
# Nowa Strategia Cyberbezpieczeństwa RP na lata 2017-2022 – główne założenia i cele


- Dariusz Deptała


Serock, 29-31 maja 2017 r.

- Strategia Cyberbezpieczeństwa RP- Krajowe Ramy Polityki Cyberbezpieczeństwa
- Ustawa o krajowym systemie cyberbezpieczeństwa
- Zintegrowany System Bieżącego Zarządzania Bezpieczeństwem Cyberprzestrzeni (ZSBZBC)
- Narodowe Centrum Cyberbezpieczeństwa
- Wspólna Infrastruktura Państwa poprzez Rządowy Klaster Bezpieczeństwa (zbudowanie architektury bezpieczeństwa państwa do poziomu woj.
- Krajowy System Oceny i Certyfikacji produktów IT (w trakcie tworzenia)
- System Łączności na potrzeby Systemu Kierowania Bezpieczeństwem Narodowym

- „Polityka ochrony cyberprzestrzeni RP” (MC, ABW)
- „Strategia bezpieczeństwa narodowego”
- „Doktryna cyberbezpieczeństwa RP” (BBN)
- Narodowy Program Ochrony Infrastruktury Krytycznej (RCB)

**UCHWAŁA NR 52/2017**
**RADY MINISTRÓW**
z dnia 27 kwietnia 2017 r.
**w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022**

- Strategia została opracowana przez grupę składającą się z przedstawicieli resortów: cyfryzacji, obrony narodowej, spraw wewnętrznych i administracji oraz przedstawicieli Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa i Biura Bezpieczeństwa Narodowego.

- Politykę Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 roku

- Dyrektywy 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 Europejskiej (Dyrektywa NIS)

# Strategia wskazuje:

- cele w zakresie bezpieczeństwa teleinformatycznego,
- główne podmioty zaangażowane we wdrażanie strategii w zakresie bezpieczeństwa teleinformatycznego,
- ramy zarządzania służące realizacji celów krajowej strategii w zakresie bezpieczeństwa teleinformatycznego,
- podejście do oceny ryzyka,
- kierunki podejścia do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa,
- działania odnoszące się do planów badawczo-rozwojowych w zakresie bezpieczeństwa teleinformatycznego,
- podejście do współpracy międzynarodowej w zakresie cyberbezpieczeństwa
- na potrzebę zapobiegania i reagowania w odniesieniu do incydentów oraz przywracania stanu normalnego zakłóconego incydentem, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym,

# Cel główny ⟶ Cele szczegółowe

- kierunki interwencji
- określone zadania (tego jeszcze nie ma)
  - ciągłe
  - projektowe

# Cel główny

- Zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych.

- Koordynator (MC) w terminie do sześciu miesięcy od przyjęcia Strategii we współpracy z członkami Rady Ministrów, kierownikami urzędów centralnych, Dyrektorem Rządowego Centrum Bezpieczeństwa opracuje Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa

# Cele szczegółowe

1. Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa

2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom.

3. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni

4. Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

## Cel szczegółowy 1

## Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa

- Dostosowanie otoczenia prawnego do potrzeb i wyzwań w obszarze cyberbezpieczeństwa
- Udoskonalenie struktury krajowego systemu cyberbezpieczeństwa
- Zwiększenie efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP
- Zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej
- Opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych
- Wypracowanie i wdrożenie systemu zarządzania ryzykiem na poziomie krajowym
- Zapewnienie bezpiecznego łańcucha dostaw
- Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń

Rozwój krajowego systemu cyberbezpieczeństwa wiąże się z rozbudową struktur zajmujących się cyberbezpieczeństwem na poziomie operacyjny

- Narodowego Centrum Cyberbezpieczeństwa (NCC)
- CSIRT Narodowego
- sektorowych zespołów reagowania na incydenty (CSIRT sektorowe)
- centrów wymiany i analizy informacji

# Cel szczegółowy 2
# Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom

- Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni
- Uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni
- Zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym
- Zbudowanie systemu bezpiecznej komunikacji na potrzeby bezpieczeństwa narodowego
- Audyty i testy bezpieczeństwa

# Cel szczegółowy 3
# Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni

- Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa
- Zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym
- Stymulowanie badań i rozwoju w obszarze bezpieczeństwa systemów teleinformatycznych
- Zwiększanie kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni
- Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli

# Cel szczegółowy 4
# Zbudowanie silnej pozycji międzynarodowej Polski w obszarze cyberbezpieczeństwa

- Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym
- Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym

