Ministerstwo Cyfryzacji

Tu tworzymy przyszłość

Departament Cyberbezpieczeństwa

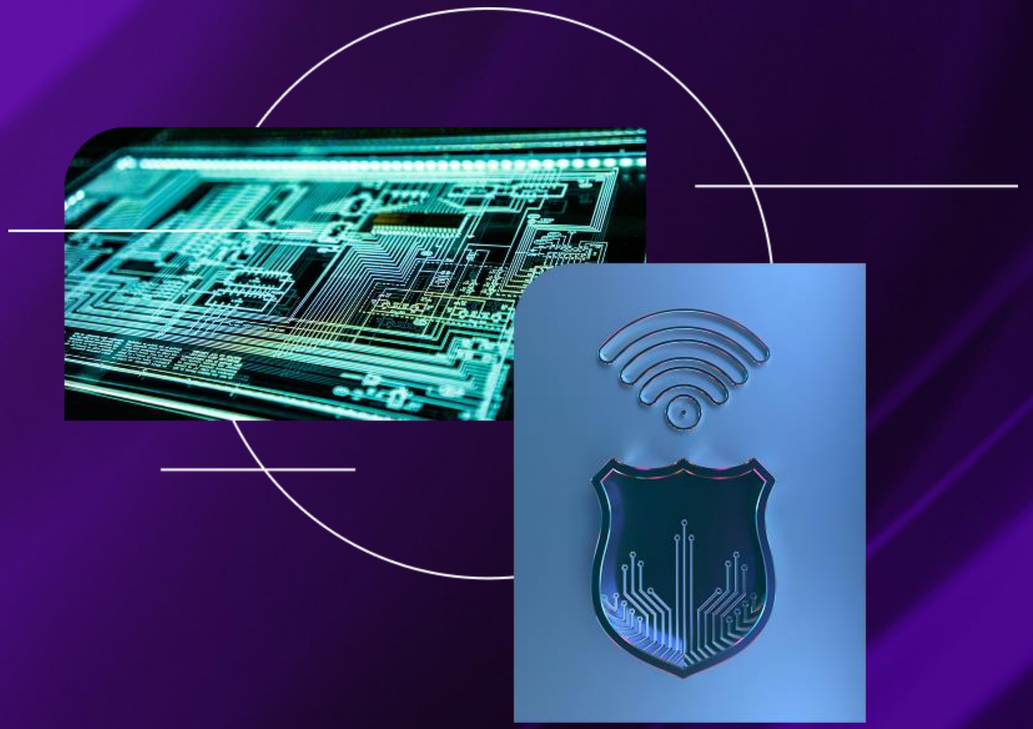
prowadzący

Łukasz Wojewoda

Dyrektor

Projekty legislacyjne 2025

W kwietniu br. **przyjęliśmy aktualizację Standardów Cyberbezpieczeństwa Chmur Obliczeniowych w związku z** zeszłoroczną nowelizacją uchwały Rady Ministrów w sprawie inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”



Obecnie pracujemy nad:

- Projektem ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa → projekt został przyjęty przez RM, w Sejmie po I czytaniu
- Projektem ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw → projekt został skierowany do rozpatrzenia przez SKRM
- Projektem o chmurze obliczeniowej w administracji

Nasze cele

- Ustanowienie ram dla KSCC, budowa zaufania użytkowników do certyfikowanych rozwiązań, ułatwienie decyzji zakupowych, wsparcie rozwoju nowoczesnych technologii w sektorze ICT
- Wdrożenie dyrektywy NIS 2 i Toolbox 5G
- Uporządkowanie możliwości korzystania z chmury obliczeniowej

Plany w obszarze legislacji

- Planujemy przeniesienie regulacji z zakresu chmury obliczeniowej na poziom ustawowy
- Obecnie korzystanie z chmury obliczeniowej w administracji regulowane jest przez Uchwałę RM w sprawie Inicjatywy „WIPP” oraz dokument SCCO
- Na gruncie tych aktów zidentyfikowaliśmy problemy związane m.in. z charakterem tego aktu oraz finansowaniem RCHO i ZUCH
- Prowadzimy obecnie prace koncepcyjne nad projektem ustawy o chmurze obliczeniowej w administracji

