Źródła informacji dot. cyberbezpieczeństwa

Warszawa, 2022

ENTRAST Sp. z o.o. ul. Dzielna 60, 01-029 Warszawa
Tel.:+48 791 910 931| email: iod@entrast.pl | www.entrast.pl
REGON: 382891916 | NIP: 5272887675 | KRS: 0000778304

Spis treści

Wstęp

Niniejszej opracowanie zostało stworzone w celu identyfikacji poziomu cyberbezpieczeństwa w Polsce. Spółka ENTRAST przekazuje niniejszy dokument celem zapoznania się w trakcie przeprowadzanych przez audytów lub diagnoz związanych z cyberbezpieczeństwem.

ENTRAST uznaję ten dokument jako źródło wiedzy w zakresie cyberbezpieczeństwa na terenie Polski i w sposób minimalny powinien być zapoznawany.

W pierwszej kolejność wskazano czym określa się podmiot publiczny oraz wskazano jego obowiązki. Bezsprzecznie należy wskazać, że JST (jednostki samorządu terytorialnego) w tym gminy należy do nich zaliczyć.

Następnie identyfikowano operatora usług kluczowych oraz wykazano jego obowiązki i metodykę obsługiwania incydentów. Ponadto wskazano w jaki sposób organizowany jest sektorowy zespół cyberbezpieczeństwa SZC – w kierunku CSRIT.

1. Podmioty publiczne

Podmiotem publicznym w rozumieniu ustawy o krajowym systemie bezpieczeństwa są:

- Organy władzy publicznej w tym organy administracji samorządowej, jednostki samorządu terytorialnego, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały,
- Jednostki budżetowe, samorządowe zakłady budżetowe, agencje wykonawcze, instytucje gospodarki budżetowej,
- Uczelnie publiczne i Polska Akademia Nauk,
- Zakład Ubezpieczeń Społecznych, Kasa Rolniczych Ubezpieczeń Społecznych, Narodowy Fundusz Zdrowia, Narodowy Bank Polski, Bank Gospodarstwa Krajowego,
- Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej.

Obowiązki podmiotu publicznego

Podstawowe obowiązki dla podmiotów publicznych to:

- wyznaczenie osoby kontaktowej do spraw cyberbezpieczeństwa, która będzie kontaktować się z organami właściwymi do spraw cyberbezpieczeństwa (CSIRT),
- obsługa incydentów,
- zapewnianie dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i sposobów zabezpieczania się przed tymi zagrożeniami,
- zgłaszanie incydentów do właściwego CSIRT.

Podmioty publiczne są zobligowane do zgłaszania incydentów, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez dany podmiot publiczny. Ustawa nie wprowadza progów na zgłoszenie incydentu w podmiocie publicznym, tak jak jest to w przypadku operatorów usług kluczowych czy dostawców usług cyfrowych. Oznacza to, że podmiot publiczny musi zgłaszać wszystkie incydenty, które powodują (lub mogą spowodować) obniżenie jakości lub przerwanie realizacji.

2. Operatorzy usług kluczowych

Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369) określa operatorów usług kluczowych, jako firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Kluczowe sektory gospodarki to: energetyczny, transportowy, bankowy i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej.

Kim jest operator usług kluczowych?

Operatorem usługi kluczowej (zwany dalej OUK) jest podmiot, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy (Minister odpowiedzialny za dany dział administracji rządowej) wydał decyzję o uznaniu za OUK.

Organ właściwy wydaje decyzję o uznaniu podmiotu za OUK, jeżeli:

- podmiot świadczy usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, zwaną dalej „usługą kluczową", wymienioną w wykazie usług kluczowych;
- świadczenie tej usługi kluczowej zależy od systemów informacyjnych;
- incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora.
- Rada Ministrów określiła, w drodze rozporządzenia z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806):

- wykaz usług kluczowych, kierując się przyporządkowaniem usługi kluczowej do danego sektora, podsektora i rodzaju podmiotu oraz znaczeniem usługi dla utrzymania krytycznej działalności społecznej lub gospodarczej;
- progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w wykazie usług kluczowych.

