IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

PARP Grupa PFR

Ministerstwo Rozwoju i Technologii

Cyberbezpieczeństwo przemysłowe

NIS 2, projekt nowelizacji ustawy o KSC

Michał Łoniewski, 21.11.2024 r.

#IdeaRozwojuBiznesu

Dyrektywa NIS 2

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Dyrektywa NIS 2
2022/2555

Dyrektywa NIS 2

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii

(dyr. weszła w życie 16.01.2023 r.)

Cel nadrzędny

Osiągnięcie wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii, w celu poprawy funkcjonowania rynku wewnętrznego

NIS 2 przyjęcie do 17.10.2024 r.

Dyrektywa NIS 2
Nowelizacja ustawy o KSC - projekt

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

CYBER SECURITY

Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa
Projekt z dnia 3.10.2024 r.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa - nowelizacja

Art. 1.1. Ustawa określa:

1) **organizację krajowego systemu cyberbezpieczeństwa** oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;

2) **sposób sprawowania nadzoru i kontroli** w zakresie stosowania przepisów ustawy;

3) zakres **Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej;**

4) **zakres Krajowego planu reagowania na incydenty i sytuacje kryzysowe** w cyberbezpieczeństwie na dużą skalę

Nowelizacja ustawy o KSC - projekt

Art. 4. Krajowy system cyberbezpieczeństwa obejmuje:

1) podmioty kluczowe;
2) podmioty ważne;
3) CSIRT MON;
4) CSIRT NASK;
5) CSIRT GOV;
6) CSIRT sektorowe;
7)-16) uchylone
17) organy właściwe do spraw cyberbezpieczeństwa;
17a) Połączone Centrum Operacyjne Cyberbezpieczeństwa, zwane dalej „PCOC”
18) Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa (…);
19) Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa (…);
20) Kolegium do Spraw Cyberbezpieczeństwa (…).

NIS 2/ Nowelizacja ustawy o KSC – projekt
Sektory Kluczowe

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Rodzaje **Sektorów Kluczowych** precyzuje Załącznik I dyrektywy NIS 2
oraz Załącznik nr 1 do projektu nowelizacji ustawy o KSC, podając sektory:

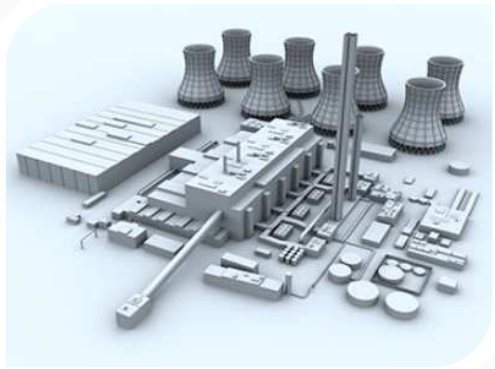
- Energetyka (podsektory: Energia elektryczna, System ciepłowniczy lub chłodniczy, Ropa naftowa, Gaz, Wodór) /

Energia (Wydobywanie kopalin, Energia elektryczna, Ciepło, Ropa i paliwa, Gaz, Energetyka Jądrowa, Dostawy i usługi dla sektora energii, Wodór)

- Transport (Transport lotniczy, kolejowy, wodny, drogowy)
- Bankowość
- Infrastruktura rynków finansowych

→ Bankowość i infrastruktura rynków finansowych

- Służba zdrowia → Ochrona zdrowia
- Woda pitna → Zaopatrzenie w wodę pitną i jej dystrybucja
- Ścieki → Zbiorowe odprowadzanie ścieków
- Infrastruktura cyfrowa
- Zarządzanie usługami ICT
- Podmioty administracji publicznej → Podmioty publiczne
- Przestrzeń kosmiczna



Podmioty Kluczowe – pr. ustawy
Podmioty Kluczowe – dyrektywa

NIS 2/ Nowelizacja ustawy o KSC – projekt
Sektory Ważne

Rodzaje **Sektorów Ważnych** precyzuje Załącznik II dyrektywy NIS 2 oraz Załącznik nr 2 do projektu nowelizacji ustawy o KSC, podając sektory:

