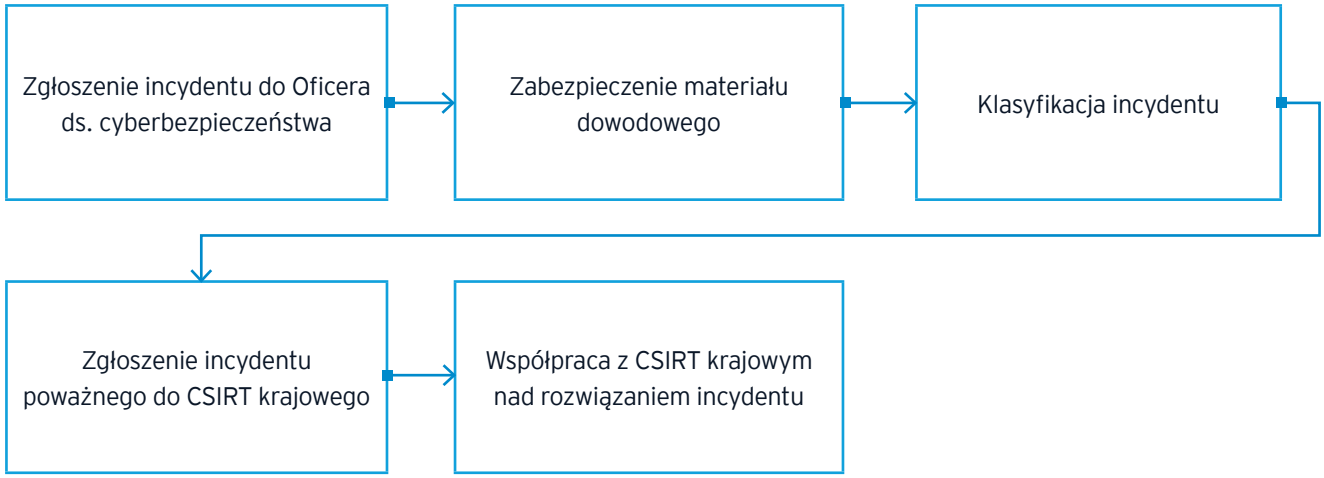
Proces raportowania i obsługi incydentu u OUK - studium przypadku

Proces raportowania i obsługi incydentu różnią się w zależności od wielkości OUK oraz tego czy dany podmiot ma wewnętrzny SOC, czy też wykupuje te usługi na ryku. Jednak wszystkie podmioty uwzględniły w swoich procedurach konieczność zgłoszenia incydentu do CSIRT-u poziomu krajowego, oraz klasyfikacje incydentu, zgodnie z ustawą. Poniżej dwa studia przypadku.

