



**Wytyczne techniczne w sprawie środków bezpieczeństwa**

*Wytyczne techniczne w sprawie środków bezpieczeństwa   
w Artykule 13a*

Wersja 2.0, październik 2014



 **Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji** [**www.enisa.europa.eu**](http://www.enisa.europa.eu)

**O ENISA**

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) to centrum wiedzy specjalistycznej z zakresu bezpieczeństwa sieci i informacji, służące UE, jej państwom członkowskim, sektorowi prywatnemu i obywatelom Europy. ENISA współdziała z tymi grupami, opracowując porady i zalecenia dotyczące dobrych praktyk w dziedzinie bezpieczeństwa informacji. Pomaga państwom członkowskim UE we wdrażaniu odpowiednich przepisów UE i pracuje nad poprawą odporności krytycznej infrastruktury teleinformatycznej i sieci w Europie. ENISA dąży do wzbogacenia wiedzy posiadanej przez państwa członkowskie UE, wspierając rozwój transgranicznych zespołów mających za zadanie podnoszenie bezpieczeństwa sieci i informacji w całej UE. Więcej informacji o ENISA i jej działalności można znaleźć pod adresem [www.enisa.europa.eu.](http://www.enisa.europa.eu/)

**Autorzy**

Dr Marnix Dekker, Christoffer Karsberg

**Kontakt**

Kontakt z autorami można uzyskać pod adresem [resilience@enisa.europa.eu.](mailto:resilience@enisa.europa.eu)

Kontakt przedstawicieli mediów w związku z niniejszym dokumentem dostępny jest pod adresem [press@enisa.europa.eu.](mailto:press@enisa.europa.eu)

**Podziękowania**

ENISA współpracowała z TNO, (przetarg ENISA nr P/28/11/TCD) aby opracować części Rozdziału 4 i 5.

W celu przygotowania niniejszych wytycznych ENISA współpracowała z grupą roboczą ekspertów krajowych organów regulacyjnych (NRA) i ministerstw państw UE w ramach Grupy Eksperckiej Artykułu 13a. Lista organizacji w grupie eksperckiej Artykułu 13a: PTS (SE), Agentschap Telecom (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ADAE (GR), CFCS (DK), RTR (AT), ANCOM (RO), CRC (BG), Ministerstwo Gospodarki, Finansów i Przemysłu (FR), Bundesnetzagentur (DE), BIPT (BE), MITYC (ES), MPO (CZ), CTO (CZ), CERT LT (LT), RA (SK), ILR (LU), AKOS (SI), MCA (MT), Ministerstwo Rozwoju Gospodarczego (IT), OCECPR (CY), NPT (NO), ETSA (EE), NMIAH (HU), ITSIRI (LV), UKE (PL), APEK (SI), Teleoff (SK), OFCOM (CH), HAKOM (HR). Jesteśmy wdzięczni za ich cenny wkład i komentarze.

Większość krajowych organów regulacyjnych zorganizowało także przegląd tego dokumentu przez dostawców w ich krajach. Jesteśmy wdzięczni za wiele przydatnych uwag i sugestii, które otrzymaliśmy od ekspertów branżowych.

|  |
| --- |
| **Informacje prawne**  O ile nie zaznaczono inaczej, niniejsza publikacja przedstawia poglądy i interpretacje autorów i redaktorów. Niniejszej publikacji nie należy traktować jako działania prawnego ENISA ani organów ENISA, chyba że została ona przyjęta zgodnie z Rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja może nie zawierać najnowszych informacji, w związku z czym może być aktualizowana przez ENISA.  Źródła zewnętrzne zostały należycie wskazane. ENISA nie odpowiada za treści przedstawiane przez źródła zewnętrzne, w tym zewnętrzne strony internetowe, do których odnośniki znajdują się w niniejszej publikacji.  Niniejsza publikacja przeznaczona jest wyłącznie do celów informacyjnych. Musi być dostępna bezpłatnie. Ani ENISA, ani żadna osoba występująca w jej imieniu nie ponosi odpowiedzialności za sposób wykorzystania informacji zawartych w niniejszej publikacji.  **Prawa autorskie**  © Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA), 2014  Powielanie dozwolone pod warunkiem podania źródła. |

**Wstęp**

Reforma ram prawnych UE dotyczących łączności elektronicznej z 2009 roku (dyrektywa UE 2009/140/WE) wprowadza Artykuł 13a do Dyrektywy Ramowej (dyrektywa 2002/21/WE, zmieniona dyrektywą 2009/140 WE). Reforma została transponowana przez większość państw członkowskich UE w połowie 2011 r.

Artykuł 13a dotyczy bezpieczeństwa i integralności sieci i usług łączności elektronicznej. Pierwsza część artykułu 13a wymaga, aby przedsiębiorcy udostępniający publiczne sieci łączności i świadczący usługi sieciowe stosowali wszelkie właściwe środki w celu zapewnienia bezpieczeństwa (ustęp 1) i integralności (ustęp 2) tych sieci i usług. Druga część artykułu 13a (ustęp 3) wymaga od tych przedsiębiorców powiadomienia o znaczących naruszeniach bezpieczeństwa lub utracie integralności właściwego krajowego organu regulacyjnego, który ma obowiązek corocznego zgłaszania tych incydentów związanych z naruszeniem bezpieczeństwa do ENISA i Komisji Europejskiej (KE).

W roku 2010 ENISA, Komisja Europejska (KE), ministerstwa i krajowe organy regulacyjne ds. komunikacji elektronicznej, zainicjowały szereg spotkań (warsztatów, telekonferencji) w celu osiągnięcia skutecznego i jednolitego wdrożenia artykułu 13a w całej UE. Grupa Ekspercka ds. Artykułu 13a składa się obecnie z ekspertów z krajowych organów regulacyjnych ze wszystkich państw UE oraz z niektórych krajów kandydujących do EFTA i UE. Spotkania (telefoniczne lub fizyczne) są organizowane i kierowane przez ekspertów technicznych z ENISA. Komisja Europejska uczestniczy w tych spotkaniach jako obserwator. Grupa Ekspertów ds. Artykułu 13a osiągnęła porozumienie w sprawie dwóch niewiążących wytycznych technicznych dla krajowych organów regulacyjnych: "Wytyczne techniczne dot. raportowania incydentów" i "Wytyczne techniczne dot. środków bezpieczeństwa" (niniejszy dokument).

Niniejszy dokument, "Wytyczne techniczne w sprawie środków bezpieczeństwa", zawiera techniczne wytyczne dla krajowych organów regulacyjnych dotyczące wdrażania postanowień ustępu 1 i 2 Artykułu 13a: jak zapewnić aby dostawcy właściwie oceniali ryzyka i podejmowali odpowiednie środki bezpieczeństwa. Dokument ten zawiera listę 25 istotnych celów bezpieczeństwa, pogrupowanych w 7 obszarów. Dla każdego celu bezpieczeństwa wymieniamy środki bezpieczeństwa, które mogą być podjęte przez dostawców/ przedsiębiorców aby osiągnąć cel bezpieczeństwa. Środki są zgrupowane w 3 poziomach o rosnącej złożoności. Wymieniamy również rodzaje dowodów, które mogą być brane pod uwagę przez kontrolera lub audytora przy ocenie, czy środki bezpieczeństwa są stosowane. Ogólna struktura celów i środków bezpieczeństwa jest przedstawiona na poniższym schemacie:

**Jedno rozwiązanie nie może być stosowane we wszystkich przypadkach:** Ani istotne cele bezpieczeństwa ani też szczegółowe środki bezpieczeństwa nie powinny być postrzegane jako wiążące zalecenia wskazujące, które środki bezpieczeństwa są odpowiednie dla dostawców. Powodem jest to, że sektor komunikacji elektronicznej jest bardzo zróżnicowany; duzi przedsiębiorcy o długiej historii (operatorzy zasiedziali), mali dostawcy usług, operatorzy ciemnych światłowodów, wirtualni operatorzy sieci łączności ruchomej, dostawcy usług internetowych oferujących tylko DSL, itp. W poszczególnych środowiskach zagrożenia są różne i to do dostawców należy właściwa ocena ryzyka i decyzja, które środki bezpieczeństwa będą odpowiednie. Niniejszy dokument ma być narzędziem wspomagającym działanie krajowych organów regulacyjnych, które nadzorują sektor. Może być używany jako schemat do samooceny, audytu i kontroli, wytyczne dla dostawców, lub jako odwzorowanie międzynarodowych norm bezpieczeństwa sieci i informacji stosowanych w branży łączności elektronicznej.

**Spis treści**

[**Wstęp iii**](#bookmark0)

1. [**Wprowadzenie 1**](#bookmark1)
2. [**Informacje wstępne**](#bookmark3) **3**
3. [**Artykuł 13a i terminologia**](#bookmark4) **5**
4. [**Ustęp 1 i 2 Artykułu 13a 5**](#bookmark5)
5. [**Terminologia 5**](#bookmark6)

[**4 Środki bezpieczeństwa 7**](#bookmark7)

1. [**Powiązane aktywa i ocena ryzyka 7**](#bookmark8)
2. [**Struktura środków bezpieczeństwa 8**](#bookmark10)
3. [**Cele i środki bezpieczeństwa 9**](#bookmark11)

[**5 Nadzór techniczny środków bezpieczeństwa 27**](#bookmark44)

1. [**Wprowadzenie obowiązkowych lub zalecanie standardów bezpieczeństwa 27**](#bookmark45)
2. [**Oceny zgodności na całym rynku 29**](#bookmark46)
3. [**Stosowanie podejścia etapowego 31**](#bookmark47)
4. [**Dostawcy usług audytorskich 32**](#bookmark48)

[**6 Powiązanie z normami międzynarodowymi 35**](#bookmark49)

[**Bibliografia 38**](#bookmark50)

**1 Wprowadzenie**

W tym dokumencie przedstawiamy wytyczne dla krajowych organów regulacyjnych ds. komunikacji elektronicznej (NRA) dotyczące środków bezpieczeństwa, o których mowa w ustępach 1 i 2 artykułu 13a Dyrektywy Ramowej (dyrektywa 2002/21/WE, zmieniona dyrektywą 2009/140/WE),

Niniejszy dokument został opracowany przez grupę roboczą ekspertów z krajowych organów regulacyjnych oraz przedstawicieli KE, wspieranych przez ekspertów technicznych ENISA (patrz Wstęp): Grupa Robocza. Artykułu 13a.

**Grupa docelowa**

Niniejszy dokument adresowany jest do ekspertów z krajowych ministerstw i organów regulacyjnych w państwach członkowskich Unii Europejskiej, których zadaniem jest wdrażanie Artykułu 13a.

Dokument ten może być przydatny także dla specjalistów pracujących w unijnym sektorze łączności elektronicznej i ekspertów pracujących w dziedzinach bezpieczeństwa cyfrowego oraz bezpieczeństwa sieci i informacji.

**Cel**

Niniejszy dokument został opublikowany przez ENISA, aby przedstawić wytyczne dla krajowych organów regulacyjnych w zakresie środków bezpieczeństwa opisanych w ustępie 1 i 2 Artykułu 13a.

**Wersje i zmiany**

ENISA aktualizuje niniejsze wytyczne okresowo, gdy jest to konieczne, w porozumieniu z krajowymi organami regulacyjnymi.

Niniejsza wersja jest uaktualnieniem wersji 1.0 Wytycznych w sprawie Minimalnych Środków Bezpieczeństwa. Obszary bezpieczeństwa nie uległy zmianie, także struktura istotnych celów bezpieczeństwa pozostaje taka sama (z wyjątkiem drobnych zmian, patrz poniżej).

Lista zmian:

* CB (Cel Bezpieczeństwa) 5.3 Procesy reagowania na incydenty i ich zgłaszania na wyższy poziom został połączony z CB 5.2 Zdolność wykrywania incydentów (obecnie CB17). Stąd wersja 2.0 ma 25 celów bezpieczeństwa, zamiast 26 wskazanych w wersji 1.0.
* Usunięto cytaty i fragmenty z norm, które służyły jako przykłady.
* Zmiana nazwy środki bezpieczeństwa na cele bezpieczeństwa.
* Do każdego celu bezpieczeństwa dodano szczegółowe środki bezpieczeństwa, które mogą być podjęte przez dostawców aby osiągnąć ten cel, a także opis dowodów jakie audytorzy/organy nadzoru mogłyby uwzględniać podczas oceny tego, czy zastosowano środki bezpieczeństwa.
* Dodano wskazówki dotyczące różnych metod jakie krajowe urzędy regulacyjne mogą zastosować w swoim nadzorze środków bezpieczeństwa. Zastępuje to krótki fragment dotyczący wdrażania, obecny w wersji 1.0.
* Zaktualizowano powiązania (odwzorowanie) w Sekcji 6 z ISO270001/2 w wersji z roku 2013.

**Struktura niniejszego dokumentu**

W [Sekcji 2](#bookmark2) podsumujemy role i cele ENISA związane z realizacją Artykułu 13a. W Sekcji 3 przedstawiamy Artykuł 13a, oraz zakres i terminologię używaną w tym dokumencie. W Sekcji 4 podajemy 25 celów bezpieczeństwa (CB), podzielonych na 7 obszarów (O), oraz podajemy szczegóły środków bezpieczeństwa i dowodów. W Sekcji 5 przedstawiamy szereg działań regulacyjnych, które mogą być zastosowane przez krajowe organy regulacyjne do oceny zgodności ze środkami bezpieczeństwa wymaganymi przez rt.. 13a. W Sekcji 6 podajemy powiązania (odwzorowanie) środków bezpieczeństwa w tych wytycznych z niektórymi znanymi normami międzynarodowymi.

**2 Informacje wstępne**

W tej sekcji podsumowujemy kontekst polityki UE i omawiamy rolę i cele ENISA.

**Kontekst polityki UE**

Niniejsze wytyczne dotyczą Artykułu 13a Dyrektywy Ramowej (dyrektywa 2002/21/WE, zmienionej dyrektywą 2009/140/WE). Istnieje szereg innych inicjatyw (prawnych lub w innych) dotyczących kwestii bezpieczeństwa publicznych sieci i usług łączności elektronicznej.

* W roku 2006, Komisja Europejska wydała Strategię bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy” [(COM (2006) 251)](http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf), która została zatwierdzona w następnym roku przez Radę Europejską [(Uchwała Rady 2007/068/01)](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:HTML). Jednym z głównych działań w ramach strategii jest dialog między wieloma interesariuszami dotyczący bezpieczeństwa i odporności sieci i systemów informatycznych: [Europejski Program Ochrony Infrastruktury Krytycznej](http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm) (EPOIK).
* W marcu roku 2009, Komisja Europejska wydała komunikat i plan działania dotyczący Ochrony Krytycznej Infrastruktury Informacyjnej (CIIP), zwany *Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności* [(COM (2009) 149)](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF). Komunikat ten skupia się na *"zapobieganiu, gotowości i świadomości"* i określa plan działania natychmiastowego w celu wzmocnienia bezpieczeństwa i odporności CII*.*
* [Wnioski Rady w sprawie ochrony krytycznej infrastruktury informatycznej](http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf) wydane w maju 2011 roku, podsumowują wyniki osiągnięte od czasu przyjęcia planu CIIP w 2009 roku, zostały wdrożone w celu wzmocnienia bezpieczeństwa i odporności kluczowych elementów infrastruktury technologii informacyjnych i komunikacyjnych.

Komisja Europejska opublikowała również Europejską Strategię Bezpieczeństwa Cyfrowego oraz zaproponowała Dyrektywę w sprawie bezpieczeństwa sieci i informacji (NIS). Strategia, dyrektywa i przemówienia w KE zawierają wyraźne odniesienia do artykułu 13a i wspominają o możliwości rozszerzenia Artykuł 13a na inne sektory społeczne.

