Spotkanie grupy roboczej do spraw LTE

Andrzej Szyszko

Departament Bezpieczeństwa i Zarządzania Kryzysowego, Ministerstwo Energii

Poziomy przeciwdziałania

- Poziom polityczny
- Poziom prawny
- Poziom organizacyjny
- Poziom technologiczny

Poziom polityczny

- dyrektywa Parlamentu i Rady UE *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*

- uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. *w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022*

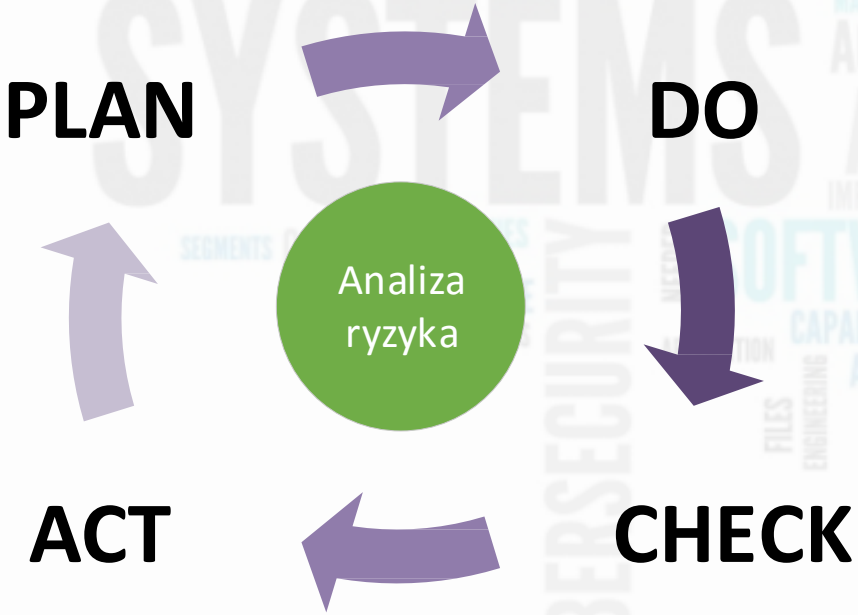
Poziom organizacyjny

System Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji

PROCESY

TECHNOLOGIA



Polityki	Organizacja	Kryptografia
Zarządzanie aktywami	Kontrola dostępu	Bezpieczeństwo zasobów ludzkich
Bezpieczeństwo fizyczne	Bezpieczeństwo operacji	Bezpieczeństwo komunikacji
Ciągłość działania	Zarządzanie dostawcami	Zarządzanie incydentami
	Zgodność	

Poziom technologiczny

- Budowa systemów teleinformatycznych zgodnie z zasadą „*secure by design*”
- Szacowanie ryzyka w czasie rzeczywistym
- Utrzymywanie systemu w aktualności
- Monitorowanie systemu w czasie rzeczywistym

Ustawa o krajowym systemie cyberbezpieczeństwa

Ustawa o ksc

- Implementacja dyrektywy 2016/1148 (Dyrektywa NIS)
- Wejście w życie – 28 sierpnia 2018 r.
- Pierwsza kompleksowa regulacja dotycząca cyberbezpieczeństwa w Polsce, dotycząca obsługi incydentów zarówno w sektorze publicznym jak i prywatnym

ISSN 1977-0766

Dziennik Urzędowy **L 194**

Unii Europejskiej

Wydanie polskie — Legislacja — Tom 59, 19 lipca 2016

Spis treści — *I Akty ustawodawcze* — Strona

DYREKTYWY

* **Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii** 1

PL

Akty, których tytuły wydrukowano zwykłą czcionką, odnoszą się do bieżącego zarządzania sprawami rolnictwa i generalnie zachowują ważność przez określony czas.

Tytuły wszystkich innych aktów poprzedza gwiazdka, a drukuje się je czcionką pogrubioną.

