Kancelaria Prezesa Rady Ministrów

Administracja samorządowa - współpraca w zakresie cyberbezpieczeństwa państwa. Rola i obowiązki jednostek samorządowych w kontekście ustawy o krajowym systemie cyberbezpieczeństwa (KSC)

Łukasz Wojewoda
Dyrektor Departamentu Cyberbezpieczeństwa KPRM

Kancelaria Prezesa Rady Ministrów

Czy samorządy mają co chronić?

Gmina:

- wydawanie dowodów osobistych
- nadawanie numerów pesel
- prowadzenie rejestracji urodzeń i zgonów
- wypłacanie świadczeń alimentacyjnych i rodzinnych

Powiat:

- wydawanie prawa jazdy
- rejestrowanie pojazdów
- wydawanie pozwoleń na budowę

Urząd marszałkowski:

- przyjmowanie zgłoszeń i **zatwierdzanie prac geodezyjnych**
- **wydawanie stypendiów** marszałka dla najzdolniejszych uczniów i sportowców z danego województwa
- Wyodrębnione procesy wewnątrz urzędu

Wewnątrz urzędu:

- **sprawy komunalne**, np. przyznawanie i monitorowanie mieszkań komunalnych, prowadzenie rejestru dłużników
- **księgowość**
- **kadry i płace**

Statystyki a życie ?
Rosnąca liczba ataków na samorządy

Kancelaria Prezesa Rady Ministrów

Polskie Radio 24.pl | Polska | Świat | Gospodarka | Sport | Historia | Nauka | Kultura | more_h

Twoje pieniądze | Praca i Firma | Infrastruktura | Rolnictwo | Energetyka

odarka

Hakerzy chcą okupu od urzędników z Kościerzyny. Czym jest ransomware?

POLSKIE RADIO 24

Urząd Gminy w Kościerzynie padł ofiarą hakerów. Internetowi przestępcy włamali się na serwery, zablokowali systemy kompute oraz dane i zażądali od samorządowców okupu za zdjęcie blokady spowodował, że wielu spraw w urzędzie nie da się załatwić, a wyp zasiłków opóźniła się. Urzędnicy padli najprawdopodobniej ofiarą ransomware - złośliwego oprogramowania, które w ostatnich lata stało się popularnym wśród ataków narzędziem do wymuszania pieniędzy.

TVP3 ŁÓDŹ | Aktualności | Program TV | Dział Reklamy | Patronaty | Więcej

dla Ciebie i całej rodziny !

www.toya.net.pl Infolinia: 42 6333 888

Hakerski atak na Urząd Gminy w Lututowie

2019-12-19 | LUTUTÓW (POW. WIERUSZOWSKI)

UDOSTĘPNIJ:

NAJNOWSZE INFORMACJE

NAUKA I ZDROWIE
Chirurg z Pabianic przegrał walkę z koronawirusem

NA SYGNALE
Była pracownica sądu wyłudziła ze skarbu państwa pół miliona zł. Usłyszała 87 zarzutów

POLITYKA
Mateusz Morawiecki: 10 tys. nowych miejsc covidowych w szpitalach tymczasowych

NA DROGACH
Nie ustają prace przy stadione ŁKS. Nocą, autostradą A1 i przez Łódź przewieziono fragmenty dachu

geoforum.pl

Geodezja | GNSS | GIS | Mapy | Teledetekcja | Narzędzia | Firma | Wojsko | Prawo | Przetargi | Geowiedza | Geodane

PRENUMERATA TRADYCYJNA

PRENUMERATA CYFROWA

Październik 2020 Nr 10 (305)

»» wiadomości »

|2020-10-08| Geodezja

To już miesiąc paraliżu chełmińskiej geodezji [AKTUALIZACJA]

Od kilku tygodni w PODGiK-u w Chełmnie (woj. kujawsko-pomorskie) geodeci nie są w stanie załatwić żadnej sprawy – zarówno elektronicznie, jak i tradycyjnie na miejscu w urzędzie. Wszystkiemu, jak się okazało, winien jest atak hakerski.