Plany w obszarze projektów współfinansowanych ze środków UE Cyberbezpieczne wodociągi

- Sierpień 2025 r. konkurs grantowy na wsparcie cyberbezpieczeństwa w podmiotach prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę korzystających z OT
- Mamy rozporządzenie w sprawie udzielania pomocy *de minimis* na wsparcie tych podmiotów w ramach KPO
- Środki alokowane na te przedsięwzięcie wyniosą łącznie **ok. 300 mln PLN netto**, a maksymalna wysokość pojedynczego grantu może wynosić **do 300 tys. EUR**

Lokalne Centra Cyberbezpieczeństwa

- Pod koniec 2025 r. planujemy uruchomić projekt wspierający tworzenie lub rozwój, w ramach dobrowolnej współpracy mikroregionalnej JST, **Lokalnych Centrów Cyberbezpieczeństwa**

Centra zapewnią wsparcie:

- Monitorowania i reagowania na incydenty
- Świadczenia usług doradczych i wsparcia technicznego, w tym audyty i tworzenie polityk bezpieczeństwa
- Prowadzenia szkoleń i warsztatów dla kadry JST
- Współpracy z CERT Polska

Przyjmuje się, że środki alokowane na ten projekt wyniosą łącznie **ok. 270 mln PLN**

Działania strategiczne

- Nowa Strategia Cyberbezpieczeństwa RP na lata 2025-2029
- W MC opracowaliśmy projekt nowej Strategii
- Obecnie pracujemy nad:
  - Wprowadzaniem do wykazu prac Rady Ministrów
  - W kolejnym kroku toczyć się będą uzgodnienia i opiniowanie w ramach rządowego procesu legislacyjnego

Działania strategiczne

Nasze cele:

- Ambitny dokument na miarę wyzwań współczesnych czasów oraz zagrożeń - jasny drogowskaz KSC, który wytyczać będzie kierunki zmian
- Przyjęte cel główny i cele szczegółowe są podobne do celów ujętych w Strategii na lata 2019-2024, ALE treść wypełniająca te cele i postawione zadania będą już znacznie inne
- Kontynuację obecnie realizowanych inicjatyw, przygotowywane przedsięwzięcia, planowane przedsięwzięcia

PWCyber - Program Współpracy w Cyberbezpieczeństwie

- Współpraca partnerska pomiędzy sektorem publicznym i prywatnym na rzecz KSC
- Obszary współpracy PWCyber:
  - Podnoszenie kompetencji administracji publicznej w zakresie cyberbezpieczeństwa
  - Wymiana informacji o cyberzagrożeniach
  - Opracowywanie rekomendacji w zakresie cyberbezpieczeństwa
  - Przygotowanie i prowadzenie oceny i certyfikacji cyberbezpieczeństwa
  - Upowszechnianie informacji o innowacjach w cyberbezpieczeństwie

Ministerstwo Cyfryzacji

Tu tworzymy przyszłość

Partnerzy programu PWCyber

Szkolenia dla podmiotów krajowego systemu cyberbezpieczeństwa

Szkolenia prowadzą eksperci i praktycy na co dzień zajmujących się kwestiami cyberbezpieczeństwa**:**

- Z NASK-PIB
- Przedstawiciele partnerów PWCyber

Szkolenia realizowane są na różnym poziomie zaawansowania wiedzy z zakresu cyberbezpieczeństwa, dostosowane do bieżącej sytuacji i zgłaszanych potrzeb:

- Szkolenia 100 - cyberhigiena dla każdego
- Szkolenia 200 - dla kadry zarządzającej, pracowników działów IT
- Szkolenia 300 - warsztaty dla specjalistów IT, programistów, osób zarządzających cyberbezpieczeństwem w podmiotach krajowego systemu cyberbezpieczeństwa

