Podsumowanie prac Zespołów Grupy Roboczej ds. Cyberbezpieczeństwa w 2018 r.

Warszawa, dn. 19.12.2018 r.

Spis treści

I. Zespół I – Duże Przedsiębiorstwa

1. Adresaci działań edukacyjnych:

Najwięksi przedsiębiorcy z kluczowych sektorów gospodarki, Operatorzy Usług Kluczowych (OUK).

CEL:

Podnoszenie świadomości organów zarządczych przedsiębiorstw z grupy docelowej w kontekście wejścia w życie Ustawy o krajowym systemie cyberbezpieczeństwa (KSC) wdrażającej dyrektywę NIS.

Skład Zespołu:

Jacek Niedziałkowski – Przewodniczący	
Wiesław Paluszyński	Robert Siudak
Jacek Czech	Paweł Gruszecki
Artur Piechocki	Cyprian Gutkowski
Daniel Siciński	Aleksandra Kopciuch
Marek Godala	Andrzej Kozłowski
Tomasz Chomicki	Jerzy Waśkiewicz
Sebastian Christow	Julia Jędraszek
Janusz Żmudziński	Paweł Gruszecki
Maciej Smyk	Tomasz Kędziora
Błażej Szymczak	Jarosław Majczyk
Jędrzej Trzciński	Rafał Rojewski
Maciej Smyk	Krzysztof Białek
	Dominik Dobek

2. Operatorzy Usług Kluczowych (OUK)

Ogólne założenia i wytyczne dotyczące działań edukacyjnych w grupie docelowej.

Głównym założeniem niniejszego dokumentu jest walka ze stereotypem, że duże przedsiębiorstwa, ważne dla polskiej gospodarki realizują odpowiednie budżety i są dobrze przygotowane do zadań związanych z cyberbezpieczeństwem.

Praktyka dnia codziennego pokazuje, że jest bardzo szerokie spektrum przygotowania i poziomu dojrzałości w zakresie cyberbezpieczeństwa, od bardzo dobrego (głównie w sektorze finansowym) do niemal zerowego.

W ustawie o Krajowym Systemie Cyberbezpieczeństwa, mowa jest o:

1) operatorach usług kluczowych (OUK), czyli m.in. największe banki, firmy z sektora energetycznego, przewoźnicy lotniczy i kolejowi, armatorzy, szpitale;

2) dostawcach usług cyfrowych (DUC), czyli m.in. internetowych platformach handlowych;

3) organach właściwych (OW), czyli instytucjach publicznych, w których kompetencjach znajdzie się nadzór nad danym istotnym sektorem dla gospodarki np. dla firm zajmujących się transportem lotniczym organem właściwym jest minister infrastruktury;

Skupiając się na grupie operatorów usług kluczowych (OUK) oraz operatorów usług kluczowych jednocześnie wchodzących w skład infrastruktury krytycznej, należy zwrócić uwagę, że bezpośrednimi adresatami przekazu powinni być Prezesi, Zarządy, Rady Nadzorcze, tych firm.

Takie podejście wskazane jest ze względu na fakt, że odpowiedzialność i czynności w obszarze cyberbezpieczeństwa zazwyczaj postrzegane są jako działania techniczno - operacyjne i delegowane są do CIO lub CTO lub członków Zarządu odpowiedzialnych dotychczas za bezpieczeństwo fizyczne.

Utrudnia to lub wręcz uniemożliwia podjęcie kompleksowych działań dotyczących całych organizacji.

W przekazie należy podkreślić, że wymagane **działania w obszarze Cyberbezpieczeństwa są kwestiami i wymogami organizacyjno-procesowymi <u>będącymi w ścisłej kompetencji Zarządów.</u>**

Głównym celem działań edukacyjnych powinno być uświadomienie:

- wejścia w życie przepisów ustawy oraz nałożonych w ten sposób obowiązków,

- faktu, że cyberbezpieczeństwo to procesy organizacyjne będące w odpowiedzialności Zarządów, podlegające ciągłym zmianom oraz wymagający cyklicznego przeglądu i analizy ryzyka
- odpowiedzialności karnej i finansowej za brak działań.

Dodatkowy przekaz powinien zmierzać do uświadomienia:

- konsekwencji ekonomicznych i społecznych spełnienia się ryzyk
- konsekwencji wizerunkowych wynikających ze spełnienia się ryzyk
- najczęstszych scenariuszy prowadzących do spełnienia się ryzyk

Należy tu wyraźnie podkreślić, że przekaz powinien odbywać się przy użyciu nie-technologicznego języka komunikacji.

Proponowane do przygotowania materiały i działania edukacyjne:

- Wstępne i okresowe badanie świadomości Zarządów
- Krótki poradnik ISO2700x i zachęta do certyfikacji, Case Study
- White Paper – Dobre Praktyki / Wzorzec (prosto o zagrożeniach dla osób nietechnicznych)
- Konferencja dla Zarządów OUK z omówieniem tematyki bezpieczeństwa i ryzyk
- Nagrody / Wyróżnienia / Certyfikaty – (motywatory) leżące w kompetencji organów uprawnionych np. OW, Zarząd, Rada Nadzorcza.
- E-Learning: np. krótki materiał wideo uświadamiający wymogi i konsekwencje dla Zarządów oraz jak dojść do spełnienia wymogów (x kroków Step by Step)
- Ankieta Self Assessment dla Zarządów i Pełnomocników – nasza świadomość / nasza gotowość w zakresie KSC
- Strona internetowa / Blog / Zamknięte Forum dla Pełnomocników KSC w Zarządach oraz Departamentów odpowiedzialnych za KSC w organach nadzorczych.

Celem tych działań edukacyjnych jest dotarcie z treścią do jak największej liczby odbiorców:

- Poprzez Organy Właściwe w porozumieniu z Ministerstwem Cyfryzacji
- Pisma / Broszura informacyjna sygnowane przez Ministra Cyfryzacji w zakresie ogólno-ustawowym.
- Komunikaty Ministra Cyfryzacji propagowane przez PAP i media w zakresie ogólno-ustawowym.
- Konferencja dla Zarządów OUK
- Mailing

3. Zadania edukacyjne, są to zadania dla różnych interesariuszy rynku cyberbezpieczeństwa.

Działania krótkoterminowe

Informacja dla Zarządów operatorów usług kluczowych

W perspektywie krótkoterminowej, a nawet niezwłocznie, do zarządów OUK oprócz decyzji administracyjnej należy dostarczyć informację o powstaniu nowych obowiązków wynikających z wprowadzenia w życie ustawy KSC. Pismo o treści zawierającej elementy podane poniżej ma za zadanie sprowokować natychmiastowe działania OUK związane z oceną stanu przygotowania przedsiębiorstwa do funkcjonowania w nowym otoczeniu prawnym i współczesnymi wyzwaniami związanym z cyberbezpieczeństwem.

Komunikacja ta powinna być skierowana do organów zarządczych, najlepiej do Prezesów, Dyrektorów Generalnych i wskazane jest nadanie pismu wagi np. przez podpis Ministra Organu Właściwego.

Poniżej przykładowa treść komunikatu. Jest tylko sugestia, która przede wszystkim wskazuje dobór retoryki i języka komunikacji. Przy redagowaniu rzeczywistego pisma należy wziąć pod uwagę treść decyzji administracyjnej dostarczonej do OUK tak, żeby te dokumenty uzupełniały się:

W dniu 28 sierpnia 2018 r. weszła w życie **ustawa o krajowym systemie cyberbezpieczeństwa** (Dz. U. 2018 poz.1560, stanowiąca wdrożenie unijnej dyrektywy NIS.

Przepisy te stanowią odpowiedź na rosnące zagrożenia związane z cyberatakami oraz mają na celu stworzenie spójnego systemu zabezpieczeń przed nimi na szczeblu krajowym.

Obecnie działalność większości firm opiera się na wykorzystywaniu nowoczesnych rozwiązań informatycznych dla wspierania procesu zarządzania, produkcji lub świadczenia usług. Stosowanie tych technologii wiąże się jednocześnie z ryzykiem wykorzystania istniejących w systemach podatności przez cyberprzestępców. Włamanie do niezabezpieczonej sieci firmowej, zainfekowanie systemu wirusem w wyniku nieopatrznego otworzenia przez pracownika załącznika do maila, zablokowanie dostępu do danych połączone z żądaniem

okupu, to tylko niektóre ze scenariuszy, które mogą spotkać obecnie niemal każdego przedsiębiorcę, narażając go na dotkliwe konsekwencje. Tym samym niezmiernie istotne jest wdrożenie kompleksowego systemu zabezpieczeń przed takimi atakami, szczególnie przez przedsiębiorców świadczących usługi o istotnym znaczeniu dla dobra publicznego. Obowiązek ten obejmuje operatorów, wobec których zostanie wydana decyzja o uznaniu ich za operatorów usług kluczowych.

4. Nowe przepisy w obszarze cyberbezpieczeństwa obowiązujące OUK

Nowe obowiązki dla operatorów usług kluczowych

Poza określeniem ram krajowej strategii cyberbezpieczeństwa, nowa ustawa nakłada także szereg obowiązków na przedsiębiorców dostarczających usługi kluczowe dla utrzymania krytycznej działalności społecznej lub gospodarczej (tzw. operatorzy usług kluczowych). Obejmuje to operatorów działających w sektorach: energetyki, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia i dystrybucji wody pitnej oraz infrastruktury cyfrowej. Przepisom ustawy podlegają jednak wyłącznie przedsiębiorcy mający największy wpływ na działanie danego sektora, wobec których zostanie wydana decyzja o uznaniu ich za operatorów usług kluczowych.

Pierwsza kategoria obowiązków nałożonych na operatorów wiąże się z koniecznością przyjęcia w organizacji programu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, obejmującego systematyczne szacowanie i zarządzanie ryzykiem oraz wdrażanie proporcjonalnych do niego technicznych i organizacyjnych środków bezpieczeństwa. Wiąże się to z koniecznością przyjęcia stosownych procedur, polityk oraz dokumentacji z zakresu cyberbezpieczeństwa oraz wdrożenia technicznych środków zapobiegających i ograniczających wpływ incydentów cyberbezpieczeństwa. Z wymogami tymi związany jest również obowiązek prowadzenia co najmniej raz na dwa lata audytu bezpieczeństwa systemu informacyjnego.

Drugi rodzaj obowiązków obejmuje notyfikację występowania poważnych incydentów cyberbezpieczeństwa do specjalnie utworzonych zespołów reagowania na incydenty (tzw. CSIRT) oraz współdziałanie z tymi zespołami w obsłudze takich incydentów.

W celu realizacji powyższych obowiązków operatorzy zobowiązani są wyodrębnić w swojej organizacji wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zlecić realizację usług w tym zakresie wyspecjalizowanym podmiotom. Ponadto w zakresie realizowania obowiązków wynikających z nowych przepisów operatorzy podlegają nadzorowi organów właściwych ds. cyberbezpieczeństwa (tj. ministrów odpowiedzialnym za dany sektor gospodarki), które są uprawnione przeprowadzać w tym zakresie kontrole.

OBOWIĄZKI OPERATORA USŁUGI KLUCZOWEJ zgodnie z ustawą (terminy biegną od momentu otrzymania decyzji administracyjnej uznającej podmiot za operatora usługi kluczowej)		
Po 3 miesiącach	Po 6 miesiącach	Po 12 miesiącach
dokonuje szacowania ryzyka dla swoich usług kluczowych	wdraża odpowiednie i adekwatne do oszacowanego ryzyka środki techniczne i organizacyjne	przygotowuje pierwszy audyt w rozumieniu ustawy (następnie minimum raz na dwa lata)
zarządza incydentami	zbiera informacje o zagrożeniach i podatnościach	
wyznacza osobę kontaktową z właściwym CSIRT i PPK przy MC	stosuje środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego	
prowadzi działania informacyjne nt. cyberzagrożeń wobec użytkowników	stosuje wymaganą dokumentację	przekazuje sprawozdanie z audytu, wskazanym w ustawie podmiotom
obsługuje incydenty we własnych systemach		
zgłasza incydenty poważne		
usuwa wskazywane podatności		

Źródło: https://www.gov.pl/web/cyfryzacja/dzialalnosc-krajowa

Informacja o konsekwencji niedostosowania się do nowych przepisów:

Nowe przepisy przewidują wysokie kary pieniężne w przypadku niedostosowania się do nowych obowiązków. W zależności od rodzaju naruszenia, kara taka może wynieść od 1 tys.

do 200 tys. złotych, natomiast w przypadku uporczywych naruszeń może to być nawet 1 mln złotych.