O całej sprawie poinformował nas jeden z czytelników Geoforum.pl, który skarżył się, że od kilku tygodni nie jest w stanie zgłosić nowej pracy czy

Po Otwocku, Nowinach, Konstancinie-Jeziornie i Krakowie najnowszy atak ransomware – 5 grudnia 2022 r. skierowany w Urząd Marszałkowski Województwa Mazowieckiego

Kancelaria Prezesa Rady Ministrów

Kancelaria Prezesa Rady Ministrów

Skutki ataku – przykłady:

- **Utrata danych (wszelkiego typu), w tym unijnych**
- **Brak możliwości świadczenia usług**
- **Opóźnienia w wypłatach świadczeń (np. zasiłki)**
- **Utrata bazy danych mieszkańców gminy**
- **Utrata zaufania obywateli**
- **Koszty finansowe**
- **Odpowiedzialność karna z tytułu RODO**

Jak chronione są strony internetowe samorządów? Wyniki badania CSIRT NASK

- **Ponad 50% zbadanych stron internetowych JST jest podatna na krytyczne problemy bezpieczeństwa (ostatnie badania z roku 2020)**
- **W 2021 zespół CSIRT NASK odnotował 124 incydenty dot. zagrożenia ransomware, w tym 13 incydentów dotyczyło JST**
- **W 2022 do końca listopada zostało zarejestrowanych 77 incydentów dot. zagrożenia ransomware, w tym 7 w JST**
- **W 2021 zespół CSIRT NASK otrzymał 610 zgłoszeń od JST, natomiast w 2022 do końca listopada było to już 1077 zgłoszeń**

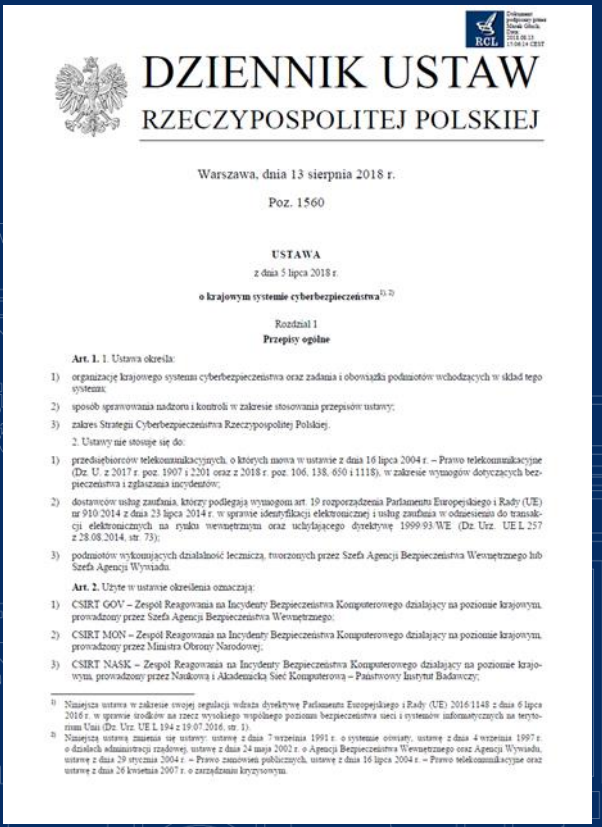
Ile jednostek (JST) przekazało do CSIRT NASK dane osób kontaktowych z podmiotami KSC?

Dane NASK-PIB z dnia 10.12.2022 r.:

- **14 z 16 urzędów marszałkowskich (87,5%)** - brak zgłoszeń z województwa kujawsko-pomorskiego i wielkopolskiego
- **237 z 314 starostw powiatowych (75%)**: najmniej w województwie małopolskim (58%), najwięcej w województwie warmińsko-mazurskim (95%)
- **1995 z 2477 urzędów gmin (81%)**: najmniej w województwie mazowieckim (69%), najwięcej w województwie warmińsko-mazurskim (87%)

Obowiązki JST związane z cyberbezpieczeństwem

- wyznaczenie **osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa** (art. 21)
- **zgłaszanie incydentu niezwłocznie,** nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT - w przypadku JST jest to CSIRT NASK
- **zapewnienie obsługi incydentu** w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe



DZIENNIK USTAW
RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 13 sierpnia 2018 r.