Ministerstwo Cyfryzacji

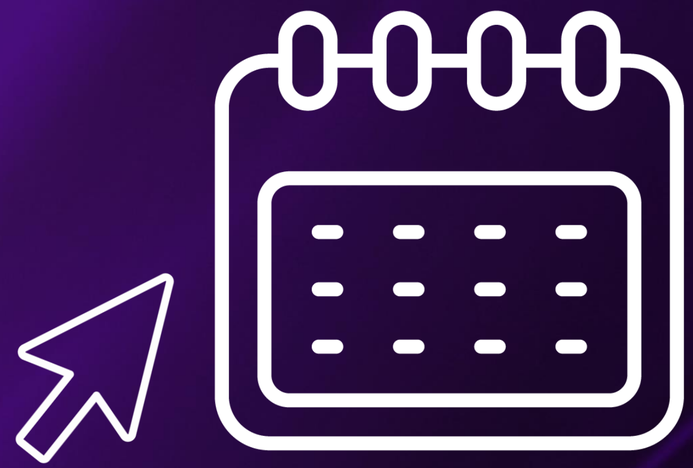
Tu tworzymy przyszłość

Szkolenia dla podmiotów krajowego systemu cyberbezpieczeństwa

Od 2020 roku przeprowadzono **138 szkoleń**, w których uczestniczyło przeszło **90 tys. osób.**

Informacja o szkoleniach wraz z możliwością zapisów dostępna jest w bazie wiedzy o cyberbezpieczeństwie na portalu gov.pl

https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen



Ćwiczenia krajowego systemu cyberbezpieczeństwa KSC-EXE

KSC-EXE 2024 - Listopad 2024

W ćwiczeniach udział wzięło prawie 6 przedstawicieli podmiotów krajowego systemu cyberbezpieczeństwa, w tym:

- organy właściwe ds. cyberbezpieczeństwa: MC, MKiŚ, MI, MZ, KNF, MC
- zespoły reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego, czyli: CSIRT GOV, CSIRT MON, CSIRT NASK
- przedstawiciele: MSZ, PK, RCB, UKE, CBZC

Szkolenia SecureV

- Od 2021 r. Minister Cyfryzacji we współpracy z NASK-PIB prowadzi projekty prewencyjno-edukacyjne (tzw. projekty SecureV).
- Szkolenia z zakresu cyberbezpieczeństwa dla kluczowych osób w państwie.
- Każda indywidualnie przeszkolona osoba zostaje wyposażona w uniwersalne narzędzia służące do silnego uwierzytelnienia.
- Od 2021 r. przeszkolonych ponad 12. tys. osób.
- Obecna edycja na lata 2025-2026 zakłada przeprowadzenie 8 tys. szkoleń.

Ochrona AntyDDoS

- Projekt AntyDDoS uruchomiony przez MC i realizowany przez NASK-PIB. MC zapewnia centralnie ochronę przed atakami DDoS dla ponad 70 instytucji, w tym dla wielu urzędów centralnych, jak również dla Sił Zbrojnych RP oraz służb specjalnych
- Ochrona w ramach 2 systemów: jeden z nich zapewnia ochronę obejmując łącznie 600 witryn internetowych (aplikacje), 30 sieci, 4 adresy IP, 104 strefy DNS, a drugi: 17 witryn internetowych (aplikacje)
- Intensyfikacja ataków, a jednocześnie skuteczność środków ochrony, prowadzi do wniosku, że projekt AntyDDoS musi być w dalszym ciągu wspierany i kontynuowany
- Kluczowym celem na 2025 r. i kolejne lata jest zwiększenie liczby podmiotów korzystających z ochrony w ramach projektu AntyDDoS

Planowane działania Krajowego Centrum Kompetencji Cyberbezpieczeństwa w ramach projektu NCC-PL

- Badanie MŚP z branży cyberbezpieczeństwa
  - cel: identyfikacja barier hamujących rozwój MŚP na rynku, form wsparcia, którego potrzebują ze strony instytucji publicznych
  - raport zawierający wnioski z badania będzie gotowy w II połowie 2025 r.
- Konkurs grantowy dla MŚP prowadzących działalność w obszarze cyberbezpieczeństwa
  - całkowita wartość planowanego dofinansowania - **1 800 000 EUR**
  - planowane wsparcie w obszarach: rozwoju istniejącego produktu lub usługi, stworzenia nowego rozwiązania, zwiększenia rozpoznawalności na rynku oraz certyfikacji produktu

Planowane działania Krajowego Centrum Kompetencji Cyberbezpieczeństwa w ramach projektu NCC-PL