Cel ustawy:

- implementacja **dyrektywy NIS**
- utworzenie efektywnego **systemu bezpieczeństwa teleinformatycznego funkcjonowania państwa.**

Podmioty krajowego systemu cyberbezpieczeństwa

1) **Organy właściwe do spraw cyberbezpieczeństwa**;
2) **CSIRT poziomu krajowego**;
3) **Operatorzy usług kluczowych i dostawcy usług cyfrowych**;
4) **Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa**
5) Podmioty świadczące usługi z zakresu cyberbezpieczeństwa (CSIRT komercyjne)
6) Rządowe Centrum Bezpieczeństwa (w zakresie zarządzania kryzysowego i ochrony infrastruktury krytycznej)
7) Przedsiębiorcy telekomunikacyjni
8) Administracja publiczna

Pojęcia ustawowe

Usługa kluczowa - usługa mająca kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej

Operator usługi kluczowej – podmiot z sektora energii, transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną, infrastruktury cyfrowej

→ spełniający kryteria określone w ustawie

CSIRT – zespół reagowania na incydenty bezpieczeństwa komputerowego

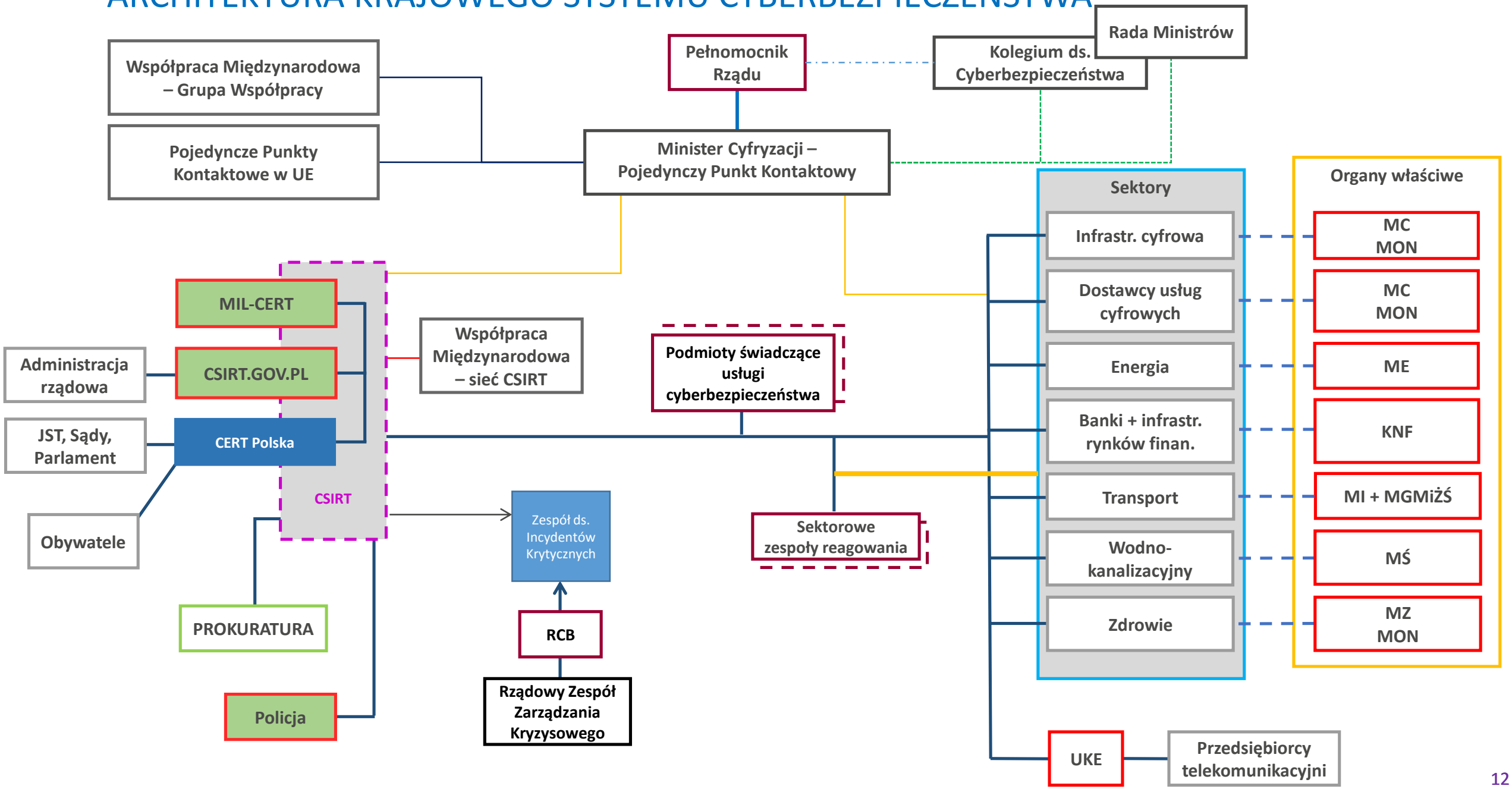
Definicje

Cyberbezpieczeństwo – stan systemów informacyjnych oznaczający odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne

Incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo

Poważny incydent – incydent lub grupę incydentów, które powodują lub mogą spowodować krytyczne obniżenie jakości świadczonej usługi lub przerwanie ciągłości działania świadczonej usługi

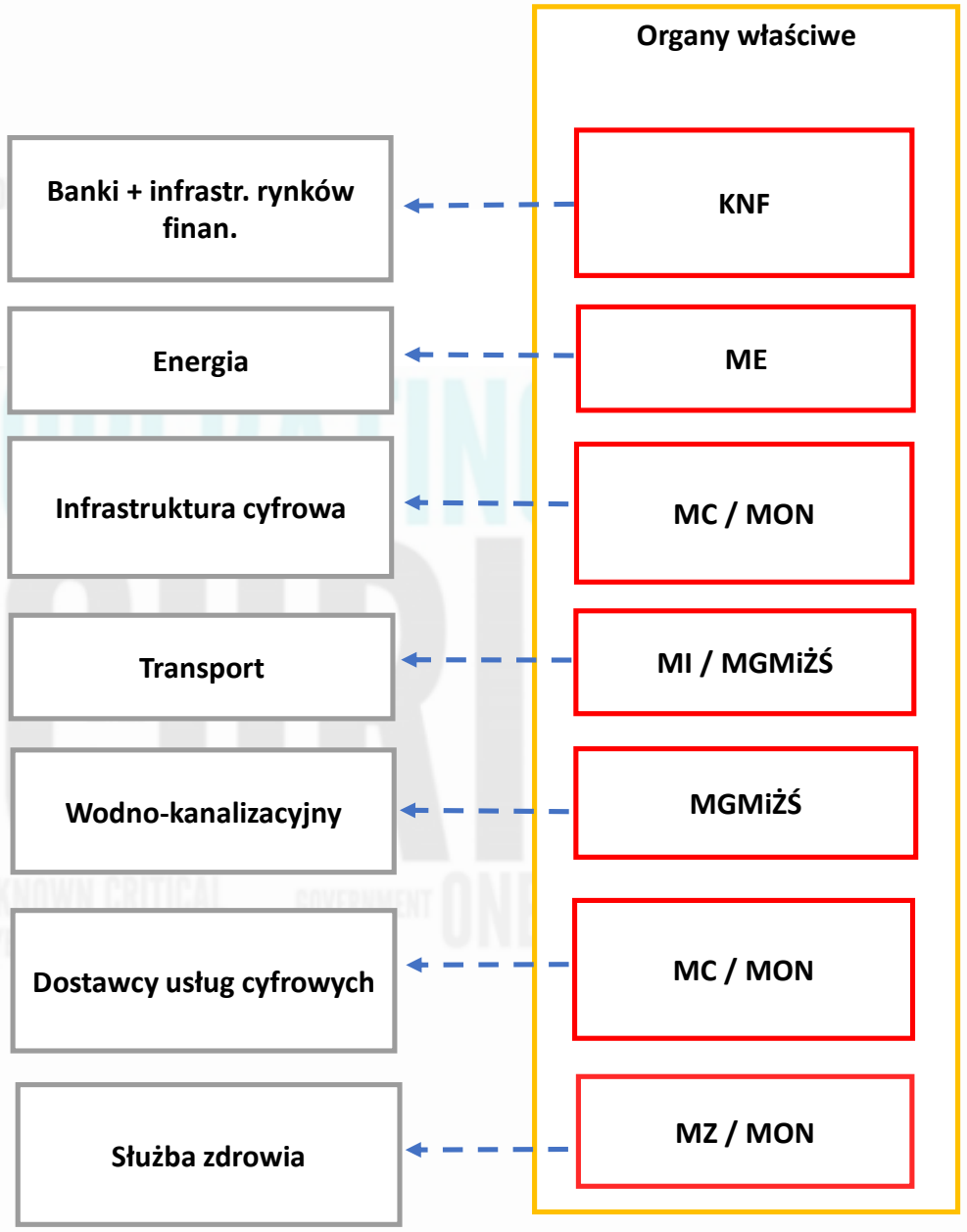
ARCHITEKTURA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA



Organy właściwe

Organy właściwe do spraw cyberbezpieczeństwa:

1. analizują sektor
2. wydają decyzje
3. przygotowują rekomendacje
4. realizują wybrane aspekty współpracy międzynarodowej



Etapy obsługi incydentów wg UKSC

Obsługa incydentu – czynności umożliwiające:

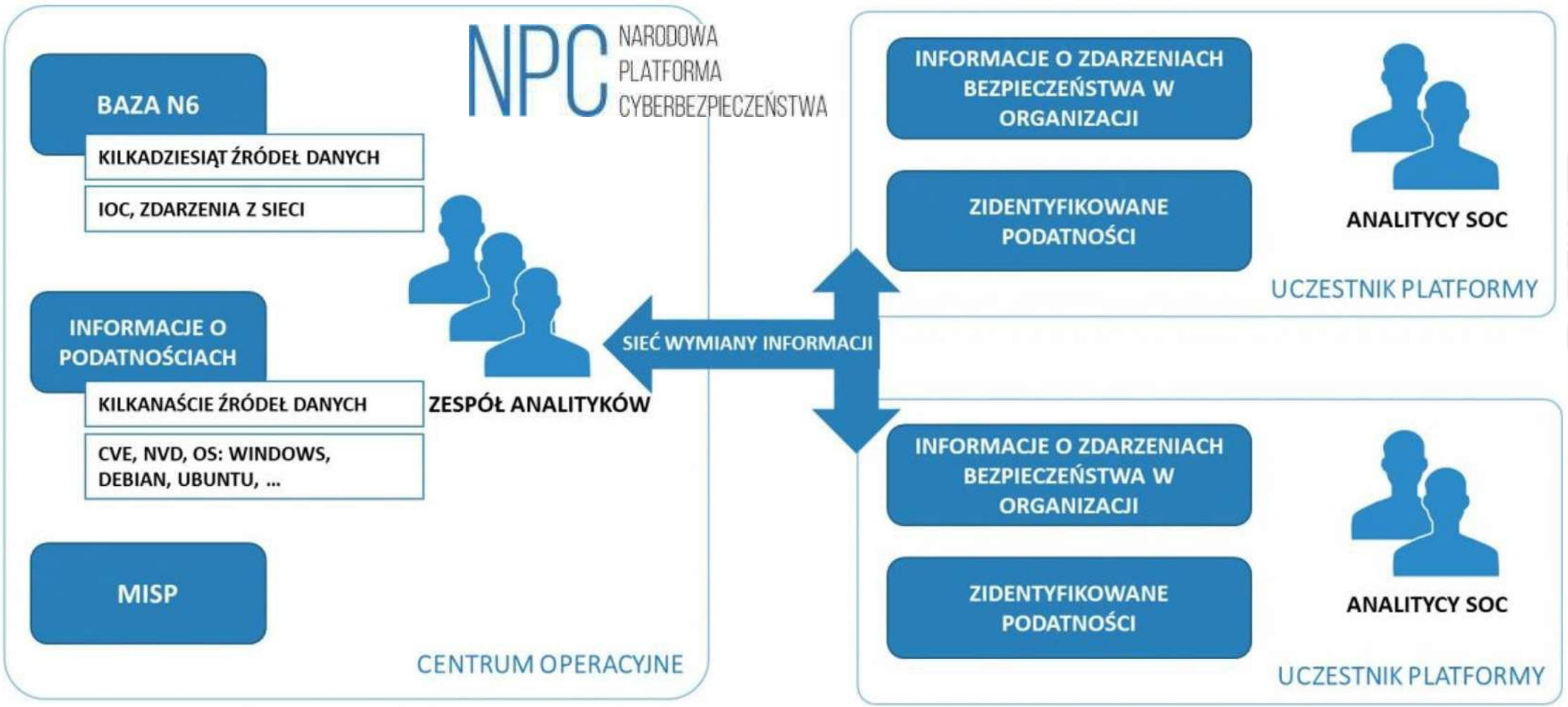
- wykrywanie,
- rejestrowanie,
- analizowanie,
- klasyfikowanie,
- priorytetyzację,
- podejmowanie działań naprawczych,
- ograniczenie skutków incydentu;