Nie tylko perspektywa kar pieniężnych powinna motywować operatorów do podjęcia działań dostosowawczych. Skuteczne działania przeciwdziałające utracie danych, chroniące przed dostępem osób nieuprawnionych do danych poufnych, jak również ryzyko zniszczenia firmowej infrastruktury IT powinno być priorytetem dla Zarządów. Zaniedbanie odpowiednich działań, może zakłócić ciągłość świadczenia usług lub produkcji, pociągając za sobą znacznie większe niż kary straty finansowe oraz negatywne konsekwencje wizerunkowe dla firmy.

Dostosowanie się do nowych przepisów nie powinno być pozostawione wyłącznie działom IT lub bezpieczeństwa. Działania w obszarze cyberbezpieczeństwa wiążą się z kwestiami organizacyjno-procesowymi, które ze względu na swoją doniosłość dla całej organizacji powinny znajdować się w ścisłej kompetencji Zarządów. Tym samym zalecane jest, aby operatorzy usług kluczowych zapoznali się ze szczegółowymi wymaganiami wynikającymi z nowych przepisów oraz aby Zarządy tych podmiotów niezwłocznie zainicjowały działania dostosowawcze. Jest to szczególnie istotne ze względu na fakt, że część obowiązków powinna zostać zrealizowana przez operatorów już w ciągu 3 miesięcy od otrzymania decyzji o uznaniu za operatora usługi kluczowej

Pismo zawierające powyższe elementy powinno w treści wskazać źródła informacji szczegółowych.

W przekazie pisma można zawrzeć również w formie załącznika np. wyciąg z ustawy o KSC. Materiał może być w formie skrótowego **poradnika dla Operatorów Usług Kluczowych.**

5. Obowiązki.

Operatorem usługi kluczowej („OUK") jest podmiot, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu go za operatora usługi kluczowej. Zakres sektorowy OUK obejmuje: energię, transport, bankowość, infrastrukturę rynków finansowych, ochronę zdrowia, zaopatrzenie w wodę pitną i jej dystrybucję, infrastrukturę cyfrową.

Oznacza to, że podmioty z tych sektorów, o ile świadczą usługę kluczową, zależną od systemów informacyjnych, a ewentualny incydent dotyczący cyberbezpieczeństwa mógłby mieć istotny skutek zakłócający na świadczenie usługi kluczowej, zostały objęte obowiązkami wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa ("z ustawy KSC").

Wykaz OUK prowadzić* będzie *minister właściwy ds. informatyzacji

Obowiązki OUK w zakresie cyberbezpieczeństwa, określone w ustawie:

Obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniającego:

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.
   a. Obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz przekazania danych tej osoby w terminie 14 dni od daty jej wyznaczenia, do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowego zespołu cyberbezpieczeństwa.
   <u>CSIRT oznacza Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego.</u>
   b. Obowiązek zapewnienia użytkownikowi usługi kluczowej dostępu 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.
   c. Obowiązek opracowania, wdrożenia i aktualizacji dokumentacji cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.
   d. Obowiązek ustanowienia nadzoru nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zapewniającego:
      i. dostępność dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami;
      ii. ochronę dokumentów przed niewłaściwym użyciem lub utratą integralności;
      iii. oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w tych dokumentach.
   e. Obowiązek obsługi incydentów, zgłaszania incydentów poważnych i współdziałania przy obsłudze incydentu poważnego i incydentu krytycznego
      i. zapewnia obsługę incydentu;
      ii. zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań;

iii. klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny;
iv. zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
v. zgłoszenie powinno zostać dokonane w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej
vi. przy użyciu innych dostępnych środków komunikacji.
vii. współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
viii. usuwa podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, incydentu istotnego lub krytycznego, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.

Dodatkowo, w przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa OUK:

- przekazuje jednocześnie temu zespołowi w postaci elektronicznej zgłoszenie, o którym mowa powyżej;
- współdziała z tym zespołem na poziomie sektora lub podsektora podczas obsługi incydentu poważnego lub incydentu krytycznego, przekazując niezbędne dane, w tym dane osobowe;
- zapewnia temu zespołowi dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań.

- **obowiązek powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcie umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (informacja o zawarciu umowy powinna zostać przekazana w terminie 14 dni od jej zawarcia do organu właściwego do spraw cyberbezpieczeństwa i właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowego zespołu cyberbezpieczeństwa).**

Wewnętrze struktury powinny:

1. spełniać warunki organizacyjne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej, tj.:
    a. posiadać i utrzymywać w aktualności system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001;

b. zapewnić ciągłość działania usłudze reagowania na incydenty, polegającej na podejmowaniu działań w zakresie rejestrowania i obsługi zdarzeń naruszających bezpieczeństwo systemów informacyjnych zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301;
c. zapewnić wsparcie operatorowi usługi kluczowej w trybie całodobowym przez wszystkie dni w roku, z czasem reakcji adekwatnym do charakteru usługi kluczowej;
d. dysponować personelem posiadającym umiejętności i doświadczenie w zakresie:
    i. identyfikowania zagrożeń w odniesieniu do systemów informacyjnych,
    ii. analizowania oprogramowania szkodliwego i określania jego wpływu na system informacyjny operatora usługi kluczowej,
    iii. zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania.

Dodatkowo, podmiot zewnętrzny powinien posiadać i udostępniać w języku polskim i angielskim deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF).

2. Wewnętrzne struktury organizacyjne lub podmiot zewnętrzny, powinny spełniać warunki techniczne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej, tj. dysponować:
    a. sprzętem komputerowym oraz specjalizowanymi narzędziami informatycznymi umożliwiającymi:
        i. automatyczne rejestrowanie zgłoszeń incydentów,
        ii. analizę kodu oprogramowania uznanego za szkodliwe,
        iii. badanie odporności systemów informacyjnych na przełamanie zabezpieczeń,
        iv. zabezpieczanie śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania;
    b. środkami łączności umożliwiającymi wymianę informacji z podmiotami, dla których świadczą usługi, oraz właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działającym na poziomie krajowym.
3. Dysponować pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty, zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi, tj. dysponować prawem do wyłącznego korzystania z pomieszczeń, które wyposażone są w zabezpieczenia techniczne adekwatne do przeprowadzonego szacowania ryzyka, w tym co najmniej w:

a. system sygnalizacji włamania i napadu klasy 2 według Polskiej Normy PN-EN 50131-1;
b. system kontroli dostępu klasy 2 według Polskiej Normy PN-EN 60839-11-1, zapewniający osobie przyznanie dostępu do pomieszczenia przez rzecz posiadaną przez tą osobę oraz zapamiętanie zdarzenia przyznania dostępu danej osobie wraz z datą i czasem;
c. system wykrywania i sygnalizacji pożaru z powiadamianiem do centrum odbiorczego alarmów pożarowych (dopuszcza się, po wykonaniu szacowania ryzyka i gdy brak jest przeciwwskazań wynikających z innych przepisów, wyposażenie tych pomieszczeń w czujki wykrywające pożar podłączone do systemu sygnalizacji włamania i napadu, o ile stacja monitorująca alarmy z tego systemu będzie w stanie ustalić przyczynę poszczególnych alarmów);
d. szafy służące do przechowywania dokumentów oraz informatycznych nośników danych o istotnym znaczeniu dla prowadzonej działalności, klasy S1 spełniającymi wymagania Polskiej Normy PN-EN 14450, chyba że inne przepisy wymagają wyższej klasy odporności szaf;
e. zewnętrzne drzwi wejściowe do pomieszczeń o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki o klasie nie niższej niż klasa odporności drzwi;
f. wewnętrzne drzwi do pomieszczeń o klasie odporności RC2 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki o klasie nie niższej niż klasa odporności drzwi;
g. okna o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich rodziłby nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia;
h. ściany zewnętrzne o odporności na włamanie równoważnej odporności muru o grubości 25 cm wykonanego z pełnej cegły;
i. ściany wewnętrzne o odporności na włamanie adekwatnej do klasy odporności drzwi.
j. stosować zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.
    i. **Obowiązek zapewnienia przeprowadzenia, co najmniej raz na 2 lata (pierwszy audyt w terminie roku od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej), audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.**

Audyt, może być przeprowadzony przez:

1. jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
2. co najmniej dwóch audytorów posiadających:
    a. certyfikaty uprawniających do przeprowadzenia audytu lub
    b. co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub
    c. co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;
3. sektorowy zespół cyberbezpieczeństwa, ustanowiony w ramach sektora lub podsektora, jeżeli audytorzy spełniają warunki, o których mowa w pkt 2 powyżej.

Z zastrzeżeniem obowiązku dotyczącego przeprowadzenia audytu bezpieczeństwa systemów informacyjnych poszczególne obowiązki będą musiały być realizowane w terminach wynikających z ustawy, tj. od 3-6 miesięcy, w zależności od obowiązku.

Organami właściwymi ds. cyberbezpieczeństwa są ministrowie właściwi dla danych sektorów, przy czym dla sektora bankowego właściwym organem jest Komisja Nadzoru Finansowego

Organy właściwe do spraw cyberbezpieczeństwa sprawują nadzór w zakresie wykonywania przez OUK obowiązków wynikających z ustawy dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów poważnych (incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej).

W ramach nadzoru Organ Właściwy:
• Organ Właściwy do spraw cyberbezpieczeństwa lub minister właściwy do spraw informatyzacji prowadzi kontrole; • Organ Właściwy do spraw cyberbezpieczeństwa nakłada kary pieniężne na OUK.

Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ma prawo do:

- swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki;
- wglądu do dokumentów dotyczących działalności podmiotu kontrolowanego, pobierania za pokwitowaniem oraz zabezpieczania dokumentów związanych z zakresem kontroli, z zachowaniem przepisów o tajemnicy prawnie chronionej;
- sporządzania, a w razie potrzeby żądania sporządzenia, niezbędnych do kontroli kopii, odpisów lub wyciągów z dokumentów oraz zestawień lub obliczeń;
- przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli;
- żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu kontroli;
- przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych.

Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ właściwy do spraw cyberbezpieczeństwa lub minister właściwy do spraw informatyzacji uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości.

Od zaleceń pokontrolnych nie przysługują środki odwoławcze.

Podmiot kontrolowany, w wyznaczonym terminie, informuje organ właściwy do spraw cyberbezpieczeństwa lub ministra właściwego do spraw informatyzacji o sposobie wykonania zaleceń.

Karze pieniężnej podlega operator usługi kluczowej, który:

Czynność zaniechana	Wymiar kary
nie przeprowadza systematycznego szacowania ryzyka lub nie zarządza ryzykiem wystąpienia incydentu;	kara wynosi do 150 000 zł
nie wdrożył środków technicznych i organizacyjnych uwzględniających najnowszy stan wiedzy, odpowiednich i proporcjonalnych do oszacowanego ryzyka	kara wynosi do 100 000 zł
nie stosuje środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej	kara wynosi do 50 000 zł
nie wyznaczył osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa	kara wynosi do 15 000 zł
nie opracowuje, stosuje i aktualizuje dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej	kara wynosi do 50 000 zł
nie zapewnia obsługi incydentu za każdy stwierdzony przypadek zaniechania obsługi incydentu	kara wynosi do 15 000 zł
nie zgłasza incydentu poważnego niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV za każdy stwierdzony przypadek niezgłoszenia incydentu poważnego	kara wynosi do 20 000 zł

Czynność zaniechana	Wymiar kary
nie współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;	kara wynosi do 20 000 zł
nie usuwa podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, incydentu istotnego lub krytycznego	kara wynosi do 20 000 zł
nie powołuje wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub nie zawiera umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa	kara wynosi do 100 000 zł
nie przeprowadza audytu	kara wynosi do 200 000 zł
uniemożliwia lub utrudnia wykonywanie kontroli	kara wynosi do 50 000 zł
nie wykonuje w wyznaczonym terminie zaleceń pokontrolnych	kara wynosi do 200 000 zł

Jeżeli w wyniku kontroli organ właściwy do spraw cyberbezpieczeństwa stwierdzi, że operator usługi kluczowej albo dostawca usługi cyfrowej uporczywie narusza przepisy ustawy, powodując:

1. bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,
2. zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych

- organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 1 000 000 zł.