Poz. 1560

USTAWA
z dnia 5 lipca 2018 r.
o krajowym systemie cyberbezpieczeństwa

Rozdział 1
Przepisy ogólne

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.
2. Ustawy nie stosuje się do:
1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138, 650 i 1118), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;
2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73);
3) podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.
Art. 2. Użyte w ustawie określenia oznaczają:
1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
2) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;
3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;

1) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę 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 (Dz. Urz. UE L 194 z 19.07.2016, str. 1).
2) Niniejsza ustawa zmienia nie ustawy: ustawę z dnia 7 września 1991 r. o systemie oświaty, ustawę z dnia 4 września 1997 r. o działach administracji rządowej, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

Kancelaria Prezesa Rady Ministrów

Czy mój podmiot jest objęty KSC?

- **Co zrobić, jeśli podejrzewamy, że nasza jednostka należy do krajowego systemu cyberbezpieczeństwa?**
- **Po pierwsze należy zadać sobie pytanie: Czy mój podmiot realizuje chociaż jedno zadanie publiczne zależne od systemu informacyjnego?**
- **Jeśli TAK – jednostka objęta jest KSC, np. szkoła poprzez korzystanie z dziennika elektronicznego Librus; osobę kontaktową zgłasza za pośrednictwem gminy (art. 21 ust. 1) lub samodzielnie (art. 21 ust. 3)**

Incydent wg KSC

- **incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo**
- **incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15 ustawy o krajowym systemie cyberbezpieczeństwa (KSC)**

Gdzie zgłaszać incydenty ?

Jeżeli incydent wystąpił w służbowej sieci lub urządzeniu, niezwłocznie powiadom o tym zespół IT lub przełożonego i podążaj za ich wskazówkami

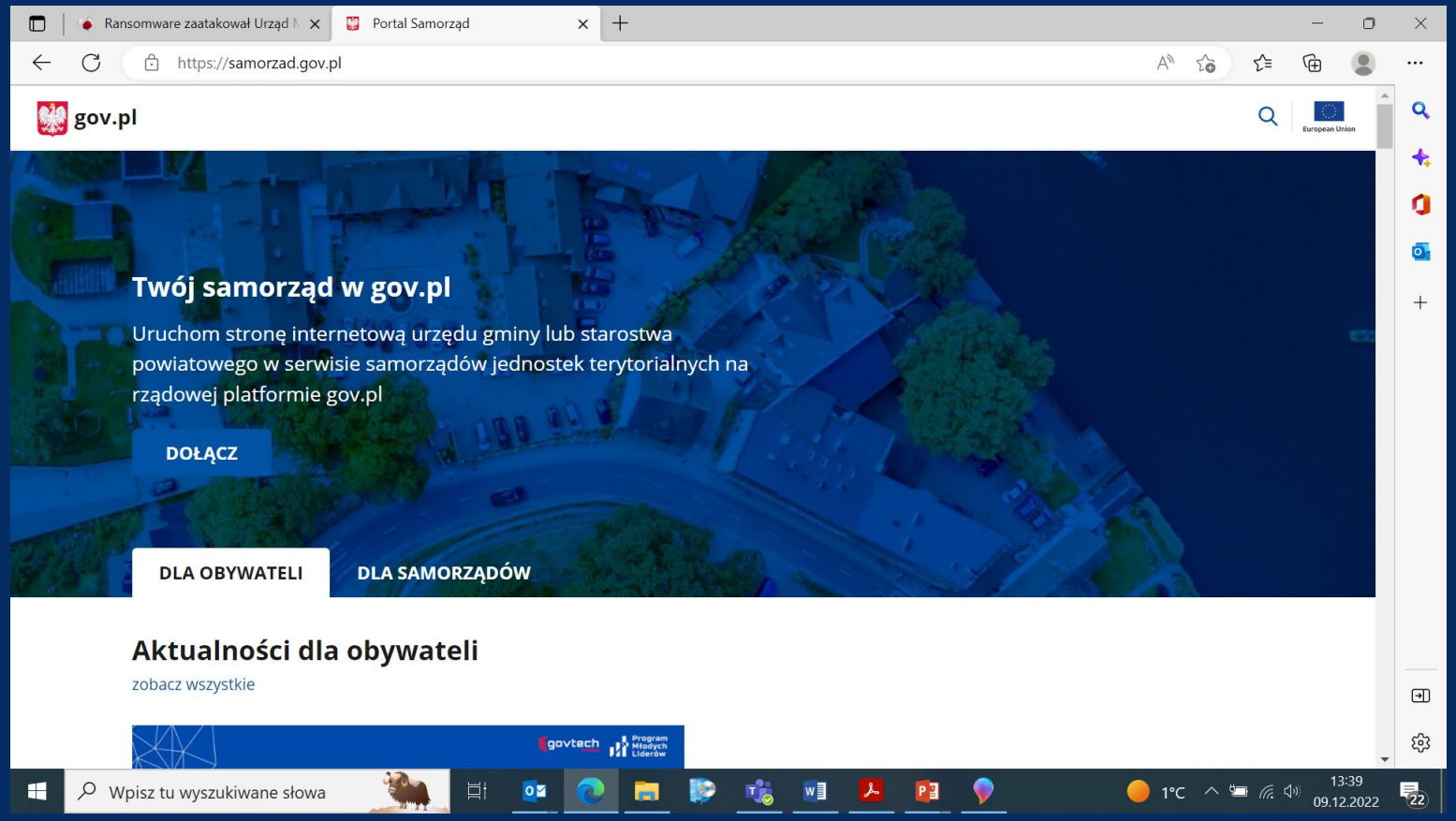
Obowiązek zgłaszania incydentów przez wyznaczoną osobę do CSIRT NASK