Operatorzy usług kluczowych - obowiązki

Do najważniejszych grup obowiązków OUK należą:

- zarządzanie ryzykiem (w tym szacowanie ryzyka);
- wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych (w tym utrzymanie i bezpieczną eksploatację systemu informacyjnego; bezpieczeństwo fizyczne i środowiskowe; bezpieczeństwo i ciągłość dostaw; wdrażanie, dokumentowanie i utrzymywanie planów działania);
- zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty;
- zgłaszanie incydentu poważnego do właściwego zespołu CSIRT;
- obsługa incydentów i współpraca w tym zakresie z właściwym CSIRT;
- wyznaczenie osoby kontaktowej na potrzeby krajowego systemu cyberbezpieczeństwa.

W momencie otrzymania od organu właściwego decyzji administracyjnej OUK zobowiązany jest dokonać następujących działań:

W terminie 3 miesięcy od dnia otrzymania decyzji od organu właściwego operator: dokonuje szacowania ryzyka dla swoich usług kluczowych, zarządza incydentami, wyznacza osobę kontaktową z właściwym CSIRT i organem właściwym do spraw cyberbezpieczeństwa, prowadzi działania edukacyjne wobec użytkowników, obsługuje incydenty we własnych systemach, zgłasza incydenty poważne, usuwa wskazywane podatności;

W terminie 6 miesięcy od dnia otrzymania decyzji: wdraża odpowiednie i adekwatne do oszacowanego ryzyka środki techniczne i organizacyjne, zbiera informacje o zagrożeniach i podatnościach, stosuje środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego, stosuje wymaganą dokumentację;

W terminie 12 miesięcy od dnia otrzymania decyzji: przygotowuje pierwszy audyt w rozumieniu ustawy, przekazuje sprawozdanie z audytu, wskazanym w ustawie podmiotom.

Jednocześnie za niewykonanie ww. obowiązków wynikających z ustawy, przewidziano zastosowanie kar finansowych.

Przekazanie przez UOK informacji dotyczących incydentu

OUK przekazuje informacje nt. incydentu poważnego będącego incydentem, który powoduje lub może spowodować poważne obniżenie, jakości lub przerwanie ciągłości działania świadczonej usługi kluczowej;

Jednocześnie należy zauważyć, że CSIRT może zmienić klasyfikację incydentu na incydent krytyczny skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi.

Sposób przekazania przez OUK informacji dotyczących incydentu:

- Operator zgłasza incydent niezwłocznie, nie później niż w ciągu 24H od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV,
- Operator współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane,
- Operator usuwa wskazane podatności oraz informuje o ich usunięciu organ właściwy,
- Ustawa przedstawia szczegółowo klasyfikację incydentów oraz zakres kompetencji CSIRT MON, CSIRT NASK, CSIRT GOV.

W momencie wystąpienia incydentu OUK, po jego uprzednim zgłoszeniu przystępuje do jego obsługi zgodnie z następującym schematem działań:

- Wykrywanie;
- Rejestrowanie;
- Analizowanie;
- Klasyfikowanie;
- Priorytetyzowanie;

- Podejmowanie działań naprawczych;
- Ograniczenie skutków incydentu.

Sektorowy Zespół Cyberbezpieczeństwa (SZC)

Organ właściwy w celu koordynacji incydentów w regulowanym przez siebie sektorze może powołać Sektorowy Zespół Cyberbezpieczeństwa. Do jego zadań w szczególności należy:

- przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w ich obsłudze;
- wspieranie operatorów usług kluczowych w wykonywaniu obowiązków;
- analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z ich obsługi;
- współpraca z właściwym CSIRT NASK, CSIRT GOV, CSIRT MON w zakresie koordynowania obsługi incydentów poważnych;
- SZC może przekazywać do innych państw i przyjmować od nich informacje o incydentach poważnych, w tym dot. dwóch lub większej liczby państw członkowskich UE.
- SZC może otrzymywać zgłoszenia incydentu poważnego z innego państwa członkowskiego UE, dot. dwóch lub większej liczby państw. Takie zgłoszenia przekazuje do właściwego CSIRT NASK, CSIRT GOV, CSIRT MON oraz PPK.