Organ właściwy do spraw cyberbezpieczeństwa może nałożyć karę pieniężną na kierownika operatora usługi kluczowej w przypadku, gdy nie dochował należytej staranności celem spełnienia obowiązków szacowania i zarządzania ryzykiem, wyznaczenia osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, przeprowadzania audytu, z tym, że kara ta może być wymierzona w kwocie nie większej niż 200% jego miesięcznego wynagrodzenia.

6. Działania długoterminowe

Operatorów Usług Kluczowych, do których będą skierowane działania informacyjne można podzielić ze wzgl. na strukturę właścicielską.

Podmioty te zależne są od:

- skarbu państwa
- jednostek samorządu terytorialnego
- kapitału prywatnego

Spojrzenie z takiej perspektywy umożliwia dywersyfikację dalszych działań z OUK w następstwie pierwszej komunikacji, czyli uświadomienie Radom Nadzorczym, Właścicielom aby egzekwowały od podległych im Zarządów firm podejmowanie działań podnoszących poziom cyberbezpieczeństwa.

Oczekuje się, że w ramach nałożonych przez ustawę KSC obowiązków zostaną przeprowadzone audyty bezpieczeństwa, które następnie dadzą zarządom wiedzę nt. stanu/poziomu cyberbezpieczeństwa w ich organizacji, pomogą stworzyć mapę priorytetów oraz działań dostosowujących do zaleceń lub obowiązków wynikających z ustawy KSC. W perspektywie długoterminowej organy nadzorcze powinny monitorować czy w następstwie ww. audytów doszło do dalszych działań.

Aby ułatwić zarządom działania związane z cyberbezpieczeństwem dobrze, aby OUK samodzielnie mogli wykonywać pre-audyty stanu bezpieczeństwa i działań z nim związanych.

W tym celu sugeruje się przygotowanie (tj. zlecenie przez Ministerstwo opracowania) odpowiednich dedykowanych ankiet z odpowiednimi metrykami oceniającymi poziom dojrzałości w poszczególnych domenach bezpieczeństwa (np. wg. ISO27001) Ankiety takie pomogą ocenić kompletność działań, jakie podjęły i podejmują zarządy w wykonaniu przepisów ustawy. Wypełnione ankiety powinny być przesyłane do MC w celach ewidencyjnych.

Przy okazji tych działań pre-audytowych pojawia też możliwość wprowadzenia KPI:

- monitorowanie liczby przeprowadzonych audytów bezpieczeństwa do momentu podjęcia działań informacyjnych (komunikacji z MC)
- monitorowanie liczby przeprowadzonych audytów w wyniku komunikacji z MC
- liczba przedsiębiorstw z wdrożoną normą ISO2700x
- w przypadku realizacji działań związanych z ankieta pre-audytową, liczba wypełnionych ankiet przesłanych do MC

Spółki skarbu Państwa

W przypadku spółek, gdzie jest większościowy udział skarbu Państwa, w drugim etapie proponuje się przyjąć następujący schemat działania:

- Po miesiącu od wysłania listu do Zarządów Spółek należy wysłać List Ministra Cyfryzacji do Organów Właścicielskich tych spółek (właściwych Ministrów), przesłany do wiadomości właściwej komórki Kancelarii Prezesa Rady Ministrów nadzorującej kwestie właścicielskie. W liście należy poinformować o wysłanym wcześniej do zarządów spółek liście oraz załączyć ankietę pre-audytową (opisaną powyżej), którą powinni otrzymać od właściciela jego przedstawiciele w Radach Nadzorczych tych spółek. Zgodnie z prośbą zawartą w tej korespondencji, Rady Nadzorcze powinny skontrolować w zakresie przewidzianym w ankiecie skuteczność podjętych przez Zarządy działań wynikających z Ustawy i przekazać zwrotnie wypełnione ankiety do Ministerstwa Cyfryzacji.
- Po pół roku od wysłania tej korespondencji należy podsumować jej efekt i podjąć działania interwencyjne przez Organy nadzoru właścicielskiego w przypadku firm, które zlekceważyły swoje obowiązki.

Organy Właścicielskie powinny systematycznie prowadzić kontrole czy audyty są prowadzone (w OUK po 12 miesiącach od wręczenia decyzji o uznaniu za OUK należy przeprowadzić pierwszy audyt) i zalecane jest również systematyczne kontrolowanie wprowadzania zalecanych przez audyty rozwiązań.

W celu rozpoczęcia tego działania, oprócz wcześniej opisanych działań OW powinien przygotować:

- Listy informacyjne do organów właścicielskich spółek np. o obowiązku raportowania audytów i realizacji zaleceń po audytowych
- Określić zasady wsparcia merytorycznego i sposób kontaktowania się w celu jego uzyskania

Spółki jednostek samorządu terytorialnego

Jednostki samorządu terytorialnego (JST) oprócz swoich instytucji administracyjnych, dla których dedykowane działania są opracowywane osobno **(podgrupa III grupy roboczej ds. Cyberbezpieczeństwa działającej przy Ministerstwie Cyfryzacji),** mają również szereg podległych sobie podmiotów strategicznych jak wodociągi, szpitale, etc.

Proponuje się, żeby kwestia ustawy KSC oraz wynikających z niej implikacji dla JST została niezwłocznie przedstawiona na Komisji Wspólnej Rządu i Samorządu Terytorialnego, w której MC ma swojego stałego przedstawiciela.

Oczekiwany skutek tego działania to stworzenie możliwości dotarcia do Włodarza (Marszałka, Prezydenta, Burmistrza, ew. Starosty) i przedstawienia mu w spotkaniu bezpośrednim celów, szans i zagrożeń związanych z wprowadzeniem ustawy KSC. Włodarze powinni otrzymać ankiety pre-audytowe, skontrolować w zakresie przewidzianym w ankiecie skuteczność podjętych przez Zarządy działań wynikających z Ustawy i przekazać zwrotnie wypełnione ankiety do Ministerstwa Cyfryzacji.

Ponieważ można się spodziewać, że wystąpią naturalne problemy JST z finansowaniem zgodnych z prawem inwestycji/zmian (obowiązki nałożone bez wskazania źródła finansowania), warto byłoby zainicjować proaktywne działania związane z wydatkowaniem przez JST środków na cel cyberbezpieczeństwo z II Osi POPC oraz z Funduszy Regionalnych.

Aby działania związane z cyberbezpieczeństwem miały charakter stały, proponuje się powołanie Podkomisji ds. Cyberbezpieczeństwa przy Komisji Wspólnej Rządu i Samorządu Terytorialnego. Jest to dobry moment, ponieważ Komisja będzie się właśnie na nowo konstytuować.

Spółki z kapitałem prywatnym

Nie ma rekomendacji co do dalszych działań (kolejne etapy) wymuszających inicjatywy związane z cyberbezpieczeństwem w tej grupie. Może to być kierunkiem dalszych prac.

Na obecnym etapie słuszna wydaje się inicjatywa uświadamiania zagrożeń i informowania Zarządów spółek z kapitałem prywatnym o istniejących regulacjach prawnych za pomocą zróżnicowanych kanałów komunikacyjnych. Zasadnym było by opracowanie rekomendacji (dobrych praktyk).

7. Propozycje kanałów komunikacji

Portal informacyjny

Szeroko dostępna platforma informacyjna dedykowana zagadnieniom cyberbezpieczeństwa powinna być uniwersalna, zawierać materiały dla wszystkich podmiotów i osób fizycznych szukających wiedzy związanej z cyberbezpieczeństwem i KSC. Poniższe odnosi się tylko do części dedykowanej odbiorcom typu OUK, tzn. „portal" oznacza „część portalu dedykowana OUK"

Forma realizacji portalu www, tzn. czy zostanie utworzony w ramach środków i pod auspicjami MC czy podmiotów stowarzyszonych (np. NASK) jest uzależniona od zasobów i możliwości, których niniejsza Grupa Robocza nie jest w stanie ocenić. Platforma taka winna być tworzona przy współpracy z OW i CSIRTami.

Podstawowe cele, na których powinien się skupić portal, to:

- Budowa świadomości, że cyberbezpieczeństwo wymaga zaangażowania i odpowiedzialności od każdego pracownika;
- Budowa świadomości, że promowanie odpowiedzialnych zachowań w zakresie cyberbezpieczeństwa jest istotnym, niezbywalnym zadaniem współczesnych liderów;
- Ilustracja tematów i wynikających z nich odpowiedzialności zawartych w treści ustawy o krajowym systemie cyberbezpieczeństwa;
- Pomoc w odnalezieniu istotnych publikacji obowiązujących i wspierających OUK w zakresie cyberbezpieczeństwa.

Zakres merytoryczny

Kluczowym aspektem przydatności portalu jest jego aktualność, rzetelność i łatwość odnalezienia publikowanych materiałów. Jest to istotniejsze niż obszerność zawartych tam treści. Należy to przewidzieć przy planowaniu środków na działanie portalu.

Publikowane treści powinny być formułowane w sposób łatwy do zrozumienia dla osób, które na co dzień nie zajmują się zagadnieniami cyberbezpieczeństwa. Powinny być krótkie i praktycznie odnoszące się do biznesowych i operacyjnych realiów działania przedsiębiorstw.

Powinny obejmować:

1. Podstawowe obowiązki wynikające z ustawy:
    a. wejście w życie przepisów ustawy oraz nałożonych w ten sposób obowiązków,
    b. cyberbezpieczeństwo jako procesy organizacyjne będące w odpowiedzialności Zarządów, podlegające ciągłym zmianom oraz wymagające cyklicznego przeglądu i analizy ryzyka,

    c. odpowiedzialność karna i finansowa za brak działań Zarządu;
2. Przykłady biznesowych szkód/kosztów zagrożeń wynikających z ataków cyberbezpieczeństwa
    a. konsekwencje ekonomiczne i społeczne spełnienia się ryzyk,
    b. konsekwencje wizerunkowych wynikających ze spełnienia się ryzyk,
    c. najczęstsze scenariusze prowadzące do spełnienia się ryzyk;
3. Informacje liczbowe dotyczące zagrożeń Cyberbezpieczenstwa Raporty. (np. CERT Polska, IBM X-Force, etc.);
4. Komentarze, z perspektywy biznesowej, do w/w zaleceń i publikacji;
5. Promowanie dobrych praktyk i inicjatyw z zakresu Cyberbezpieczeństwa w polskich firmach
6. Ankiety (lub zestawy ankiet) umożliwiające samodzielną ocenę przygotowania przedsiębiorstwa do spełnienia wymagań[1];
7. Odpowiedzi na najczęściej zadawane pytania (FAQ)[2];
8. Wskazanie organów krajowych powoływanych/wskazywanych w ramach ustawy odpowiedzialnych za realizację ustawy i promowanie Cyberbezpieczeństwa[3];
9. Wskazanie organizacji międzynarodowych zaangażowanych we wdrożenie Dyrektywy NIS oraz promowanie cyberbezpieczeństwa[4];
10. Wskazywanie, w formie aktualności, nowych zaleceń i publikacji tych organizacji.

Celem portalu nie powinno być konkurowanie z innymi specjalistycznymi portalami z obszaru cyberbezpieczeństwa. Również cytowanie i wskazywanie na takie portale powinno być ograniczone, ze względu na brak możliwości nadzoru merytorycznego nad publikowanymi tam treściami i ich zmiennością w czasie. Bardziej wskazane jest odwołanie do dobrych praktyk, pojęć, norm, o których osoba kierująca mogłaby/powinna wiedzieć, a które, w razie potrzeby, może odnaleźć poza portalem.

[1] Wymaga zlecenia do opracowania przez ekspertów z zakresu cyberbezpieczeństwa. Dobrym rozwiązaniem może być przygotowanie szeregu krótkich ankiet odnoszących się do spełnienia poszczególnych wymagań z ustawy dotyczących OUK.

