NASK

CERT.PL

Rola CSIRT NASK w systemie cyberbezpieczeństwa

Przemek Jaroszewski

22 października 2020. XXI Bezpieczeństwo w Internecie. Cyberpandemia. Online

CERT Polska

- Zespół powołany w 1996 r. (jako CERT NASK) aby dbać o bezpieczeństwo polskich internautów
- Badania z dziedziny bezpieczeństwa sieci i systemów
  - identyfikacja nowych zagrożeń, narzędzi, metod ataków
  - identyfikacja krytycznych miejsc otwierających płaszczyzny ataku
- Ostrzeganie i budowanie świadomości
- Współpraca międzynarodowa
- Współpraca z organami ścigania
  - identyfikacja grup cyberprzestępczych oraz rozpoznawanie ich ‘warsztatu’
  - ocena skuteczności prowadzonych kampanii, ustalanie ofiar, zasięgu
- Od 2018 roku nałożone dodatkowe zadania związane z pełnieniem przez NASK roli CSIRT NASK
- Finansowanie:
  - Środki własne NASK, m.in. z rejestracji domen .pl
  - Granty z funduszy europejskich, NCBiR i in.
  - Do 2018 roku usługi komercyjne
  - Od 2018 roku dotacja podmiotowa z budżetu państwa, ze środków ministra właściwego ds. informatyzacji (maks. 8,5 mln. PLN)

USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

- **Ustawa o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 2018 poz. 1560) obowiązuje od 28 sierpnia 2018 roku** i zapewnia implementację dyrektywy NIS*,
- ustanawia ramy prawne funkcjonowania KSC,
- rozszerza obszar oddziaływania w stosunku do dyrektywy NIS, np.:
  - włącza sektor administracji publicznej,
  - włącza sektor telekomunikacyjny.

- **Implementacja Dyrektywy NIS to początek działań zmierzających do podniesienia poziomu cyberbezpieczeństwa w Europie.**

- Dla KE tematyka cyberbezpieczeństwa jest związana nie tylko z bezpieczeństwem narodowym, ale także z rozwojem gospodarczym - budowa Jednolitego Rynku Cyfrowego w taki sposób, aby obywatele mieli zaufanie do świadczonych na nim usług.

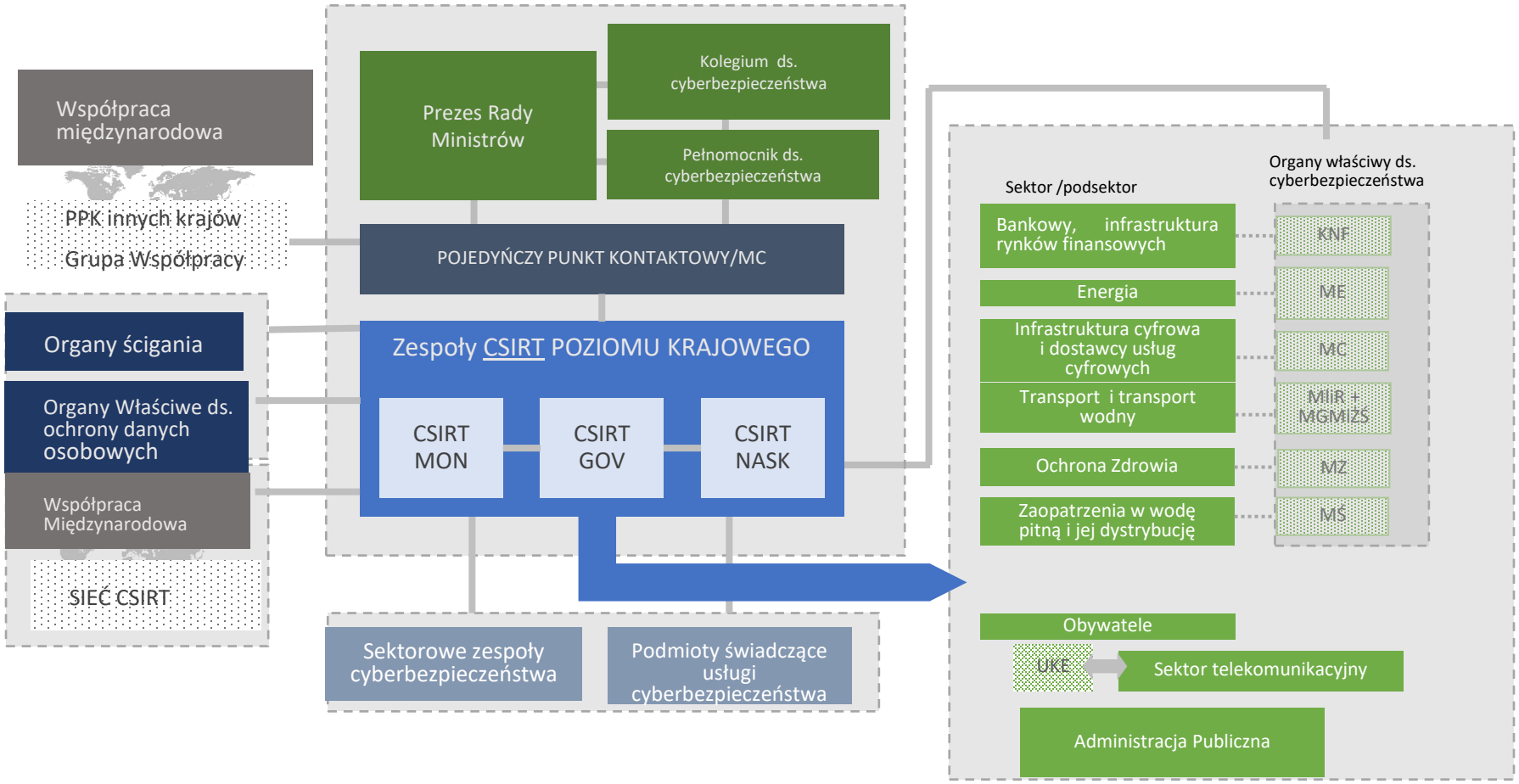
* Dyrektywa Parlamentu Europejskiego i Rady UE 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