3. Organy właściwe

Ustawa o krajowym systemie cyberbezpieczeństwa wyróżnia kilka sektorów będących sektorami kluczowymi dla funkcjonowania Państwa. Poszczególne sektory są nadzorowane przez Ministerstwa odpowiedzialne za poszczególne działy gospodarki.

Sektory te to:

- sektor energetyczny,
- transportowy,
- bankowy i infrastruktury rynków finansowych,
- ochrony zdrowia,
- zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej.

W ustawie o KSC określono organy właściwe nadzorujące ww. sektory:

- Minister właściwy ds. energii i gospodarki wodnej (Ministerstwo Klimatu i Środowiska) – dla sektora energii i gospodarki wodnej;
- Minister właściwy ds. transportu (Ministerstwo Infrastruktury) - dla sektora transportu (włącznie z podsektorem transport wodny),
- Komisja Nadzoru Finansowego - dla sektora bankowego i infrastruktury rynków finansowych,
- Minister właściwy ds. zdrowia (Ministerstwo Zdrowia) - dla sektora ochrony zdrowia,
- Minister właściwy ds. informatyzacji (Kancelaria Prezesa Rady Ministrów) - dla sektora infrastruktury cyfrowej,
- Minister obrony narodowej (Ministerstwo Obrony Narodowej) dla sektora zdrowia i infrastruktury cyfrowej w zakresie podmiotów podległych Ministrowi obrony narodowej.

Zadania Organu Właściwego:

- na bieżąco prowadzi analizę podmiotów w danym sektorze lub podsektorze pod katem uznania ich za operatora usługi kluczowej;
- wydaje decyzje o uznaniu podmiotu za operatora usługi kluczowej;
- przygotowuje rekomendacje działań mających na calu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące działania incydentów (współpraca z CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa);
- prowadzi kontrole operatorów usług kluczowych i dostawców usług cyfrowych (monitoruje stosowanie przez nich przepisów ustawy);
- na wniosek CSIRT NASK, CSIRT GOV LUB CSIRT MON wzywa operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie podatności które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego;
- uczestniczy w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w RP lub UE;
- dla danego sektora lub podsektora może organ właściwy może ustanowić, sektorowy zespół cyberbezpieczeństwa (organy właściwe decydują jak je ustanawiają i w jakiej formie prawnej).

W zakresie wyznaczenia przez dany organ właściwy operatorów usług kluczowych obowiązuje następująca procedura:

- organ właściwy bada rynek w celu identyfikacji potencjalnych operatorów usług kluczowych,

- organ właściwy zaczyna postepowanie administracyjne i zbiera informacje o podmiocie,
- organ właściwy sprawdza, czy podmiot spełnia wymogi rozporządzenia,
- organ właściwy wskazuje operatora usługi kluczowej poprzez wydanie decyzji administracyjnej,
- operator usługi kluczowej ma od 3 do 12 miesięcy na dostosowanie się do wymogów zawartych w rozporządzeniu,
- operator usługi kluczowej realizuje obowiązki wynikające z ustawy

4. Dostawcy usług cyfrowych

04.04.2019

Wymogami ustawy o KSC zostali także objęci dostawcy usług cyfrowych, czyli internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe. Z racji międzynarodowej specyfiki tych podmiotów, obowiązki dla dostawców usług cyfrowych są objęte zharmonizowanym na poziomie UE reżimem regulacyjnym.

Kim jest Dostawca Usług Cyfrowych?

Dostawcami usług cyfrowych (dalej: „DUC") są osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej, mające siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadczące określone w ustawie o KSC usługi cyfrowe.

Ustawa nakłada na DUC obowiązek zapewnienia poziomu bezpieczeństwa współmiernego do stopnia ryzyka, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług cyfrowych, ze względu na znaczenie tych usług dla działalności innych przedsiębiorców w Unii.

Zharmonizowane podejście na poziomie Unii mają zapewnić akty wykonawcze, w tym rozporządzenie wykonawcze Komisji Europejskiej 2018/151. W rozporządzeniu doprecyzowano elementy, jakie mają zostać uwzględnione przez dostawców usług cyfrowych przy określaniu i przedsiębraniu środków mających na celu zapewnienie poziomu bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez nich w kontekście oferowania usług, jak również parametry, które należy wziąć pod uwagę w celu ustalenia, czy incydent ma istotny wpływ na świadczenie tych usług.