[2] Obecna forma ustawy nie przewiduje wśród zadań Pełnomocnika ds. cyberbezpieczeństwa roli pełnomocnika jako organu odpowiedzialnego za zbieranie i udzielanie odpowiedzi w zakresie wdrażania Ustawy. Do dalszego ustalenie, gdzie takie pytania mogą być kierowane i obsługiwane

[3] Organy/źródła krajowe: Rozporządzenia RM do ustawy, Pełnomocnik, CSIRT GOV, CSIRT MON, CSIRT NASK, Sektorowe zespoły cyberbezpieczeństwa, Publikacje organów właściwych do spraw cyberbezpieczeństwa (Art. 41 ust.), Inne portale/inicjatywy tworzone dla promowania cyberbezpieczeństwa ze środków państwowych i EU na zlecenie ministerstwa (np. NASK).

[4] Organy/źródła zagraniczne: Komisja Europejska strony dotyczące dyrektywy NIS; CSIRT EU; ENISA.

Organizacja portalu

Dobrym rozwiązaniem może być merytoryczne zorganizowanie portalu tematycznie wokół głównych obowiązków wynikających z ustawy.

Dla ułatwienia wyszukiwania informacji oraz grupowania treści warto pomyśleć o dobrym i spójnym systemie tagowania. Może on zawierać:

- wskazanie wymagania z ustawy,
- sektora,
- źródła publikacji (organ publikujący),
- rodzaju publikacji (ustawa, rozporządzenie, informacja, opis przypadku).

Formy przekazu

Sugerowane formy przekazu, do wykorzystania w ramach portalu:

- Infografiki;
- Diagramy;
- Krótkie filmy;
- Komentarze ekspertów (biznesowych, prawnych, cyberbezpieczeństwa)
    - analiza zaistniałych zagrożeń w kraju i na świecie,
    - dobre praktyki I korzyści z ich stosowania,
    - wyciągi z aktów prawnych;
- Ankieta Pre-Audytowa Self Assessment;
- FAQ;
- Blog/ Zamknięte forum;
- Wywiady.

Pojedynczy Punkt Kontaktowy

Art. 48 ustawy KSC nakłada na MC obowiązek prowadzenia Pojedynczego Punktu Kontaktowego. Ustawa, jednakże wskazuje, że to Organy Właściwe są podstawowym źródłem informacji dla OUK (w sensie przekaźnikiem), a nie PPK.

Do Zadań PPK należy:

1. odbieranie zgłoszeń incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej, a także przekazywanie tych zgłoszeń do CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowych

zespołów cyberbezpieczeństwa (nie obejmuje to wszystkich wchodzących w skład KSC);

2. przekazywanie, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zgłoszenia incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej;
3. zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy;
4. zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa;
5. koordynacja współpracy między organami właściwymi i organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;
6. zapewnienie wymiany informacji na potrzeby Grupy Współpracy oraz Sieci CSIRT.

Jeżeli chodzi o informowanie podmiotów objętych KSC to minister właściwy ds. informatyzacji ma następujące zadania (informacyjne); **- prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników. Dotyczy to podstawowych zasad np. cyber higieny, kampanii świadomościowych itd., nie jest to rola zdefiniowanego w ustawie KSC punktu informacyjnego.**

Dlatego Sugeruje się, żeby rozszerzyć zadania i cele punktu kontaktowego wykonującego zadania ustawowe tak, żeby stanowił też punkt informacyjny dla podmiotów objętych obowiązkami wynikającymi z KSC.

Dobrym pomysłem wydaje się zbudowanie **w przyszłości** „punktu kontaktowego" w sposób analogiczny do tego obsługującego informacyjnie CEiDG w ramach serwisu www.firma.gov.pl. (dokument załączony do niniejszego opracowania). Jest to inicjatywa wymagająca nakładów finansowych i pozyskania ekspertów do obsługi takiego punktu informacyjnego. Jednakże,być może w przyszłości powstaną takie platformy informacyjne.

Dobre praktyki

Doświadczenia ostatnich lat pokazują, że nawet certyfikowane i weryfikowane przez audyty systemy bezpieczeństwa często okazywały się nieszczelne i pozostawały podatne na włamania. W wielu przypadkach skala zniszczeń spowodowanych atakami zagrażała istnieniu całych przedsiębiorstw. W następstwie takich zdarzeń dotychczasowe sposoby weryfikacji efektywności systemów bezpieczeństwa teleinformatycznego zaczęły budzić coraz więcej wątpliwości.

Obecnie, zgodnie z opinią wielu ekspertów najbardziej wiarygodnym sposobem określenia skuteczności systemu bezpieczeństwa jest holistyczna analiza jego dojrzałości, obejmująca technologię, procesy i organizację, metody zarządzania oraz techniki ilościowego mierzenia skuteczności ich działania.

Poniżej przedstawiono jedną z propozycji mapowania zagadnień cyberbezpieczeństwa w organizacji pochodzącą z opracowanej przez IBM metodyki 10 Essential Practices (10EP). Opracowana przez IBM metodyka jest całościowym sposobem szacowania dojrzałości systemu bezpieczeństwa teleinformatycznego, który obejmuje swoim zakresem dziesięć domen/obszarów uznanych przez IBM jako najważniejsze dla zapewnienia bezpieczeństwa.

Nie jest to oczywiście jedyna tego typu metodyka, można a nawet trzeba rozważyć konstrukcję podobnego mapowania domen bezpieczeństwa w oparciu o normę ISO 27001, jako najbardziej rozpoznawalną i najczęściej stosowaną w tym zakresie normę w RP (ISO 27001 mapuje 14 domen bezpieczeństwa)

Ważne, żeby jakkolwiek nie dobrany, system oceny stanu bezpieczeństwa w przedsiębiorstwie uwzględniał pięć funkcji, których stan stanowi składowe ogólnego poziomu ocenianego systemu bezpieczeństwa w przedsiębiorstwie/organizacji.

- Procesy
- Zarządzanie
- Technologia
- Organizacja
- Metryki

Jest to uniwersalne podejście zarówno w ocenie, np. w ramach ankiet self-assessment'owych, o których mowa wcześniej, jak i w odniesieniu do dobrych praktyk.

Dobre praktyki dla podmiotów objętych obowiązkami wynikającymi z ustawy KSC powinny znajdować się we wszystkich kanałach komunikacji, warto rozważyć też poświęcone temu wydawnictwa/broszury.

8. Przykłady:

Zbuduj organizację świadomą zagrożeń oraz właściwy system zarządzania ryzykiem.

Kluczowe pytanie: **Czy kultura pracy w Twojej firmie pozwala na ryzykowne zachowania? Czy egzekwuje przestrzeganie zasad bezpieczeństwa?**

Używając technologii, każdy w organizacji jest potencjalnym źródłem zagrożenia dla całej firmy - otwierając podejrzany załącznik lub też przez zaniechanie instalacji patch'a bezpieczeństwa na smartfonie.

Zbudowanie kultury świadomości zagrożeń wymaga zdefiniowania ryzyk i celów, a następnie ich popularyzacji. Tak więc kierownictwo musi nieustannie propagować tak zdefiniowaną zmianę w dół organizacji, implementując równocześnie odpowiednie narzędzia do monitorowania postępów.

Najlepsze praktyki:

- Rozwiń misję bezpieczeństwa korporacyjnego zmieniając status działu IT ze „sklepu" dostarczającego narzędzia i technologie w IT zarządzające ryzykiem w całym przedsiębiorstwie, kierowane przez lidera posiadającego strategiczne umocowanie w strukturach firmy.
- Zaprojektuj strukturę organizacyjną i model zarządzania, które umożliwią proaktywne identyfikowanie i zarządzanie ryzykami.
- Buduj i zwiększaj świadomość odnośnie potencjalnych cyberzagrożeń.
- Zbuduj system zarządzania oparty na przyswajalnych politykach, metrykach i właściwych narzędziach.

Kluczowe elementy:

- Zarządzanie IT i bezpieczeństwem w całym przedsiębiorstwie
- Procesy identyfikacji i zarządzania ryzykiem
- Przywracanie stanu sprzed incydentu bezpieczeństwa
- Komunikacja i edukacja
- Polityki, metryki, narzędzia

Zarządzaj incydentami bezpieczeństwa z większą świadomością i w oparciu o dane analityczne.

Kluczowe pytanie: **W jaki sposób używać wiedzy nt. bezpieczeństwa (ang threat intelligence) do wspierania biznesu?**

Wyobraźmy sobie dwa podobne incydenty bezpieczeństwa zachodzące w zupełnie różnych miejscach na świecie. Zdarzenia te mogą być skorelowane, jednak bez wykorzystania tzw. threat intelligence, które mogłoby te zdarzenia połączyć, ważny wzór ataku mógłby pozostać nierozpoznany.

Dlatego tak ważne są wysiłki firm dążące do zaimplementowania inteligentnych analityk i automatyzacji reagowania na incydenty. Stworzenie automatycznego i zunifikowanego systemu pozwoli przedsiębiorstwu monitorować swoją działalność i szybko reagować.

Najlepsze praktyki:

Jeśli masz możliwości:

- Zbuduj wykwalifikowany zespół do zarządzania incydentami i reagowania wyposażony w odpowiednie środki śledcze.
- Rozwiń zunifikowane polityki i procesy obsługi incydentów.
- Wykorzystaj spójne narzędzia i dane wywiadowcze (security intelligence) do zarządzania incydentami i czynności śledczych.
- Zbuduj funkcjonalność Security Information Event Management (SIEM) do wykrywania i śledzenia wszystkich zdarzeń bezpieczeństwa.

UWAGA: uoKSC daje możliwość outsorcowania usług bezpieczeństwa (np. monitorowanie, threat intelligence, incydent management, itp.)

Kluczowe elementy:

- Zarządzanie incydentami i reagowanie
- Polityka i procesy obsługi incydentów
- Dane analityczne nt. bezpieczeństwa i narzędzia doradcze
- Security Information Event Management (SIEM)
- Role i obowiązki zw. z operacjami bezpieczeństwa

Chroń stanowiska pracy mając na uwadze nowe trendy i standardy: mobilność i media społecznościowe

Kluczowe pytanie: **Co powinniśmy brać pod uwagę w ochronie swojej przestrzeni roboczej?**

Pracownicy chętnie korzystają z własnych urządzeń i coraz intensywniej wykorzystują social media do efektywnej komunikacji.

Każda stacja robocza, laptop lub smartfon stanowi potencjalne wejście dla szkodliwego oprogramowania. Ustawienia urządzeń nie mogą zatem pozostawać w gestii niezależnych osób czy grup, lecz powinny być przedmiotem narzuconego, scentralizowanego zarządzania.

Zabezpieczenie przestrzeni roboczej oznacza znalezienie właściwej równowagi pomiędzy otwartością i zarządzaniem ryzykiem.

Najlepsze praktyki:

- Pozwalaj pracownikom na BYOD i korzystanie z social media do rozwijania biznesu, przy jednoczesnym zapewnieniu ochrony zasobów i danych przedsiębiorstwa.

- Zabezpiecz platformy (np. aplikacyjne) użytkowników końcowych pod kątem zgodności z profilem ryzyka typowego dla poszczególnych stanowisk pracy.
- Uruchom automatyczne wymuszane ustawień bezpieczeństwa wszystkich stacji roboczych, urządzeń mobilnych i obrazów chmurowych (images) desktop'ów.
- Izoluj dane prywatne, klientów oraz biznesowe i chroń je.

Kluczowe elementy:

- BYOD i social media
- Segmentacja danych biznesowych i prywatnych
- Bezpieczne dla użytkowników końcowych platformy przetwarzania
- Bezpieczeństwo stacji roboczych, laptopów, urządzeń typu smart
- Ochrona danych

Projektuj produkty i usługi z uwzględnieniem bezpieczeństwa

Kluczowe pytanie: **Co znaczy dla biznesu projektowanie z uwzględnieniem bezpieczeństwa?**

Wyobraźmy sobie, że producenci samochodów nie produkowaliby samochodów wyposażonych w pasy bezpieczeństwa i poduszki powietrzne, tylko dodawali je później.

Byłoby to zarówno bezsensowne jak i ponadnormatywnie drogie.

W podobny sposób powstają podatności systemów informatycznych, w których najpierw implementowane są usługi, a następnie poprawia się je i łata w celu poprawy bezpieczeństwa.

Dlatego najlepszym rozwiązaniem jest budowanie bezpieczeństwa od samego początku, a następnie regularne, automatyczne testowanie celem monitorowania jego adekwatności.