Odnośnie do przeglądu wielu artykułów bezpieczeństwa, dotyczących środków bezpieczeństwa i raportowania incydentów przywołujemy dokument ENISA [Raportowanie Cyfrowe Incydentów w UE](http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu), podsumowujący i porównujący Artykuł 13a Dyrektywy Ramowej, Artykuł 4 Dyrektywy o prywatności i łączności elektronicznej, Artykuł 15 projektu rozporządzenia e-Trust / e-ID oraz wymogi raportowania w proponowanej reformie ochrony danych.

**Rola ENISA**

Pokrótce opisujemy rolę i cele ENISA w realizacji dyrektywy ramowej (2002/21/WE zmienionej dyrektywą 2009/140/WE), a w szczególności Art. 13a.

ENISA jest wymieniona w preambule dyrektywy ramowej:

* Preambuła 44 dyrektywy ramowej wymaga od ENISA, aby przyczyniała się do zwiększania poziomu bezpieczeństwa łączności elektronicznej, na przykład przez *"dostarczanie wiedzy i doświadczeń, oraz promowanie wymiany najlepszych praktyk"*.
* Preambuła 44 dyrektywy ramowej stanowi, że ENISA powinna dysponować niezbędnymi środkami do wykonywania swoich obowiązków, w tym uprawnieniami "*do uzyskiwania informacji wystarczających do oceny poziomu bezpieczeństwa sieci lub usług*".
* Preambuła 46 dyrektywy ramowej wymaga od ENISA "*przyczyniania się do harmonizacji odpowiednich technicznych i organizacyjnych środków bezpieczeństwa poprzez zapewnianie opinii ekspertów*”.

ENISA jest również wymieniona w art 13a dyrektywy ramowej:

* Ustęp 3 Artykułu 13a wymaga, aby w stosownych przypadkach dany krajowy organ regulacyjny informował krajowe organy regulacyjne innych państw członkowskich oraz Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) o przypadkach zagrożenia bezpieczeństwa.
  + Ustęp 3 Artykułu 13a wymaga od krajowych organów regulacyjnych przekazania Komisji Europejskiej i ENISA sprawozdania podsumowującego otrzymane zgłoszenia i działania podjęte w związku z nimi.
  + Artykuł 13a stanowi, że Komisja Europejska może przyjąć właściwe techniczne środki wykonawcze mając na celu harmonizację środków, o których mowa w ust. 1, 2 i 3, art. 13a. Artykuł 13 mówi, że w tym przypadku Komisja Europejska weźmie pod uwagę opinię ENISA.

**Cele ENISA**

Pierwszym celem ENISA jest wdrożenie raportowania incydentów nakazane w Artykule 13a, czyli uzgodnienie z państwami członkowskimi skutecznego wdrożenia ogólnoeuropejskiego raportowania incydentów, w tym procesy raportowania ad-hoc o zdarzeniach o charakterze transgranicznym, a także rocznego raportowania podsumowującego.

Po drugie, ENISA ma na celu wspieranie krajowych organów regulacyjnych, których zadaniem jest zapewnienie, że dostawcy podejmują odpowiednie środki bezpieczeństwa i działania nadzorcze, w tym zbieranie krajowych raportów o incydentach, śledzenie ich, analiza i łagodzenie powszechnych przyczyn pierwotnych, oraz formułowanie wytycznych dla dostawców itp.

W ten sposób ENISA wspiera sprawne i zharmonizowane wdrażanie artykułu 13a w całej UE. Zharmonizowane wdrożenie prawodawstwa jest ważne, aby stworzyć równość szans na rynku i ułatwić dostawcom i użytkownikom działanie w różnych krajach UE.

**3 Artykuł 13a i terminologia**

W tej sekcji przedstawiamy odpowiednie części artykułu 13a i związane z nimi określenia używane w niniejszym dokumencie.

**3.1 Ustęp 1 i 2 Artykułu 13a**

Ze względu na możliwość odniesienia, odtwarzamy poniżej ustęp 1 i 2 Artykułu 13a.

*“1. Państwa członkowskie zapewniają, aby przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej podejmowały właściwe środki techniczne i organizacyjne w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. Środki te zapewniają poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu wiedzy i technologii. W szczególności należy podjąć środki zapobiegające wpływowi i minimalizujące wpływ, jaki na użytkowników i wzajemnie połączone sieci mogą mieć przypadki stwarzające zagrożenie bezpieczeństwa*

*2. Państwa członkowskie zapewniają, aby przedsiębiorstwa udostępniające publiczne sieci łączności stosowały wszelkie właściwe środki w celu zapewnienia integralności swoich sieci, a tym samym zapewniały ciągłość świadczenia usług za pośrednictwem tych sieci. [...]"*

**3.2 Terminologia**

W trosce o zwięzłość, używamy następujących pojęć w tym dokumencie:

* + Dostawca: Termin "dostawca" jest używany w odniesieniu do *"przedsiębiorstwa udostępniającego publiczne sieci informacyjne lub publicznie dostępne usługi łączności elektronicznej"*.
  + Krajowe organy regulacyjne: Skrót "NRA" jest używany w odniesieniu do właściwego organu z artykułu 13a czyli  *"krajowego organu regulacyjnego"* jak wspomniano w Artykule 13a, którym może być ministerstwo lub agencja rządowa, w zależności od sytuacji w danym kraju.
  + Sieci i usługi łączności: Określenie *"sieci i usługi łączności" jest używane jako skrót terminu "publiczne sieci łączności lub publicznie dostępne usługi łączności elektronicznej"*, jak wymieniono w Artykule 13a. Obejmuje to operatorów telekomunikacyjnych, operatorów sieci komórkowych, dostawców usług internetowych itp.

**3.2.1 Bezpieczeństwo, integralność, ciągłość**

Ustępy 1 i 2 Artykułu 13a zawierają dwa różne wymogi:

* + Ustęp 1 wymaga od krajowych organów regulacyjnych, aby *"podejmowały właściwe środki techniczne i organizacyjne w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług* "oraz realizowały działania "*zapobiegające wpływowi i minimalizujące wpływ, jaki na użytkowników i wzajemnie połączone sieci mogą mieć przypadki stwarzające zagrożenie bezpieczeństwa".*
  + Ustęp 2 wymaga od krajowych organów regulacyjnych zapewnienia, żeby przedsiębiorstwa „*stosowały wszelkie właściwe środki w celu zapewnienia integralności swoich sieci, a tym samym zapewniały ciągłość świadczenia usług za pośrednictwem tych sieci"*.

Zastosowanie terminu 'integralność' (sieci[[1]](#footnote-1)) w tekście tego ustępu może być mylące dla niektórych czytelników. W literaturze fachowej na temat sieci i wzajemnych połączeń sieciowych[[2]](#footnote-2), termin 'integralność' definiowany jest jako *"zdolność systemu do utrzymania swoich określonych cech w zakresie wydajności i funkcjonalności"*. Termin 'integralność' w tekście ustępu może być też nazywany "odpornością" lub "ciągłością" w innej literaturze dotyczącej bezpieczeństwa informacji.

W tym dokumencie zajmujemy się zarówno bezpieczeństwem (ustęp 1), jak i integralnością (ustęp 2), podając zestaw "środków bezpieczeństwa", który obejmuje "*środki techniczne i organizacyjne"* w ustępie pierwszym i *kroki*, o których mowa w drugim ustępie artykułu.

W niniejszym dokumencie, aby być bardziej zgodnymi z większością publikacji na temat bezpieczeństwa sieci i informacji, używamy pojęć "bezpieczeństwo" i "ciągłość" aby odpowiedzieć na te wymagania, lub po prostu "bezpieczeństwo" (ponieważ w większości publikacji nt. bezpieczeństwa ciągłość postrzegana jest jako aspekt bezpieczeństwa).

**3.2.2 Przypadki stwarzające zagrożenie bezpieczeństwa**

Artykuł 13a wymienia „przypadki stwarzające zagrożenie bezpieczeństwa”, „naruszenia bezpieczeństwa" i „utratę integralności":

* + Ustęp 1 wymaga, aby "*podjąć środki zapobiegające wpływowi i minimalizujące wpływ, jaki na użytkowników i wzajemnie połączone sieci mogą mieć przypadki stwarzające zagrożenie bezpieczeństwa”*
  + Ustęp 2 wymaga, aby dostawcy stosowali *"wszelkie właściwe środki w celu zapewnienia integralności swoich sieci, a tym samym zapewniali ciągłość świadczenia usług za pośrednictwem tych sieci"*.
  + Ustęp 3 wymaga *"aby powiadomić właściwy krajowy organ regulacyjny o każdym naruszeniu bezpieczeństwa lub utracie integralności, które miały znaczący wpływ na sieci lub usług."*

W niniejszych wytycznych używamy jedynie termin "incydenty bezpieczeństwa", który ma następującą definicję:

|  |
| --- |
| Incydent bezpieczeństwa: naruszenie bezpieczeństwa lub utrata integralności, które mogłyby mieć wpływ na działanie sieci i usług telekomunikacyjnych. |

Jest to identyczna definicja, jak ta zastosowana w "Wytycznych technicznych dotyczących raportowania incydentów"[[3]](#footnote-3).

**4 Środki bezpieczeństwa**

W tej sekcji przedstawiamy listę 25 celów bezpieczeństwa, które krajowe organy regulacyjne powinny wziąć pod uwagę przy ocenie zgodności dostawców z Artykułem 13a (ustępy 1 i 2).

Podkreślamy, że niniejsze wytyczne są wytycznymi dla krajowych organów regulacyjnych i że jest to od ich decyzji zależy, czy będą wymagały lub tylko zalecały inne cele bezpieczeństwa lub inne środki bezpieczeństwa, albo jedynie część przedstawionych środków i/lub dodatkowych środków bezpieczeństwa.

Należy pamiętać, że niektóre z celów lub środków bezpieczeństwa mogą być nieodpowiednie lub niewłaściwe dla wszystkich środowisk dla wszystkich rodzajów dostawców, w zależności od typu sieci lub oferowanych usług[[4]](#footnote-4).

**4.1 Powiązane aktywa i ocena ryzyka**

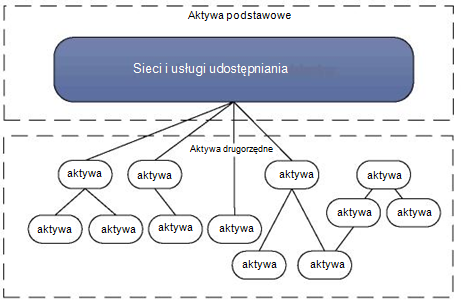
Zakres środków ochrony jest zdefiniowany w następujący sposób.

|  |
| --- |
| Powiązane aktywa: Wszystkie aktywa dostawcy, które po naruszeniu i/lub awarii, mogą mieć negatywny wpływ na bezpieczeństwo lub ciągłość sieci lub usług łączności elektronicznej. |

Dostawcy powinni wykonać ocenę ryzyka specyficzną dla ich środowiska/otoczenia, aby określić, które aktywa są powiązane i jakie środki bezpieczeństwa są właściwe. Oceny ryzyka wymagają aktualizacji, aby odpowiadały zmianom i incydentom z przeszłości, ponieważ ryzyko zmienia się w czasie. Należy pamiętać, że niniejsze wytyczne *nie* dotyczą szczegółów oceny ryzyka. Istnieje kilka standardowych metodologii, które mogą być użyte przez dostawców do tego celu (patrz Bibliografia).

***Uwaga dotycząca zarządzania ryzykiem przedsiębiorstwa:*** *Warto tutaj wspomnieć, że istnieje wiele publikacji dotyczących bezpieczeństwa informacji, które skupiają się na tym, jak organizacja może zarządzać ryzykiem bezpieczeństwa informacji związanym z korzystaniem z bezpieczeństwa sieci i informacji: obszar ten nazywany jest zarządzaniem ryzykiem przedsiębiorstwa. Dobrze znanym przykładem jest ISO27001. Artykuł 13a jednak wymienia tylko zagrożenia dla użytkowników, którzy korzystają z sieci i usług łączności świadczonych przez dostawców, a nie zagrożenia dla operatora. W praktyce oznacza to, że choć metody zarządzania ryzykiem przedsiębiorstwa są bardzo pomocne, nie mogą być one wykorzystywane w odniesieniu do Artykułu 13a bez odpowiedniej adaptacji.*

**4.1.1 Aktywa podstawowe i drugorzędne**

W niektórych publikacjach istnieje rozróżnienie między aktywami podstawowymi a drugorzędnymi (pomocniczymi). W omawianym kontekście (Art. 13a), aktywami podstawowymi są elektroniczne sieci komunikacyjne i usługi dostarczane przez dostawcę (patrz wykres po prawej).

W niniejszym dokumencie, gdy mówimy o aktywach mamy na myśli aktywa *drugorzędne* tj. systemy i procesy wspierające dostarczanie sieci i usługi komunikacji elektronicznej (takie jak stacje bazowe, routery, rejestry, zasilanie itp.)

**4.1.2 Aktywa krytyczne**

W dalszej części niniejszego dokumentu, używamy terminu *aktywa krytyczne* aby określić aktywa (sieci i systemy informatyczne, procesy, dane itp.), które, w razie awarii będą miały *poważny* wpływ na bezpieczeństwo lub ciągłość sieci i usług. Aktywa krytyczne należy (co jest oczywiste) zabezpieczyć w sposób priorytetowy.

**4.1.3 Kluczowy personel**

W niniejszym dokumencie używamy terminu "kluczowy personel" do określenia głównych ról w organizacji w zakresie bezpieczeństwa i ciągłości. Teraz dostawcy nie są wszędzie tacy sami, a organizacje oraz profile zawodowe są różne - jednak zazwyczaj "kluczowy personel" będzie obejmować funkcje takie, jak CEO, CIO, CISO, kierownik ciągłości działania oraz administratorzy systemów krytycznych.

**4.1.4 Strony trzecie i outsourcing**

W niniejszym dokumencie używamy terminu "strony trzecie" odnośnie stron (organizacji, osób fizycznych) z którymi współpracuje dostawca w celu świadczenia usług, tj. sprzedawcy produktów do dostawcy, inni dostawcy, konsultanci doradzający dostawcy, audytorzy dokonujący badania dostawcy, firmy którym dostawca zleca prace, itp.[[5]](#footnote-5).

Strony trzecie i aktywa stron trzecich znajdują się w zakresie zainteresowania, tak jak gdyby były to aktywa dostawców. Innymi słowy, nawet jeśli pewne procesy są zlecane na zewnątrz, operator pozostaje odpowiedzialny za zapewnienie, że zostaną podjęte odpowiednie środki bezpieczeństwa w celu ochrony bezpieczeństwa i ciągłości sieci i usług, które świadczy.

**4.2 Struktura środków bezpieczeństwa**

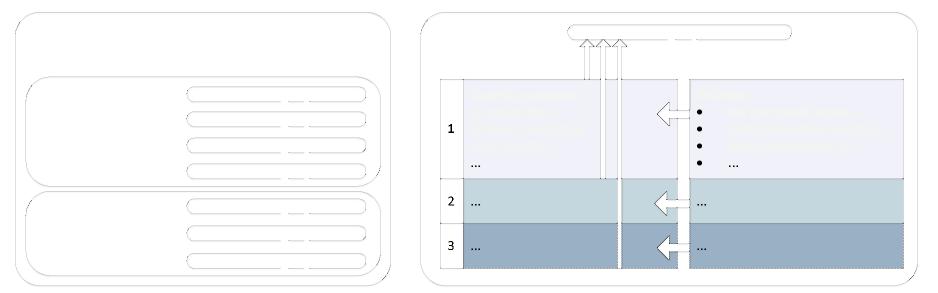
Niniejszy dokument wymienia 25 celów bezpieczeństwa[[6]](#footnote-6), które zostały opracowane na bazie szeregu międzynarodowych i krajowych norm powszechnie stosowanych przez dostawców w sektorze łączności elektronicznej w UE (patrz Bibliografia). Dla każdego celu bezpieczeństwa podajemy bardziej szczegółowe środki bezpieczeństwa, które mogą być wdrożone przez dostawców/przedsiębiorców aby osiągnąć cel bezpieczeństwa. Dla każdego celu bezpieczeństwa podajemy także listy szczegółowych dowodów, które mogłyby wskazywać, że środek bezpieczeństwa jest stosowany. Należy pamiętać, że środki bezpieczeństwa lub dowody nie powinny być postrzegane jako punkt odniesienia lub lista minimalnych wymagań dla dostawców (patrz uwaga poniżej).