Zintegrowany system zarządzania bezpieczeństwem cyberprzestrzeni RP

Art. 46. **Minister Cyfryzacji** zapewnia rozwój lub utrzymanie **systemu teleinformatycznego** wspierającego:

- **wymianę informacji** na potrzeby współpracy podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa,
- **generowanie i przekazywanie rekomendacji** dotyczących działań podnoszących poziom cyberbezpieczeństwa,
- zgłaszanie i **obsługę incydentów,**
- **szacowanie ryzyka** na poziomie krajowym,
- **ostrzeganie o zagrożeniach** cyberbezpieczeństwa.

Narodowa Platforma Cyberbezpieczeństwa



Rozporządzenia wykonawcze

- **Rozporządzenie RM ws. usług kluczowych (RC39)**
- **Rozporządzenie RM ws. incydentu poważnego (RC38)**
- Rozporządzenie RM ws. dokumentacji (RD387)
- Rozporządzenie MC ws. warunków organizacyjnych (111)
- Rozporządzenie MC ws. certyfikatów (112)
- Rozporządzenie RM ws. Kolegium Cyberbezpieczeństwa (RD388)
- Rozporządzenie MC ws. formularza (113)
- Rozporządzenie MC ws. kryteriów (114)

Wykaz usług kluczowych

„Art. 5. ust. 2. Organ właściwy do spraw cyberbezpieczeństwa wydaje decyzję o uznaniu podmiotu za operatora usługi kluczowej, jeżeli:

1) podmiot świadczy usługę kluczową;
2) świadczenie tej usługi zależy od systemów informacyjnych;
3) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora.”

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

Istotny skutek zakłócający

- **liczby użytkowników** zależnych od świadczonej usługi;
- **zależności innych sektorów** od usługi świadczonej przez ten podmiot;
- **wpływu**, jaki incydent mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne;
- **udziału** podmiotu świadczącego usługę kluczową **w rynku**;
- **zasięgu geograficznego** związanego z obszarem, którego mógłby dotyczyć incydent;
- **znaczenie podmiotu** dla utrzymywania wystarczającego poziomu świadczenia usługi przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia.

Progi incydentów poważnych

- „Art. 11 ust. 1. Operator usługi kluczowej (…) **klasyfikuje incydent jako poważny** na podstawie progów uznawania incydentu za poważny [oraz] **zgłasza incydent poważny** niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT (…)”

- Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny

- Dostępny na stronie RCL

Dokumentacja

- „Art. 10 ust. 1. Operator usługi kluczowej opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej”

- Rozporządzenie Rady Ministrów w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych

- Dostępny na stronie RCL

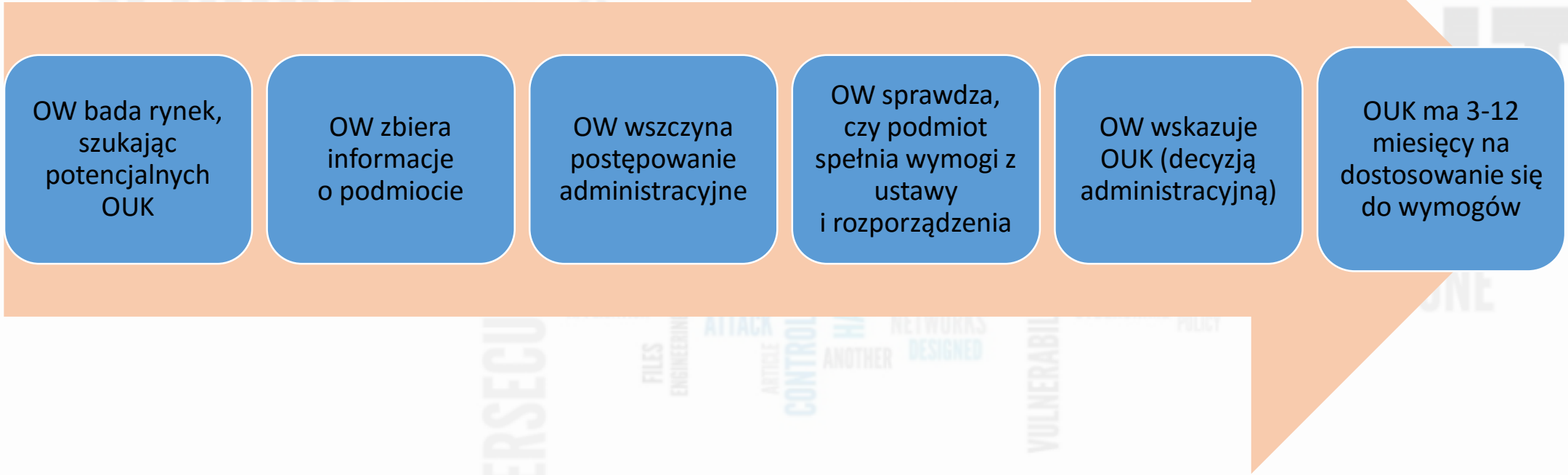
Warunki organizacyjne

- „Art. 14. 1. Operator usługi kluczowej w celu realizacji zadań (…) powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa.”

- Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

- Publikator: Dz. U. poz. 1780

Wyznaczanie operatora usługi kluczowej



OUK realizuje obowiązki wynikające z ustawy

Wyznaczanie operatora usługi kluczowej

DECYZJA ADMINISTRACYJNA

- decyzja jest natychmiast wykonalna
- od dnia otrzymania decyzji biegną terminy dotyczące realizacji obowiązków
- wpis do wykazu operatorów usług kluczowych i wykreślenie z tego wykazu następuje na wniosek ME (nie ma wpływu na obowiązki operatora - czynność techniczna)

Obowiązki operatora usługi kluczowej

WDROŻENIE SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM W SYSTEMIE INFORMACYJNYM

- systematyczne szacowanie ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem,
- wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy,
- zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego,
- zarządzanie incydentami,
- stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego,
- stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Obowiązki operatora usługi kluczowej

Środki techniczne i organizacyjne:

- utrzymanie i bezpieczna eksploatacja systemu informacyjnego
- bezpieczeństwo fizyczne, środowiskowe
- kontrola dostępu
- bezpieczeństwo i ciągłość dostaw usług
- wdrożenie planów działania - niezakłócone świadczenie usługi, zapewnienie poufności, integralności, dostępności i autentyczność informacji
- system monitorowania w trybie ciągłym

Obowiązki operatora usługi kluczowej

Środki zapobiegające i ograniczające wpływ incydentów:

- mechanizmy zapewniające poufność, integralność, dostępność i autentyczność danych
- aktualizacja oprogramowania
- ochrona przed nieuprawnioną modyfikacją danych
- podejmowanie działań po dostrzeżeniu podatności lub zagrożeń

Obowiązki operatora usługi kluczowej

OSOBY KONTAKTOWE I INFORMACJE

- Operator wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z innymi podmiotami krajowego systemu cyberbezpieczeństwa

- Operator przekazuje do organu właściwego do spraw cyberbezpieczeństwa, właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowego zespołu cyberbezpieczeństwa dane osoby kontaktowej w terminie 14 dni od dnia jej wyznaczenia/zmiany

- Operator zapewnia użytkownikom usługi kluczowej dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami - publikowanie informacji na ten temat na stronie internetowej

Obowiązki operatora usługi kluczowej

INFORMACJE O INCYDENTACH

- Operator zgłasza (musi zgłosić) incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV

- Operator przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu poważnego

- Operator może przekazywać jednocześnie takie informacje do sektorowego CSIRT

- Operator usługi kluczowej może przekazywać do właściwego CSIRT o innych incydentach, jak również o zagrożeniach cyberbezpieczeństwa, informacje dotyczące szacowania ryzyka, informacje o podatnościach systemu oraz o wykorzystywanych technologiach

Terminy realizacji obowiązków

Terminy realizacji obowiązków

W TERMINIE 3 MIESIĘCY:

- systematyczne szacowanie ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem
- zarządzanie incydentami
- przekazywanie informacji o incydentach do CSIRT
- wyznaczenie osoby kontaktowej
- informacje i działania edukacyjne dla użytkowników (strony www itp.)
- obsługa incydentów we własnych systemach
- wskazywane i usuwanie podatności
- zgłaszanie poważnych incydentów
- powołanie wewnętrznych struktur cyberbezpieczeństwa lub zawarcie umowy

Terminy realizacji obowiązków

W TERMINIE 6 MIESIĘCY:

- wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych
- zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu
- stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego
- stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach ksc
- opracowanie i wdrożenie dokumentacji dotyczącej cyberbezpieczeństwa systemu
- ustanowienie nadzoru nad dokumentacją i zasad jej przechowywania

Terminy realizacji obowiązków

W TERMINIE 12 MIESIĘCY:

- przeprowadzenie audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
- przekazanie sprawozdania z audytu wskazanym w ustawie podmiotom

Nowe inicjatywy europejskie w obszarze cyberbezpieczeństwa

Nowe inicjatywy europejskie w obszarze cyberbezpieczeństwa

Cybersecurity Act

- Rozporządzenie UE

- Cele:
  - Stały mandat dla ENISA
  - Stworzenie europejskich ram certyfikacji cyberbezpieczeństwa:
    - Europejski certyfikat cyberbezpieczeństwa
    - Unijna deklaracja zgodności

- Stan prac nad rozporządzeniem:
  - grudzień 2018 r. – uzgodniono ostateczną treść Aktu;
  - Połowa marca br. – głosowanie w PE;
  - Wejście w życie – II kwartał 2019 r.
  - Wniosek do ENISA o przygotowanie propozycji europejskiego programu certyfikacji – II kwartał 2019 r.

Cybersecurity Act w Polsce

- Dostosowanie polskiego prawa do rozporządzenia UE
- Utworzenie urzędu ds. nadzoru nad certyfikacją cyberbezpieczeństwa
- Wyznaczenie jednostki oceniającej zgodność
- Utworzenie Krajowego Systemu

  Certyfikacji Cyberbezpieczeństwa (KSCCyber)

Certyfikacja cyberbezpieczeństwa urządzeń, oprogramowania i usług

Ustanowienie w Polsce skutecznego i efektywnego systemu certyfikacji wyrobów, usług i procesów sektora technologii informacyjno-komunikacyjnych jest warunkiem zapewnienia **bezpiecznego łańcucha dostaw**

Elementy Krajowego Systemu Certyfikacji Cyberbezpieczeństwa

- Krajowy organ nadzoru nad systemem oceny i certyfikacji – współpraca z Polskim Centrum Akredytacji
- Jednostki certyfikujące
- Laboratoria dokonujące oceny wyrobów, usług lub procesów zgodnie z przyjętymi programami certyfikacji (na poziomie krajowym i UE)
- Kryteria oceny i wymagania bezpieczeństwa
- Deklaracje zgodności producentów

Certyfikacja cyberbezpieczeństwa urządzeń, oprogramowania i usług – KSO3C

KSO3C

Projekt "Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria" (KSO3C) jest realizowany przez Konsorcjum naukowe złożone z trzech jednostek naukowo-badawczych, nadzorowanych przez Ministra Cyfryzacji tzn: Instytut Łączności – Państwowy Instytut Badawczy (Lider Konsorcjum), Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy oraz Instytut Technik Innowacyjnych EMAG.

NASK

INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY

emag

Narodowe Centrum
Badań i Rozwoju

Projekt KSO3C jest współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach Programu CyberSecIdent.

Dziękuję za uwagę

Andrzej Szyszko

Departament Bezpieczeństwa i Zarządzania Kryzysowego

Ministerstwa Energii