Zgłaszanie incydentów - https://incydent.cert.pl/

Kancelaria Prezesa Rady Ministrów

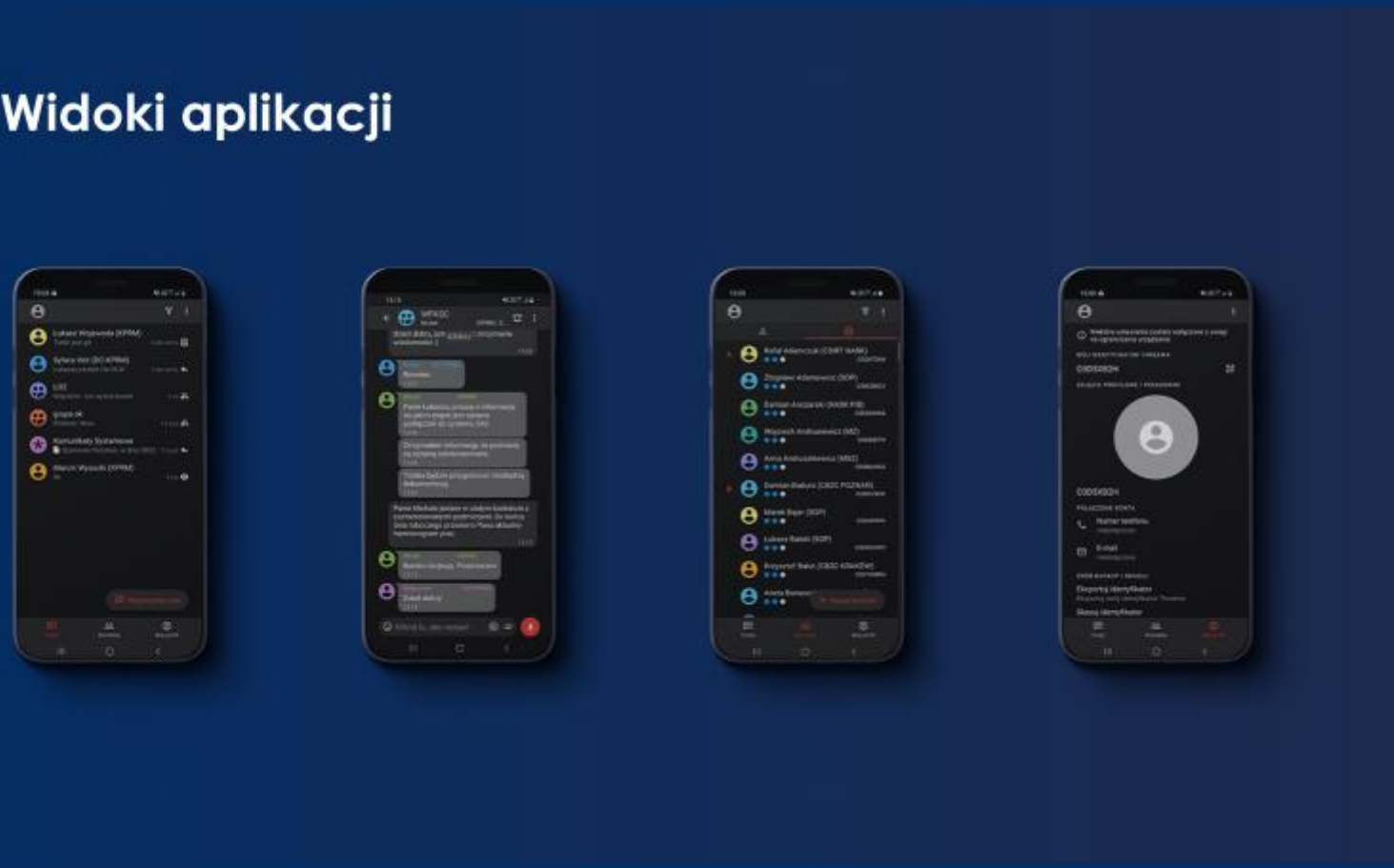
Propozycja dla JST w zakresie usług informacyjnych dla obywateli