Środki bezpieczeństwa są pogrupowane w 3 różnych poziomach zaawansowania, które określa się w następujący sposób.

|  |
| --- |
| **Opis poziomów zaawansowania** |
| **Poziom zaawansowania 1 (podstawowy):**   * Podstawowe środki bezpieczeństwa, które mogą być wdrożone w celu osiągnięcia celu bezpieczeństwa * Dowody, że podstawowe środki są obecne. |
| **Poziom zaawansowania 2 (standard branżowy):**   * Środki bezpieczeństwa standardowe dla branży pomagające osiągnąć cel i nieplanowane (ad-hoc) kontrole realizacji, po zmianach lub incydentach. * Dowody standardowych branżowych środków i przeglądów działań realizowanych po zmianach lub po incydentach. |
| **Poziom zaawansowania 3 (wysoce zaawansowany):**   * + Najnowocześniejsze (zaawansowane) środki bezpieczeństwa i ciągłe monitorowanie wdrażania, strukturalna kontrola wdrażania uwzględniająca zmiany, incydenty, testy i ćwiczenia, w celu aktywnego poprawiania procesu wdrażania środków bezpieczeństwa.   + Dowody zaawansowanej realizacji, dowody strukturalnej kontroli procesu wdrażania i dowody aktywnego poprawiania procesu wdrażania środków bezpieczeństwa. |

Poziomy mają charakter kumulatywny. Innymi słowy, na poziomie 2 nie powtarzamy środków bezpieczeństwa i dowodów poziomu 1, aby zachować przejrzystość - zakładamy że są one włączone (skumulowane). Podobnie na poziomie 3 - przyjmuje się, że zawarte są w nim środki bezpieczeństwa z poziomu 1 i 2. Jeżeli środki bezpieczeństwa poziomu 1, nie są (w pełni) zrealizowane, to poziom można nazwać poziomem 0 - jednak w niniejszym dokumencie nie wskazujemy bezpośrednio poziomu 0.

Ogólna struktura celów i środków bezpieczeństwa jest przedstawiona na Rysunku 1.



Cel bezpieczeństwa

**7** obszarów **25** Cele bezpieczeństwa

Ox Obszar bezpieczeństwa

**Dowód**

**Środki bezpieczeństwa**

a. zapewniają, że ...

b. istnieje procedura

c. określają zasady

CB x: Cel bezpieczeństwa

kluczowy personel zna... politykę/procedury dotyczące narzędzia /mechanizmy...

CB x: Cel bezpieczeństwa

CB x: Cel bezpieczeństwa

CB x: Cel bezpieczeństwa

Ox Obszar bezpieczeństwa

CB x: Cel bezpieczeństwa

CB x: Cel bezpieczeństwa

CB x: Cel bezpieczeństwa

**Rysunek 1. Struktura celów i środków bezpieczeństwa.**

***Uwaga o profilach:*** *Poziomy zaawansowania mogą być wykorzystywane do tworzenia profili dostawców, pokazujących zaawansowanie środków bezpieczeństwa w całym obszarze. Takie profile mogą być stosowane przez krajowe organy regulacyjne, np. podczas oceny stanu wdrożenia środków bezpieczeństwa w całym sektorze. Omawiamy metody nadzoru w Sekcji 5 i podajemy tam przykłady dwóch profili.*

***Uwaga o minimalnych środkach bezpieczeństwa;*** *Ani istotne cele bezpieczeństwa, ani też szczegółowe środki bezpieczeństwa nie mogą być postrzegane jako wiążące zalecenia wskazujące na to, które środki bezpieczeństwa są odpowiednimi dla indywidualnych dostawców. Tak więc, np. środki bezpieczeństwa na poziomie 1, nie mogą być uważane za "minimum" dla danego sektora. Zagrożenia te są różne dla różnych dostawców i zależą od specyfiki (otoczenia, typu dostawcy, rodzaju oferowanych usług, rozpatrywanych aktywów, itp.) tego, które cele są ważne oraz które środki są odpowiednie.*

***Uwaga o odrębnych środkach****: Podajemy środki bezpieczeństwa oddzielnie dla każdego celu bezpieczeństwa, lecz nie należy tego postrzegać jako zalecenie do podziału działań na odrębne części, lub do prowadzenia osobnych dokumentów albo plików. Na przykład, jeden zestaw aktywów może być wykorzystany do oceny ryzyka, ale również do wspierania procedur zarządzania zmianą i zarządzania aktywami.*

**4.3 Cele i środki bezpieczeństwa**

Poniżej wymieniamy 25 istotnych Celów Bezpieczeństwa (CB1, CB2, ...), zgrupowanych w 7 Obszarach (O1, O2, ...). Dla każdego celu bezpieczeństwa podajemy środki bezpieczeństwa, które mogą być wdrożone przez dostawców/ przedsiębiorców aby osiągnąć cel bezpieczeństwa, oraz szczegółowe dowody, które mogą być brane pod uwagę przez kontrolera lub audytora przy ocenie tego, czy środki bezpieczeństwa są stosowane. (patrz poprzedni punkt).

Poniżej zamieszczamy spis treści w celu ułatwienia przeszukiwania dokumentu:

[**O1: Kierowanie i zarządzanie ryzykiem 11**](#bookmark12)

[**CB 1: Polityka bezpieczeństwa informacji 11**](#bookmark13)

[**CB 2: Kierowanie i zarządzanie ryzykiem 11**](#bookmark14)

[**CB 3: Role i obowiązki bezpieczeństwa 12**](#bookmark15)

[**CB 4: Bezpieczeństwo aktywów stron trzecich 12**](#bookmark16)

[**O2: Bezpieczeństwo zasobów ludzkich 13**](#bookmark17)

[**CB 5: Kontrole przygotowania 13**](#bookmark18)

[**CB 6: Wiedza i szkolenia z obszaru bezpieczeństwa 14**](#bookmark19)

[**CB 7: Zmiany personalne 14**](#bookmark20)

[**CB 8: Postępowanie z naruszeniami 15**](#bookmark21)

[**O3: Bezpieczeństwo systemów i obiektów 15**](#bookmark22)

[**CB 9: Bezpieczeństwo fizyczne i środowiskowe 15**](#bookmark23)

[**CB 10: Bezpieczeństwo dostaw 16**](#bookmark24)

[**CB 11: Kontrola dostępu do sieci i systemów informatycznych 17**](#bookmark25)

[**CB 12: Integralność sieci i systemów informatycznych 17**](#bookmark26)

[**O4: Zarządzanie operacyjne 18**](#bookmark27)

[**CB 13: Procedury operacyjne 18**](#bookmark28)

[**CB 14: Zarządzanie zmianą 19**](#bookmark29)

[**CB 15: Zarządzanie aktywami 19**](#bookmark30)

[**O5: Zarządzanie incydentami 20**](#bookmark31)

[**CB 16: Procedury zarządzania incydentami 20**](#bookmark32)

[**CB 17: Potencjał wykrywania incydentów 20**](#bookmark33)

[**CB 18: Raportowanie i komunikowanie incydentów 21**](#bookmark34)

[**O6: Zarządzanie ciągłością działalności 21**](#bookmark35)

[**CB 19: Strategia ciągłości usług i plany awaryjne 21**](#bookmark36)

[**CB 20: Możliwości usuwania skutków awarii 22**](#bookmark37)

[**O7: Monitorowanie, audytowanie i testowanie 23**](#bookmark38)

[**CB 21: Zasady monitorowania i rejestrowania 23**](#bookmark39)

[**CB 22: Ćwiczenie planów awaryjnych 23**](#bookmark40)

[**CB 23: Testowanie sieci i systemów informatycznych 24**](#bookmark41)

[**CB 24: Oceny bezpieczeństwa 25**](#bookmark42)

[**CB 25: Monitorowanie zgodności 25**](#bookmark43)

**D1: Kierowanie i zarządzanie ryzykiem**

Obszar "Kierowanie i zarządzanie ryzykiem" obejmuje cele bezpieczeństwa związane z kierowaniem i zarządzaniem ryzykiem w zakresie bezpieczeństwa sieci i informacji.

**CB 1: Polityka bezpieczeństwa informacji**

Ustalenie i utrzymanie właściwej polityki bezpieczeństwa informacji.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Określenie polityki bezpieczeństwa na wysokim poziomie, aby zapewnić bezpieczeństwo i ciągłość działania sieci i/lub świadczonych usług komunikacyjnych.  b) Zaznajomienie personelu kluczowego z polityką bezpieczeństwa. | * + Udokumentowana polityka bezpieczeństwa, w tym objęte sieci i usługi, krytyczne aktywa wspierające je oraz cele bezpieczeństwa. * Kluczowy personel zna politykę bezpieczeństwa i jej cele (wywiad). |
| **2** | c) Określenie szczegółowych zasad bezpieczeństwa informacji dla krytycznych zasobów i procesów biznesowych.  d) Cały personel zna politykę bezpieczeństwa i jest świadomy jak wpływa ona na ich pracę  e) Analiza polityki bezpieczeństwa po incydentach. | * + Udokumentowanie polityki bezpieczeństwa informacji zatwierdzonej przez kierownictwo, obejmującej obowiązujące prawo i przepisy, dostępne dla personelu.   + Pracownicy są świadomi polityki bezpieczeństwa informacji i tego jak wpływa ona na ich pracę (wywiad). * Analiza komentarzy lub rejestrów zmian polityki. |
| **3** | f) Przegląd okresowy polityki bezpieczeństwa informacji i uwzględnienie naruszeń, wyjątków, incydentów z przeszłości, ostatnich badań/ćwiczeń i incydentów mających wpływ innych (podobnych) dostawców w branży. | * + Polityka bezpieczeństwa informacji jest aktualna i zatwierdzona przez kierownictwo wyższego szczebla.   + Rejestr wyjątków od polityki, zatwierdzony przez osoby o odpowiednich rolach. * Proces przeglądu jest udokumentowany, z uwzględnieniem zmian i przeszłych zdarzeń. |

**CB 2: Kierowanie i zarządzanie ryzykiem**

Ustalenie i utrzymanie właściwych ram kierowania i zarządzania ryzykiem, w celu określania i reagowania na zagrożenia dla sieci informacyjnych i usług.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Przygotowanie listy głównych zagrożeń dla bezpieczeństwa i ciągłości sieci komunikacyjnych i usług, z uwzględnieniem głównych zagrożeń dla aktywów krytycznych.  b) Zapewnienie, że kluczowy personel zna główne ryzyka i sposoby ich ograniczania. | * + Lista głównych czynników ryzyka opisanych na wysokim poziomie, w tym na zagrożenie(a) i ich potencjalny wpływ na bezpieczeństwo i ciągłość usług i sieci. * Kluczowi pracownicy znają główne rodzaje ryzyka (wywiad). |
| **2** | c) Stworzenie metodologii i/lub narzędzi zarządzania ryzykiem w oparciu o standardy branżowe.  d) Zapewnienie, że personel kluczowy stosuje metodologię i narzędzia zarządzania ryzykiem  e) Analiza ocen ryzyka po zmianach lub incydentach.  f) Zapewnienie, że pozostałe rodzaje ryzyka są zaakceptowane przez kierownictwo. | * Udokumentowane metody i/lub narzędzia zarządzania ryzykiem. |
| **3** | g) Przegląd metodologii i/lub narzędzi zarządzania ryzykiem, okresowo, z uwzględnieniem zmian i incydentów z przeszłości. | * Dokumentacja procesu przeglądu i aktualizacja metodologii i/lub narzędzi zarządzania ryzykiem. |

**CB 3: Role i obowiązki bezpieczeństwa**

Ustalenie i utrzymanie właściwej struktury ról i obowiązków bezpieczeństwa.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Przypisywanie ról i obowiązków bezpieczeństwa pracownikom.  b) Zapewnienie, że role bezpieczeństwa są dostępne w przypadku incydentów bezpieczeństwa. | * Lista ról bezpieczeństwa (CISO, DPO, menedżer utrzymania ciągłości, etc.), osób, które je pełnią i informacje kontaktowe. |
| **2** | c) Personelowi formalnie wyznaczono role bezpieczeństwa.  d) Zapoznać pracowników z rolami bezpieczeństwa w organizacji i z tym, kiedy należy się z nimi kontaktować. | * Lista wyznaczonych funkcji (CISO, DPO, itp.), oraz opis obowiązków i zadań dla ról ważnych dla bezpieczeństwa (CISO, DPO, itp). * Materiały budujące świadomość/ rozpowszechniające wiedzę dostępne dla personelu, w celu wyjaśnienia ról ważnych dla bezpieczeństwa i przypadków kiedy/jak kontaktować się z osobami pełniącymi te role. |
| **3** | e) Struktura ról i obowiązków związanych z bezpieczeństwem jest regularnie sprawdzana i zmieniana w oparciu o zmiany i/lub incydenty z przeszłości. | * Aktualna dokumentacja struktury przypisania ról bezpieczeństwa i odpowiedzialności * Proces przeglądu jest udokumentowany, z uwzględnieniem zmian i przeszłych wydarzeń. |

**CB 4: Bezpieczeństwo aktywów stron trzecich**

Ustanowienie i utrzymanie polityki, wymogów bezpieczeństwa w odniesieniu do umów ze stronami trzecimi (patrz Sekcja [4.1.4)](#bookmark9), aby zapewnić, że zależność od stron trzecich nie wpływa negatywnie na bezpieczeństwo sieci i/lub usług.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** | |
| **1** | a) Włączenie wymogów bezpieczeństwa w umowy ze stronami trzecimi. | | * Jasno sprecyzowane wymagania dotyczące bezpieczeństwa w umowach ze stronami trzecimi dostarczającymi produkty i usługi informatyczne, outsourcing procesów biznesowych, helpdeski, call center, wzajemne połączenia, wspólne obiekty, itp. |
| **2** | b) Określenie polityki bezpieczeństwa dla umów ze stronami trzecimi  c) Zapewnienie, że wszystkie zamówienia publiczne na usługi/produkty od stron trzecich są zgodne zobowiązująca polityką.  d) Przegląd polityki bezpieczeństwa wobec stron trzecich, po incydentach lub zmianach.  e) Ograniczanie ryzyka resztkowego, którego kwestia nie jest rozwiązana przez strony trzecie. | | * + Udokumentowanie polityki bezpieczeństwa dla umów ze stronami trzecimi   + Lista umów z firmami zewnętrznymi.   + Umowy na usługi stron trzecich zawierają wymogi bezpieczeństwa, zgodnie z polityką bezpieczeństwa dla zamówień.   + Analiza komentarzy lub rejestrów zmian polityki. * Pozostałe ryzyka wynikające z zależności od stron trzecich są wymienione i łagodzone. |
| **3** | f) Śledzenie incydentów bezpieczeństwa związanych lub spowodowanych przez strony trzecie.  g) Okresowy przegląd i aktualizacja polityki bezpieczeństwa wobec stron trzecich, w regularnych odstępach czasu, biorąc pod uwagę incydenty z przeszłości, zmiany, itp. | | * + Lista incydentów bezpieczeństwa związanych lub spowodowanych kontaktem ze stronami trzecimi. * Dokumentacja procesu przeglądu polityki. |

**O2: Bezpieczeństwo zasobów ludzkich**

Obszar “Bezpieczeństwo zasobów ludzkich” obejmuje cele związane z bezpieczeństwem personelu.