- Usługi pocztowe i kurierskie → Usługi pocztowe
- Gospodarowanie odpadami
- Produkcja, wytwarzanie i dystrybucja chemikaliów
- Produkcja, przetwarzanie i dystrybucja żywności
- Produkcja (wyroby medyczne i wyroby medyczne do diagnostyki in vitro; komputery, wyroby elektroniczne i optyczne; urządzenia elektryczne; maszyny i urządzenia; pojazdy samochodowe, przyczepy i naczepy; pozostały sprzęt transportowy)
- Dostawcy usług cyfrowych
- Badania naukowe

Podmioty Ważne – pr. ustawy
Podmioty Ważne – dyrektywa

Poza dostawcami usług cyfrowych, żaden z podmiotów nie był, jak dotąd, objęty dyrektywą NIS

Nowelizacja ustawy o KSC – projekt
Podmioty Kluczowe i Ważne

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

➢ Art. 7 pr. ustawy o KSC – wykaz PK i PW

Art. 7b. 1. Zawiadomienie o wpisie do wykazu, z urzędu, minister właściwy do spraw informatyzacji doręcza podmiotom kluczowym lub podmiotom ważnym

PK

Art. 7c. 1. Podmiot kluczowy i podmiot ważny składają wniosek o wpis w wykazie, w terminie 3 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

PW

Nowelizacja ustawy o KSC – projekt
Podmioty Kluczowe i Ważne

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

➢ Uzasadnienie do pr. Ustawy o KSC - obowiązki PK i PW (różnice)

- Podstawowa różnica między podmiotem kluczowym a podmiotem ważnym wyraża się w kwestiach nadzorczych
- Wobec podmiotu kluczowego można prowadzić czynności nadzorcze uprzednie *ex ante* (przed faktem) i następcze *ex post* (po fakcie)
- Wobec podmiotu ważnego czynności nadzorcze można prowadzić tylko *ex post* (po fakcie)
- Pozostałe obowiązki podmiotów kluczowych i podmiotów ważnych są identyczne z wyjątkiem kwestii obowiązkowych audytów

PK

PW

System informacyjny

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

System informacyjny – system teleinformatyczny (…) wraz z przetwarzanymi w nim danymi w postaci elektronicznej

System teleinformatyczny – system informatyczny połączony z innymi systemami za pomocą sieci telekomunikacyjnych

System informatyczny – część systemu informacyjnego, w której do przetwarzania informacji wykorzystywane są środki techniki komputerowej

Nowelizacja ustawy o KSC – projekt

Art. 2 pr. ustawy o KSC - definicje

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

Przemysłowe systemy sterowania (ICS)

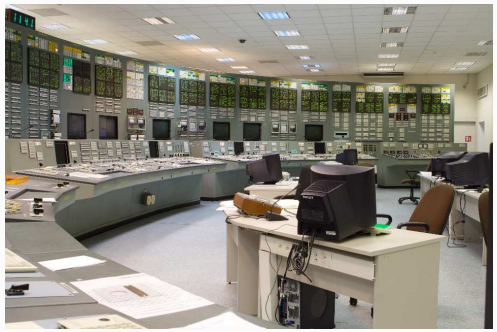
Industrial Control Systems (ICS) to:
IACS (Industrial Automation and Control Systems) Przemysłowe systemy automatyki i sterowania Skrót zdefiniowany w normie IEC 62443
SCADA (Supervisory Control And Data Acquisition) Systemy sterowania i akwizycji danych
DCS (Distributed Control Systems) Rozproszone systemy sterowania
BPCS (Basic Process Control System) Podstawowy system sterowania procesem Skrót zdefiniowany w normie PN-EN 61511
SIS (Safety Instrumented System) Przyrządowy system bezpieczeństwa Skrót zdefiniowany w normie PN-EN 61511

Cyberbezpieczeństwo i bezpieczeństwo funkcjonalne

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

- W myśl zapisów ustawy o KSC **Podmioty kluczowe i ważne są odpowiedzialne za zapewnienie bezpieczeństwa świadczonych usług oraz nieprzerwane ich świadczenie.**
- W przypadku gałęzi przemysłu wykorzystującego systemy SCADA/DCS **(sektor energia/transport/woda pitna)** zapewnienie bezpieczeństwa usługi kluczowej, a więc najczęściej procesu oraz jego nieprzerwanej ciągłości można osiągnąć tylko poprzez działania podnoszące poziom:
  - security (ochrona, cyberbezpieczeństwo) oraz
  - safety (bezpieczeństwo funkcjonalne, niezawodność).