- Budowanie Społeczności Kompetentnej w obszarze cyberbezpieczeństwa angażowanie podmiotów ze wszystkich sektorów do działań tej Społeczności i współpracy z NCC-PL i ECCC
- Wsparcie polskich podmiotów w aplikowaniu o granty na projekty w obszarze cyberbezpieczeństwa (nabory w programach Cyfrowa Europa i Horyzont Europa)
- Organizacja udziału polskiej drużyny uczennic w międzynarodowym obozie letnim CyberWizards w Estonii

Działania na arenie międzynarodowej

- Realizacja priorytetów polskiej prezydencji w zakresie cyberbezpieczeństwa, w tym przede wszystkim
  - Cel 1 – przyjęcie w trakcie posiedzenia COREPER w dniu 21 maja, ostatecznej wersji Blueprint;
  - Rozpoczęcie w ramach prac trio (PL, DK, CY) dalszych prac dotyczących wdrożenia.
  - Cel 2 – przekazanie rozpoczętych prac, w tym dot. Współpracy cywilno-wojskowej, single entry point for incydent notification, do dalszych prac w ramach trio

Działania na arenie międzynarodowej

Działania w ramach organizacji międzynarodowych

- Dalsze prace we współpracy z MSZ w ONZ w grupie OEWG (Open-ended working group on security) (ONZ), na której omawiane są kwestie związane z cyberbezpieczeństwem, przede wszystkim wypracowanie stałego mechanizmu prac nad rezolucjami ONZ w zakresie odpowiedzialnego zachowania państw w cyberprzestrzeni.
- Dalsza współpraca w ramach RCDC (Regional Cyber Defence Center) gdzie Polska wraz z LT, UA, GRU oraz współudziale USA działa w celu wykrywania cyberzagrożeń i ich analiz, budując w ten sposób wspólną bezpieczną cyberprzestrzeń oraz wymianę informacji między krajami.

Działania na arenie międzynarodowej

- Warsztat dla sektora energii współrealizowany z DoE USA - grudzień 2025 Cel: przekazanie wiedzy bezpośrednio do krajów, by te mogły szkolić swoich ekspertów
- Counter Ransomware Iniciative - Polska jest aktywnym członkiem społeczności CRI
- Mechanizm Talliński - Realizacja projektu w ramach ukraińskiej platformy, w celu wzmocnienie cyberbezpieczeństwa, jej instytucji publicznych
- Podpisanie Memorandum of Understanding - obecnie negocjujemy porozumienia z wieloma krajami Indo-Pacyfiku: Indie, Wietnam, Tajwan, Filipiny, Singapur; W drugiej połowie 2025 planowane jest także podpisanie porozumienia ze Słowenią

Ministerstwo Cyfryzacji

Tu tworzymy przyszłość

Platforma wymiany informacji i harmonizacji KSC

Czym jest System S46?

System S46 jest platformą w portfolio Ministerstwa Cyfryzacji rozwijaną i utrzymywaną przez NASK PIB

System S46 zostanie zaktualizowany i dostosowany po nowelizacji UKSC w 2025. Platforma będzie rozwijana i utrzymywana przez NASK PIB.

Uruchamiamy również Rejestr KSC oraz wprowadzamy możliwość uzyskania dostępu do S46 za pośrednictwem Węzła Krajowego

System S46 aktualnie odpowiada na potrzeby poniżej przytoczonego fragmentu

Artykuł 46 ustawy z dnia 5 lipca 2018 roku o Krajowym Systemie Cyberbezpieczeństwa (**KSC**)