**CB 5: Kontrole przygotowania**

Wykonanie odpowiednich kontroli przygotowania personelu (pracownicy, wykonawcy i użytkownicy będący stronami trzecimi), jeśli wymagają tego ich zadania i obowiązki.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Sprawdzenie kwalifikacji zawodowych personelu kluczowego (administratorów, pracowników ochrony, strażników itp.). | * Dokumentacja kontroli kwalifikacji zawodowych personelu kluczowego. |
| **2** | b) Przeprowadzenie kontroli/przeglądu przygotowania personelu kluczowego, gdy jest to potrzebne i dozwolone przez prawo.  c) Określenie polityki i procedur dla kontroli przygotowania. | * + Polityka i procedury dla kontroli/przeglądu przygotowania. * Wytyczne dla personelu dotyczące tego kiedy/jak przeprowadzać kontrole/przeglądy przygotowania. |
| **3** | d) Weryfikacja i aktualizacja zasad/procedur kontroli przygotowania i kontroli odniesienia - w regularnych odstępach czasu, z uwzględnieniem zmian i incydentów z przeszłości. | * Analiza komentarzy lub rejestrów zmian polityki/procedur. |

**CB 6: Wiedza i szkolenia z obszaru bezpieczeństwa**

Upewnienie się, że pracownicy mają wystarczającą wiedzę dotyczącą bezpieczeństwa oraz, że są objęci regularnymi szkoleniami bezpieczeństwa.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Zapewnienie kluczowemu personelowi odpowiednich szkoleń i materiałów na temat bezpieczeństwa. | * Kluczowy personel przeszedł szkolenia bezpieczeństwa i ma wystarczającą wiedzę z zakresu bezpieczeństwa (wywiad). |
| **2** | b) Wdrożenie programu szkoleń, upewniając się, że kluczowy personel ma wystarczającą i aktualną wiedzę na temat bezpieczeństwa.  c) Organizowanie szkoleń i sesji uświadamiających dla personelu w zakresie zagadnień bezpieczeństwa ważnych w organizacji. | * Pracownicy uczestniczyli w sesjach informacyjnych na tematy bezpieczeństwa. * Udokumentowany program szkoleń w zakresie umiejętności bezpieczeństwa, w tym cele różnych ról i sposoby ich osiągnięcia (np. przez szkolenia, podnoszenie świadomości, itp.). |
| **3** | d) Przegląd i aktualizacja programu szkoleń okresowych, z uwzględnieniem zmian i incydentów z przeszłości.  e) Sprawdzenie wiedzy personelu z zakresu bezpieczeństwa. | * Aktualizacja świadomości na temat bezpieczeństwa i programów szkoleniowych. * Wyniki sprawdzenia wiedzy personelu z zakresu bezpieczeństwa. * Analiza komentarzy lub rejestrów zmian programu. |

**CB 7: Zmiany personalne**

Ustalenie i utrzymanie właściwego procesu zarządzania zmianami personalnymi lub zmianami ról i obowiązków pracowników.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Po zmianach personalnych - anulowanie uprawnień dostępu dla pracowników, unieważnienie kart dostępu (identyfikatorów), wyposażenia itp., jeśli nie są już potrzebne lub dozwolone.  b) Wprowadzenie i edukowanie nowych pracowników w zakresie zasad i procedur. obowiązujących w organizacji. | * Dowody, że po zmianach personalnych nastąpiło odpowiednie wygaszenie praw dostępu, ważności kart dostępu (identyfikatorów), wyposażenia itp. * Dowód, że nowi pracownicy zostali wprowadzeni i wyedukowani w zakresie zasad i procedur obowiązujących w organizacji. |
| **2** | c) Wdrożenie polityk/procedur zmian personalnych, biorąc pod uwagę terminowe wygaszenie praw dostępu, ważności kart dostępu (identyfikatorów), wyposażenia itp.  d) Wdrożenie polityk/procedur dla szkolenia i edukowania pracowników w ich nowych rolach. | * Dokumentacja procesu zmian personalnych, w tym odpowiedzialności za zarządzanie zmianami, opisu praw dostępu i posiadania aktywów w danej roli, procedur wprowadzania i szkolenia pracowników w nowych rolach. * Dowód, że zmiany personalne zostały przeprowadzone zgodnie z wymogami procesu i że prawa dostępu zostały zaktualizowane w odpowiednim czasie (np. listy kontrolne). |
| **3** | e) Okresowa kontrola skuteczności polityki/procedur.  f) Przegląd i ocena polityki/procedury zmian personalnych, z uwzględnieniem zmian lub incydentów z przeszłości. | * Dowody kontroli uprawnień do dostępu itp. * Aktualne polityki / procedury zarządzania zmianami personalnymi. * Kontrola komentarzy lub rejestru zmian. |

**CB 8: Postępowanie z naruszeniami**

Ustanowienie i utrzymanie procesu dyscyplinarnego dla pracowników, którzy naruszają zasady bezpieczeństwa, lub posiadanie szerszego procesu, obejmującego naruszenia bezpieczeństwa spowodowane przez personel.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Wyznaczenie zakresu odpowiedzialności pracowników za naruszenia bezpieczeństwa spowodowane łamaniem przez nich ustalonych zasad, np. poprzez odpowiednie zapisy w umowie o pracę. | * Zasady obowiązujące personel, w tym obowiązki, kodeks postępowania, polityka wobec łamania zasad, itp.- jeśli możliwe to jako część umowy o pracę. |
| **2** | b) Ustanowienie procedur w przypadku naruszenia zasad przez personel. | * Dokumentacja procedur, obejmująca rodzaje naruszeń, które mogą być przedmiotem postępowań dyscyplinarnych, oraz rodzaje postępowania dyscyplinarnego. |
| **3** | c) Okresowy przegląd i aktualizacja procesu dyscyplinarnego, w oparciu o zmiany i incydenty z przeszłości. | * Kontrola komentarzy lub rejestru zmian. |

**O3: Bezpieczeństwo systemów i obiektów**

Ten obszar "Bezpieczeństwo systemów i obiektów" obejmuje fizyczne i logiczne bezpieczeństwo systemów oraz urządzeń sieciowych i informatycznych.

**CB 9: Bezpieczeństwo fizyczne i środowiskowe**

Ustanowienie i utrzymanie odpowiedniego fizycznego i środowiskowego bezpieczeństwa systemów oraz urządzeń sieciowych i informatycznych.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Zapobieganie nieautoryzowanemu dostępowi do obiektów i infrastruktury oraz stworzenie kontroli środowiskowej, w celu ochrony przed nieautoryzowanym dostępem, włamaniami, pożarem, powodzią itp. | * Podstawowe wdrażanie środków bezpieczeństwa fizycznego i kontroli środowiskowych, takich jak zamki w drzwiach i szafach, alarmy przeciwwłamaniowe, alarmy przeciwpożarowe, gaśnice itp. |

|  |  |  |
| --- | --- | --- |
| **2** | b) Wdrożenie polityki stosowania środków ochrony fizycznej i kontroli środowiska.  c) Wdrożenie branżowych standardów w środki ochrony fizycznej i kontroli środowiska. | * + Udokumentowana polityka środków bezpieczeństwa fizycznego i kontroli środowiska, w tym opis urządzeń i systemów w zakresie. * Kontrole fizyczne i środowiskowe, takie jak elektroniczna kontrola dostępu wejścia i kontroli, segmentacja przestrzeni według poziomów uprawnień, automatyczne gaśnice fluorowcowodorowe, itp. |
| **3** | d) Ocena skuteczności kontroli fizycznych i środowiskowych - okresowo.  e) Przegląd i aktualizacja polityki na rzecz środków bezpieczeństwa fizycznego i kontroli środowiska, z uwzględnieniem zmian i incydentów z przeszłości. | * + Aktualizacja polityki stosowania środków ochrony fizycznej i kontroli środowiska. * Dokumentacja dotycząca oceny kontroli środowiska, analiza komentarzy lub rejestrów zmian. |

**CB 10: Bezpieczeństwo dostaw**

Ustanowienie i utrzymanie odpowiedniego bezpieczeństwa dostaw (energii elektrycznej, paliwa itp).

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Zapewnienie bezpieczeństwa dostaw, takich jak energia elektryczna, paliwo lub chłodzenie. | * Bezpieczeństwo dostaw jest chronione w zasadniczy sposób, np. zasilanie awaryjne i/lub zapas paliwa są dostępne. |
| **2** | b) Wdrożenie polityki bezpieczeństwa dostaw krytycznych, takich jak energia elektryczna, paliwa, itp.  c) Wdrożenie branżowych standardów bezpieczeństwa w celu ochrony dostaw i obiektów wsparcia. | * Udokumentowana polityka ochrony krytycznych dostaw, takich jak energia elektryczna, paliwo, itp. opisująca różne rodzaje dostaw i środków bezpieczeństwa chroniących dostawy. * Dowody realizowania branżowych standardów, zapewniających bezpieczeństwo dostaw, np. pasywne chłodzenie, automatyczny restart po zaniku zasilania, awaryjne zasilanie akumulatorowe, generatory dieslowskie, zapas paliwa, itp. |
| **3** | d) Wdrożenie zaawansowanych środków bezpieczeństwa w celu ochrony dostaw.  e) Regularny przegląd i aktualizacja polityki i procedur bezpiecznych dostaw, z uwzględnieniem zmian i incydentów z przeszłości. | * Dowody realizowania zaawansowanych środków bezpieczeństwa w celu ochrony dostaw, takich jak aktywne chłodzenie, UP, gorące generatory prądu w trybie gotowości, odpowiednie umowy o gwarantowanym poziomie świadczenia usług w zakresie dostawy paliwa, zapasowe systemy chłodzenia i zasilania awaryjnego. * Aktualna polityka zabezpieczenia dostaw oraz wspierania obiektów, analiza komentarzy i/lub rejestrów zmian. |

**CB 11: Kontrola dostępu do sieci i systemów informatycznych**

Ustanowienie i utrzymanie właściwej (logicznej) kontroli dostępu do sieci i systemów informatycznych.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Użytkownicy i systemy posiadają unikalne identyfikatory i są uwierzytelniane przed uzyskaniem dostępu do usług lub systemów.  b) Wdrożenie (logicznego) mechanizmu kontroli dostępu do sieci i systemów informatycznych, umożliwiającego jedynie autoryzowane użytkowanie. | * Rejestry dostępu pokazują poszczególne identyfikatory użytkowników i systemy przyznania lub odmówienia dostępu. * Przegląd metod uwierzytelniania i kontroli dostępu w odniesieniu do systemów i użytkowników. |
| **2** | c) Wdrożenie polityki na rzecz ochrony dostępu do sieci i systemów informatycznych, z uwzględnieniem np. ról, praw, obowiązków i procedur przypisywania i cofania uprawnień.  d) Wybór odpowiednich mechanizmów uwierzytelniania, w zależności od typu dostępu.  e) Monitorowanie dostępu do sieci i systemów informatycznych, obecność procesu zatwierdzania wyjątków i rejestracji naruszeń. | * Polityka kontroli dostępu w tym opis ról, grup praw dostępu, procedur udzielania i cofania dostępu. * Różne rodzaje mechanizmów uwierzytelniania dla różnych rodzajów dostępu. * Rejestr naruszeń i wyjątków od polityki kontroli dostępu, zatwierdzony przez pracownika ochrony. |
| **3** | f) Ocena skuteczności polityki i procedur kontroli dostępu i wdrożenie kontroli krzyżowych mechanizmów kontroli dostępu.  h) Polityka kontroli dostępu i mechanizmy kontroli dostępu i są sprawdzane i w razie potrzeby korygowane. | * Raporty z testów (bezpieczeństwa) mechanizmów kontroli dostępu. * Narzędzia do wykrywania niewłaściwego wykorzystania systemów lub niewłaściwych zachowań systemów (np. systemy wykrywania włamań i anomalii). * Rejestry wykrywania włamań i systemy wykrywania anomalii. * Aktualizacje polityki kontroli dostępu, analiza komentarzy lub rejestrów zmian. |

**CB 12: Integralność sieci i systemów informatycznych**

Ustanowienie i utrzymanie integralności sieci i systemów informatycznych oraz ochrona przed wirusami, wstrzykiwaniem kodu i innym złośliwym oprogramowaniem, które może zmieniać funkcjonalność systemów.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Zapewnienie, że oprogramowanie sieci i systemów informatycznych nie jest naruszone lub zmienione, na przykład za pomocą kontroli wejścia i zapór typu "firewall".  b) Zapewnienie, że zabezpieczenia ważnych danych (np. haseł, wspólnych informacji tajnych, prywatnych kluczy etc.) nie są ujawniane lub przerabiane. | * Oprogramowanie i dane w sieci i w systemach informatycznych są chronione za pomocą kontroli dostępu, zapór typu "firewall", szyfrowania i podpisów elektronicznych i tradycyjnych. * Dane krytyczne dla bezpieczeństwa są chronione przy użyciu mechanizmów ochrony takich jak oddzielne przechowywanie, szyfrowanie, przemieszczanie itp. |

|  |  |  |
| --- | --- | --- |
|  | c) Kontrola pod kątem złośliwego oprogramowania w (wewnętrznych) sieciach i systemach informatycznych. | * Systemy wykrywania szkodliwego oprogramowania są obecne i aktualizowane. |
| **2** | d) Wdrożenie standardowych branżowych środków bezpieczeństwa, zapewniając silną ochronę przed ingerencją i zmianą systemów. | * Dokumentacja tego, jak realizowana jest ochrona oprogramowania i danych w sieci i systemach informacyjnych. * Narzędzia do wykrywania niewłaściwego wykorzystania systemów lub niewłaściwych zachowań systemów (np. systemy wykrywania włamań i anomalii). * Rejestry wykrywania włamań i systemy wykrywania anomalii. |
| **3** | e) Ustanowienie najnowocześniejszych sposobów ochrony integralności systemów.  f) Ocena i przegląd skuteczności środków ochrony integralności systemów. | * Zaawansowane sposoby ochrony integralności systemów, takie jak podpisywanie kodów, tripwire, itp. * Dokumentacja procesu sprawdzania systemów rejestrowania wykrytych anomalii i włamań. |

**O4: Zarządzanie operacyjne**

Obszar "Zarządzanie operacyjne" obejmuje procedury operacyjne, zarządzanie zmianą i zarządzanie aktywami.