No safety without security



Ciągłość działania OT

Dostępność, poufność, integralność, autentyczność ICS (SCADA, DCS)

#IdeaRozwojuBiznesu

Cyberbezpieczeństwo i bezpieczeństwo funkcjonalne

Utrata ciągłości działania krytycznych systemów ICS może odbyć się na skutek:

- Awarii sprzętu i/lub oprogramowania, błędu ludzkiego (zdarzenie losowe) – **bezpieczeństwo funkcjonalne**

Poziomy nienaruszalności bezpieczeństwa SIL (Safety Integrity Levels)
wg PN-EN 61508, PN-EN 61511, PN-EN IEC 62061 dla automatyki (systemów sterowania) operacyjnej i zabezpieczającej
(podejście ilościowe)

- Awarii spowodowanej złą wolą i/lub nieuprawnionym działaniem zarówno zamierzonym jak i niezamierzonym – **cyberbezpieczeństwo**

Poziomy bezpieczeństwa SL (Security Levels) – w tym SL-A, SL-C, SL-T
Poziomy dojrzałości organizacji ML (Maturity Levels)
wg ISA/IEC 62443 (ANSI/ISA 99)
(podejście jakościowe)

Nowelizacja ustawy o KSC – projekt
Obowiązki Podmiotów Kluczowych i Ważnych

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Art. 8.1 pr. ustawy o KSC – obowiązki PK i PW

Art. 8. 1. **Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji (SZBI) w systemie informacyjnym** wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, **zapewniający:**

1) **prowadzenie systematycznego szacowania ryzyka** wystąpienia incydentu oraz zarządzanie tym ryzykiem;

2) **wdrożenie** odpowiednich i proporcjonalnych do oszacowanego ryzyka **środków technicznych i organizacyjnych**, (…);

3) **zbieranie informacji o cyberzagrożeniach i podatnościach** na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;

4) **zarządzanie incydentami**;

5) **stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego** wykorzystywanego do świadczenia usługi (…);

Bezpieczeństwo systemów informacyjnych

- Budowanie odporności systemów informacyjnych na incydenty z zakresu bezpieczeństwa informacyjnego jest procesem ciągłym i powiązanym z ryzykiem

Ryzyko wystąpienia potencjalnego zagrożenia (w tym incydentu bezpieczeństwa informacyjnego) i jego konsekwencji

- Bezpieczeństwo systemów informacyjnych i ich odporność na incydenty są wartościami niemierzalnymi

Nie można stwierdzić, czy systemy informacyjne mają w danym momencie odpowiedni (wystarczający) poziom bezpieczeństwa i odporności na incydenty

Zarządzanie ryzykiem

- Możemy natomiast zidentyfikować:
  - kluczowe procesy przedsiębiorstwa,
  - potencjalne zagrożenia dla tych procesów,
  - podatności systemów informacyjnych
- Możemy oszacować i ocenić ryzyko (stosując odpowiednie metody ilościowe lub jakościowe analizy ryzyka)
- Możemy opracować **zasady postępowania z ryzykiem**
- Możemy określić kryteria akceptacji ryzyka (resztkowego)

Proces zarządzania ryzykiem

Skuteczna realizacja procesu zarz. ryzykiem

Zapewnienie odporności systemów informacyjnych na incydenty na poziomie wyznaczonym ryzykiem akceptowalnym

Zasady postępowania z ryzykiem

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Reakcja na ryzyko - redukcja ryzyka*

- unikanie ryzyka
- transfer ryzyka
  - outsourcing,
  - ubezpieczenie ryzyka,
  - uczestniczenie partnera zewnętrznego w ryzyku
- **kontrolowanie ryzyka**
- retencja/zatrzymanie ryzyka
  - przygotowanie planów odtwarzania;
  - przyjęcie do wiadomości wielkości ryzyka:
    ryzyko warunkowo tolerowane, tolerowane i akceptowalne

Kontrolowanie ryzyka

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Umiejętne kontrolowanie ryzyka* → Bezpieczne funkcjonowanie przedsiębiorstwa