# Aktualny podział kompetencji:

- **Ministerstwo Cyfryzacji** – kluczowa rola w procesach związanych z ochroną cyberprzestrzeni. Strategiczno-polityczny koordynator systemu ochrony cyberprzestrzeni RP. We współpracy z ABW opracowało w 2013 roku „Politykę ochrony cyberprzestrzeni RP”;
- **Ministerstwo Obrony Narodowej** – odpowiada za wojskową sferę ochrony cyberprzestrzeni RP. W ramach MON funkcjonuje Inspektorat Systemów Informacyjnych, działający na potrzeby resortu MIL-CERT oraz Narodowe Centrum Kryptologii (NCK);
- **Biuro Bezpieczeństwa Narodowego** – organ doradczy prezydenta RP, w którym opracowano „Doktrynę cyberbezpieczeństwa Rzeczypospolitej Polskiej”;
- **Agencja Bezpieczeństwa Wewnętrznego** – rozpoznaje, zapobiega i zwalcza zagrożenia godzące w bezpieczeństwo wewnętrzne państwa. W strukturze Agencji funkcjonuje Departament Bezpieczeństwa Teleinformatycznego, w ramach którego działa Rządowy Zespół Reagowania na Incydenty Komputerowe – CERT.GOV.PL;
- **Ministerstwo Spraw Wewnętrznych i Administracj**i – nadzoruje działania policji w zakresie zwalczania cyberprzestępczości;
- **Policja** – zwalcza cyberprzestępczość. W strukturach policji funkcjonuje POL-CERT;
- **Urząd Komunikacji Elektronicznej** – regulator rynku telekomunikacyjnego i pocztowego. Zapewnia implementacje prawa telekomunikacyjnego w kontekście bezpieczeństwa w cyberprzestrzeni;
- **Rządowe Centrum Bezpieczeństwa** – odgrywa przodującą rolę w obszarze zarządzania kryzysowego i ochrony infrastruktury krytycznej, przygotowuje Narodowy Program Ochrony Infrastruktury Krytycznej, a także Krajowy Plan Zarządzania Kryzysowego oraz „Raport o zagrożeniach bezpieczeństwa narodowego”. W centrum znajduje się 24-godzinna służba dyżurna, która odpowiada za przekazywanie informacji o zagrożeniach;
- **Ministerstwo Sprawiedliwości** – kreuje prawo w zakresie cyberprzestępczości i nadzoruje jego właściwe wykonanie;
- **Ministerstwo Finansów** – odpowiada za kwestie budżetowe, w tym za sprawy związane z cyberbezpieczeństwem;
- **Naukowa i Akademicka Sieć Komputerowa** – instytut badawczy nadzorowany przez Ministerstwo Cyfryzacji. W ramach NASK funkcjonuje zespół CERT.POLSKA, który pełni de facto rolę krajowego CERT/CSIRT.

# Projekt ustawy o krajowym systemie cyberbezpieczeństwa

- ustanowienie na szczeblu krajowym architektury ochrony systemów teleinformatycznych z uwzględnieniem regulacji międzynarodowych, oraz wskazanie organów władzy publicznej odpowiedzialnych za zarządzanie bezpieczeństwem informacji;
- ustanowienie krajowego systemu reagowania na zagrożenia dla bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych, pochodzące z cyberprzestrzeni;
- ustalenie zasad współpracy podmiotów zobowiązanych do wykrywania incydentów spowodowanych zagrożeniami cyberprzestrzeni i sposobów postępowania w okresie trwania tych incydentów;
- prawne umocowanie dokumentu ustanawiającego krajową strategię bezpieczeństwa sieci i informacji mającą na celu osiągnięcie akceptowalnego poziomu cyberbezpieczeństwa Rzeczpospolitej Polskiej;
- wskazanie sektorów gospodarki narodowej, dla których zastosowanie będą miały przepisy ustawy oraz określenie kryteriów kwalifikacji podmiotów objętych regulacją;
- ustalenie poziomu istotności incydentu z zakresu bezpieczeństwa oraz wprowadzenie obowiązku notyfikowania incydentów wskazanemu organowi władzy publicznej;
- ustalenie ustawowych wymagań i powinności z zakresu cyberbezpieczeństwa dla jednostek organizacyjnych z zakresu podmiotowego w obszarze organizacyjnym i technologicznym oraz delegowanie do aktów wykonawczych ustalenia szczegółów tych wymagań.

# *Dziękuję za uwagę!*

**Dariusz Deptała**

**E-mail: ddeptala@ksoin.pl**

**tel.: +48-601-284-209**

- KONSULTACJE
- DORADZTWO
- SZKOLENIA
- AUDYT

KRAJOWE STOWARZYSZENIE OCHRONY INFORMACJI NIEJAWNYCH

- PROFESJONALIZM
- DOŚWIADCZENIE
- KOMPETENCJE