**CB 13: Procedury operacyjne**

Ustanowienie i utrzymanie procedur operacyjnych dotyczących funkcjonowania krytycznych sieci i systemów informatycznych przez pracowników.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Ustanowienie procedur operacyjnych i przypisanie odpowiedzialności za obsługę systemów krytycznych. | * Dokumentacja procedur operacyjnych i zakresów odpowiedzialności za kluczowe sieci i systemy informatyczne. |
| **2** | b) Wdrożenie polityki obsługi systemów, aby zapewnić, że wszystkie systemy krytyczne są obsługiwane i zarządzane zgodnie z wcześniej zdefiniowanymi procedurami. | * Udokumentowana polityka funkcjonowania systemów krytycznych, w tym informacje o sieci i systemach informatycznych w tym zakresie. |
| **3** | c) Weryfikacja i aktualizacja polityk/procedur obsługi systemów krytycznych, z uwzględnieniem incydentów i/lub zmian. | * Aktualizowane polityki/procedury obsługi systemów krytycznych, analiza komentarzy i/lub rejestrów zmian. |

**CB 14: Zarządzanie zmianą**

Ustanowienie procedur zarządzania zmianą dla krytycznych sieci i systemów informatycznych w celu zminimalizowania prawdopodobieństwa incydentów spowodowanych przez zmiany.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Przestrzeganie ustalonych procedur podczas dokonywania zmian w systemach krytycznych. | * Dokumentacja procedur zarządzanie zmianą dla systemów krytycznych. |
| **2** | b) Wdrożenie polityk/procedur zarządzania zmianą, aby upewnić się, że zmiany systemów krytycznych są zawsze wykonywane w ustalony sposób.  c) Dokumentowanie procedur zarządzania zmianą i zapisywanie każdego etapu zmiany w wykonywanej procedurze. | * Dokumentacja polityk/procedur zarządzania zmianą, w tym systemów będących przedmiotem polityki, celów, procedur wycofania itp. * Dla każdej zmiany, dostępny jest raport opisujący kroki i wyniki zmian(y). |
| **3** | d) Regularny przegląd i aktualizacja procedur zarządzania zmianą, z uwzględnieniem zmian i incydentów z przeszłości. | * Aktualizacja procedur zarządzania zmianą, analiza komentarzy i/lub rejestrów zmian. |

**CB 15: Zarządzanie aktywami**

Ustanowienie i utrzymanie procedur w zakresie zarządzania aktywami i kontroli konfiguracji w celu zarządzania dostępnością aktywów i konfiguracji sieci i systemów informatycznych o znaczeniu krytycznym.

|  |  |  |  |
| --- | --- | --- | --- |
|  | | **Środki bezpieczeństwa** | **Dowód** |
| **1** | | a) Zarządzanie aktywami krytycznymi i konfiguracje systemów krytycznych. | * Lista krytycznych zasobów i systemów krytycznych. |
| **2** | | b) Wdrożenie polityki/ procedur zarządzania aktywami i kontrolą konfiguracji. | * Udokumentowane polityki/procedury w zakresie zarządzania aktywami, w tym role i obowiązki, aktywa i konfiguracje, które są przedmiotem polityki, a także cele zarządzania aktywami. * Inwentaryzacja albo inwentaryzacje spisów i zapasów, zawierających aktywa krytyczne i zależności pomiędzy aktywami. * Konfiguracja kontroli lub inwentaryzacji zapasów, obejmująca konfiguracje systemów krytycznych. |
| **3** | c) Regularny przegląd i aktualizacja polityki zarządzania aktywami, na podstawie zmian i incydentów z przeszłości. | | * Bieżące polityki/procedury zarządzania aktywami, analiza komentarzy i/lub rejestrów zmian. |

**O5: Zarządzanie incydentami**

Obszar "Zarządzanie incydentami" obejmuje wykrywanie, reakcję, raportowanie i komunikowanie o incydentach.[[7]](#footnote-7)

**CB 16: Procedury zarządzania incydentami**

Ustanowienie i utrzymanie procedur zarządzania incydentami i przekazywanie ich do odpowiednich pracowników (triage).

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Zapewnienie, że personel jest dostępny i przygotowany do zarządzania i radzenia sobie z incydentami.  b) Prowadzenie rejestru wszystkich większych incydentów | * Personel wie jak radzić sobie z incydentami i kiedy zgłaszać je dalej. * Wykaz głównych incydentów i dla każdego incydentu: jego wpływ, przyczyny, podjęte działania, wnioski. |
| **2** | c) Wdrożenie polityki/procedur zarządzania incydentami. | * Polityki/procedury zarządzania incydentami, w tym: typy incydentów, które mogą wystąpić, cele, role i obowiązki, szczegółowy opis oraz dla każdego incydentu: sposób postępowania, kiedy zgłaszać go dalej do przełożonych wyższego szczebla (np. CISO) itp. |
| **3** | d) Zbadanie poważnych incydentów oraz sporządzenie raportów końcowych, obejmujących podjęte działania i zalecenia mające na celu ograniczenie przyszłego wystąpienia tego typu incydentów.  e) Ocena polityk/procedur zarządzania incydentami, w oparciu o incydenty z przeszłości. | * Indywidualne raporty z radzenia sobie z poważnymi incydentami. * Bieżące polityki/procedury zarządzania incydentami, analiza komentarzy i/lub rejestrów zmian. |

**CB 17: Potencjał wykrywania incydentów**

Określenie i utrzymanie potencjału wykrywania incydentów.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Ustanowienie procesów lub systemów wykrywania incydentów. | * Wcześniejsze incydenty zostały wykryte i terminowo przekazane do odpowiednich osób. |
| **2** | b) Wdrożenie standardowych branżowych systemów i procedur wykrywania incydentów.  c) Wdrożenie systemów i procedur rejestracji i przekazywania incydentów w sposób terminowy do odpowiednich osób. | * Systemy wykrywania incydentów i procedury, takie jak narzędzia Zarządzenia Incydentami i Wydarzeniami Bezpieczeństwa (SIEM), działy wsparcia bezpieczeństwa dla personelu, raporty i biuletyny z CERT, narzędzia do wykrywania nieprawidłowości itp. |
| **3** | d) Regularny przegląd systemów i procesów wykrywania incydentów i ich aktualizacja z uwzględnieniem zmian i incydentów z przeszłości. | * Aktualna dokumentacja systemów i procesów wykrywania incydentów. * Dokumentacja przeglądu procesu wykrywania incydentów, analiza komentarzy, i/lub rejestrów zmian. |

**CB 18: Raportowanie i komunikowanie incydentów**

Ustanowienie i utrzymanie odpowiednich procedur raportowania i komunikowania incydentów, z uwzględnieniem przepisów krajowych w sprawie raportowania incydentów do władz rządowych[[8]](#footnote-8).

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Komunikowanie i raportowanie bieżących i przeszłych incydentów do stron trzecich, klientów i/lub władz, jeśli to konieczne. | * Dowody pokazujące zgłaszanie i raportowanie incydentów z przeszłości. |
| **2** | b) Wdrażanie polityki i procedur komunikowania i raportowania incydentów. | * Udokumentowana polityka i procedury komunikacji i raportowania o zdarzeniach, z opisem powodów/motywacji komunikowania i raportowania (powody biznesowe, powody prawne itp.), rodzaje objętych incydentów, wymagane treści komunikatów, zawiadomień lub raportów, kanały jakie mają być stosowane, oraz role osób odpowiedzialnych za komunikowanie, powiadamianie i raportowanie. * Szablony dla raportowania i komunikowania incydentów |
| **3** | c) Ocena raportowania i komunikowania incydentów  d) Weryfikacja i aktualizacja planów raportowania i komunikowania, w oparciu o zmiany lub incydenty z przeszłości. | * Lista przeszłych raportów i zgłoszeń incydentów * Aktualna polityka reagowania na incydenty i komunikowania ich, analiza komentarzy, i/lub rejestrów zmian. |

**O6: Zarządzanie ciągłością działalności**

Obszar "Zarządzanie ciągłością działalności" obejmuje strategie ciągłości i plany awaryjne łagodzące skutki poważnych awarii i/lub katastrof naturalnych.

**CB 19: Strategia ciągłości usług i plany awaryjne**

Określenie i utrzymanie planów awaryjnych i strategii zapewnienia ciągłości działania sieci i usług komunikacyjnych.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Wdrożenie strategii ciągłości usług dla sieci informacyjnych i/lub świadczonych usług. | * + Udokumentowana strategia ciągłości usług, w tym cele w zakresie czasu przywrócenia kluczowych usług i procesów. |
| **2** | b) Wdrożenie planów awaryjnych dla systemów krytycznych.  c) Monitorowanie aktywacji i realizacji planów awaryjnych, rejestracja czasu udanego i nieudanego przywracania funkcjonalności. | * + Plany awaryjne dla systemów krytycznych, w tym jasne kroki i procedury reagowania na powszechne zagrożenia, progi aktywacji, kroki i docelowe czasy przywrócenia funkcjonalności.   + Proces podejmowania decyzji uruchomienia planów awaryjnych. * Rejestry uruchamiania i realizacji planów awaryjnych, w tym podjętych decyzji, wykonane kroki, końcowy czas przywrócenia funkcjonalności. |
| **3** | d) Okresowy przegląd i analiza strategii ciągłości usług.  e) Przegląd i zmiana planów awaryjnych na podstawie zmian i incydentów z przeszłości. | * + Aktualna strategia ciągłości i plany awaryjne, analiza komentarzy i/lub rejestrów zmian. |

**CB 20: Możliwości usuwania skutków awarii**

Ustalenie i utrzymanie odpowiedniej zdolności usuwania skutków awarii w celu przywrócenia usług sieciowych i komunikacyjnych, w przypadku naturalnych i/lub poważnych awarii.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Przygotowanie do odzyskiwania i przywracania usług po awariach. | * Wdrożono środki mające na celu radzenie sobie z awariami/katastrofami, takich jak awarie jednostek w innych regionach, kopie zapasowe ważnych danych z odległych jednostek itp. |
| **2** | b) Wdrożenie zasad/procedur aktywacji potencjału przywracania funkcjonalności po awarii.  c) Wdrożenie standardowych, branżowych możliwości usuwania skutków awarii lub zapewnienie, że są one dostępne od stron trzecich (takich jak krajowe sieci awaryjne). | * Udokumentowane polityki/procedury wdrażania możliwości przywracania funkcjonalności po awarii, w tym lista naturalnych i/lub poważnych klęsk żywiołowych, które mogłyby mieć wpływ na usługi, oraz lista możliwości przywracania funkcjonalności (zarówno tych dostępnych wewnętrznie lub świadczonych przez strony trzecie). * Wdrożenie standardowych branżowych możliwości reagowania na awarie, takich jak sprzęt ruchomy, instalacje mobilne, instalacje zapasowy odporne na awarie, itp. |
| **3** | c) Zorganizowanie zaawansowanych możliwości usuwania skutków awarii aby zmniejszać skutki poważnych awarii i/lub katastrof naturalnych.  d) Regularny przegląd i aktualizacja możliwości usuwania skutków awarii, z uwzględnieniem zmian, przeszłych incydentów i wyników testów i ćwiczeń. | * Zaawansowane możliwości usuwania skutków awarii, takie jak mechanizmy mocy zapasowych i przełączania awaryjnego podczas znaczących awarii i katastrof naturalnych. * Aktualna dokumentacje możliwości usuwania skutków awarii, analiza komentarzy i/lub rejestrów zmian. |

**O7: Monitorowanie, audytowanie i testowanie**

Obszar "Monitorowanie, audytowanie i testowanie" obejmuje monitorowanie, badanie i audyt sieci i systemów urządzeń informatycznych oraz obiektów.

**CB 21: Zasady monitorowania i rejestrowania**

Ustanawianie i utrzymanie systemów i funkcji monitorowania i rejestrowania krytycznych sieci i systemów komunikacyjnych.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Wdrażanie monitorowania i rejestrowania systemów krytycznych. | * Rejestry i sprawozdania z monitorowania krytycznych sieci i systemów informatycznych. |
| **2** | b) Wdrażanie polityki rejestrowania i monitorowania systemów krytycznych.  c) Konfiguracja narzędzi do monitorowania systemów krytycznych  d) Konfiguracja narzędzi do zbierania i przechowywania rejestrów systemów krytycznych. | * + Udokumentowana polityka w zakresie monitorowania i rejestrowania, zawierająca minimalne wymogi w zakresie monitorowania i rejestrowania, okres przechowywania i ogólne cele przechowywania danych monitorowania i rejestrów. * Narzędzia dla systemów monitorowania i gromadzenia danych rejestrowych. * Lista monitorowania danych i plików rejestrów, zgodnych z polityką. |
| **3** | e) Zorganizowanie narzędzi do automatycznego zbierania i analizy danych z monitoringu i rejestrów.  f) Przegląd i aktualizacja polityki i procedur logowania i monitorowania, z uwzględnieniem zmian i incydentów z przeszłości. | * + Narzędzia ułatwiające strukturalny zapis i analizę danych z monitorowania i rejestrów. * Zaktualizowana dokumentacja polityk/procedur monitorowania i rejestrowania, analiza komentarzy, i/lub rejestrów zmian. |

**CB 22: Ćwiczenie planów awaryjnych**

Ustanowienie i utrzymanie polityki testowania i ćwiczenia wykonywania kopii zapasowych i planów awaryjnych, jeżeli są konieczne we współpracy ze stronami trzecimi.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Wykonanie i przetestowanie kopii zapasowych i planów awaryjnych, aby upewnić się że systemy i procesy robocze oraz personel są przygotowani na duże awarie i nieprzewidziane wydarzenia. | * Raporty z ostatniego wykonania kopii zapasowych i planów awaryjnych. |
| **2** | b) Wdrożenie programu regularnego wykonywania kopii zapasowych i planów awaryjnych, używając realistycznych scenariuszy obejmujące szereg różnych scenariuszy na przestrzeni czasu.  c) Zapewnienie, że problemy i wnioski wyciągnięte z ćwiczeń są rozpatrywane przez odpowiedzialnych pracowników i że odpowiednie procesy i systemy są odpowiednio zaktualizowane. | * + Program ćwiczeń dla wykonywania kopii zapasowych i planów awaryjnych, obejmujących nieprzewidziane okoliczności, częstotliwość, role i obowiązki, szablony i procedury dla prowadzących ćwiczenia, szablony wykonywania raportów.   + Raporty z ćwiczeń i wykonywania planów awaryjnych, wraz z wnioskami wyciągniętymi z ćwiczeń. * Problemy i wnioski wyciągnięte z ćwiczeń zostały rozpatrzone przez odpowiednie osoby. |
| **3** | d) Weryfikacja i aktualizacja planów ćwiczeń, z uwzględnieniem zmian i incydentów z przeszłości oraz okoliczności, które nie zostały objęte programem ćwiczeń.  e) Zaangażowanie w ćwiczenia dostawców i innych stron trzecich, np. partnerów biznesowych i klientów. | * + Zaktualizowane plany ćwiczeń, analiza komentarzy, i/lub rejestrów zmian. * Wkład dostawców i innych zaangażowanych stron trzecich w to, jak poprawić scenariusze ćwiczeń. |

**CB 23: Testowanie sieci i systemów informatycznych**

Ustanowienie i utrzymanie polityki testowania sieci i systemów informatycznych, w szczególności w przypadku podłączenia do nowych sieci lub systemów.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Testowanie sieci i systemów informatycznych przed ich użyciem lub podłączaniem ich do istniejących systemów. | * Raporty z testów sieci i systemów informatycznych, w tym testów po dużych zmianach lub wdrożeniu nowych systemów. |
| **2** | b) Wdrożenie zasad/procedur testowania sieci i systemów informatycznych,  c) Wdrożenie narzędzi do automatycznego testowania | * Polityki/procedury testowania sieci i systemów informatycznych, obejmujące wymagany czas testowania, plany testów, przypadki testowe, szablony raportów z testu. |
| **3** | d) Przegląd i aktualizacja polityki i procedur testowania, z uwzględnieniem zmian i incydentów z przeszłości. | * Lista raportów z badań. * Aktualizowane polityki/procedury testowania sieci i systemów informatycznych, analiza komentarzy i/lub rejestrów zmian. |

**CB 24: Oceny bezpieczeństwa**

Ustalenie i utrzymanie właściwej polityki dokonywania oceny bezpieczeństwa sieci i systemów informatycznych.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Zapewnienie, że systemy krytyczne poddawane są regularnie skanowaniu bezpieczeństwa i testowaniu zabezpieczeń, zwłaszcza gdy nowe systemy są wdrażane i po zmianach. | * Raporty z poprzednich operacji skanowania bezpieczeństwa i testów bezpieczeństwa. |
| **2** | b) Wdrożenie polityk/procedur oceny bezpieczeństwa i testowania bezpieczeństwa. | * Udokumentowane polityki/procedur oceny bezpieczeństwa i testowania bezpieczeństwa, wraz z informacjami o tym, które aktywa testować, w jakich okolicznościach, rodzaj ocen bezpieczeństwa i testów, częstotliwość, zatwierdzone osoby/strony (wewnętrzne lub zewnętrzne), poziom poufności dla oceny i wyników testów i ocen bezpieczeństwa cele i badania. |
| **3** | c) Ocena skuteczności polityk/procedur oceny bezpieczeństwa i testowania bezpieczeństwa.  d) Przegląd i aktualizacja polityki i procedur ocen bezpieczeństwa i testowania bezpieczeństwa, z uwzględnieniem zmian i incydentów z przeszłości. | * + Wykaz raportów dotyczących oceny bezpieczeństwa i testów bezpieczeństwa   + Raporty dotyczące działań zalecanych po ocenie bazujące na wynikach ocen i testów * Aktualne polityki/procedury oceny bezpieczeństwa i testów bezpieczeństwa, analiza komentarzy i/lub rejestrów zmian. |

**CB 25: Monitorowanie zgodności**

Ustanowienie i utrzymanie polityki monitorowania zgodności z normami i wymogami prawnymi.

|  |  |  |
| --- | --- | --- |
|  | **Środki bezpieczeństwa** | **Dowód** |
| **1** | a) Monitorowanie zgodności z normami i wymogami prawnymi. | * Raporty opisujące wyniki monitorowania zgodności. |
| **2** | b) Wdrożenie polityki/procedur dla monitorowania zgodności i audytowania. | * + Udokumentowane polityki/procedury monitorowania zgodności i audytowania, obejmujące informacje o tym, co monitorować (aktywa, procesy, infrastruktura), częstotliwość, wytyczne dotyczące audytorów (wewnętrzni lub zewnętrzni), odpowiednie zasady bezpieczeństwa, które podlegają kontroli zgodności i audytom, cele i istotne podejście do monitorowania zgodności i audytu, szablony raportów z audytu. * Szczegółowe plany monitorowania i audytów, w tym długoterminowe istotne cele i planowanie |
| **3** | c) Oceny polityki / procedur zgodności i prowadzenia audytów.  d) Przegląd i aktualizacja polityki i procedur zgodności i prowadzenia audytów, z uwzględnieniem zmian i incydentów z przeszłości. | * Lista wszystkich raportów zgodności i audytowych * Aktualizowane polityki/procedur zgodności i prowadzenia audytów, analiza komentarzy i/lub rejestrów zmian. |

**5 Nadzór techniczny środków bezpieczeństwa**

Ustępy 1 i 2 of Artykułu 13a wymagają od krajowych organów regulacyjnych zapewnienia, że usługodawcy przeprowadzą ocenę ryzyka oraz podejmą odpowiednie środki bezpieczeństwa. W tej sekcji omówimy szczegóły techniczne nadzorowania, które dostawcy podejmują aby zapewnić odpowiednie środki bezpieczeństwa[[9]](#footnote-9).