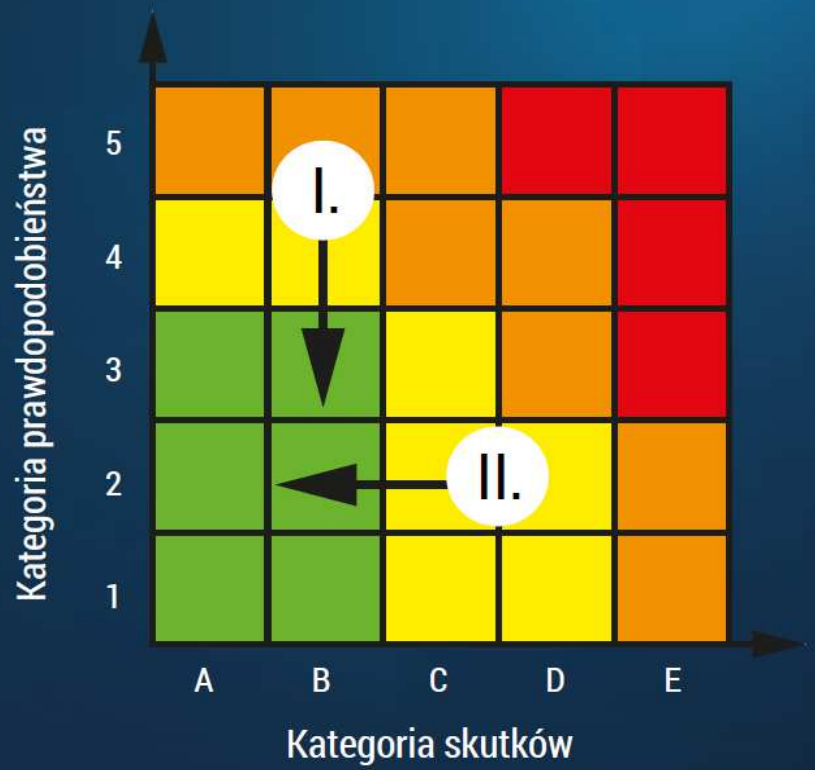
Prewencja poprzez stosowanie odpowiednich środków/technik ochronnych (zabezpieczeń)

Zapewnienie planów ciągłości działania (np. zgodnie ze standardem PN-EN ISO 22301)

PN-EN ISO 22301:2020-04 Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania

*Kontrolowanie ryzyka na podstawie: Liderman K.: *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017

Matryca ryzyka



I. Zmniejszenie ryzyka (prawdopodobieństwa materializacji zagrożenia) poprzez zastosowanie środków organizacyjnych, np. odpowiednią politykę bezpieczeństwa (procedury) czy też strategię obrony w głąb (Defence in Depth), poziomy SL (IEC 62443)

II. Zmniejszenie ryzyka (konsekwencji materializacji zagrożenia) poprzez zastosowanie środków technicznych np. systemów typu IDS, IPS, SIEM, przemysłowego firewallu

Objaśnienia:
Pole zielone – ryzyko akceptowalne (A),
pole żółte – ryzyko tolerowane (TA),
pole pomarańczowe – ryzyko tolerowane nieakceptowalne / warunkowo tolerowane (TNA),
pole czerwone – ryzyko nieakceptowalne (NA).

Środki ochronne (zabezpieczenia organizacyjne)

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Zabezpieczenia czyli środki ochronne zmniejszające ryzyko:

➢ **zabezpieczenia organizacyjne** (wspierające skuteczność zabezpieczeń fizycznych i technicznych)

- Polityka bezpieczeństwa (informacyjnego, w tym systemów informacyjnych)
- Zintegrowany system zarządzania
  (bezpieczeństwem informacji, ciągłością działania, w tym: ryzykiem, incydentami, podatnościami, aktualizacjami, kopiami bezpieczeństwa, uprawnieniami dostępu, zdalnym dostępem, …)
- Cykliczne audyty bezpieczeństwa
- CSIRT, SOC (wewnętrzny i/lub zewnętrzny)
- Edukacja i budowanie świadomości pracowników
- Weryfikacja dostawców

Środki ochronne (zabezpieczenia fizyczne)

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Zabezpieczenia czyli środki ochronne zmniejszające ryzyko:

➢**zabezpieczenia fizyczne** (obiektów, łączy i urządzeń)