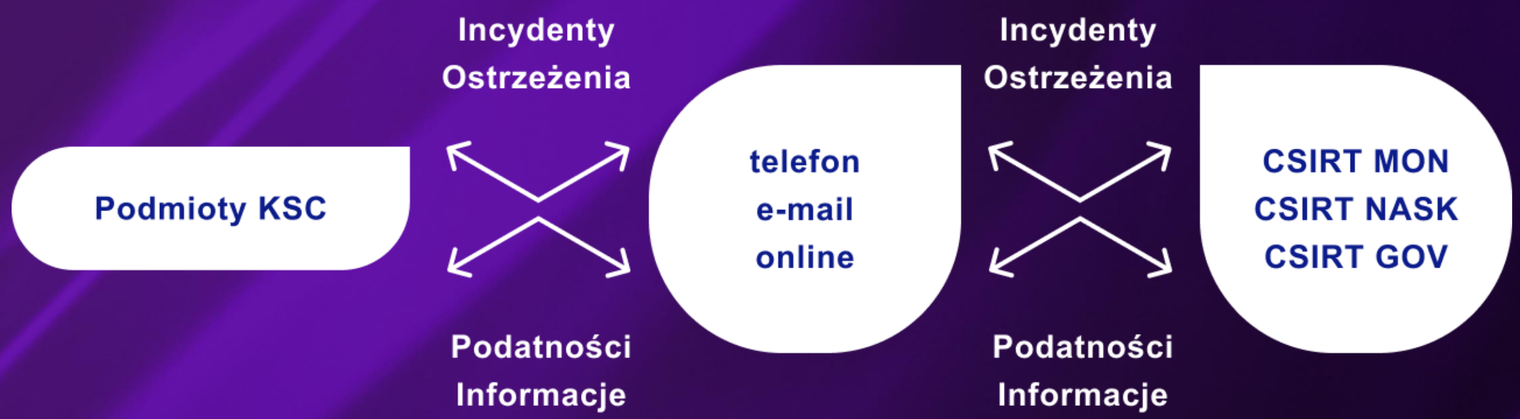
1. Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:
   1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
   2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
   3) zgłaszanie i obsługę incydentów;
   4) szacowanie ryzyka na poziomie krajowym;
   5) ostrzeganie o zagrożeniach cyberbezpieczeństwa.

2. CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej mogą korzystać z systemu teleinformatycznego na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.

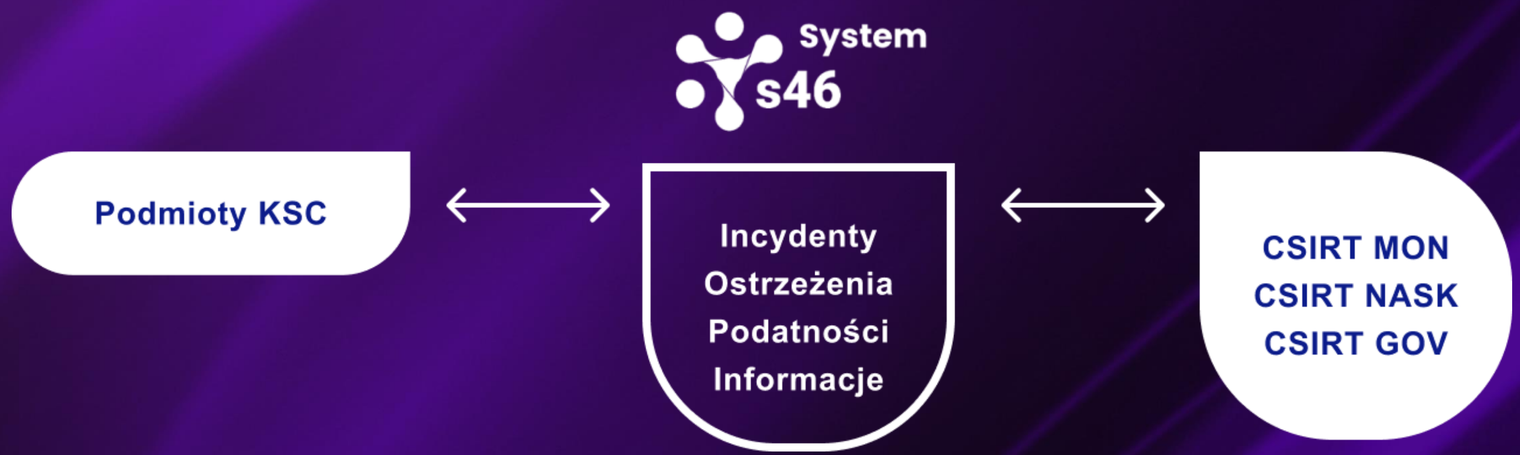
3. W porozumieniu określa się zakres i warunki korzystania z systemu teleinformatycznego.