Najczęstsze działania regulacyjne krajowych organów regulacyjnych dotyczące nadzoru środków bezpieczeństwa to[[10]](#footnote-10):

* + - Wprowadzenie obowiązkowych lub zalecanie standardów bezpieczeństwa
    - Oceny zgodności na całym rynku
    - Realizacja etapowego podejście do nadzoru
    - Audyt dostawców (okresowo, losowo i/lub po incydentach)

W dalszej części tej sekcji omawiamy techniczne aspekty każdej z tych działalności.

**5.1 Wprowadzenie obowiązkowych lub zalecanie standardów bezpieczeństwa**

Może istnieć kilka powodów wymagania lub zalecania norm dla środków bezpieczeństwa:

* + - przedstawienie **wytycznych** dotyczących tego, jakie środki bezpieczeństwa należy realizować, np. poprzez wyjaśnienie istotnych celów lub szczegółowych środków bezpieczeństwa;
    - przedstawienie **terminologii** użytecznej w omawianiu celów bezpieczeństwa lub środków bezpieczeństwa.
    - przedstawienie **struktury** nadzoru i audytów przez podział kwestii bezpieczeństwa na różne obszary;
    - przedstawienie **poziomu odniesienia (poziomu podstawowego),** czyli minimalnego zestawu środków bezpieczeństwa, które muszą być wdrożone, np. dlatego, że bez nich trudne może być przeprowadzenie audytu, gdyż brakuje kluczowych dowodów, takich jak rejestry, zapisy incydentów itp.;
    - przedstawienie **odwzorowania (związków)** różnych istniejących norm, np. w celu umożliwienia porównywania zgodności i przygotowania raportów z audytu, opartych na różnych normach.

Poniżej podajemy szczegóły różnych opcji.

**5.1.1 Wprowadzenie obowiązkowych kontra zalecanie standardów bezpieczeństwa**

Przy omawianiu nadzoru prawodawstwa dotyczącego bezpieczeństwa przez organy rządowe, często dochodzi do dyskusji na temat tego, czy organ rządowy powinien wymagać, silnie sugerować czy tylko zalecać określoną listę środków bezpieczeństwa. Można argumentować, że wprowadzenie obowiązkowej normy stworzy jasność co do tego, co dostawcy muszą zrobić, aby uzyskać zgodność z tą normą. Z drugiej strony, można też twierdzić, że w większości warunków branżowych, zaangażowanych organizacji i stosowanych technologii są po prostu zbyt zróżnicowane, aby stworzyć jedną listę kontrolną minimalnych środków bezpieczeństwa dla całego sektora. Często jedynie normy bezpieczeństwa wysokiego rzędu mogą być racjonalnie zastosowane do większej liczby organizacji. Nieuchronnie takie istotne lecz ogólne normy bezpieczeństwa pozostawiają wiele ważnych kwestii technicznych nierozwiązanych. Dlatego tak trudno jest uchwycić wszystkie wymogi bezpieczeństwa Artykułu 13a w sposób *kompleksowy* w jednej normie. W tym samym czasie dla *konkretnych* warunków lub specyficznych problemów krajowe organa regulacyjne mogą wymagać zastosowania *konkretnych* środków bezpieczeństwa. Na przykład, NRA może poprosić wszystkich dostawców, aby podali krajowym organom regulacyjnym punkt kontaktowy na wypadek wydarzeń nieprzewidzianych, lub poprosić wszystkich dostawców o posiadanie czterogodzinnego zasilania awaryjnego dla sterowników stacji bazowych.

Należy pamiętać, że czyniąc określone środki obowiązkowymi dla konkretnych aspektów, ważne jest, aby wcześniej krajowe organy regulacyjne omówiły z dostawcami ich skuteczność i możliwość stosowania. Takie dyskusje mogą być wywołane przez duże incydenty z przeszłości, często powtarzające się przyczyny awarii i/lub inne wspólne problemy (np. luki w zabezpieczeniach oprogramowania popularnych urządzeń informatycznych).

Najlepsze praktyki w zakresie bezpieczeństwa sieci i informacji zmieniają się bardzo szybko, ponieważ szybko zmienia się technologia informacyjna oraz szybko zmieniają się zdolności agresorów. Krajowy organ regulacyjny ma wyjątkową rolę wspierania i promowania wymiany wiedzy i dyskusji na temat najlepszych praktyk pomiędzy ekspertami z różnych dostawców. W ten sposób krajowe organy regulacyjne wspierają przyjęcie najlepszych praktyk w całej branży. Szczególnie dostawcy z mniejszym doświadczeniem i mniejsza wiedzą mogą bardzo skorzystać z takich dyskusji i wymiany wiedzy.

**5.1.2 Korzystanie z wytycznych ENISA jako rekomendacji**

Krajowe organy regulacyjne mogą wykorzystać te wytyczne ENISA do opracowania wytycznych dla dostawców. Wytyczne ENISA obejmują 25 istotnych celów bezpieczeństwa uzyskanych z różnych norm (patrz Bibliografia). Aby osiągnąć cele bezpieczeństwa, dostawcy powinni wybrać odpowiednie środki bezpieczeństwa technicznego. Niniejszy dokument wymienia szczegółowe środki bezpieczeństwa, które dostawcy mogą podjąć, aby osiągnąć cele bezpieczeństwa. Środki bezpieczeństwa są podzielone na trzy poziomy (zaawansowania), począwszy od 1) podstawowego, przez 2) standard branżowy, do 3) zaawansowanego. Dostawcy powinni ocenić ryzyko swoich sieci i usług, aby zrozumieć, jakie środki bezpieczeństwa są właściwe.

**5.1.3 Korzystanie z wytycznych ENISA jako wzorca**

Wielu (zwłaszcza dużych) dostawców opracowało już standardy bezpieczeństwa lub ramy zarządzania bezpieczeństwem, często w oparciu o normy międzynarodowe. Niniejsze wytyczne ENISA mogą być wykorzystane jako neutralny sposób odwzorowania (mapowania) różnych norm wykorzystywanych w branży. Takie odwzorowanie pozwoli dostawcom kontynuować stosowanie istniejących norm międzynarodowych i unikanie niepotrzebnych kosztów przy spełnianiu wymogów Art. 13a.

W praktyce np. dostawcy mogą wykazać zgodność z artykułem 13a poprzez dostarczanie raportów z audytu i certyfikatów potwierdzających zgodność z istniejącymi normami branżowymi, w połączeniu z odwzorowaniem tych norm z wymogami niniejszych wytycznych ENISA. W Sekcji 6 podajemy przykład powiązania (odwzorowania) tych wytycznych z niektórymi znanymi normami międzynarodowymi.

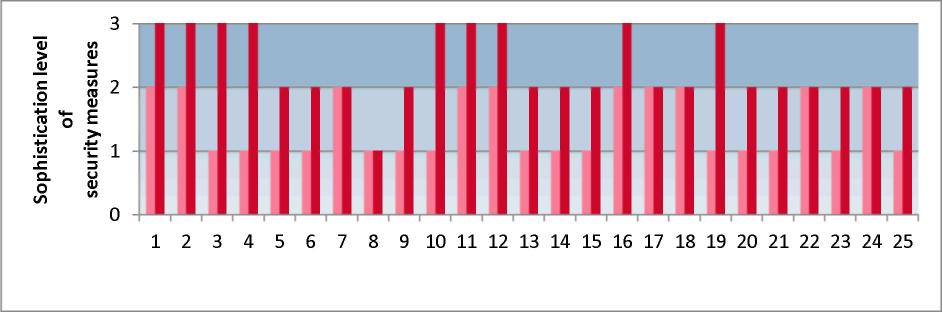
**5.1.4 Korzystanie z istniejących norm krajowych lub międzynarodowych lub najlepszych praktyk**

Krajowe organy regulacyjne mogą odnosić się do obowiązujących norm i wymogów krajowych lub międzynarodowych - traktując je jako wymogi podstawowe lub rekomendacje. Przegląd norm i standardów powszechnie stosowanych w branży jest załączony w sekcji Bibliografia. Krajowe organy regulacyjne powinny uwzględniać uwarunkowania krajowe przy wyborze odpowiedniego zestawu norm lub najlepszych praktyk. Chcielibyśmy przedstawić trzy uwagi w tym zakresie:

* + - Krajowe organy regulacyjne powinny wziąć pod uwagę, że niektórzy (zwłaszcza więksi) dostawcy mogą działać w kilku krajach UE, i że uciążliwe będzie dla tych dostawców przyjęcie różnych norm/standardów w różnych krajach. W związku z tym, użyteczne może okazać się pozwolenie tym dostawcom na stosowanie norm międzynarodowych, które są powszechnie stosowane w całej UE, i w ten sposób zmniejszenie kosztów osiągnięcia zgodności z przepisami przez tych operatorów.
    - W większości krajów sektor łączności elektronicznej jest duży (setki dostawców) i obejmuje zarówno dużych dostawców (>10% udziału w rynku) i bardzo małych dostawców (<1% rynku)[[11]](#footnote-11). Krajowe organy regulacyjne powinny również uwzględniać różnice między dostawcami w swoim kraju. To, co może działać w odniesieniu do dużych dostawców, może być przytłaczające dla mniejszych operatorów i odwrotnie - to, co działa dla jednego operatora może być nieodpowiednie dla innego.
* Wreszcie, krajowe organy regulacyjne powinny wziąć pod uwagę, że najlepsze praktyki w zakresie bezpieczeństwa sieci i informacji zmieniają się bardzo szybko, ponieważ szybko zmienia się technologia informacyjna oraz szybko zmieniają się zdolności agresorów. To sprawia, że trudno uchwycić istotne wymagania bezpieczeństwa Artykułu 13a w sposób kompleksowy w formie listy szczegółowych środków bezpieczeństwa. Wobec tego, krajowe organy regulacyjne powinny koncentrować się przede wszystkim na nadzorowaniu tego, czy dostawcy ocenili ryzyko i aktywnie wdrażają odpowiednie środki bezpieczeństwa, a nie na tym, by dokładnie określić szczegółowe i niezmienne środki bezpieczeństwa.

**5.2 Ocena zgodności na całym rynku**

Samoocena może być wykorzystana do uzyskania ogólnych informacji na temat rodzaju środków bezpieczeństwa stosowanych przez dostawców w całym sektorze. Cele i środki bezpieczeństwa wymienione w Sekcji 4 mogą być wykorzystane bezpośrednio w formularzu samooceny. Poziomy zaawansowania (patrz Sekcja 4) pozwalają dostawcom na wskazanie środków bezpieczeństwa stosowanych w odniesieniu do poszczególnych celów bezpieczeństwa. Stosowane w ten sposób poziomy zaawansowania przedstawią profil dostawcy, pozwalając na szybkie porównanie dostawców w całym sektorze.



**Poziom zaawansowania środków** bezpieczeństwa

**Rysunek 2: Dwa różne profile z różnym poziomem zaawansowanie środków bezpieczeństwa dla każdego celu bezpieczeństwa.**

**Cele bezpieczeństwa**

Na rysunku 2 przedstawiamy dwa przykładowe profile na jednym schemacie. Oś pionowa obejmuje poziomy zaawansowania a oś pozioma przedstawia cele bezpieczeństwa. Ciemnoczerwony kolor wskazuje dostawcę z bardziej zaawansowanymi środkami bezpieczeństwa. Jasnoczerwony kolor wskazuje dostawcę z mniej zaawansowanymi środkami bezpieczeństwa. Różnica w poziomie zaawansowania może być wyjaśniona np. przez różnicę w rodzaju usług komunikacyjnych i sieci oferowanych przez dwóch operatorów.

W zależności od powodu samooceny NRA może skupić się na podgrupie celów bezpieczeństwa. Na przykład, krajowy organ regulacyjny może być zainteresowany obszarem ciągłości działania lub obszarem szczególnych celów bezpieczeństwa związanych z zarządzaniem zmianą.

Krajowe organy regulacyjne mogą również ograniczyć samoocenę do podzbioru branżowego, np. do dostawców z pewną liczby użytkowników (np. udział w rynku większy niż 10%), określonych usług (np. sieci telefonii komórkowej), lub oferujących niektóre usługi krytyczne (np. komunikacja w portach i na lotniskach).

Podajemy dwa uproszczone przykłady jak krajowy organ regulacyjny może skonfigurować formularz samooceny. W pierwszym przykładzie, krajowy organ regulacyjny ocenia środki bezpieczeństwa wszystkich dostawców w sektorze, ale z naciskiem na podzbiór celów bezpieczeństwa.