Studium 1



Studium 2



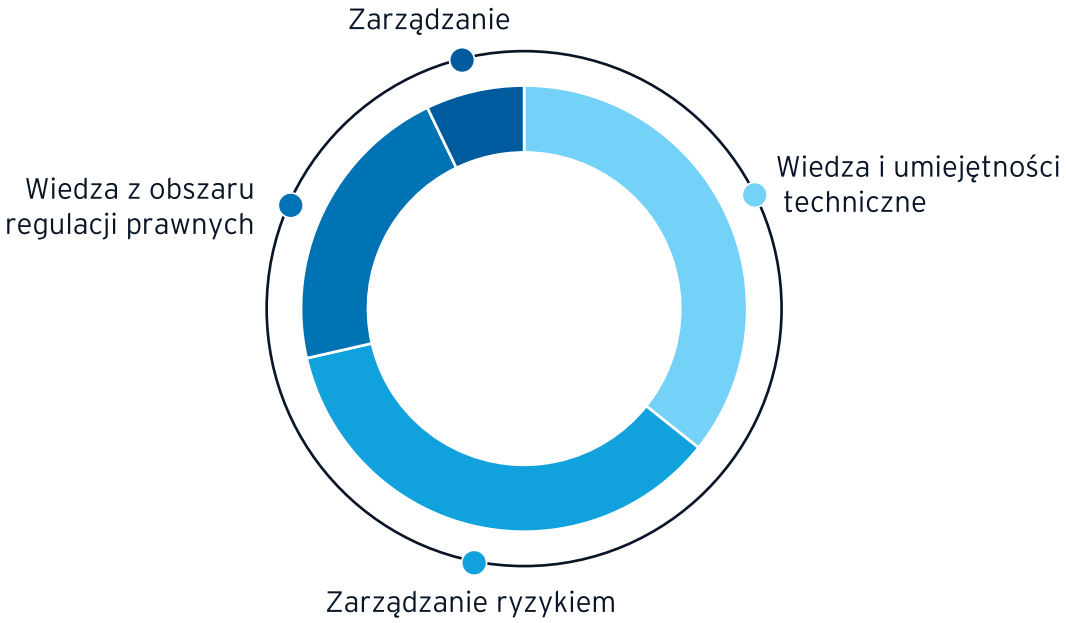
56 Rozporządzeniu Rady Ministrów w sprawie progów uznania incydentu za poważny (incydent dotyczący armatorów w transporcie morskim pasażerów podczas żeglugi, incydent dotyczący armatorów w transporcie morskim pasażerów podczas cumowania, incydent dotyczący armatorów w transporcie morskim towarów podczas żeglugi, incydent dotyczący armatorów w transporcie morskim towarów podczas cumowania, incydent dotyczący armatorów w transporcie wodnym śródlądowym pasażerskim, incydent dotyczący armatorów w transporcie wodnym śródlądowym towarów, incydent dotyczący funkcjonowania organów zarządzających portami, incydent dotyczący bezpieczeństwa organów zarządzających portami, incydent dotyczący funkcjonowania organów zarządzających obiektami portowymi, incydent dotyczący bezpieczeństwa organów zarządzających obiektami portowymi, incydent dotyczący funkcjonowania podmiotów prowadzących na terenie portu działalność wspomagającą transport morski, incydent dotyczący bezpieczeństwa podmiotów prowadzących na terenie portu działalność wspomagającą transport morski, incydent dotyczący funkcjonowania VTS (Służba Kontroli Ruchu Statków), incydent dotyczący bezpieczeństwa VTS (Służba Kontroli Ruchu Statków).

Zespół

Wszyscy respondenci potwierdzili, że zespół zajmujący się bezpieczeństwem teleinformatycznym posiada wiedzę i umiejętności do realizacji wyznaczonych im ról i odpowiedzialności.

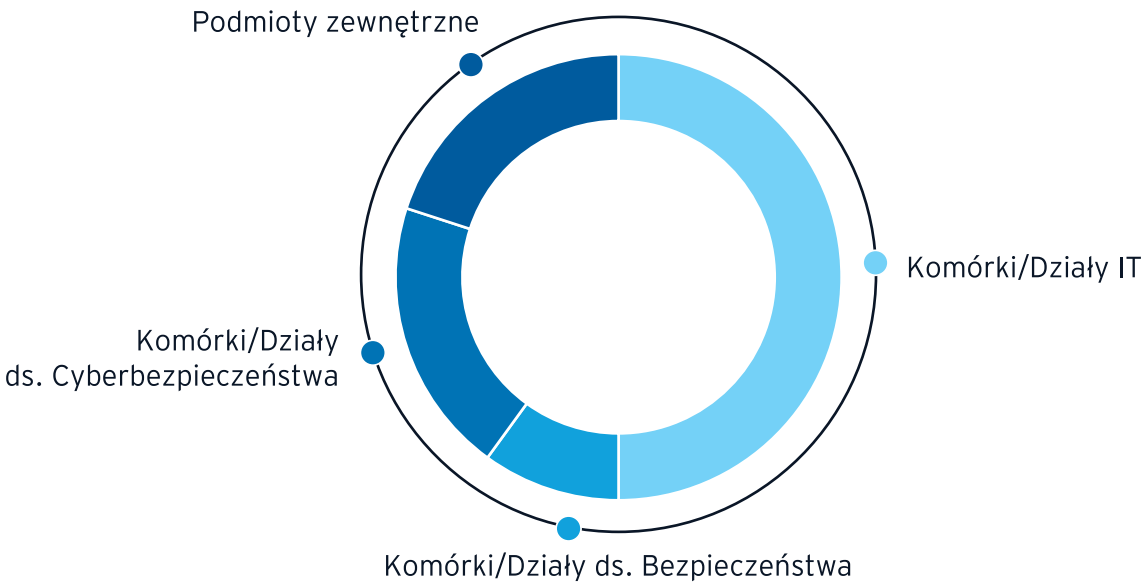
Zdecydowana większość badanych podmiotów ma zdefiniowane odpowiednie role i obszary odpowiedzialności związane z cyberbezpieczeństwem (9 na 10 podmiotów). Większość podmiotów posiada również dedykowany zespół do działań związanych z zarządzaniem cyberbezpieczeństwem (7 na 10 odpowiedzi). Są to zespoły interdyscyplinarne, gdzie obok specjalistów z wiedzą techniczną, obecni są specjaliści z obszaru zarządzania ryzykiem, regulacji prawnych oraz managerowie.