Podobnie jak w przypadku operatorów usług kluczowych za niewykonanie obowiązków przez DUC wynikających z ustawy o krajowym systemie cyberbezpieczeństwa, przewidziano zastosowanie kar finansowych.

Główne obowiązki Dostawcy Usług Cyfrowych

- przeprowadza czynności umożliwiające wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów,
- zapewnia w niezbędnym zakresie dostęp do informacji właściwemu CSIRT o incydentach zakwalifikowanych jako krytyczne przez właściwy CSIRT,
- klasyfikuje incydent jako istotny,
- zgłasza incydent istotny niezwłocznie, nie później jednak niż w ciągu 24H od momentu wykrycia, do właściwego CSIRT,
- zapewnia obsługę incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT, przekazując niezbędne dane,
- usuwa podatności,
- przekazuje operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora.

Dostawca usług cyfrowych przekazuje informacje dotyczące incydentu istotnego będącego incydentem, który ma istotny wpływ na świadczenie usługi cyfrowej.

Dostawca usługi cyfrowej w celu sklasyfikowania incydentu jako istotnego uwzględnia w szczególności:

- liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług,
- czas trwania incydentu,
- zasięg geograficzny obszaru, którego dotyczy incydent,
- zakres zakłócenia funkcjonowania usługi,
- zakres wpływu incydentu na działalność gospodarczą i społeczną.

Dostawca usługi cyfrowej nie ma obowiązku dokonania zgłoszenia, gdy nie posiada informacji pozwalających na ocenę istotności wpływu incydentu na świadczenie usługi cyfrowej.

5. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)

04.04.2019

Ustawa o krajowym systemie cyberbezpieczeństwa ustanowiła trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego: CSIRT NASK, CSIRT GOV oraz CSIRT MON. Każdy z CSIRT odpowiedzialny jest za koordynację incydentów zgłaszanych przez przyporządkowane zgodnie z ustawą podmioty.

CSIRT NASK

CSIRT NASK – prowadzony jest przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Do głównych zadań zespołu CSIRT NASK należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników;
- współpraca z innymi zespołami CERT/CSIRT w Polsce i na świecie;
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego;
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa,
- analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach;
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń;
- regularne publikowanie Raportu CSIRT NASK o bezpieczeństwie polskich zasobów Internetu;
- działania informacyjno-edukacyjne, zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego.

Jednocześnie NASK jako jednostka badawcza prowadzi szereg różnych projektów. Jednym z najistotniejszych projektów prowadzonych przez instytucję w chwili obecnej jest projekt SiSSDeN w ramach europejskich programów badawczych Horizon 2020, którego celem jest poprawa stanu cyberbezpieczeństwa europejskich instytucji i użytkowników końcowych poprzez rozwój świadomości sytuacyjnej oraz współdzielenie użytecznych informacji o zagrożeniach. Projekt zapewni nieodpłatne usługi powiadamiania ofiar o ataku oraz bliską współpracę ze CSIRT-ami krajowymi, dostawcami usług internetowych, właścicielami sieci i organami ścigania.

CSIRT NASK zobowiązany jest do koordynacji incydentów zgłaszanych przez następujące podmioty:

- jednostki samorządu terytorialnego,
- jednostki budżetowe, samorządowe zakłady budżetowe,
- agencje wykonawcze, instytucje gospodarki budżetowej,
- uczelnie publiczne i Polską Akademię Nauk,
- Urząd Dozoru Technicznego, Polskie Centrum Akredytacji,
- Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,
- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej.

Jednocześnie informujemy, że CSIRT NASK przyjmuje zgłoszenia incydentów od obywateli, do czego serdecznie zachęcamy gdyż informacje te przyczyniają się do zwiększenia bezpieczeństwa cyberprzestrzeni RP.

CSIRT GOV

CSIRT GOV – prowadzony jest przez Agencję Bezpieczeństwa Wewnętrznego.

Główne zadania CSIRT GOV to:

Rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej.