Najlepsze praktyki:

- Oceń, gdzie powinny się znajdować optymalne punkty kontroli jakości
- Obniżaj koszty tworzenia rozwiązań bezpiecznych poprzez umieszczanie wymagań bezpieczeństwa na wczesnych etapach projektowania
- Proaktywnie odkrywaj podatności i słabości poprzez testy penetracyjne i działania etycznych hacker'ów

Kluczowe elementy:

- Polityki bezpieczeństwa i zgodności dla SDLC (systems development life cycle)
- Bezpieczeństwo osadzone w procesie projektowania
- Ethical Hacking i testy penetracyjne
- Stosowanie bezpiecznych interfejsów i komercyjnych programów „z półki"

Zautomatyzuj "higienę" bezpieczeństwa

Kluczowe pytanie: **Jakie ryzyka wiążą się z ciągłym patch'owaniem i używaniem starszego oprogramowania?**

Ludzie mają naturalną tendencję do utrzymywania starego oprogramowania, ponieważ je znają i czują się z nim komfortowo. Zarządzanie aktualizacjami tak zbudowanego środowiska może stać się w przedsiębiorstwie misją niemożliwą.

Wdrożenie zunifikowanej metodyki zarządzania i aktualizacji pozwala uczynić system bardziej bezpiecznym, w którym administratorzy mogą śledzić każdy program, który jest uruchomiony i mieć pewność, że jest on aktualny. Mogą też za jego pośrednictwem instalować aktualizacje i poprawki - jak tylko zostaną wydane.

Taki sposób zarządzania powinien być standardem w administracji każdego środowiska.

Najlepsze praktyki:

- Inwentaryzuj wszystkie komponenty infrastruktury IT i sukcesywnie wymieniaj przestarzałe elementy
- Automatyzuj zarządzanie patchami i zachęcaj organizację do działań zabezpieczających infrastrukturę przed współczesnymi zagrożeniami
- Identyfikuj możliwości outsource'owania rutynowych działań monitorujących

Kluczowe elementy:

- Inwentaryzacja komponentów infrastruktury IT
- Wycofywanie przestarzałych elementów IT
- Rutynowe przeglądy
- Zgodność integrowanych danych
- Efektywne zarządzanie aktualizacjami
- Funkcje skanowania i testowania zgodności

Buduj bezpieczną sieć, kontroluj dostęp

Kluczowe pytanie: **W jaki sposób poprawić kontrolę dostępu do sieci i jej odporność na naruszenia bezpieczeństwa?**

Wyobraźmy sobie infrastrukturę IT w przedsiębiorstwie jako gigantyczny hotel z ponad 65 tysiącami drzwi i okien. Podczas gdy do hotelowego lobby może mieć wejście każdy, dostęp do pokoi musi być kontrolowany przez recepcję i opiekę nad kluczami.

Podobnie rzecz się ma w przypadku danych. Narzędzia zabezpieczające sieci IT dają organizacjom możliwości kontrolowania dostępu do „pokoi" gdzie przechowywane są poufne dane i gdzie funkcjonują systemy krytyczne.

Najlepsze praktyki:

- Optymalizuj wydatki i wykorzystuj technologie do monitorowania i ochrony przed zagrożeniami.
- Wykrywaj i blokuj złośliwe działania w sieci z wykorzystaniem kombinacji narzędzi do: logowania, monitorowania i zaawansowanej analityki
- Priorytetyzuj, co powinno być kontrolowane, a co nie
- Zoptymalizuj infrastrukturę sieciową, aby zapewnić odpowiednią wydajność a jednocześnie: bezpieczeństwo i zarządzanie ryzykiem

Kluczowe elementy:

- Ochrona sieci
- Wykrywanie złośliwych działań w sieci
- Rozwiązania do logowania, monitorowania, filtrowania i zaawansowanej analityki
- Optymalizacja infrastruktury sieciowej

Wyjdź naprzeciw złożoności Chmury i Wirtualizacji.

Kluczowe pytanie: **W jaki sposób należy chronić siebie i dane, jeśli nie można kontrolować używanej infrastruktury?**

Przetwarzanie w chmurze zapewnia niespotykaną efektywność, ale może to też wiązać się z określonym ryzykiem. W momencie, gdy przedsiębiorstwo decyduje się na migrację pewnych usług IT do chmury obliczeniowej, narasta poczucie zbytniego „odkrycia się" i zbytniego „zbliżenia" danych do innych osób - w tym również do przestępców. Używając przykładu z poprzedniego obszaru, można to też porównać do sytuacji, kiedy jakiś procent mieszkańców hotelu jest na przykład nosicielem zakaźnej choroby. Aby bezpiecznie funkcjonować w takim środowisku, pozostali goście muszą posiadać odpowiednie narzędzia i procedury, które pozwolą im odpowiednio izolować się od innych i monitorować ewentualne zagrożenie.

Najlepsze praktyki:

- Opracuj i rozwijaj strategię dla lepszego zabezpieczenia swoich usług w chmurze
- Promuj kontrole i oceniaj raporty bezpieczeństwa dostawców usług w chmurze
- Dbaj o dobre rozumienie mocnych stron i zagrożeń twojej architektury chmurowej, programów, polityk i praktyk.

– Buduj usługi w chmurze z wykorzystaniem wyższego poziomu kontroli i niezawodności

Kluczowe elementy:

– Lepsze bezpieczeństwo usług w chmurze
– Kontrole bezpieczeństwa dostawców usług w chmurze.
– Podatności architektury chmurowej, polityk oraz praktyk
– Definicja zadań dla bezpieczeństwa chmury

Zadbaj o zgodność firm trzecich i kontrahentów z normami i standardami bezpieczeństwa

Kluczowe pytanie: **W jaki sposób kontrahenci i współpracownicy narażają mnie na ryzyko?**

Załóżmy, że pracownik tymczasowy lub kontraktor potrzebuje dostępu do systemu. Jak zapewnić mu poprawne hasło? Dać na kartce? Wysłać sms-em? Takie działania wiążą się z ryzykiem.

Korporacyjna kultura bezpieczeństwa musi wykraczać poza standardowe ramy przedsiębiorstwa i ustanawiać najlepsze możliwe praktyki również wśród kontraktorów i dostawców. Jest to proces podobny do tego, jakiego niedawno jeszcze używano celem podnoszenia jakości. Jego logika jest taka sama: bezpieczeństwo tak jak doskonałość powinno być wszczepione w cały ekosystem, gdyż efekty niedbalstwa w zaledwie jednej firmie mogą być rujnujące nawet dla całego sektora.

Najlepsze praktyki:

– Zintegruj bezpieczeństwo w procesach z kontrahentami.
– Oceniaj bezpieczeństwo po stronie dostawców, ich polityki oraz praktyki zarządzania ryzykiem, edukuj ich w kierunku zgodności
– Oceniaj zgodność z branżowymi wymogami dot. procesów i ochrony danych (regulacje: PCI, GLBA2, HIPAA3, SOX4, Ochrona Danych Osobowych, itp.)
– Zarządzaj cyklem życia ryzyka dostawcy

Kluczowe elementy:

– Dobrze zarządzane fuzje i przejęcia (M&A), joint ventures
– Praktyki bezpieczeństwa i zarządzanie ryzykiem przez dostawców, firmy trzecie
– Edukacja kooperantów w zakresie zgodności polityk i procesów
– Edukacja w zakresie obsługi incydentów i raportowania
– Zgodność dostawców z wymogami i regulacjami

Chroń dane i prywatność

Kluczowe pytanie: **Czy naprawdę wiemy, co ochraniamy?**

Gdzieś w „skarbcu danych" przechowywane są najważniejsze dane firmy - mogą to być dane techniczne, naukowe albo dokumenty finansowe firmy lub jej Klientów.

Te dane – intelektualna własność przedsiębiorstwa – mogą być elementem przesądzającym o przewadze konkurencyjnej. Dlatego też każde przedsiębiorstwo powinno obchodzić się z takimi danymi ze specjalną troską.

Każdy z takich priorytetowych elementów powinien być chroniony, śledzony i zaszyfrowany - jeśli zależy od niego przyszłość przedsiębiorstwa.

Najlepsze praktyki:

- Zidentyfikuj wartość Twoich poufnych danych i wpływ na biznes w przypadku ich utraty
- Oceń braki w bezpieczeństwie z zdefiniuj strategię ochrony: zarządzającą ryzykiem utraty danych, odpowiadającą wymaganiom klientów i regulacyjnym
- Zaprojektuj solidną architekturę zarządzania, która ochroni Twoje dane wrażliwe lub poufne
- Wdrażaj i używaj najlepszych technologii ochrony

Kluczowe elementy:

- Klasyfikacja danych
- Strategia i technologie ochrony danych i prywatności
- Zapobieganie utracie danych
- Architektura zarządzania danymi
- Polityka zgodności ochrony danych

Zarządzaj cyklem życia tożsamości

Kluczowe pytanie: **Skąd wiemy, czy ktoś kto ma dostęp do naszego środowiska jest tym, za kogo się podaje? Jak wpuścić uprawnionych i nikogo więcej?**

Powiedzmy, że pracownik tymczasowy zostaje zatrudniony w pełnym wymiarze godzin. Sześć miesięcy później dostaje awans. Rok po tym zmienia prace i przechodzi do konkurencji. W jaki sposób system przez cały ten czas będzie traktował tę osobę?

Najpierw musiałby przyznać ograniczony dostęp, później otworzyć więcej drzwi, żeby finalnie odciąć jakiekolwiek dostępy. Tak właśnie wygląda zarządzanie cyklem życia tożsamości. Jest to bardzo istotne - przedsiębiorstwa i organizacje, które ten obszar zaniedbują lub nieprawidłowo zarządzają tożsamościami, działają po omacku i narażają się na włamania.

Takiemu ryzyku można zaradzić dzięki zastosowaniu dedykowanych narzędzi do identyfikacji osób, zarządzania ich uprawnieniami i odbieraniu np. w przypadku odejścia.

Najlepsze praktyki:

- Stosuj zoptymalizowaną strategię zarządzania tożsamością i dostępem.
- Zaimplementuj standardowe, oparte na politykach, mechanizmy kontroli i inteligentnego monitorowania
- Centralizuj i automatyzuj zarządzanie rozdziałem obowiązków
- Stosuj rozwiązania single-sign-on zarówno dla komputerów stacjonarnych jak i dostępów internetowych

Kluczowe elementy:

- Zarządzanie dostępem i tożsamością
- Standardowe mechanizmy kontroli i monitorowania
- Inteligentne monitorowanie
- Zarządzanie rozdziałem obowiązków
- Single-sign-on

II. Zespół II – Małe i Średnie Przedsiębiorstwa

1. Cel

Zwiększenie świadomości oraz edukacja sektora MŚP

2. Skład zespołu

Robert Siudak – Instytut Kościuszki

Artur Marek Maciąg – Porozmawiajmy o Kulturze Bezpieczeństwa

Janusz Żmudziński – Polskie Towarzystwo Informatyczne

Michał Rosiak – Orange

Przemysław Dęba – Orange

Andrzej Kozłowski – CyberDefence24

Ewa Białek – Dynacon

Andrzej Cieślak – Dynacon

3. Adresaci

MŚP zgodnie z ilościową częścią definicji przyjętej przez Unię Europejską, która dotyczy ilości zatrudnionego personelu:

- 0-10: mikro przedsiębiorstwo
- 10-50: małe przedsiębiorstwo
- 50-250: średnie przedsiębiorstwo

Źródło: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

Wszelkie branże oraz zakres geograficzny obejmujący cały kraj.