Po nowelizacji ustawy o KSC

Różne formy wymiany informacji



Jeden kanał wymiany informacji



Cyberbezpieczeństwo a zamówienia publiczne

Projekt Strategii Cyberbezpieczeństwa na lata 2025-2029 zakłada:

- wyłączenie stosowania PZP lub wprowadzenie odrębnego trybu w zakresie zakupu pilnych usług i produktów związanych z cyberbezpieczeństwem
- uwzględnianie certyfikatów cyberbezpieczeństwa wydawanych na podstawie europejskich programów certyfikacji cyberbezpieczeństwa

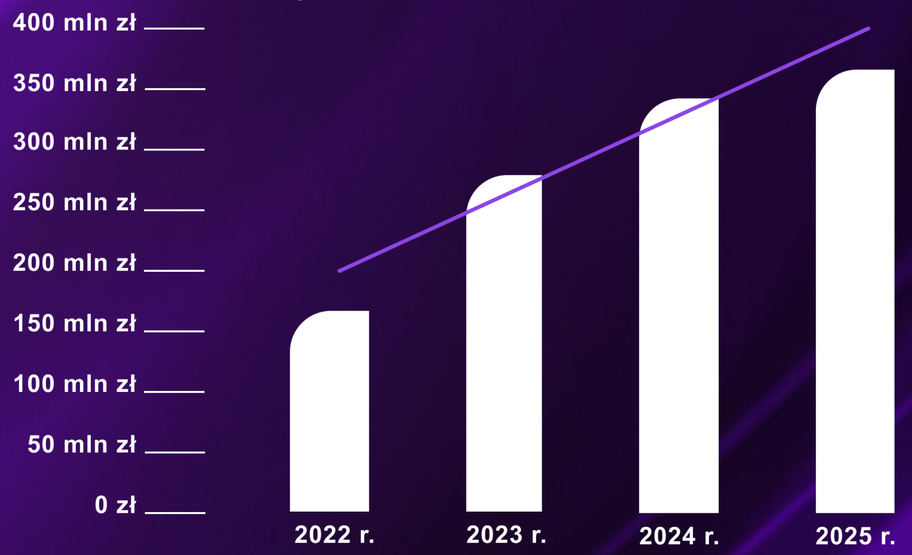
Propozycje zgłoszone przez MC w ramach przeglądu dyrektyw z zakresu zamówień publicznych:

- wyłączenie zakupów związanych z cyberbezpieczeństwem spod wymogów zamówień publicznych, podobnie jak ma to zastosowanie do zamówień obejmujących aspekty obronności lub bezpieczeństwa;
- transparentne rozdzielanie zamówień z zakresu cyberbezpieczeństwa od zamówień IT;
- wprowadzenie mechanizmu uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT i usług ICT oraz specyfikacji tych wymogów;
- wprowadzenie mechanizmu umożliwiającego wyłączenie pilnych zakupów związanych z cyberbezpieczeństwem spod wymogów PZP, co pozwoli uniknąć długotrwałych postępowań przetargowych negatywnie oddziałujących na cyberbezpieczeństwa państwa.

Fundusz Cyberbezpieczeństwa

- Wsparcie działań zmierzających do zapewnienia bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami
- Środki Funduszu przeznacza się na świadczenia teleinformatyczne, tj. dodatki do wynagrodzenia za pracę, a w przypadku funkcjonariuszy i żołnierzy zawodowych - świadczenia pieniężne
- Świadczenia teleinformatyczne mogą zostać przyznane osobom realizującym zadania z zakresu cyberbezpieczeństwa
- Pracujemy nad zwiększeniem finansowania Funduszu do **500 000 000,00 zł** środków z dotacji z budżetu państwa, tj. zwiększenie dotacji o 100%.

Budżet Funduszu Cyberbezpieczeństwa



	2022 r.	2023 r.	2024 r.	2025 r.
Budżet	170 mln zł	287 mln zł	346 mln zł	355 mln zł
Liczba beneficjentów	34	79	112	153

Ministerstwo Cyfryzacji

Tu tworzymy przyszłość

Łukasz Wojewoda

Dyrektor

Dziękujemy za uwagę!