CSIRT GOV zobowiązany jest do koordynacji incydentów zgłaszanych przez następujące podmioty:

organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;

ZUS, KRUS, NFZ, Polską Agencję Żeglugi Powietrznej;

Narodowy Bank Polski, Bank Gospodarstwa Krajowego.

CSIRT GOV wraz z CSIRT NASK obsługują system ARAKIS-GOV będący systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. System ten jest efektem współpracy Departamentu Bezpieczeństwa Teleinformatycznego ABW oraz działającego w ramach NASK zespołu CSIRT. ARAKIS-GOV powstał na potrzeby wsparcia ochrony zasobów teleinformatycznych administracji państwowej w wyniku rozszerzenie stworzonego przez CSIRT NASK systemu ARAKIS o dodatkową funkcjonalność.

CSIRT MON

CSIRT MON – prowadzony przez Ministerstwo Obrony Narodowej.

CSIRT MON zobowiązany jest do koordynacji incydentów zgłaszanych przez następujące podmioty:

podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej;

przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa jest Minister Obrony Narodowej.

Inne uprawnienia CSIRT-ów

Poza wymienionymi wyżej zadaniami CSIRT-ów ustawa o krajowym systemie cyberbezpieczeństwa umożliwia skoordynowane działania wszystkich CSIRT-ów w Polsce. Mogą one współpracować ze sobą

wspólnie opracowując główne elementy procedur postępowania w przypadku incydentu, którego koordynacja wymaga współpracy. Określają we współpracy z sektorowymi zespołami cyberbezpieczeństwa sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu.

Jednocześnie zespoły CSIRT w drodze porozumienia mogą powierzać sobie wzajemnie wykonywanie zadań w stosunku do niektórych rodzajów podmiotów.

Kolejnym ważnym elementem, który wprowadza ustawa w zakresie cyberbezpieczeństwa jest możliwość wykonywania przez zespoły CSIRT badań urządzeń lub oprogramowania w celu identyfikacji podatności, które wykorzystywane mogą być w celu zagrożenia integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Na podstawie ww. badań CSIRT mogą składać rekomendacje w celu usunięcia podatności urządzeń lub oprogramowania stosowane przez podmioty krajowego systemu cyberbezpieczeństwa.

6. Akty prawne

Poniżej przedstawiamy adresy publikacyjne aktów prawnych związanych z krajowym systemem cyberbezpieczeństwa:

Ustawa o KSC

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560)

Notatka prasowa

Usługi kluczowe

Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806)

Notatka prasowa

Incydenty poważne

Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180)

Notatka prasowa

Dokumentacja

Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080)

Notatka prasowa

Certyfikaty

Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. poz. 1999)

Notatka prasowa

Kolegium

Rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa (Dz. U. poz. 1952)

Notatka prasowa

Warunki organizacyjne

Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479)

Notka prasowa

Formularz PT

Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz. U. poz. 1831)

Notatka prasowa

Kryteria PT

Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. poz. 1830)

7. Przydatne LINKI:

- https://www.nask.pl/
- https://cert.pl/
- https://csirt.gov.pl/
- https://csirt-mon.wp.mil.pl/pl/
- https://uodo.gov.pl/pl
- https://www.europol.europa.eu/
- https://uke.gov.pl/

Regulacje UKNF w zakresie ryzyka IT i bezpieczeństwa informacji

1. https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_733016.pdf
2. https://www.knf.gov.pl/knf/pl/komponenty/img/Reko_SKOK_D_47953.pdf
3. https://www.knf.gov.pl/knf/pl/komponenty/img/knf_125701_PTE_Wytyczne_IT_16_12_2014_40005.pdf
8. https://www.knf.gov.pl/knf/pl/komponenty/img/ZU_Wytyczne_IT_16_12_2014_40004.pdf
4. https://www.knf.gov.pl/knf/pl/komponenty/img/Wytyczne_IT_TFI_39999.pdf
5. https://www.knf.gov.pl/knf/pl/komponenty/img/wytyczne_IT_firmy_inwestycyjne_40002.pdf
9. https://www.knf.gov.pl/knf/pl/komponenty/img/Wytyczne%20_IT_infrastruktura_40003.pdf
10. https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacje_bezpieczenstwo_platnosci_internetowych_37934.pdf
11. https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_dot_korzystania_przez_podmioty_nadzorowane_z_uslug_przetwarzania_danych_w_chmurze_obliczeniowej_59626.pdf
12. https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf
13. https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf

Informacje dot. działań KNF w zakresie cyberbezpieczeństwa rynku finansowego

1. https://cyberpolicy.nask.pl/aktualnosci/csirt-knf-sektorowy-zespolcyberbezpieczenstwa-sektora-bankowego/
2. https://fintek.pl/knf-powola-zespol-ds-cyberbezpieczenstwa-csirt/
3. https://www.cyberdefence24.pl/wiadomosci/knf-startuje-z-csirtem-sektorowym
4. https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1482164,knf-instytucjafinansowa-cyberprzestepstwo.html
5. https://www.cashless.pl/7930-knf-zespol-ds-cyberbezpieczenstwa
6. https://forsal.pl/artykuly/1482174,knf-zawalczy-z-cyberprzestepcami-od-lipca-ruszaspecjalny-zespol.html
7. https://wiadomosci.dziennik.pl/wydarzenia/artykuly/7739255,knf-cyberprzestepcypomoc-instytucje-finansowe.html
8. http://www.beinsured.pl/artykuly/w-knf-powstanie-zespol-odpowiedzialny-zabezpieczenstwo-cyfrowe-sektora-finansowego,7095.html
9. https://biznes.interia.pl/gospodarka/news-knf-zawalczy-z-cyberprzestepcami-od-lipcaruszа-specjalny-ze,nId,4544634
10. https://businessinsider.com.pl/technologie/nowe-technologie/cyberprzestepczosc-ktonas-oszukuje-tlumaczy-csirt-knf/zwwyl4f
11. https://comparic.pl/falszywy-knf-zniecheca-do-zglaszania-oszustwkryptowalutowych-cyberprzestepcy-atakuja-w-swieta/
12. https://biznes.wprost.pl/koronawirus/10396297/nowe-metody-oszustow-naskarbowke-na-nfz-i-na-sanepid.html
13. https://superbiz.se.pl/wiadomosci/oszukuja-podajac-sie-za-skarbowke-nfz-czysanepid-uwazaj-na-takie-wiadomosci-aa-ioSo-JxBF-gc3i.html
14. https://www.msn.com/pl-pl/finanse/najpopularniejsze-artykuly/nowe-metodyoszust%C3%B3w-na-skarb%C3%B3wk%C4%99-na-nfz-i-na-sanepid/ar-BB1bHuqn
15. https://www.onet.pl/?utm_source=sentione.com_viasg_businessinsider&utm_medium=referal&utm_campaign=leo_automatic&srcc=ucs&pid=fb840a04-f25b-4447-993ee67e97140c7b&sid=ca05277f-7c3f-495c-9acc-986177acd173&utm_v=2