https://samorzad.gov.pl/



Komunikator

- Threema OnPrem
- Bezpieczny darmowy komunikator dla administracji publicznej



Bezpłatne szkolenia online

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

Szkolenia dla samorządu

- Pilotażowy projekt prewencyjno-edukacyjny z zakresu cyberbezpieczeństwa dla przedstawicieli JST w województwie podlaskim - działanie na rzecz podniesienia poziomu cyberbezpieczeństwa JST, w ramach którego:
  - eksperci NASK PIB przeprowadzają specjalistyczne szkolenia z obszaru cyberbezpieczeństwa dla przedstawicieli organów JST w województwie podlaskim
  - założono przeszkolenie 570 osób (95% grupy docelowej zapisało się na szkolenie). Szkolenia będą kontynuowane na większą skalę od 2023 r. Obecnie trwają prace nad planowaniem ww. działań szkoleniowych w latach 2023-2024

Kancelaria Prezesa Rady Ministrów

System S46 – nowoczesna platforma wymiany informacji

Celem jest podłączenie wszystkich podmiotów KSC

Możliwość finansowania inwestycji w sprzęt i łącza

- kilkadziesiąt podmiotów KSC planowanych do podłączenia z dotacji celowej na System S46 w kolejnych latach
- co najmniej 100 podmiotów publicznych planowanych do podłączenia z REACT-EU w latach 2022-2023
- blisko 400 podmiotów KSC planowanych do podłączenia z KPO w latach 2022-2026

Kancelaria Prezesa Rady Ministrów

Dyrektywa NIS2

- Dyrektywa dyrektywa NIS 2 – to nowelizacja dyrektywy NIS, pierwszego europejskiego prawa w zakresie cyberbezpieczeństwa.

- Jedną ze zmian jest dodanie nowych sektorów kluczowych, np. **administracji publicznej**, w tym:
- podmiotów administracji publicznej w ramach instytucji rządowych na szczeblu centralnym zdefiniowanych przez państwo członkowskie zgodnie z prawem krajowym
- podmiotów administracji publicznej **na szczeblu regionalnym** zdefiniowanych przez państwo członkowskie zgodnie z prawem krajowym**(w tym JST)**

RegioSOC z KPO - utworzenie sieci 7 regionalnych centrów cyberbezpieczeństwa

- realizacja w latach 2023-2026 na poziomie regionów
- cel: ochrona JST oraz innych podmiotów (m.in. podmiotów komunalnych) przed naruszeniami bezpieczeństwa poprzez identyfikację, analizę i reagowanie na zagrożenia i ataki cyberbezpieczeństwa
- w NASK-PIB rozbudowana zostanie zdolność do prowadzenia analiz i możliwość wymiany informacji między RegioSOC-ami

CYBER-GMINA z KPO - wsparcie 400 podmiotów w zakresie modernizacji i rozbudowy infrastruktury cyberbezpieczeństwa

- **realizacja w latach 2023-2026**
- Cel: wzmocnienie potencjału oraz modernizacja systemów IT oraz OT, w tym infrastruktury (sprzęt) oraz oprogramowania w podmiotach publicznych pod kątem zapewniania cyberbezpieczeństwa w gminach.
- **Kryteria**:
- Dochód gminy na jednego mieszkańca poniżej średniej krajowej (kryterium punktowane w przypadku najniższego dochodu na mieszkańca)
- Przeprowadzenie audytu Cyberbezpieczeństwa (kryterium punktowane w przypadku przeprowadzonych audytów)

KRAJOWY PLAN ODBUDOWY

Dziękuję za uwagę

sekretariat.dc@mc.gov.pl