DYREKTYWA NIS

Wybrane obowiązki nałożone na państwa członkowskie:

- Identyfikacja **operatorów usług kluczowych w kilku sektorach** oraz określenie wymagań bezpieczeństwa teleinformatycznego.
- Wyznaczenie **organów właściwych** dla operatorów usług kluczowych i dostawców usług cyfrowych.
- Wyznaczenie **pojedynczego punktu kontaktowego.**
- Wyznaczenie **CSIRT*** dla operatorów usług kluczowych i dostawców usług cyfrowych.
- Wymiana informacji i **raportowanie** na poziomie UE na temat **poważnych incydentów** u operatorów usług kluczowych oraz **istotnych incydentów** u dostawców usług cyfrowych.
- Przyjęcie w unijnej **procedurze komitetowej** wymagań dla dostawców usług cyfrowych.
- Przyjęcie krajowej **strategii** bezpieczeństwa sieci i informacji.

ARCHITEKTURA KRAJOWEGO SYSTEMU CYBERBEPZIECZEŃSTWA



PODZIAŁ ODPOWIEDZIALNOŚCI (art. 26 uoksc)

- CSIRT MON
  - Wojsko – podmioty podległe i nadzorowane przez MON
  - przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa w rozumieniu art. 5 pkt 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. poz. 1320 oraz z 2002 r. poz. 1571) jest Minister Obrony Narodowej
- CSIRT GOV (ABW)
  - Administracja centralna (jednostki podległe i nadzorowane przez PRM)
  - NBP, BGK
  - Operatorzy IK poza podległością MON
  - Incydenty o charakterze terrorystycznym
- CSIRT NASK
  - operatorzy usług kluczowych, z wyj. Powyższych
  - dostawcy usług cyfrowych
  - niższe szczeble administracji, w tym administracja samorządowa i jednostki podległe
  - osoby fizyczne, małe i średnie przedsiębiorstwa i in.

ZADANIA CSIRTów (art. 26 ust. 3 uoksc)

- **monitorowanie zagrożeń** cyberbezpieczeństwa i incydentów na poziomie krajowym, szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;
- **przekazywanie informacji** dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa, wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
- **reagowanie na zgłoszone incydenty**, klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;
- **zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego**, które w szczególności:
  - prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności,
  - monitoruje wskaźniki zagrożeń cyberbezpieczeństwa,
  - rozwija narzędzia i metody do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa,
  - prowadzi analizy i opracowuje standardy, rekomendacje i dobre praktyki w zakresie cyberbezpieczeństwa,
  - wspiera podmioty krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa,
  - prowadzi działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa,
  - współpracuje w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa;
- **koordynacja incydentów** w ramach swojego *constituency*, a także wspólnie z pozostałymi CSIRTami;
- **zapewnienie możliwości dokonywania zgłoszeń** i przekazywania informacji, o których mowa w art. 11 ust. 1 pkt 4, art. 13 ust. 1, art. 18 ust. 1 pkt 4, art. 20, art. 22 ust. 1 pkt 2, art. 24 i art. 30 ust. 1, oraz udostępnienie i obsługa środków komunikacji pozwalających na dokonywanie tych zgłoszeń;

ZADANIA CSIRTów (art. 26 ust. 2, art. 30 uoksc)

- CSIRT MON, CSIRT NASK i CSIRT GOV **w uzasadnionych przypadkach na wniosek** operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych, o których mowa w art. 4 pkt 7–15, sektorowych zespołów cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, **mogą zapewnić wsparcie** w obsłudze incydentów.
- Art. 30. 1. **Podmioty inne** niż operatorzy usług kluczowych i dostawcy usług cyfrowych, w tym osoby fizyczne, mogą zgłosić incydent do CSIRT NASK. (…)

2. Zgłoszenia incydentów od operatorów usług kluczowych oraz dostawców usług cyfrowych są traktowane priorytetowo względem zgłoszeń, o których mowa w ust. 1.