Kampanie informacyjne i edukacyjne w obszarze cyberbezpieczeństwa

1. Kampania UKNF „Uwaga cyberoszust”

a) https://www.knf.gov.pl/dla_konsumenta/kampanie_spoleczne/uwaga_cyberoszust
b) https://www.bankier.pl/wiadomosc/KNF-i-policja-zaczynaja-kampanieinformacyjna-UWAGA-CYBEROSZUST-8023399.html
c) https://www.cyberdefence24.pl/uwaga-cyberoszust-knf-i-policja-ostrzegaja-przednowa-metoda-oszustow
d) https://policja.pl/pol/aktualnosci/197486,UWAGA-CYBEROSZUST-startkampanii-informacyjnej.html
e) https://www.wnp.pl/finanse/knf-i-policja-zaczynaja-kampanie-informacyjnauwaga-cyberoszust,438989.html
f) https://serwisy.gazetaprawna.pl/finanse-osobiste/artykuly/8048232,knf-policjakampania-informacyjna-uwaga-cybeoszust.html
g) https://wgospodarce.pl/informacje/89691-uwaga-cyberoszust-metoda-na-knf
h) https://fintek.pl/oszusci-wykorzystuja-logo-knf-nadzorca-i-policja-ostrzegaja/
i) https://www.parkiet.com/Finanse/312189923-Uwaga-na-oszustowpodszywajacych-sie-pod-KNF.html
j) https://twitter.com/jmbarszczewski/status/1339895020581756929
k) https://www.rp.pl/Finanse/312189935-Uwaga-na-oszustow-podszywajacych-siepod-KNF.html
l) https://telewizjarepublika.pl/komisja-nadzoru-finansowego-ostrzega-uwaga-nacyberoszustow,108530.html
m) https://tech.wp.pl/nowe-oszustwo-policja-ostrzega-cyberprzestepcy-chcawyludzic-pieniadze-metoda-na-knf-6587945220045632a
n) https://biznes.interia.pl/finanse/news-oszusci-posluguja-sie-sfalszowanymidokumentami-knf-uknf-zac,nId,4935002
o) https://polskieradio24.pl/5/1222/Artykul/2643933,Komisja-Nadzoru-Finansowego-ostrzega-przed-oszustami-podszywajacymi-sie-pod-KNF
p) https://warszawa.tvp.pl/51418270/uwaga-cyberoszust-uknf-wraz-z-polska-policjaostrzegaja-przed-oszustami
q) https://prnews.pl/knf-i-policja-ostrzegaja-przed-oszustami-poslugujacymi-siesfalszowanymi-dokumentami-z-logotypami-knf-455778/uwaga-cyberoszust
r) https://forexrev.pl/knf-rusza-z-kampania-uwaga-cyberoszust/
s) https://wartowiedziec.pl/serwis-glowny/styl-zycia/57959-uwaga-cyberoszust
t) https://gostynin.info/informacje/uwaga-cyberoszust/

u) https://kolniak24.eu/pl/473_na_sygnale/13760_knf-i-policja-zaczynaja-kampanieinformacyjna-uwaga-cyberoszust.html
v) https://sompolno24.pl/pl/11_wiadomosci/26936_knf-i-policja-zaczynajakampanie-informacyjna-uwaga-cyberoszust.html
w) https://kolobrzeg.twoje-miasto.pl/art-gospodarka/knf-i-policja-zaczynajakampanie-i167803

x) https://zambrow.org/artykul/wystartowala-kampania/1115635
y) https://telewizjarepublika.pl/komisja-nadzoru-finansowego-ostrzega-uwaga-nacyberoszustow,108530.html
z) https://adwokatnowakowska.pl/2020/12/18/uwaga-cyberoszust/
aa) https://brandsit.pl/knf-i-policja-zaczynaja-kampanie-informacyjna-uwagacyberoszust/
bb) https://www.polska-ie.com/uwaga-cyberoszust-start-kampanii-informacyjnej/
cc) http://halootwock.pl/wiadomosci/uwaga-cyberoszust/cid,13268,a
dd) https://www.ostrowmaz24.pl/amp/34038/start-kampanii-informacyjna-polskiejpolicji-uwaga-cyberoszust
ee) https://bielskonews.pl/20201218352635/policja-bielsko-biala-uwaga-cyberoszuststart-kampanii-informacyjnej1608289202
ff) https://twitter.com/mgrSkiba/status/1341281227169550337
gg) https://twitter.com/ForexrevP/status/1343496802302103557?s=20
hh) https://twitter.com/wgospodarce/status/1339903242365530113?s=20
ii) https://twitter.com/BrandsIT_pl/status/13398794787267174 42?s=20
jj) https://www.facebook.com/HexaBank/posts/3377966172315213#_=_
kk) https://www.facebook.com/CyberDefence24/posts/3657960420948743