4. Zdiagnozowane potrzeby

- Szerzej kwestę uświadamiania grupy docelowej, którą zidentyfikowano jako najważniejsza z potrzeb, opisano w części" Proponowane działania i rozwiązania"
- W ramach prac grupy dokonano ewaluacji oraz omówienia materiałów edukacyjnych dostępnych na rynku, m.in.:
    - Dziennik internautów, Firma Bezpieczna w Internecie, 2016, LINK
    - Cyber Security Coalition, Cyber Security Guide for SME, LINK
    - National Cyber Security Center UK, Cyber Security: Small Business Guide, 2017, LINK
    - Munich Re, Cyber security for small and medium-sized businesses, 2015, LINK
    - Center for Internet Security, Implementation Guide for Small- and Medium-Sized Enterprises (SMEs), LINK
    - International Society of Automation, Industrial Cybersecurity for Small- and Medium-Sized Businesses a Practical Guide, LINK
    - National Institute of Standards and Technology, NIST SP 800-171, 2016/18, LINK
    - National Institute of Standards and Technology, NIST Cyber Security Framework, 2018, LINK
    - SANS Institute, Incident Handling for SMEs (Small to Medium Enterprises), 2008, LINK
    - SANS Institute, Network Security – A guide for Small and Mid-sized Businesses, 2004 LINK
- Kluczowe oprócz edukacji jest także stymulowanie MŚP do dbania o cyberbezpieczeństwo poprzez zachęty. Należy zastanowić się nad szerokim wachlarzem dostępnych środków i narzędzi:
    - Ulgi podatkowe (np. kwalifikacja wydatków na cyberbezpieczeństwo jako inwestycji w innowacje).
    - Wsparcie celowe – np. „Bony na cyberbezpieczeństwo" (w formule już sprawdzonej i znanej dla administracji z „bonów na innowacje")
    - Nagrody - ogólnopolskie, sektorowe, regionalne – np. wykorzystujące istniejące już marki takie jak Teraz Polska, Dobra Marka, Diamenty, Orły, Nagroda Gospodarcza Prezydenta RP etc.
- Ze względu na co najmniej kilka czynników dotyczących uświadamiania i edukacji grupy MŚP w zakresie cyberbezpieczeństwa tworzenie komunikatów doraźnych bez konsultacji i badania ich z potencjalnymi odbiorcami jest założeniem błędnym:
    - Istnieją już dedykowane materiały na rynku – problemem jest nie ich brak ale odpowiednie sprofilowanie informacji oraz wykorzystanie optymalnych kanałów dotarcia;

- Odpowiednie kanały dystrybucji pociągają potrzebę zaangażowania podmiotów zewnętrznych (US, ZUS, operatorzy telekomunikacyjni, banki, Rzecznik RPO) oraz koszty związane z dystrybucją;
- Ilość potencjalnych odbiorców wyklucza dedykowaną wysyłkę (możliwe w wypadku np. Operatorów Usług Kluczowych);

Biorąc pod uwagę powyższe, proces planowania oraz dystrybucji informacji i materiałów do tak szerokiej i zróżnicowanej grupy, powinien być przeprowadzony zgodnie przedstawionym w dalszej części planem działań.

5. Proponowane działania i rozwiązania

Wynik prac:

Poradnik dla MŚP w formie cyfrowej, roboczy tytuł „Cyberbezpieczeństwo twojej firmy”

Strona www

Infografika

Plakat

Skierowany do odbiorcy nietechnicznego z segmentu mikro/małych/średnich firm. Format ma zachęcić osoby niezainteresowane tematyką cyberbezpieczeństwa do zapoznania się z:

- Podstawowymi treściami stworzonymi w ramach prac grupy MC
- Biblioteką materiałów/linków/odnośników która może służyć do pogłębienia swojej wiedzy

Kanały dotarcia:

- Dwa podstawowe to:
  - kampania społeczna
  - kanały dedykowane: ZUS/US, Banki, operatorzy telekomunikacyjni, Rzecznika RPO.
- Opcjonalne nawiązanie współpracy z punktami obsługi przedsiębiorcy, na poziomie centralnym (Centrum Pomocy Przedsiębiorcy) oraz regionalnym (regionalne

dedykowane agencje/urzędy), oraz wykorzystanie polskich Digital Innovation Hubs oraz Parków Technologicznych jako kanałów dotarcia.

Treść podstawowa:

Podział na 3 segmenty, będące 3 grupami identyfikowalnymi, zrozumiałymi i namacalnymi z perspektywy odbiorcy. Cyberbezpieczeństwo firmy to wyzwanie dla:

Ciebie i twoich współpracowników

Twoich systemów

Twoich procesów biznesowych

W ramach każdego z segmentów powstanie lista porad/wskazówek/" przykazań" – jeśli to możliwe 10. Lista ta pojawi się na infografice. Dodatkowo każda ze wskazówek powinna być rozbudowana na nie więcej niż paragraf lub dwa z ew. odesłaniem do odpowiednich źródeł, które będą także zagregowane w ramach biblioteki. Rozbudowana część zostanie umieszczona na stronie www.

Kluczowe, aby materiał posługiwał się językiem nietechnicznym, ale biznesowym, dyskursem, który znają i wykorzystują na co dzień przedsiębiorcy. Także sama logika tłumaczenia określonych potrzeb użytkownika w zakresie bezpieczeństwa cyfrowego - porównania, metafory oraz wyjaśnienia – nie powinna opierać się na terminach wykorzystywanych w dokumentach czy standardach branżowych IT, ale na szeroko rozumianym dyskursie biznesowym.

Można w tym celu posłużyć się koncepcją „walki z mitami", wspartej statystyką z dostępnych raportów (np. w odniesieniu do trójkąta Pracownik-Infrastruktura-Biznes):

- Człowiek jest najczęściej atakowanym celem w Twojej firmie.
- Rozwiązania jakich używasz, bez względu na to, ile za nie zapłacisz, nie zapewnią 100% bezpieczeństwa Twojej firmie.
- Ludzie i technologie, aby bezpiecznie współistniały, muszą być dopasowane do codziennej aktywności Twojej firmy i jej celów.

W ramach proponowanych konkretnych porad materiał powinien uwzględnić kluczowe charakterystyki/trendy:

- wskazywanie na proceduralny, ciągły charakter cyberbezpieczeństwa – „nie budowanie zamków, a nauka tworzenia i zarządzania bezpiecznymi procesami”;
- odejście od podejścia „zrób wszystko sam” – które często zniechęca przedsiębiorców. Wskazanie możliwości wykorzystania szeregu (darmowych, płatnych lub wspieranych w ramach różnorodnych dotacji) produktów, usług jak i działań wdrożeniowych – z wyraźnym naciskiem na unikanie „wymyślania koła na nowo” jako praktycznej minimalizacji kosztów;
- zachęta do postrzegania świata jako katalogu usług (cyfrowych), który można użyć do stworzenia własnego unikalnego produktu biznesowego, z wszelkimi konsekwencjami konieczności zabezpieczeń „łańcucha dostaw”, wskazując na problemy „lock-in” oraz zarządzania dostawcami wraz z rozwiązaniami.
- zerwanie z językiem „ekskluzywności” świata cyfrowego i prezentowanie procesów i narzędzi oraz nawyków ludzi w ujęciu cyfryzacji globalnej, gdzie informacja=cyfrowa informacja, przez co staje się powszechnym i głównym medium wpływu na świat realny, wartym inwestycji, w tym w bezpieczeństwo.
- prezentowanie problematyki bezpieczeństwa cyfrowego z perspektywy korzyści biznesowych jakie niesie odpowiednie przygotowanie: pewność prowadzenia działalności, reputacja w oczach kontrahentów, zaufanie klientów.
- Wyjaśnienie znaczenia cyberbezpieczeństwa dla prawidłowego funkcjonowania MŚP
- Delikatnie zarysowana kwestia transparentności i wymiany/raportowania informacji o incydentach w związku z ustawą o Krajowym Systemie Cyberbezpieczeństwa oraz RODO w ujęciu odpowiedzialnego budowania bezpiecznego ekosystemu biznesowego zdolnego do wspólnej i koordynowanej reakcji na zagrożenia, które w pojedynkę nie są możliwe do zaadresowania.
- Minimalizacja użycia słowa „cyber” ☺ (z uwagi na np. pkt. 4)

6. Timeline

Grudzień 2018	Styczeń - Luty 2019	Marzec 2019	Marzec - Czerwiec 2019

- Podział prac w grupie - Rozpoczęcie tworzenia materiałów	- Stworzenie materiałów - Przeprowadzenie dwóch grup fokusowych - Kontakt z ZUS/US oraz ZBP/operatorami telco/rzecznik MŚP	- Stworzenie ostatecznego materiału - Zaplanowanie działań zewnętrznych (PR, kanały dotarcia)	- Uruchomienie strony - Kampania społeczna

Potrzeby logistyczne/wsparcie Ministerstwa Cyfryzacji:

- Styczeń-Luty 2019: Sfinansowanie/zrealizowanie dwóch grup fokusowych z MŚP
- Styczeń-Luty 2019: Zaaranżowanie współpracy grupy z ZUS/US oraz ZBP/operatorami telekomunikacyjnymi/Rzecznik MŚP
- Marzec 2019: Stworzenie materiałów graficznych – praca grafika
- Marzec 2019: Stworzenie strony www – praca informatyka + domena
- Marzec – Maj 2019: Sfinansowanie kampanii PR/społecznej

KPI:

- Liczba odsłon strony w okresie Marzec – Wrzesień 2019: 50 000
- Dotarcie z materiałem (infografika) poprzez kanały: 20 000 przedsiębiorstw (≈1% MŚP)
- Liczba impresji w mediach społecznościowych (własne + obce): 20 000
- Liczba artykułów oraz cytowań: 200

III. Zespół III – Jednostki Samorządu Terytorialnego

1. Cel główny

Zwiększanie świadomości i budowanie kompetencji w zakresie cyberbezpieczeństwa wśród jednostek samorządu terytorialnego w kontekście przyjęcia ustawy o krajowym systemie cyberbezpieczeństwa.

2. Cele szczegółowe

- Zaprojektowanie krótkoterminowych działań informacyjnych na temat ustawy o krajowym systemie cyberbezpieczeństwa kierowanych do jednostek samorządu terytorialnego.
- Zaprojektowanie długoterminowych działań zmierzających do podnoszenia poziomu cyberbezpieczeństwa wśród jednostek samorządu terytorialnego.

3. Skład zespołu

- dr hab. inż. Andrzej Białas, prof. Instytutu EMAG
- Ewelina Gładki, p.o. Dyrektora, Departament Społeczeństwa Informacyjnego, Urząd Marszałkowski Województwa Świętokrzyskiego
- Agnieszka Aleksiejczuk, Dyrektor, Departament Społeczeństwa Informacyjnego, Urząd Marszałkowski Województwa Podlaskiego
- Krzysztof Jędrzejewski, Kierownik Referatu Informatyzacji Urzędu, Departament Społeczeństwa Informacyjnego i Informatyki, Urząd Marszałkowski Województwa Pomorskiego
- Jacek Trzebiatowski, Administrator Bezpieczeństwa Teleinformatycznego, Departament Społeczeństwa Informacyjnego, Urząd Marszałkowski Województwa Warmińsko – Mazurskiego w Olsztynie
- Michał Jaworski, PIIT
- Paweł Walczak, PIIT
- Wiesław Paluszyński, PIIT
- Rafał Babraj, Zespół Analiz Strategicznych i Wpływu Nowoczesnych Technologii, NASK-PIB

Przewodniczący**: Magdalena Górnisiewicz**, Kierownik Zespołu Analiz Strategicznych i Wpływu Nowoczesnych Technologii, NASK PIB

4. Adresaci

Jednostki samorządu terytorialnego na trzech poziomach:

- poziom województwa (urzędy marszałkowskie),
- poziom powiatowy (powiaty, miasta na prawach powiatu),

– poziom gminny (miejskie, miejsko-wiejskie i wiejskie).

Dodatkowo proponujemy, żeby na każdym poziomie, działania prowadzone były w dwóch wymiarach:

– działania skierowane do każdego pracownika urzędu,
– działania skierowane do pracowników urzędów odpowiedzialnych za realizację zadań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa.

5. Zdiagnozowane potrzeby

Jednostki samorządu terytorialnego nie były do tej pory objęte obowiązkiem raportowania incydentów cyberbezpieczeństwa. Jest to bardzo duża i różnorodna grupa (małe i duże urzędy), dlatego działania powinny mieć wielowymiarowy charakter.

W pierwszej kolejności rekomendujemy poinformowanie wszystkich jednostek samorządu terytorialnego o ustawie o krajowym systemie cyberbezpieczeństwa oraz wynikających z niej obowiązkach, w tym przede wszystkim o obowiązku raportowania incydentów.