3. Zgłoszenia, o których mowa w ust. 1, mogą zostać rozpatrzone, gdy nie stanowi to nieproporcjonalnego czy nadmiernego obciążenia dla CSIRT NASK.

OBOWIĄZKI OUK, DUC, PP w relacji z CSIRT

- Wyznaczenie i zgłoszenie osoby kontaktowej (nie dotyczy DUC)
- Zgłaszanie (ponadprogowych) incydentów – niezwłocznie
- Zapewnienie obsługi incydentu
- Przekazywanie niezbędnych informacji w związku z incydentem, w tym prawnie chronionych

CERT.PL Zgłoś incydent PL EN

Zgłoszenia do CSIRT NASK

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki **CSIRT NASK** wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:
Zgłaszanie osoby kontaktowej do CSIRT NASK.

Jeżeli chcą Państwo zgłosić złośliwą domenę, proszę użyć poniższego odnośnika:
Zgłaszanie domeny internetowej służącej do wyłudzeń danych i środków finansowych.

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

Osoba fizyczna / inne podmioty

Operator usług kluczowych

Dostawca usługi cyfrowej

Podmiot publiczny

Osoba fizyczna / inne podmioty

Operator usług kluczowych

Dostawca usługi cyfrowej

Podmiot publiczny

Prosimy o wybranie odpowiedniej kategorii:

Podejrzana wiadomość e-mail

Podejrzane załączniki, phishing, szantaż

$ Próba oszustwa

Fałszywe sklepy internetowe i inne próby podszywania się

Złośliwe oprogramowanie

Próbki wirusów lub pliki zaszyfrowane ransomware

Podatności

Błędy w oprogramowaniu lub aplikacjach internetowych

Nielegalne treści

Zgłoszenia przeznaczone dla zespołu Dyżurnet.pl

Inne

Wszystkie inne incydenty niepasujące do poprzednich kategorii

Zgłaszanie osób kontaktowych do CSIRT NASK

Obowiązkowi zgłoszenia osób kontaktowych właściwemu CSIRT podlegają wg ustawy z dnia 5 lipca 2018 r. o krajowym cyberbezpieczeństwa (Dz. U. poz. 1560) **operatorzy usług kluczowych** (art 9 ust 1) oraz **podmioty publiczne** (art 22 ust 1 pkt 5).

Jeżeli chcą Państwo zgłosić incydent proszę użyć poniższego odnośnika:
Zgłaszanie incydentu do CSIRT NASK.

Aby zgłosić osoby kontaktowe do CSIRT NASK lub zaktualizować ich dane należy:

- wypełnić poniższy formularz,
- wygenerowane pismo przedstawić do podpisu kierownikowi instytucji,
- przesłać pismo na wskazany w nim adres (w przypadku operatora usługi kluczowej załączając skan decyzji administracyjnej uznającej podmiot za operatora usługi kluczowej).

Przed wypełnieniem ponizszego formularza polecamy zapoznać się ze wspólnymi **rekomendacjami CSIRT NASK oraz CSIRT GOV** w zakresie wyznaczania osób kontaktowych.

Jaki podmiot Państwo reprezentują?

Operator usługi kluczowej	Podmiot publiczny	Inny podmiot
Wypełnienie obowiązku wynikającego z art 9 ust 1 ustawy o KSC	Wypełnienie obowiązku wynikającego z art 22 ust 1 pkt 5 ustawy o KSC	

Jaki podmiot Państwo reprezentują?

Operator usługi kluczowej

Wypełnienie obowiązku wynikającego z art 9 ust 1 ustawy o KSC

Podmiot publiczny

Wypełnienie obowiązku wynikającego z art 22 ust 1 pkt 5 ustawy o KSC

Inny podmiot

Zgłoszenie kontaktu od niezobowiązanego podmiotu

Podmioty niebędące operatorami usług kluczowych (tj. nie otrzymali Państwo decyzji administracyjnej o uznaniu za taki podmiot) ani podmiotami publicznymi nie są zobligowane do przekazywania CSIRT poziomu krajowego danych osób kontaktowych.
Jednocześnie zachęcamy do dobrowolnego udziału w ramach bezpłatnych narzędzi udostępnianych przez CERT Polska:

- n6 - system wymiany informacji o zagrożeniach w sieciach [więcej informacji],
- mwdb - baza danych złośliwego oprogramowania [więcej informacji]

Kontakt z CSIRT NASK niebędący zgłoszeniem incydentu możliwy jest również za pomocą poczty elektronicznej pod adresem info@cert.pl.

KONTAKT

- https://www.cert.pl/, info@cert.pl
- Zgłoszenia incydentów: https://incydent.cert.pl/, cert@cert.pl
- Facebook: CERT.Polska
- Twitter: @CERT_Polska
- YouTube: CERTPolska

- Przemek.Jaroszewski@cert.pl