Kompetencje zespołów odpowiedzialnych za cyberbezpieczeństwo



OUK wskazali, że najczęściej zespoły zajmujące się cyberbezpieczeństwem są ulokowane głównie w komórkach związanych z IT, czasem istnieje osobna komórka dedykowana do tematyki cyberbezpieczeństwa. Są też jednak przypadki gdy cyberbezpieczeństwo umieszczone zostało w strukturze działu bezpieczeństwa. Część podmiotów przyznała natomiast, że nie ma takich osób w strukturach swojej organizacji, i że jest w tym zakresie zależna od firm zewnętrznych.

Zespoły ds. cyberbezpieczeństwa w strukturze OUK



OUK wskazali, że szkolenia dla pracowników związanych z obszarem cyberbezpieczeństwa realizowane są z takich obszarów:

- Zarządzanie incydentami.
- Źródła cyberzagrożeń.
- Zarządzanie bezpieczeństwem infrastruktury sieciowej.
- Zarządzanie bezpieczeństwem aplikacji internetowych.
- Bezpieczeństwo stacji roboczych.
- Projektowanie systemów analizy logów oraz zarządzania bezpieczeństwem.
- Automatyzacja obsługi incydentów bezpieczeństwa.
- Zarządzanie podatnościami, analiza i zarządzanie ryzykiem w obszarze cyberbezpieczeństwa
- Zarządzanie bezpieczeństwem urządzeń mobilnych.
- Konfiguracja i praktyczne wykorzystanie narzędzia Splunk do analizy logów i tworzenia alertów.
- Wykrywanie zagrożeń, ochrona sieci i systemów ICS/OT/SCADA.
- Monitorowanie Sieci OT (IPS/IDS).
- Zagrożenia IT.
- Bezpieczeństwo informacji.
- RODO itp.
- Systemy zarządzania ryzykiem (MoR, ISO 27001).
- Systemy zarządzania ciągłością działania.
- Bezpieczeństwo systemów IT.
- Administracja i zarządzanie systemami oraz infrastrukturą IT.
- Technologie sieciowe.
- Szkolenia oparte o ISO 27001.
- Webinary dotyczące nowych technologii.
- Konfiguracja i obsługa wdrożonych systemów bezpieczeństwa.

Ponadto część OUK z podsektora transportu wodnego realizują szkolenia z aspektów cyberbezpieczeństwa dla całej organizacji. Takie szkolenia odbywają się najczęściej z częstotliwością raz na dwa lata. Jeden podmiot odpowiedział, że w jego organizacji szkolenia dla całej organizacji z tematów związanych z cyberbezpieczeństwem odbywają się raz na 6 miesięcy, inny natomiast, że są realizowane na bieżąco.