- Ochrona osobowa – straż, firma ochroniarska
- Służby wewnętrzne
- Ogrodzenia, przegrody budowlane
- Bunkry
- Drzwi, zamki, kraty
- Sejfy, szafy pancerne

Środki ochronne (zabezpieczenia techniczne)

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Zabezpieczenia czyli środki ochronne zmniejszające ryzyko:

➢ **zabezpieczenia techniczne**

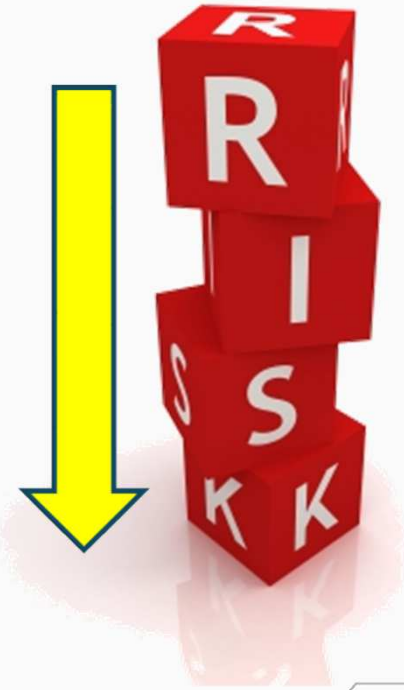
- Obiektów, łączy i urządzeń
  - ✓Systemy ppoż/pgaz
  - ✓Systemy sygnalizacji napadu i włamania
  - ✓Systemy kontroli dostępu
  - ✓Systemy rejestracji czasu pracy
  - ✓Systemy nadzoru wizyjnego

Środki ochronne (zabezpieczenia techniczne)

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

➢zabezpieczenia techniczne c.d.

- Sprzętowo-programowe (informacji przetwarzanej, przechowywanej i przesyłanej w systemach teleinformatycznych) - produkty realizujące funkcje ochronne
  - ✓Segmentacja sieci (model Purdue, DMZ, VLAN)
  - ✓Monitorowanie sieci (SIEM, IDS/IPS, SOAR)
  - ✓Komunikacja jednokierunkowa (data diodes)
  - ✓Firewall
  - ✓Oprogramowanie antywirusowe
  - ✓Szyfrowanie transmisji danych oraz plików
  - ✓Bezpieczne metody uwierzytelniania
  - ✓Regularne kopie bezpieczeństwa
  - ✓Terminowe aktualizacje
  - ✓Ograniczone wykorzystanie pamięci przenośnych



Nowelizacja ustawy o KSC – projekt
Obowiązki Podmiotów Kluczowych i Ważnych

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Art. 9.1, 10.1 pr. ustawy o KSC – obowiązki PK i PW

Art. 9. 1. Podmiot kluczowy i podmiot ważny:

1) wyznacza co najmniej dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;

2) zapewnia użytkownikowi usługi dostęp do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej;

Art. 10. 1. Podmiot kluczowy i podmiot ważny opracowuje, stosuje i aktualizuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi.

Nowelizacja ustawy o KSC – projekt
Obowiązki Podmiotów Kluczowych i Ważnych

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Art. 10.2, 10.3, 10.4 pr. ustawy o KSC – obowiązki PK i PW (dokumentacja)

➢ **Dokumentacja normatywna**

1) Dokumentacja SZBI
2) Dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa, (…)
3) Dokumentacja SZCD
4) Dokumentacja techniczna systemu informacyjnego wykorzystywanego w procesie świadczenia usługi
5) Dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze/podsektorze

➢ **Dokumentacja operacyjna**

Dokumentację operacyjną stanowią zapisy poświadczające wykonywanie czynności wymaganych przez postanowienia zawarte w dokumentacji normatywnej, w tym automatycznie generowane zapisy w dziennikach systemów informacyjnych.