W drugiej kolejności rekomendujemy podjęcie działań zmierzających do budowy kompetencji w zakresie cyberbezpieczeństwa wśród jednostek samorządu terytorialnego. Zarówno wśród wszystkich pracowników, jak i wśród osób odpowiadających za realizację zadań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa. W tym aspekcie niezwykle istotne są szkolenia, których zakres jest uzależniony od specyfiki urzędu. Dlatego proponujemy, aby działania realizowane były na trzech poziomach: województwa, powiatu i gminy.

6. Proponowane działania i rozwiązania

Propozycje działań skierowane do **pracowników urzędów odpowiedzialnych za realizację zadań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa**

działanie	harmonogram	zaangażowane podmioty	mierniki
inicjatywy krótkoterminowe o wysokim priorytecie realizacji			
Zadanie 1. Przygotowanie materiałów informacyjnych na temat ustawy o krajowym systemie cyberbezpieczeństwa i współpracy z CERT Polska			
przygotowanie „toolbox” w zakresie zgłaszania	grudzień 2018	NASK PIB	„toolbox” w formie pdf gotowy do dystrybucji wśród

działanie	harmonogram	zaangażowane podmioty	mierniki
incydentów do CERT Polska (NASK)			jednostek samorządu terytorialnego
przygotowanie krótkiego opracowania na temat ustawy i wynikających z niej dla samorządu zadań i obowiązków (NASK)	grudzień 2018	NASK PIB	opracowanie w formie pdf gotowego do dystrybucji wśród jednostek samorządu terytorialnego
przygotowanie „toolbox” na temat zadań osoby kontaktowej	grudzień 2018	NASK PIB	opracowanie w formie pdf gotowego do dystrybucji wśród jednostek samorządu terytorialnego
Zadanie 2. Przekazanie informacji na temat ustawy o krajowym systemie cyberbezpieczeństwa do jednostek samorządu terytorialnego			
rozesłanie pisma do jednostek samorządu terytorialnego, informującego o zadaniach i obowiązkach wynikających zustawy o krajowym systemie cyberbezpieczeństwa	styczeń 2019	MC, MSWiA	rozesłanie pisma
wystąpienie ministra na Komisji Wspólnej Rządu i Samorządu (prezentacja „toolbox” i opracowania)	pierwszy kwartał 2019	MC	wystąpienie ministra
inicjatywy długoterminowe			
Zadanie 1. Podnoszenie kwalifikacji pracowników urzędów odpowiedzialnych za realizację zadań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa			

działanie	harmonogram	zaangażowane podmioty	mierniki
specjalistyczne szkolenia we współpracy z NASK (zakres ćwiczeń uzależniony od kompetencji i potrzeb konkretnego urzędu) przykłady szkoleń: szkolenie z zakresu ustawy o krajowym systemie cyberbezpieczeństwa – co wynika z nowych przepisów dla samorządów? jakie są zadania/ obowiązki? szkolenie z zakresu współpracy z CERT Polska szkolenie z zakresu tworzenia Zespołu Reagowania na Incydenty Komputerowe szkolenie z zakresu obsługi incydentu – procedury	pierwsze szkolenia: pierwsza połowa 2019	NASK PIB, MC	listy obecności ze szkoleń
specjalistyczne szkolenia we współpracy z PIIT (zakres ćwiczeń uzależniony od kompetencji i potrzeb konkretnego urzędu) przykłady szkoleń: zabezpieczenia systemów operacyjnych: Linux, Windows Server oraz stacji roboczych Windows	pierwsze szkolenia: pierwsza połowa 2019	MC, PIIT	listy obecności ze szkoleń

działanie	harmonogram	zaangażowane podmioty	mierniki
bezpieczeństwo usług: Serwery WWW, Active Directory, Exchange, Sharepoint itp. bezpieczeństwo aktywnych urządzeń sieci komputerowej (różni vendorzy) bezpieczny pracownik (szkolenie dla każdego pracownika) szkolenie podnoszące świadomość bezpieczeństwa IT – dla pracowników nietechnicznych laboratorium analizy malware'u powłamaniowa analiza incydentów bezpieczeństwa IT tworzenie i zarządzanie zespołami obsługi incydentów naruszenia bezpieczeństwa CERT/CSIRT zarządzanie incydentami bezpieczeństwa teleinformatycznego rozpoznanie i obrona przed atakami socjotechnicznymi aktualne metody oszustw internetowych organizacja cyberbezpieczeństwa w jednostkach samorządu terytorialnego			

działanie	harmonogram	zaangażowane podmioty	mierniki
utworzenie platformy e-learningowej – system samodoskonalenia dla pracowników urzędów	koniec 2019	NASK PIB, MC	zarejestrowanie na platformie 10 jednostek samorządu terytorialnego
Zadanie 2. Regularne ćwiczenia z zakresu cyberbezpieczeństwa mające na celu testowanie współpracy z CERT Polska i zarządzanie kryzysowe w przypadku incydentów teleinformatycznych (krótkie ćwiczenia proceduralne – raz na 2/ 3 miesiące; coroczne ćwiczenia typu „tabletop")			
przygotowanie planu ćwiczeń	połowa 2019	MC, NASK PIB	plan przygotowany przez NASK uzyskuje akceptację MC
przeprowadzenie pilotażowych ćwiczeń proceduralnych	2019	MC, MSWiA, NASK PIB, RCB	sprawozdanie z ćwiczenia
przeprowadzenie pilotażowych ćwiczeń tabletop	2019	MC, MSWiA, NASK PIB, RCB	sprawozdanie z ćwiczenia
regularne ćwiczenia proceduralne i tabletop	działanie ciągłe	MC, MSWiA, NASK, PIB RCB	sprawozdanie z ćwiczenia

Propozycje działań skierowane **do każdego pracownika urzędu**

działanie	harmonogram	zaangażowane podmioty	mierniki
inicjatywy krótkoterminowe o wysokim priorytecie realizacji			
Zadanie 1. Uwzględnienie raportowania incydentów w polityce bezpieczeństwa urzędu			
ustanowienie procedury raportowania incydentów w urzędzie	pierwszy kwartał 2019	każdy urząd	procedury raportowania incydentów uwzględnione w polityce bezpieczeństwa urzędu

działanie	harmonogram	zaangażowane podmioty	mierniki
wyznaczenie osoby do kontaktów z CERT Polska i przekazanie tych informacji do NASK PIB	pierwszy kwartał 2019	każdy urząd NASK/ CERT Polska	lista osób kontaktowych z jednostek samorządu terytorialnego w NASK PIB
Zadanie 2. Przeszkolenie pracowników urzędu z raportowania incydentów			
przygotowanie „toolbox" na temat zgłaszania incydentów w urzędzie	pierwszy kwartał 2019	każdy urząd	„toolbox" w formie pdf gotowy do dystrybucji wśród pracowników
dystrybucja „toolbox" wśród pracowników urzędów	pierwszy kwartał 2019	każdy urząd	
inicjatywy długoterminowe			
Zadanie 1. Wprowadzenie szkoleń z zakresu podstawowej wiedzy na temat cyberbezpieczeństwa: szkolenia wstępne – razem ze szkoleniami BHP i ODO oraz szkolenia okresowe (raz na 2 lata)			
przygotowanie „toolbox" dla trenerów i materiałów edukacyjnych	pierwszy kwartał 2019	MC, NASK PIB, PIIT	„toolbox" w formie pdf gotowy do dystrybucji wśród jednostek samorządu terytorialnego
szkolenia trenerów z urzędów, tak aby mogli dalej przekazywać wiedzę w sposób kaskadowy	pierwsza połowa 2019	MC, NASK PIB, PIIT	listy obecności ze szkoleń
szkolenie z zasad cyberhigieny – przygotowanie quizu i gry paragrafowej dla pracowników urzędów	koniec 2019 (zadanie zlecone dla NASK)	MC, NASK PIB	przygotowanie quizu i gry paragrafowej
Zadanie 2. Regularne ćwiczenia z zakresu cyberbezpieczeństwa (krótkie ćwiczenia proceduralne – raz na 2/ 3 miesiące; coroczne ćwiczenia typu „tabletop")			
przygotowanie „toolbox" dla koordynatorów ćwiczeń w urzędach	połowa 2019	MC, NASK PIB	„toolbox" w formie pdf gotowy do dystrybucji wśród

działanie	harmonogram	zaangażowane podmioty	mierniki
			jednostek samorządu terytorialnego
szkolenia dla koordynatorów ćwiczeń w urzędach, tak aby mogli z powodzeniem przygotować ćwiczenia typu tabletop	2019 - 2020	MC, NASK PIB	listy obecności ze szkoleń
przeprowadzenie ćwiczeń	działanie ciągłe	JST	sprawozdanie z ćwiczeń

Załączniki:

Załącznik 1: Toolbox – zgłaszanie incydentów do CERT Polska

Załącznik 2: Poradnik dla samorządów – ustawa o KSC

IV. Zespół IV – Indywidualni użytkownicy Internetu

1. Cel:

Zwiększenie kompetencji bezpiecznego korzystania z internetu wśród osób dorosłych.

2. Skład zespołu:

Dorota Górecka (Fundacja Nowoczesna Polska),

Magdalena Górnisiewicz (NASK),

Justyna Balcewicz (NASK),

Tomasz Bukowski (Krajowa Izba Komunikacji Ethernetowej).

Konsultacja: Anna Obem (Fundacja Panoptykon).

3. Adresaci:

Osoby w wieku 18-65, które zakończyły edukację formalną i są aktywne na rynku pracy

4. Zdiagnozowane potrzeby

Aby skutecznie podnieść poziom cyberbezpieczeństwa wśród indywidualnych użytkowników internetu musimy kompleksowo oddziaływać na ogólny poziom kompetencji cyfrowych społeczeństwa. Należy zatem przyjąć szeroką definicję kompetencji cyfrowych, uwzględniającą zarówno umiejętność korzystania z odpowiednich narzędzi i zabezpieczeń technicznych, jak również kompetencje miękkie, w tym przede wszystkim umiejętność krytycznego myślenia, analizy informacji i dbania o własną prywatność. Bez odpowiednich kompetencji miękkich użytkownicy nie będą w stanie oceniać ryzyka i odpowiadać na wyzwania w dynamicznie zmieniającym się świecie technologii. Takie podejście zastosowano w „Katalogu kompetencji medialnych, informacyjnych i cyfrowych”[5] opracowanym w ramach projektu dofinansowanego przez Ministerstwo Cyfryzacji. Fragmenty bezpośrednio związane z zagadnieniami dot. bezpieczeństwa stanowią załącznik do niniejszego raportu.

W edukacji nt. cyberbezpieczeństwa kluczowe jest także znalezienie równowagi pomiędzy zwracaniem uwagi na zagrożenia i korzyści związane z korzystaniem z sieci. Przedstawiając możliwe zagrożenia łatwo jest zniechęcić zwłaszcza początkujących użytkowników do korzystania z Internetu. Dlatego warto pokazywać, że wdrożenie podstawowych zasad

[5] *Katalog kompetencji medialnych, informacyjnych i cyfrowych,* Fundacja Nowoczesna Polska, 2014, http://katalog.edukacjamedialna.edu.pl/, CC BY-SA (dostęp 4.12.2018)

bezpiecznego korzystania z narzędzi cyfrowych znacznie może podnieść poziom naszego bezpieczeństwa.

Kolejną potrzebą jest edukacja dotycząca mechanizmów działania technologii. Zrozumienie tego, jak działa internet i związane z nim technologie oraz jak są one wykorzystywane przez różne podmioty. Dzięki temu użytkownicy będą mogli świadomie podjąć decyzję odnośnie swoich zachowań w sieci oraz zabezpieczeń, które chcą stosować.

Rekomendujemy także kontynuację dotychczasowych działań, takich jak:

- Europejski Miesiąc Cyberbezpieczeństwa
- Szkolenia dla dorosłych organizowane w ramach konkursów POPC
- Wielki Test o Internecie transmitowany w TVP
- Współpraca z artystami na rzecz podnoszenia świadomości wyzwań związanych z technologiami cyfrowymi (przykładem takiego działania był konkurs na plakat „Inspiracja – interakcja – internet" organizowany przez Akademię NASK)

5. Proponowane działania i rozwiązania

W krótkiej perspektywie

Przygotowanie otwartego konkursu grantowego dla organizacji pozarządowych na prowadzenie kampanii i działań edukacyjnych. Rekomendujemy sformułowanie regulaminu konkursu w ten sposób, aby umożliwić wnioskodawcom zgłaszanie własnych, innowacyjnych pomysłów, które realizują wskazany w konkursie cel, zamiast zlecanie wykonania z góry zaprogramowanego zadania.