Przykład: krajowy organ regulacyjny z kraju D zorganizował samoocenę skupiającą się na kierowaniu i zarządzaniu ryzykiem (Obszar D1 w wytycznych ENISA). Formularze samooceny są wysyłane e-mailem do wszystkich dostawców:

|  |
| --- |
| **Wskaż swój szacunkowy udział w rynku: (wybierz: <1%, >10%, >10%)**  **Wskaż, które usługi oferujesz: (telefonii stacjonarna/komórkowa, Internet stacjonarny/mobilny).**  **Dla każdego celu bezpieczeństwa wskaż poziom zaawansowania i jeśli możesz przedstaw dowody.**  **CB 1: Polityka bezpieczeństwa informacji**  Poziom zaawansowania: (wybierz z 0, 1, 2, 3). Istnieją dowody: (wybrać tak lub nie).  **CB 2: Kierowanie i ramy zarządzania ryzykiem**  Poziom zaawansowania: (wybierz z 0, 1, 2, 3). Istnieją dowody: (wybrać tak lub nie).  **SO3: Role i obowiązki bezpieczeństwa**  Poziom zaawansowania: (wybierz z 0, 1, 2, 3). Istnieją dowody: (wybrać tak lub nie).  **CB4: Zarządzanie sieciami i usługami stron trzecich**  Poziom zaawansowania: (wybierz z 0, 1, 2, 3). Istnieją dowody: (wybrać tak lub nie). |

W drugim przykładzie krajowy organ regulacyjny skupia się na podgrupie środków bezpieczeństwa i podzbiorze dostawców:

Przykład: krajowy organ regulacyjny w kraju E chce się skupić na kwestii wielu dużych awarii sieci komórkowej w ubiegłym roku, które były powodowane przez przerwy w dostawie prądu, przecięcia kabli i klęski żywiołowe. Krajowy organ regulacyjny koncentruje się na środkach bezpieczeństwa, które są najbardziej istotne w tym kontekście. Formularze samooceny są wysyłane tylko do operatorów sieci komórkowych z dużym udziałem w rynku (>10%). Pytania są kombinacją odpowiedzi wielokrotnego wyboru i pytań otwartych umożliwiających opis zastosowanych środków bezpieczeństwa oraz pytań otwartych umożliwiających przedstawienie dowodów, że dostawca może uzasadnić swoje odpowiedzi.

|  |
| --- |
| **Dla każdego celu bezpieczeństwa CB9 (Bezpieczeństwo fizyczne i środowiskowe), CB10 (Bezpieczeństwo dostaw), CB19 (Strategia ciągłości usług i plany awaryjne ), CB20 (Możliwości usuwania skutków awarii), CB22 (Ćwiczenie planów awaryjnych), wskaż poziom zaawansowania na skali od 0 do 3 (0 brak, 1 podstawowy, 2 standard branżowy, 3 zaawansowany):**  Opisz zastosowane środki mające za zadanie osiągnięcie celu: (maks. 200 słów)  Opisz dowody, jakie możesz dostarczyć do krajowego organu regulacyjnego, które mógłby uzasadnić, że środki zostały wdrożone: (0 brak, 1 dokumentacja wewnętrzna, 2 Sprawozdanie z audytu wykonanego przez audytora zewnętrznego) |

***Uwaga dotycząca poufności:*** *Wyniki samooceny lub profile mogą być poufne i ważne jest, aby zapewnić im poufność w odniesieniu do innych dostawców i/lub społeczeństwa. Ważne jest, aby wyjaśnić dokładnie cel oceny (np. tłumacząc, że nie ma ona żadnych skutków prawnych) i dać wyraźne gwarancje dostawcom, zapewniające o poufności wyników.*

**5.3 Stosowanie podejścia etapowego**

W zależności od krajowych okoliczności, krajowe organy regulacyjne mogą chcieć przyjąć etapowe podejście w nadzorowaniu (i egzekwowaniu) zgodności z wymogami bezpieczeństwa Artykułu 13a. Na przykład, gdy niektórzy dostawcy nie mają (jeszcze) wdrożonych odpowiednich środków bezpieczeństwa (lub gdy nie mogą tego dowieść) krajowe organy regulacyjne mogą dać dostawcom nieco czasu na uzyskanie zgodności stopniowo (w etapach). Krajowe organy regulacyjne mogą wykorzystać te wytyczne, aby przyjąć podejście etapowe. Poniżej omówimy kilka możliwych opcji:

* **Objęte usługi lub aktywa:** Można skoncentrować się na podgrupie usług (p.. sieci komórkowych) lub podgrupie aktywów (np. sieci szkieletowe), i zająć się innymi usługami później.

Przykład: NRA w kraju A chce najpierw skupić się na sieciach komórkowych, ponieważ są one (na poziomie krajowym) najbardziej krytyczne. Krajowy urząd regulacyjny zaczyna od samooceny wszystkich dostawców sieci komórkowych. Przedmiotem oceny są "aktywa wspierające sieci telefonii komórkowej". Pozostałe usługi są początkowo poza zakresem, podobnie jak i dostawcy, którzy nie oferują usług telefonii komórkowej.

* + - **Objęcie dostawcy:** Można skupić się najpierw na podgrupie dostawców np..z dużym udziałem w rynku i zająć się innymi dostawcami na późniejszym etapie.

Przykład: NRA w kraju B chce skupić się najpierw na dostawcach z dużym udziałem w rynku, ponieważ w tym przypadku zagrożona jest duża liczba użytkowników. Krajowy organ regulacyjny rozpoczyna zbieranie raportów samooceny od głównych dostawców (>10% udziału w rynku). Po badaniu następuje przez szereg warsztatów, w trakcie których omawiane są główne przyczyny incydentów. W kolejnym roku krajowy organ regulacyjny rozpocznie oddzielny program nadzoru dla mniejszych operatorów (koncentrując się bardziej na wytycznych).

* + - **Obszary bezpieczeństwa:** Można skupić się najpierw na podgrupie celów bezpieczeństwa, np. na ciągłości działania i zająć się innymi celami na późniejszym etapie.

Przykład: Krajowy organ regulacyjny w kraju C chce najpierw skupić się na głównych incydentach, z uwzględnieniem incydentów zgłaszanych przez dostawców. Jako że w ubiegłym roku w kraju A incydenty były spowodowane głównie klęskami żywiołowymi, NRA w swoim nadzorze koncentruje się najpierw na środkach dotyczących celów bezpieczeństwa CB9, CB10, CB19, CB20, CB22. Krajowy organ regulacyjny zajmie się innymi środkami bezpieczeństwa w późniejszym czasie.

* + - **Poziomy zaawansowania i poziomy odniesienia:** Krajowe organy regulacyjne mogą skupić się najpierw na tym, czy wszyscy dostawcy wdrożyli podstawowe środki bezpieczeństwa, np. poziomu 1, jak określono w niniejszych wytycznych, a dopiero później skupią się na upewnieniu się, że dostawcy podjęli bardziej zaawansowane środki bezpieczeństwa. Należy tutaj podkreślić, że takie podejście będzie mieć pewne ograniczenia: zwłaszcza gdy sektor ma zarówno dużych i małych dostawców. Dla dużych dostawców podstawowe środki bezpieczeństwa mogą być niewystarczające, a dla małych dostawców mogą być więcej niż wystarczające. Lepiej byłoby uwzględnić różnice w całym sektorze i zdefiniować różne poziomy odniesienia dla dostawców o różnej wielkości.

Przykład: NRA w kraju D definiuje dwa profile jako poziomy podstawowe.

* + - Pierwszy profil zawiera podstawowe środki bezpieczeństwa tylko dla obszarów O1 Kierowanie i zarządzanie ryzykiem, O2 Bezpieczeństwo zasobów ludzkich, O3 Bezpieczeństwo systemów i obiektów – jest to poziom podstawowy dla małych dostawców (<10% udziału w rynku).
* Drugi profil zawiera branżowe standardowe środki bezpieczeństwa dla wszystkich obszarów (O1, … O7) – jest to poziom podstawowy dla dużych dostawców (>10% udziału w rynku).

Na późniejszym etapie NRA dokona przeglądu profili, a w razie potrzeby podniesie wymagania w pewnych obszarach lub zdefiniuje inne poziomy podstawowe dla innych typów dostawców (np. IXP).

**5.4 Dostawcy usług audytorskich**

W zależności od zastosowanych rozwiązań, krajowe organy regulacyjne mogą zobowiązać dostawców do przejścia audytu. W zależności od zastosowanych rozwiązań i celu, potrzebne mogą być różne rodzaje audytu. W tej sekcji omówimy różne opcje dla dostawców audytu.

Należy pamiętać, że audyt nie zawsze jest łatwy, ponieważ sieci i systemy informatyczne są często skomplikowane. Aby zrozumieć, czy konkretne podzespoły pracują prawidłowo, audytor może potrzebować głębokiej wiedzy i doświadczenia: w sprawach bezpieczeństwa "diabeł tkwi w szczegółach". Wystarczy podać jeden prosty przykład: audytor może odkryć, że zapora "firewall" stosowana jest do ochrony niektórych systemów, ale to szczegółowe reguły działania tej zapory określają jej skuteczność. Jedna reguła zawierająca jeden błąd może sprawić, że cała zapora stanie się bezużyteczna.

***Uwaga na temat kosztów audytu:*** *krajowe organy regulacyjne powinny uwzględniać koszty audytów przeprowadzanych przez strony trzecie, zwłaszcza w przypadku mniejszych dostawców. Samoocena (patrz poprzedni punkt) może być podejściem o lżejszym charakterze.*

***Uwaga na temat skuteczności audytu****: Częste skargi od organizacji podlegających audytom bezpieczeństwa informacji dotyczą tego, że audyt często zmusza je do dużego nakładu „papierkowej” pracy i że jest to nie tylko bezużyteczne, ale również traci się czas i środki potrzebne do bieżącej działalności: czyli zabezpieczania sieci i systemów informatycznych. Krajowe organy regulacyjne powinny wziąć pod uwagę, że niektórzy operatorzy posiadają poświadczoną zgodność lub certyfikaty (dobrowolnie lub w ramach innego ustawodawstwa) i są już poddawani audytom (wewnętrznym lub zewnętrznym). Jeśli potrzebny jest audyt, ważne jest, aby w miarę możliwości wykorzystać istniejące raporty z audytu i dowody zgodności.*

***Uwaga na temat języka i operatorów międzynarodowych:*** *W przypadku żądania dokumentów lub dowodów od dostawców, krajowe organy regulacyjne powinny wziąć pod uwagę, że dostawcy mogą mieć pewną część dokumentacji (instrukcje, zasady, procedury itp.) opracowane w języku angielskim ze względu na efektywność, ponieważ dostawca działa w kilku krajach lub zatrudnia pracowników z innych krajów.*

**5.4.1 Rodzaje ocen**

Audyt zawiera w sobie różne rodzaje ocen, np. przegląd polityki bezpieczeństwa lub wywiad z pracownikiem na stanowisku CISO dotyczący planowania awaryjnego. Audyty zwykle składają się z połączenia różnych rodzajów oceny. Omawiamy różne typy poniżej:

* + - **Przegląd dokumentów:** Przegląd dokumentów jest niezbędny w każdym audycie. Stosowne dokumenty mogą zawierać opisy polityk, ról i obowiązków, opisy procesów i procedur, architektury i projektów systemów, procedury testowe i rzeczywiste wyniki badań. [Rozdział 4](#bookmark7) niniejszych wytycznych zawiera opis dowodów, które mogłyby zostać wzięte pod uwagę przy ocenie wdrażania środków bezpieczeństwa.
    - **Wywiady:** Oprócz przeglądu dokumentów, wiele informacji można zebrać z wywiadów z pracownikami dostawcy. W przypadku małych dostawców może wystarczyć rozmowa z jedną lub dwiema osobami odpowiedzialnymi za kwestie handlowe i techniczne. U dużych dostawców, typowe stanowiska ankietowane to: menedżerowie poziomu C (CIO), starsi oficerowie bezpieczeństwa (CSO lub CISO), taktyczni/operacyjni oficerów bezpieczeństwa, kierownicy NOC, wewnętrzny zespół CERT, menedżerowie produktu i administratorzy systemów odpowiedzialni za procesy lub systemy krytyczne.
    - **Ocena systemu:** Oprócz dokumentów, certyfikatów i wywiadów, ostateczną kontrolą jest sprawdzenie, czy sieci i systemy informacyjne są bezpieczne i czy polityki/procedury są stosowane w praktyce - sprawdzenie to odbywa się przez inspekcję lub przetestowanie samych systemów. W niektórych środowiskach konieczny może być przegląd systemu, np. aby zrozumieć jak doszło do incydentu bezpieczeństwa. Ocena systemu powinna koncentrować się na najważniejszych systemach, ponieważ może być to czasochłonne.

**5.4.2** **Rodzaje audytorów**

Audyt może być przeprowadzany przez różne jednostki.

* + - * **Samoocena:** W samoocenie w rzeczywistości nie ma audytora, ale personel dostawcy ocenia i raportuje kwestie dotyczące zgodności. Chociaż sprawozdania z samooceny mogą być stronnicze, mogą dostarczyć użytecznych informacji dla dostawców i krajowych organów regulacyjnych. Zaletą samooceny jest stosunkowo niski koszt dla dostawców. Wcześniej w tym dokumencie, w [Sekcji 5.2,](#bookmark46) omówiliśmy samoocenę bardziej szczegółowo.
      * **Audytor wewnętrzny:** W dużych organizacjach, dostawca może poprosić audytora wewnętrznego lub dział audytu wewnętrznego aby wykonał audyt niektórych systemów lub części organizacji. W porównaniu do samooceny, audytor wewnętrzny może być mniej tendencyjny. Zaletą jest to, że audytorzy wewnętrzni często znają organizację od podszewki. Ponadto audytorzy wewnętrzni mogą łatwiej wykorzystać głęboką wiedzę na temat sieci i systemów informatycznych operatora.
      * **Audytor zewnętrzny:** Raport z audytu przeprowadzanego przez zewnętrznego audytora jest jeszcze mniej stronniczy. Jedynym problemem może być tutaj fakt, że audytor zewnętrzny może nie znać wszystkich szczegółów dotyczących organizacji i/lub jej sieci i systemów informatycznych. To może sprawić, że cały audyt będzie droższy, ponieważ z jednej strony zewnętrzny audytor będzie musiał poświęcić dużo czasu na badanie warunków i systemów u dostawcy, a sam dostawca także będzie musiał poświęcić dużo czasu, aby dostarczyć niezbędne informacje audytorowi.
      * **Krajowy organ regulacyjny jako audytor:** NRA może przeprowadzić audyt dostawcy, przy wykorzystaniu własnych pracowników z doświadczeniem audytorskim lub poprzez outsourcing audytu z firmy audytorskiej.
      * **Audytor certyfikujący:** Podczas certyfikacji, licencjonowany audytor sprawdza zgodność z określoną normą/standardem. Raport z audytu daje certyfikat zgodności wydany przez jednostkę certyfikującą. Na przykład dość typowym dla dużych dostawców jest uzyskiwanie certyfikatu ISO270001. Certyfikacja jest często odświeżana corocznie, po przeprowadzeniu ponownego audytu. Krajowe urzędy regulacyjne mogą wymagać certyfikatów i zachęcają dostawców do ich przełożenia jako sposobu na wykazanie zgodności.
      * **Audytor specjalista**: W szczególnych przypadkach krajowy organ regulacyjny może wyznaczyć konkretnego audytora w konkretnym celu lub po specyficznym incydencie. Na przykład, NRA może zobowiązać dostawców do skanowania zabezpieczeń systemów przeprowadzanego przez specjalistę ds. skanowania zabezpieczeń.
      * **Zespół/pula audytorów:** NRA może wyznaczyć pulę audytorów zewnętrznych. Kryteria doboru audytorów mogą opierać się na doświadczeniach z przeszłości (udokumentowane audyty lub testy bezpieczeństwa) lub opierać się na kryteriach badania. Na przykład, krajowe organy regulacyjne mogą wydać listę licencjonowanych audytorów[[12]](#footnote-12) i zaoferować im coroczne szkolenia, które koncentruj się na wymaganiach Artykułu 13a dla branży, tworząc w ten sposób pulę/zespół audytorów.

**5.4.3 Czas i cele audytu**

Częstotliwość i cele audytu są zmienne. Rozróżniamy dwa rodzaje audytów.

* + - * **Audyty profilaktyczne:** Audyty profilaktyczne są zwykle wykonywane okresowo - w ustalonych odstępach czasu. W przypadku certyfikacji (patrz wyżej) audyty przeprowadzane są co roku lub co dwa lata. Audyty profilaktyczne często nie mają specyficznego zakresu, jednak dobrą praktyką jest skonfigurowanie okresowych audytów profilaktycznych z planem wieloletnim i skupienie się najpierw na określonych (ważnych) kwestiach, a dopiero później, podczas kolejnych audytów, na innych sprawach. Częstotliwość kontroli musi brać pod uwagę fakt, że operatorzy mogą potrzebować trochę czasu na usunięcie niedociągnięć odkrytych podczas poprzednich audytów.