Nowelizacja ustawy o KSC – projekt
Obowiązki Podmiotów Kluczowych i Ważnych

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Art. 11.1 pr. ustawy o KSC – obowiązki PK i PW (obsługa incydentu)

Art. 11. 1. Podmiot kluczowy i podmiot ważny:

1) zapewnia obsługę incydentu;

2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań;

3) klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny;

4) zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego

4a) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego

Nowelizacja ustawy o KSC – projekt
Obowiązki Podmiotów Kluczowych i Ważnych

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Art. 11.1 pr. ustawy o KSC – obowiązki PK i PW

Zapewnienie obsługi incydentu → zarządzanie incydentami

ISO/IEC 27035

- Z uwagi na pozostające zawsze (większe, bądź mniejsze) **ryzyko resztkowe wystąpienia incydentu** z zakresu bezpieczeństwa informacyjnego, **każde przedsiębiorstwo powinno być przygotowane na jego wystąpienie**

ITIL 4
Service Operation

- Kluczowym elementem polityki bezpieczeństwa jest zatem, obok zarządzania ryzykiem w przedsiębiorstwie, **zarządzanie incydentami, których całkowita eliminacja występowania jest niemożliwa**

Nowelizacja ustawy o KSC – projekt
Obowiązki Podmiotów Kluczowych i Ważnych

Podatności to wady lub luki w:

- strukturze fizycznej organizacji,
- sprzęcie i oprogramowaniu,
- procedurach,
- zarządzaniu i administrowaniu,
- organizacji pracy,
- obsadzie stanowisk pracy personelem,

które mogą być wykorzystane przez zagrożenia do spowodowania szkód w systemie informacyjnym organizacji lub w jej działalności*.

*Definicja na podstawie: Liderman K.: *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017

Nowelizacja ustawy o KSC – projekt
Obowiązki Podmiotów Kluczowych i Ważnych

Art. 11.1 pr. ustawy o KSC – obowiązki PK i PW (podatności)

(oraz art. 32.2 i 42.1 pkt 7)

Art. 11.1 6) (PK i PW) usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa;

Art. 32.2. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego

Nowelizacja ustawy o KSC – projekt
Obowiązki Podmiotów Kluczowych i Ważnych

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Art. 15 pr. ustawy o KSC – obowiązki PK i PW (audyt)

Art. 15.1. Podmiot kluczowy przeprowadza, na własny koszt, **co najmniej raz na 3 lata**, **audyt bezpieczeństwa** systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, (…)

Art. 15.1b. Organ właściwy do spraw cyberbezpieczeństwa w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy przez podmiot kluczowy lub podmiot ważny, może nakazać temu podmiotowi, w drodze decyzji, przeprowadzenie zewnętrznego audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi

Nowelizacja ustawy o KSC – projekt
Obowiązki Podmiotów Kluczowych i Ważnych

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Art. 14, 16 pr. ustawy o KSC – obowiązki PK i PW (realizacja i terminy)

Art. 14. Podmiot kluczowy lub podmiot ważny w celu realizacji zadań, o których mowa w art. 8 oraz w art. 9-13, **powołuje wewnętrzne struktury** odpowiedzialne za cyberbezpieczeństwo lub **zawiera umowę z dostawcą usług** zarządzanych w zakresie cyberbezpieczeństwa

Art. 16. Podmiot:

1) kluczowy i podmiot ważny realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 6 miesięcy,
2) kluczowy zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 24 miesięcy

– od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny

Poradnik dobrych praktyk cyberbezpieczeństwa

Do pobrania ze strony:
udt.gov.pl/cyberbezpieczenstwo

Poradnik dobrych praktyk cyberbezpieczeństwa

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

SPIS TREŚCI

#IdeaRozwojuBiznesu

Framework UDTcyber – audyt cyberbezpieczeństwa

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

- COBIT 5
- ISO/IEC 27001
  ISO 22301
- CPA
  Cyber Program Assessment
- NIST
  Cybersecurity Framework
- IEC 62443
- USTAWA o KSC

Do pobrania ze strony:
udt.gov.pl/cyberbezpieczenstwo

#IdeaRozwojuBiznesu

Cyberbezpieczeństwo - zakres usług UDT

AUDYT CYBERBEZPIECZEŃSTWA

CERTYFIKACJA

PN-EN ISO/IEC 27001
PN-EN ISO 22301
PN-EN 61508, PN-EN 61511 (FSM)

ANALIZA RYZYKA

HAZOP
C-HAZOP

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

PARP Grupa PFR

Ministerstwo Rozwoju i Technologii

Dziękuję za uwagę!

michal.loniewski@udt.gov.pl

#IdeaRozwojuBiznesu