W badaniu zapytano również OUK jakie jest główne kryterium wyboru dostawców z obszaru cyberbezpieczeństwa. Respondenci odpowiedzieli następująco:

- Jakość usług (7 odpowiedzi).
- Cena (6 odpowiedzi).
- Wymagania norm ISO/INC 24001 oraz ISO 22301 (1 odpowiedź).
- stosunek ceny do jakości usług (1 odpowiedź).
- usługa zlokalizowana w Polsce (1 odpowiedź).
- dotychczasowa współpraca (1 odpowiedź).

8 na 10 OUK wskazało, że w przypadku usług kluczowych (transport morski pasażerski, transport morski towarów, transport wodny śródlądowy pasażerski, transport wodny śródlądowy towarów, zarządzanie portem morskim, obsługa transportu morskiego pasażerów i towarów, działalność usługowa wspomagająca transport morski, monitorowanie ruchu statków) dostawcy tych usług weryfikowani są pod kątem bezpieczeństwa teleinformatycznego.

Jako największe wyzwania w procesie wdrażania Ustawy o krajowym systemie cyberbezpieczeństwa OUK wymienili:

- Szerokie spektrum wymagań stawianych przez ustawę, w tym:
  - Stworzenie spójnego i elastycznego Systemu Zarządzania Ryzykiem, który umożliwia skuteczne identyfikację, adresowanie i zarządzanie ryzykiem zarówno związanym z cyberbezpieczeństwem, jak i tymi, które dotyczą innych obszarów działalności organizacji.
  - Zdefiniowanie właścicieli usług kluczowych w rozproszonej infrastrukturze.
  - Wymogi organizacyjno-techniczne, określone w Rozporządzeniu do Ustawy.
  - Opracowanie zasad tworzenia oraz nadzoru nad dokumentacją systemową.
- Pozyskanie środków na realizację działań związanych z przystosowaniem się do ustawy.

- Problemy kadrowe (brak specjalistów z branży cyber oraz niemożliwość zagwarantowania odpowiedniego uposażenia).
- Tempo wdrożeń, związane z byciem członkiem Grupy i koniecznością uzyskania zgody centrali.
- Pozyskanie i dostosowanie infrastruktury do potrzeb UoKSC.
- Brak Sektorowych Zespołów Cyberbezpieczeństwa rozumiejących specyfikę sektora.

Aż siedem podmiotów ma świadomość zmian wprowadzanych przez Dyrektywę NIS2 i definiują następujące wyzwania w tym zakresie:

- Zapewnienie niezawodności i bezpieczeństwa cyfrowego sieci i systemów informatycznych.
- Zapewnienie odpowiedniego poziomu przygotowania spółki na wystąpienie poważnych incydentów bezpieczeństwa sieci o szerokim zasięgu.
- Zapewnienie działania wewnętrznego SOC w systemie 24/7/365.
- Brak środków na modernizacje i rozbudowę usług wchodzących w skład usługi kluczowej.
- Problemy z zapewnieniem bezpieczeństwa komunikacji sieciowej spowodowanej rozproszeniem organizacji.
- Słaba infrastruktura teleinformatyczna województwa, brak inwestycji operatorów telekomunikacyjnych w łącza światłowodowe poza dużymi miastami.
- Skuteczna analiza ryzyka.
- Zabezpieczenie budżetowe i osobowe.

Część podmiotów wskazało, że obecnie świadomość nadchodzących zmian nie wiąże się jednak z głęboką analizą wyzwań jakie mogą przynieść nowe regulacje prawne w ich organizacji.

EY | Building a better working world

Celem działalności EY jest budowanie lepiej funkcjonującego świata - poprzez wspieranie klientów, pracowników i społeczeństwa w tworzeniu trwałych wartości - oraz budowanie zaufania na rynkach kapitałowych.

Wspomagane przez dane i technologię, zróżnicowane zespoły EY działające w ponad 150 krajach, zapewniają zaufanie dzięki usługom audytorskim oraz wspierają klientów w rozwoju, transformacji biznesowej i działalności operacyjnej.

Zespoły audytorskie, consultingowe, prawne, strategiczne, podatkowe i transakcyjne zadają nieoczywiste pytania, by móc znaleźć nowe odpowiedzi na złożone wyzwania, przed którymi stoi dziś świat.