2. Ostrzeżenie dot. wyłudzeń zwrotu podatku

a) https://twitter.com/CSIRT_KNF/status/1329060647938764802
b) https://www.gov.pl/web/kas/ostrzegamy-przed-e-mailami-podszywajacymi-siepod-podatkigovpl
c) https://www.gov.pl/web/finanse/ostrzegamy-przed-e-mailami-podszywajacymisie-pod-podatkigovpl
d) https://twitter.com/MF_GOV_PL/status/1329371563007873025?s=20
e) https://twitter.com/KAS_GOV_PL/status/1329371774547615747?s=20
f) https://tvn24.pl/biznes/z-kraju/ministerstwo-finansow-ostrzega-przed-oszustamistrona-ma-za-zadanie-wykrasc-dane-do-karty-kredytowej-4754987
g) https://www.bankier.pl/wiadomosc/Ministerstwo-Finansow-ostrzega-oszusciwyludzaja-dane-na-zwrotu-podatku-8004533.html
h) https://next.gazeta.pl/next/7,151003,26530745,krajowa-administracja-skarbowaostrzega-przed-oszustami-falszywe.html
i) https://biznes.radiozet.pl/News/Mail-o-zwrocie-podatku-to-oszustwo.-KASostrzega-przed-oszustami
j) https://pomorska.pl/uwaga-na-takie-emaile-ktore-informuja-o-mozliwosciwyplacenia-zwrotu-podatku-to-oszustwo-zdjecia/ga/c3-15300333/zd/46581089

3. Ostrzeżenie dot. PSD2

a) https://www.knf.gov.pl/o_nas/komunikaty?articleId=66987&p_id=18
b) https://www.cyberdefence24.pl/knf-ostrzega-przed-wyludzeniami-w-zwiazku-zdyrektywa-psd2

c) https://www.bgk.pl/bezpieczenstwo/komunikaty-i-poradniki-knf-oraz-zbpdotyczace-bezpieczenstwa/aktualnosci-dot-bezpieczenstwa-single/ostrzezenieuknf-dot-wyludzania-poufnych-informacji-w-zw-z-psd2/
d) https://zbp.pl/Aktualnosci/Wydarzenia/Ostrzezenie-UKNF-dot-wyludzaniapoufnych-informacji-w-zw-z-PSD2
e) https://spidersweb.pl/2019/09/psd2-knf-logowanie-oszusci.html

f) https://www.parkiet.com/Finanse/309069931-KNF-ostrzega-przedwyludzeniami.html
g) https://www.fxmag.pl/artykul/knf-ostrzega-nie-daj-sie-oszukac-na-zmiany-w-psd2
h) https://www.antyradio.pl/News/KNF-ostrzega-przed-powiadomieniami-z-bankow-Moga-byc-wysylane-przez-oszustow-35034
i) https://businessinsider.com.pl/finanse/dyrektywa-psd2-knf-ostrzega-przedoszustwami/15rhk6s
j) https://pieniadze.rp.pl/oszczednosci/konta-bankowe/21123-zmiany-w-bankach-tookazja-dla-oszustow-knf-ostrzega

4. Ostrzeżenie dot. połączenia Idea Bank oraz PEKAO S.A.

a) https://tvn24.pl/biznes/pieniadze/knf-ostrzega-przed-falszywymi-stronami-bankupekao-4920486
b) https://biznes.wprost.pl/technologie/10405069/knf-ostrzega-przejecie-idea-bankutoraj-dlacyberoszustow.html
c) https://www.cashless.pl/9182-bank-pekao-falszywa-strona
d) https://iszczecinek.pl/pl/696_o-tym-sie-mowi/22366_masz-konto-w-tym-bankulepiej-uwazaj-knf-ostrzega-przed-falszywa-strona.html
e) https://www.youtube.com/watch?v=RrWn9zJz0AI
f) https://www.msn.com/pl-pl/wiadomosci/nauka-i-technika/knf-ostrzegaprzej%C4%99cie-idea-banku-to-raj-dla-cyberoszust%C3%B3w/ar-BB1ctNXn

5. Kampania informacyjna „Black Friday - nie daj się złowić”

a) https://biznes.interia.pl/finanse/news-knf-nie-daj-sie-oszukac,nId,4385087
b) https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Aktualnosci?articleId=71519&p_id=18
c) https://www.facebook.com/cyberwomencommunity/

Profil Twitter Zespołu CSIRT KNF

https://twitter.com/CSIRT_KNF/status/1339868185735143424?s=20

Szkolenia oraz udział w ćwiczeniach

1. https://www.facebook.com/KomisjaNadzoruFinansowego/posts/3494261800592516
2. https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo---cwiczenia-ksc-exe-2020