Przykład: NRA w kraju H wymaga od dostawców przejścia corocznego audytu (profilaktycznego) przeprowadzanego przez audytorów będących stroną trzecią. W celu uproszczenia i zmniejszenia obciążeń dla dostawców, NRA działa zgodnie z trzyletnim planem nadzoru, skupiając się w pierwszej kolejności na pilnych sprawach: W pierwszym roku zakres audytu jest ograniczony do ciągłości biznesowej, katastrof naturalnych i awarii zasilania (środki do osiągnięcia celów CB9 , CB10, CB19, CB20, CB22). W drugim roku audyt koncentruje się na magazynowaniu i przechowywanie danych klienta. W trzecim roku zostaną poddane audytowi wszystkie środki bezpieczeństwa.

* + - * **Audyty po incydencie:** Audyty po incydencie przeprowadzane przez krajowy organ regulacyjny są zwykle wykonywane bez wcześniejszego planowania (ad-hoc), w zależności od rodzaju incydentu i warunków. Audyty po incydencie mają szczególny zakres - mają zwykle na celu ocenę, czy stosowane są środki bezpieczeństwa w celu zapobieżenia ponownym wystąpieniom incydentu. Audyt w tym przypadku ma określony zakres (usługi i aktywa których dotyczył incydent) i sprawdza określone środki bezpieczeństwa (te które zawiodły podczas incydentu; lub środków, które mogą zapobiec jego ponownemu wystąpieniu).

**6 Powiązanie z normami międzynarodowymi**

**6.1 Ważne jest, aby podkreślić, że środki bezpieczeństwa opisane w niniejszym dokumencie zostały opracowane na podstawie istniejących międzynarodowych norm bezpieczeństwa dla sieci i informacji. Niniejsze wytyczne nie mają na celu zastąpienia istniejących norm lub ram prawnych stosowanych przez dostawców. Dostawcy mogą wzorować normy, których używają (wewnętrznie) na środkach bezpieczeństwa z Sekcji 4, a w ten sposób wykazać zgodność z Artykułem 13a. W tej sekcji podajemy dwa przykłady takiego odwzorowania. Odwzorowanie (mapowanie) obszarów bezpieczeństwa**

Poniżej, jako przykład, odwzorowujemy obszary bezpieczeństwa z Sekcji 4 na podstawie kilku międzynarodowych norm, często używanych przez dostawców. Odwzorowujemy następujące normy/standardy:

* + - * ISO 27001:2013, norma zarządzania bezpieczeństwem informacji,
      * ISO 27002:2013, katalog środków kontrolnych bezpieczeństwa informacji,
      * ISO 27005:2011, norma zarządzania ryzykiem bezpieczeństwa informacji, oraz
      * ISO 22301:2012, norma dla zarządzania ciągłością działalności.

|  |  |  |
| --- | --- | --- |
| **Obszary bezpieczeństwa** | **Opisano w** | **Szczegóły** |
| O1: Kierowanie i zarządzanie ryzykiem | ISO 27001,  ISO 27002 i ISO 27005. | ISO 27001 przedstawia standard zarządzania ryzykiem w zakresie bezpieczeństwa informacji.  ISO 27005 podaje normę zarządzania ryzykiem.  ISO 27002 Rozdział 5 dotyczy polityki bezpieczeństwa informacji.  ISO 27002 Rozdział 7 dotyczy ról i obowiązków w zakresie bezpieczeństwa informacji.  ISO 27002 Rozdział 15 dotyczy relacji z dostawcami. |
| O2: Bezpieczeństwo zasobów ludzkich | ISO 27002 | ISO 27002 Rozdział 7 obejmuje sprawdzenie informacji (*background screening*), role i obowiązki w zakresie ochrony informacji, wiedza i szkolenia w zakresie bezpieczeństwa i zmian personalnych. |
| O3: Bezpieczeństwo systemów i urządzeń | ISO 27002 | ISO 27002 Rozdział 11 obejmuje bezpieczeństwo fizyczne i środowiskowe.  ISO 27002 Rozdział 9 obejmuje kontrolę dostępu do systemów informatycznych i urządzeń.  ISO 27002 Rozdział 13 obejmuje bezpieczeństwo sieci. |
| O4: Zarządzanie działaniami | ISO 27002 | ISO 27002 Rozdział 12 obejmuje Procedury operacyjne i Zarządzanie zmianą.  ISO27002 Rozdział 8 obejmuje zarządzanie aktywami. |
| D5: Zarządzanie incydentami | ISO 27002 | ISO 27002 - Rozdział 16 obejmuje zarządzanie incydentami bezpieczeństwa informacji, a także komunikowanie incydentów bezpieczeństwa. |
| O6: Zarządzanie ciągłością działalności | ISO 22301 | ISO 22301 obejmuje zarządzanie ciągłością działania |
| O7: Monitorowanie i testy bezpieczeństwa | ISO 27002 | Monitorowanie jest opisane w normie ISO 27002 - Rozdziały 12 i 15. Testowanie bezpieczeństwa i zgodności opisane jest w ISO 27002 rozdziały 14 i 18. |

Użyliśmy normy ISO w tym przykładzie, ale podobne mapowanie może być przeprowadzone dla innych norm krajowych lub międzynarodowych. Na przykład mapowanie będzie wyglądać podobnie, jeśli zamiast ISO27001 i ISO27005, odwzorujemy normy Międzynarodowego Związku Telekomunikacyjnego (ITU) X.1051 (zarządzanie bezpieczeństwem informacji) i X.1055 (zarządzanie ryzykiem).

**6.2 Mapowianie celów bezpieczeństwa**

Można też dokonać bardziej szczegółowego mapowania. Poniżej, jako przykład, podajemy odwzorowanie celów bezpieczeństwa w Sekcji 4 dla poszczególnych celów kontroli z załącznika do normy ISO 27001:2013.

|  |  |
| --- | --- |
| **Cele bezpieczeństwa** | **Cele kontroli w ISO 27001:2013** |
| CB 1 Polityka bezpieczeństwa informacji | A.5.1 Zarządzania kierunkiem bezpieczeństwa informacji |
| CB 2 Kierowanie i zarządzanie ryzykiem | Patrz ISO 27001 dla kierowania.  Patrz ISO 27005 dla zarządzania ryzykiem. |
| CB 3 Role i obowiązki związane z bezpieczeństwem | A.6.1 Organizacja wewnętrzna  A.7.1 Przed zatrudnieniem  A.7.2 W trakcie zatrudnienia |
| CB 4 Bezpieczeństwo aktywów osób trzecich | A.15.1: Bezpieczeństwo informacji w stosunkach z dostawcami |
| CB 5 Kontrole przygotowania | A.7.1 Przed zatrudnieniem |
| CB 6 Wiedza i szkolenia z obszaru bezpieczeństwa | A.7.1 Przed zatrudnieniem  A.7.2 W trakcie zatrudnienia  A.7.3 Zakończenie i zmiana zatrudnienia |
| CB 7 Zmiany personalne |  |
| CB 8 Postępowanie z naruszeniami |  |
| CB 9 Bezpieczeństwo fizyczne i środowiskowe | A.11.1 Obszary bezpieczne  A.11.2 Wyposażenie |
| CB 10 Bezpieczeństwo dostaw | A.11.2 Wyposażenie |

|  |  |
| --- | --- |
| CB 11: Kontrola dostępu do sieci i systemów informatycznych | A.9.1 Wymagania biznesowe dotyczące kontroli dostępu  A.9.2 Zarządzanie dostępem użytkowników  A.9.3 Obowiązki użytkownika  A.9.4 Kontrola dostępu do systemu i aplikacji  A.13.1 Zarządzanie bezpieczeństwem sieci |
| CB 12 Integralność sieci i systemów informatycznych | A.12.2 Ochrona przed złośliwym oprogramowaniem  A.12.5 Kontrola oprogramowania operacyjnego  A.12.6 Zarządzanie techniczną podatnością na ataki  A.13.1 Zarządzanie bezpieczeństwem sieci |
| CB 13 Procedury operacyjne | A.12.1 Procedury operacyjne i obowiązki. |
| CB 14 Zarządzanie zmianą |  |
| CB 15 Zarządzanie aktywami | A.8.1 Odpowiedzialność za aktywa |
| CB 16 Procedury zarządzania incydentami | A.16.1 Zarządzanie incydentami i ulepszeniami z zakresu bezpieczeństwa informacji |
| CB 17 Potencjał wykrywania incydentów |  |
| CB 18 Zgłaszanie i komunikowanie incydentów |  |
| CB 19 Strategia ciągłości usług i plany awaryjne | ISO 22301 obejmuje zarządzanie ciągłością działania |
| CB 20 Możliwości usuwania skutków awarii |  |
| CB 21 Zasady monitorowania i rejestrowania | A.12.4 Rejestrowanie i monitorowanie |
| CB 22 Ćwiczenie planów awaryjnych | ISO 22301 obejmuje zarządzanie ciągłością działania |
| CB 23 Testowanie sieci i systemów informatycznych | A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia  A.18.2 Analizy bezpieczeństwa informacji |
| CB 24 Oceny bezpieczeństwa |
| CB 25 Monitorowanie zgodności | A.18.1 Zgodność z wymogami prawnymi i umownymi |

**Bibliografia**

W tej Sekcji przedstawiamy bibliografię - odnośniki do powiązanych dokumentów ENISA i odpowiedniego prawodawstwa UE. Podajemy również niepełny wykaz wspólnych norm bezpieczeństwa zastosowanych przez nas w charakterze informacji podstawowych we wcześniejszych wersjach tego dokumentu.

**Podobne dokumenty ENISA**

* + - * ENISA opublikowała dwa raporty roczne dotyczące głównych incydentów w sektorze łączności elektronicznej w UE. Dwa raporty dotyczące incydentów w roku 2011 oraz w roku 2012 są dostępne pod adresem: [https://www.enisa.europa.eu/activities/Resilience-and- CIIP/Incidents-reporting/annual-reports](https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports)
      * Wytyczne ENISA dotyczące wdrażania Artykułu 13a są dostępne pod adresem: <https://resilience.enisa.europa.eu/article-13>
      * Biała księga ENISA dotycząca raportowania incydentów cyfrowych w UE, przedstawiająca Artykuł 13a i jego porównanie z innymi artykułami bezpieczeństwa, które wymagają raportowania incydentów i środków bezpieczeństwa:

<http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu>

* + - * Dla zainteresowanego czytelnika, dokument ENISA z roku 2009 dotyczący zgłaszania incydentów przedstawia przegląd sytuacji w UE zaistniałej 3 lata temu: [http://www.enisa.europa.eu/activities/Resilience-and- CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on- incident-reporting-1](http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1)

**Odpowiednie prawodawstwo UE**

* + - * Artykuł 13a Dyrektywy ramowej UE w zakresie łączności elektronicznej: <http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf>
      * Ramy regulacyjne łączności elektronicznej (wprowadzające reformę telekomunikacji): [http://ec.europa.eu/information\_society/policy/ecomm/doc/library/regframeforec\_dec200 9.pdf](http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf)
      * Przegląd głównych elementów reformy 2009: <http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm>
      * W 2013 r. Komisja Europejska zaproponowała strategię bezpieczeństwa cyfrowego i dyrektywę dotyczącą bezpieczeństwa cyfrowego: [http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open- internet-and-online-freedom-and-opportunity-cyber-security](http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security)

**Normy i standardy bezpieczeństwa oraz najlepsze praktyki w tym zakresie**

* + - * ISO 27001 „Systemy zarządzania bezpieczeństwem informacji"
      * ISO 27002 „Kodeks postępowania w zakresie zarządzania bezpieczeństwem informacji"
      * ISO 24762 „Wytyczne dla usług odtwarzania techniki teleinformatycznej po awarii"
      * ISO 27005 „Zarządzanie ryzykiem w bezpieczeństwie informacji"
      * ISO 27011 „Wytycznie dotyczące zarządzania bezpieczeństwem informacji w organizacjach telekomunikacyjnych"
      * ISO 22310 „Systemy zarządzania ciągłością działania"
      * ITU-T X.1056 (01/2009) “Security incident management guidelines for telecommunications organizations"
      * ITU-T Zalecenie X.1051 (02/2008) "Information security management guidelines for telecommunications organizations based on ISO/IEC 27002"
      * ITU-T X.800 (1991) "Security architecture for Open Systems Interconnection for CCITT applications"
      * ITU-T X.805 (10/2003) “Security architecture for systems providing end-to-end communications”
      * ISF Standard 2007 "The Standard of Good Practice for Information Security"
      * CobiT "Control Objectives for Information and related Technology"
      * ITIL - Wsparcie serwisowe
      * ITIL - Zarządzanie bezpieczeństwem
      * PCI DSS 1.2 Standard bezpieczeństwa danych

**Krajowe normy i dobre praktyki**

* + - * IT-Grundschutz-Kataloge - Niemcy
      * KATAKRI, bezpieczeństwa national Security auditing criteria - Finlandia
      * NIST 800 34 "Contingency Planning Guide for Federal Information Systems"
      * NIST 800 61 "Computer Security Incident Handling Guide"
      * FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems"
      * NICC ND 1643 "Minimum security standards for interconnecting communication providers"



**ENISA**

Europejska Agencja Bezpieczeństwa Sieci i Informacji

Science and Technology Park of Crete (ITE)

Vassilika Vouton, 700 13, Heraklion, Grecja

**Biuro w Atenach**

1 Vass. Sofias & Meg. Alexandrou

Marousi 151 24, Ateny, Grecja



1. A nie integralność danych. [↑](#footnote-ref-1)
2. Ward, K, 1995, ‘The Impact of Network Interconnection on Network Integrity’. British Telecommunications Engineering, 13:296–303. [↑](#footnote-ref-2)
3. Należy pamiętać, że tylko podzbiór tych incydentów, musi być raportowany do ENISA i KE, a mianowicie te incydenty, które rzeczywiście miały znaczący wpływ na świadczenie usług. [↑](#footnote-ref-3)
4. Na przykład, w przypadku operatorów ciemnych światłowodów niektóre środki bezpieczeństwa nie mogą być stosowane, ponieważ dostawcy ci nie mają bezpośrednio do czynienia z klientami i nie mają dużo pracowników. [↑](#footnote-ref-4)
5. Zatem w tym dokumencie określenie "strony trzecie" nie odnosi się do klientów, społeczeństwa, władz rządowych lub organów regulacyjnych. [↑](#footnote-ref-5)
6. W literaturze o zarządzaniu bezpieczeństwem informacji są one czasami określane jako cele kontrolne. [↑](#footnote-ref-6)
7. Definicja terminu ‘incydent’ używanego w niniejszym dokumencie znajduje się w Sekcji 2. [↑](#footnote-ref-7)
8. Na przykład Artykuł 13a, który został transponowany do prawa krajowego we wszystkich państwach członkowskich UE, wymaga od dostawców komunikacji elektronicznej raportowania "znaczących" incydentów do krajowych urzędów regulacyjnych. Progi raportowania są określone na poziomie krajowym. [↑](#footnote-ref-8)
9. Nadzór środków bezpieczeństwa nie jest łatwym zadaniem, ponieważ sieci i technologie informatyczne zmieniają się szybko, ponieważ szybko zmieniają się możliwości agresorów, oraz skuteczność środków bezpieczeństwa często zależy od technicznych szczegółów wdrożenia. Ponadto, nadzór ze strony krajowych organów regulacyjnych jest dodatkowo komplikowany przez fakt, że w większości krajów UE sektor łączności elektronicznej składa się z wielu różnych typów dostawców, w tym bardzo małych dostawców, operatorów zasiedziałych, operatorów ciemnych światłowodów, itp. [↑](#footnote-ref-9)
10. Zapytaliśmy krajowe organy regulacyjne w całej UE (za pomocą kwestionariuszy), jaki działania zostały wdrożone, a jakie planują wdrożyć. [↑](#footnote-ref-10)
11. Zapytaliśmy krajowe organy regulacyjne w całej UE (poprzez kwestionariusz) o rodzaje dostawców w ich branżach, patrząc pod kątem ich udziału w rynku. [↑](#footnote-ref-11)
12. W większości krajów istnieją na przykład organizacje, które licencjonują audytorów do przeprowadzenia audytów informatycznych. [↑](#footnote-ref-12)