Opracowanie testu kompetencji cyfrowych, uwzględniających tematykę cyberbezpieczeństwa, z komentarzami do poszczególnych pytań, dzięki któremu użytkownicy zidentyfikują obszary, w których ich wiedza wymaga uzupełnienia oraz znajdą linki do materiałów, które pomogą im w podniesieniu swoich kompetencji.

Prowadzenie przez MC oficjalnej listy rekomendowanych inicjatyw (kampanie, materiały edukacyjne, szkolenia) z obszaru cyberbezpieczeństwa. Materiały z tego obszaru zostały już zinwentaryzowane w ramach projektu edukacyjnego realizowanego przez fundację Nowoczesna Polska „Cybernauci – kształtowanie bezpiecznych zachowań w sieci" https://cybernauci.edu.pl/katalog/. Kolejnym krokiem powinna być ich weryfikacja merytoryczna oraz rozpowszechnianie.

Przygotowanie i realizacja planu promocji inicjatyw edukacyjnych, które uzyskały patronat MC, z wykorzystaniem dostępnych kanałów komunikacji Ministerstwa (obecnie przyznanie patronatu nie pociąga za sobą działań tego typu).

W dalszej perspektywie

Opracowanie kodeksu dobrych praktyk związanych z mówieniem o korzystaniu z sieci z zachowaniem równowagi pomiędzy zagrożeniami a korzyściami, z udziałem psychologów, socjologów, organizacji pozarządowych itd.

Przygotowanie atrakcyjnych materiałów edukacyjnych np. w formie wiedo, wyjaśniających mechanizmy działania technologii. Przykładowe tematy: chmura, blockchain, aplikacja.

Zaangażowanie operatorów telekomunikacyjnych w działania edukacyjne skierowane do użytkowników. Przeprowadzenie wspólnej kampanii edukacyjnej np. w ramach Szerokiego Porozumienia na rzecz Rozwoju Umiejętności Cyfrowych.

Przygotowanie szerokiej kampanii społecznej, która może uwzględniać np. wprowadzenie wątków związanych z bezpieczeństwem cyfrowym do popularnych seriali obyczajowych lub przygotowanie produktu, który jest atrakcyjny sam w sobie (np. krzyżówka dla seniorów, książka dla dzieci z treściami edukacyjnymi z zakresu cyberbezpieczeństwa). Aby zapewnić trwałość rezultatów, każda kampania musi być podbudowana materiałami edukacyjnymi, dzięki którym użytkownicy będą mogli wzmacniać swoje kompetencje.

Ścisła współpraca z Ministerstwem Edukacji w obszarze edukacji w zakresie cyberbezpieczeństwa w szkołach i wsparcia udzielanego nauczycielom w tym obszarze.

6. Załącznik 1

Wybrane kompetencje z „Katalogu kompetencji medialnych, informacyjnych i cyfrowych" (Fundacja Nowoczesna Polska, 2014)

Ochrona prywatności i wizerunku

- Umie zdecydować, czy w danej sytuacji komunikacja powinna być prywatna czy publiczna. - Zna podstawowe sposoby zapewnienia prywatności komunikacji i wie, że mogą różnić się skutecznością; np. wiadomość prywatna do konkretnej osoby zamiast rozmowy na czacie, wiadomość e-mail zamiast rozmowy na forum internetowym, SMS zamiast wiadomości w sieci społecznościowej.
- Wie, że wiadomości e-mail można szyfrować, a aplikacje umożliwiające komunikację różnią się stopniem zapewnianej prywatności i niektóre z nich również mogą zapewniać szyfrowanie.
- Umie posłużyć się najprostszymi narzędziami zwiększającymi prywatność np. pluginy, dodatki stanowiące rozszerzenia przeglądarek WWW, ustawienia prywatności w przeglądarce, ustawienia lokalizacji w telefonie.
- Umie zidentyfikować różnice pomiędzy sposobami określania jego lokalizacji używanymi w telefonach komórkowych. Potrafi określić, w których przypadkach korzystanie z danych lokalizacyjnych przez aplikacje jest uzasadnione.
- Zna przeznaczenie regulaminów na stronach WWW (serwisach WWW) i aplikacjach, z których korzysta i wie, że powinno się je poznać przed skorzystaniem z danego serwisu/aplikacji.
- Rozumie treści typowych regulaminów korzystania ze stron WWW (serwisów WWW) i aplikacji.
- Wie, że w trakcie instalacji, w zależności od systemu operacyjnego, aplikacje mogą wymagać przyznania uprawnień dostępu do różnych rodzajów funkcji urządzenia oraz danych użytkownika.
- Rozumie różnice pomiędzy różnymi grupami uprawnień i umie świadomie podjąć decyzję ich przyznaniu lub odmowie.

<u>Anonimowość</u>

- Zna przykłady narzędzi zwiększających anonimowość: np. aplikacje klienckie sieci TOR. Wie, że takie narzędzia są używane przez działaczy społecznych i politycznych, ofiary przemocy, sygnalistów (whistleblowerów). Rozumie, że narzędzia zwiększające anonimowość nie zwalniają z odpowiedzialności za własne czyny. Umie posłużyć się narzędziami o takich zastosowaniach.
- Wie, że anonimowość w sieci może być pozorna i że możliwe jest ustalenie autora danej informacji, nawet jeżeli używał pseudonimu lub fałszywych danych; np. że

w pewnych sytuacjach nawet zwykły internauta może zidentyfikować osobę ukrytą pod pseudonimem na podstawie innych udostępnionych przez nią informacji oraz że w razie potrzeby osoby lub instytucje dysponujące odpowiednimi kompetencjami mogą identyfikować autora na podstawie m.in. miejsca, urządzeń i łączy, z których korzystał.

- Wie, że nawet korzystając z odpowiednich narzędzi, może utracić anonimowość przez nieostrożne udostępnienie informacji w treści komunikacji (np. ujawniając swój adres, imię lub informacje identyfikujące pośrednio: miejsce pracy i stanowisko itp.).

Bezpieczeństwo komunikacji, pracy i transakcji

- Umie rozpoznać spam i typowe próby phishingu; np. zwraca uwagę na to, że nie zgadza się adres strony bankowej.
- Wie, że istnieją metody maskowania adresu nadawcy wiadomości.
- Wie, co to są certyfikaty uwierzytelniające (certyfikaty strony).
- Wie, że strony przetwarzające dane prywatne lub wrażliwe (np. strony banków, sieci społecznościowe, poczta, sklepy internetowe) powinny być zabezpieczone protokołem HTTPS.
- Umie postępować, kiedy napotyka najprostsze komunikaty o certyfikatach np. nie akceptuje automatycznie każdego napotkanego błędnego certyfikatu zgłoszonego przez przeglądarkę albo aplikację pocztową.
- Wie, że istnieją narzędzia zwiększające bezpieczeństwo komunikacji. Umie znaleźć przykładowe narzędzia zwiększające bezpieczeństwo komunikacji np. szyfrowanie end-to-end, poczty elektronicznej (PGP/GPG), wiadomości SMS.
- Rozumie, że poczucie bezpieczeństwa może być złudne, a zapewnienia twórców aplikacji (np. dotyczące zabezpieczeń) nie zawsze są zgodne z prawdą.
- Umie wybrać spośród różnych rodzajów połączenia np. wybiera bezpłatne wifi, aby uniknąć kosztów.
- Wie, że dokonywanie zakupów online obarczone jest ryzykiem.
- Wie, że należy być ostrożnym przy podawaniu własnych danych osobowych i danych karty kredytowej lub debetowej przy dokonywaniu zakupów online (np. trzeba zwracać uwagę na renomę sklepu czy też firmy publikującej aplikację).
- Wie, że konsekwencje zachowań komunikacyjnych (również online) mogą wpływać na inne osoby (np. informacja o bliskich lub współpracownikach może negatywnie wpłynąć na ich bezpieczeństwo lub poczucie prywatności).
- Wie, co to jest spam. Zna podstawowe reguły postępowania ze spamem.
- Umie rozpoznać stalking. Wie, że należy reagować na stalking, również w odniesieniu do osób trzecich (np. bliskich, współpracowników).
- Wie, jak postępować w przypadku telefonu od telemarketera

- Umie rozpoznać cyberbullying. Wie, że należy reagować na cyberbullying, również w odniesieniu do osób trzecich (np. bliskich, współpracowników).
- Zna pojęcie cyfrowego wizerunku. Wie, że cyfrowy wizerunek można kształtować (np. odpowiednio dobierając zdjęcia umieszczane w portalach społecznościowych).
- Umie zarządzać cyfrowym wizerunkiem; świadomie podejmuje decyzję, na ile cyfrowy wizerunek odzwierciedla jego prawdziwą tożsamość; np. o publikowaniu danych oraz o zakresie publikowanych danych umożliwiających odkrycie jego/jej tożsamości.

Nadzór nad siecią

- Zna podstawowe cele wprowadzania nadzoru; np. walka z cyberprzestępczością, uzyskiwanie przez osoby lub instytucje przychodów ze sprzedaży prywatnych danych użytkowników.
- Wie, że nadzór może być legalny lub bezprawny; że może być prowadzony nie tylko przez organy państwowe (np. policję), ale także przez osoby prywatne czy korporacje; że nawet pewne formy nadzoru przez organy państwa mogą być nielegalne.
- Wie, że istnieją metody obejścia/utrudnienia nadzoru.
- Zna pojęcie ciasteczka (cookie). Rozumie podstawowe zastosowania ciasteczek.
- Wie, że ciasteczka bywają wykorzystywane do działań sprzecznych z jego/jej interesem i bezpieczeństwem.
- Wie, że jedyną pewną metodą wyłączenia urządzenia jest wyjęcie z niego baterii.

Uzależnienia i higiena korzystania z mediów

- Umie świadomie kształtować swoje nawyki związane z korzystaniem z technologii (np. wylogowuje się z sieci społecznościowej lub zamyka komunikator, by nie rozpraszały przy pracy).
- Umie zareagować na negatywne zachowania u innych, np. pomagając uzyskać pomoc specjalisty.
- Umie zaobserwować oznaki zagrożenia uzależnieniem u siebie i u innych (np. zaniedbywanie bieżących obowiązków wskutek poświęcania zbyt dużej ilości czasu na aktywność w mediach społecznościowych).
- Wie, że istnieją powiązania pomiędzy własnymi działaniami w mediach a innymi sferami życia (np. publikowanie nieprzemyślanych wypowiedzi może skutkować złą opinią pracodawcy lub nawet zamknięciem pewnych dróg kariery).

Chmura

- Wie, że przechowywanie plików "w chmurze" wiąże się z akceptacją regulaminu i może oznaczać, że usługodawca będzie sprawdzać, jakie pliki są w niej trzymane;

może też oznaczać, że usługodawca będzie kasować pliki, które są lub wydają się niezgodne z regulaminem (np. faktyczne lub domniemane naruszenie prawa autorskiego).

- Rozumie, że pliki trzymane "w chmurze" są faktycznie pod kontrolą usługodawcy.

Ekosystem aplikacji

- Rozumie, że instalowane aplikacje mogą mieć dostęp do wielu funkcji urządzenia, a także danych użytkownika;
- Wie, że, w zależności od systemu operacyjnego, istnieje wiele źródeł aplikacji mobilnych prowadzonych przez różne podmioty;
- Umie ocenić wiarygodność aplikacji w oparciu o jej pochodzenie, dostępność kodu źródłowego itp. kryteria
- Wie, jakie są podstawowe modele funkcjonowania na rynku aplikacji mobilnych (sprzedaż aplikacji, reklama, model freemium, finansowanie publiczne, wolne oprogramowanie tworzone przez społeczność)

Zapośredniczenie komunikacji

- Wie, że operator serwisu społecznościowego może kontrolować komunikację użytkowników, decydując np. o wyświetleniu lub nie danych postów konkretnym osobom, bądź o usunięciu prowadzonej w takim serwisie „strony”.
- Umie wskazać środki komunikacji, które zostawiają większą kontrolę użytkownikom (np. e-mail, blog)