Wpływ incydentów na działanie samorządu terytorialnego

Seminarium nt. „Cyberbezpieczeństwo w jednostkach samorządu terytorialnego”, 29 czerwca 2021

Jakub Dysarz, DG CONNECT

Dzień dobry!

- Jakub Dysarz, naczelnik wydziału w Departamencie Cyberbezpieczeństwa, w KPRM; obecnie oddelegowany do DG CONNECT w Komisji Europejskiej
- Byłem członkiem zespołu pracującego nad ustawą o krajowym systemie cyberbezpieczeństwa.
- Obecnie pracuję z tzw. dużymi incydentami w skali Unii Europejskiej.

Co dziś omówimy?

- Dlaczego samorządy są atakowane?
- Studia przypadku
  - Brak zabezpieczeń
  - Ignorowanie problemu
  - Mały incydent, poważne skutki
  - Płacenie przestępcom
- Wnioski

Zamiast wstępu

Dlaczego samorządy muszą się polubić z cyberbezpieczeństwem?

European Commission

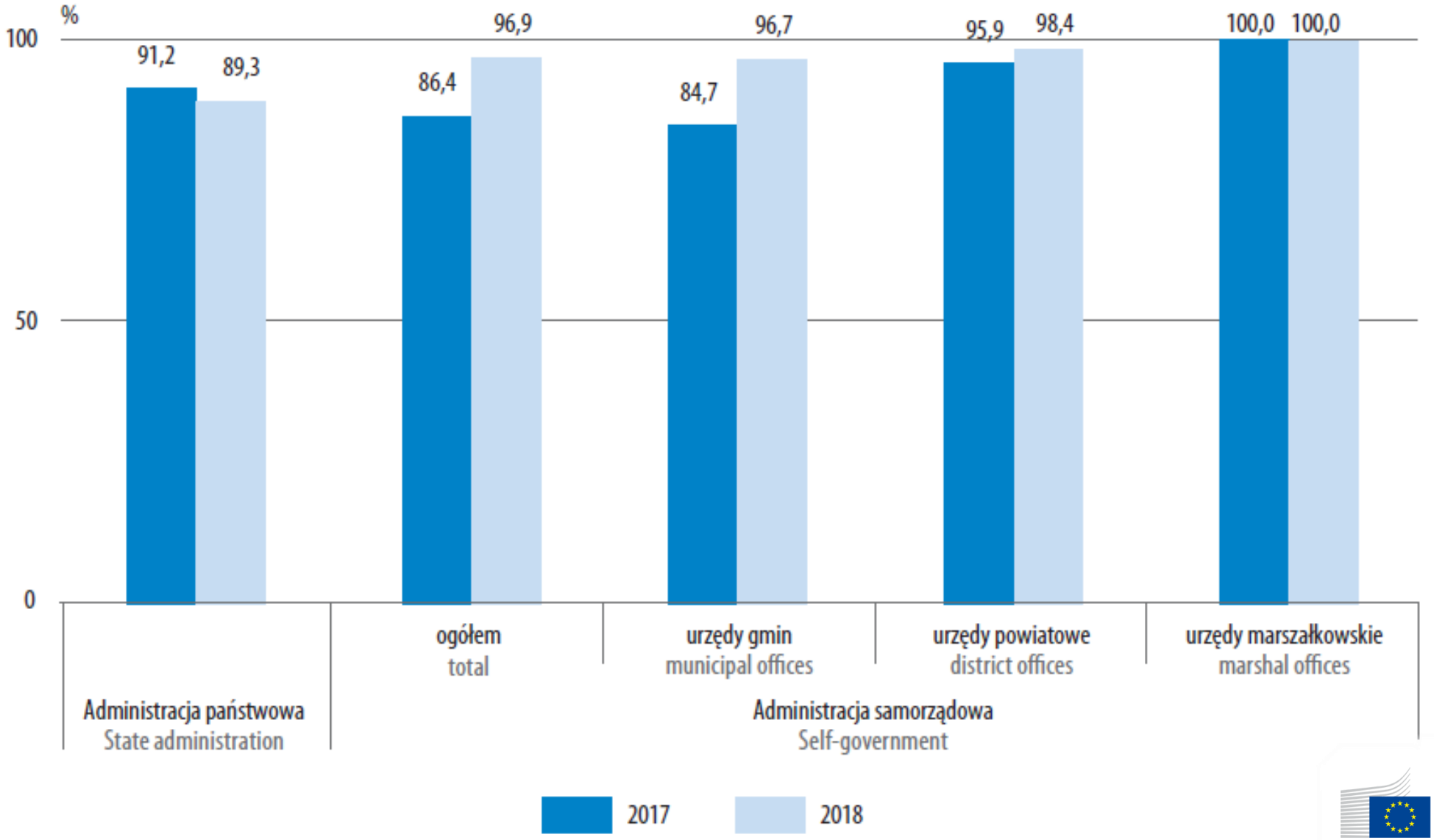
Samorządy w Polsce

- **16 województw**
- **314 powiatów**
- **66 miast** na prawach powiatu
- **2478 gmin**

European Commission

Jednostki administracji publicznej udostępniające obywatelom usługi przez Internet według rodzaju jednostek

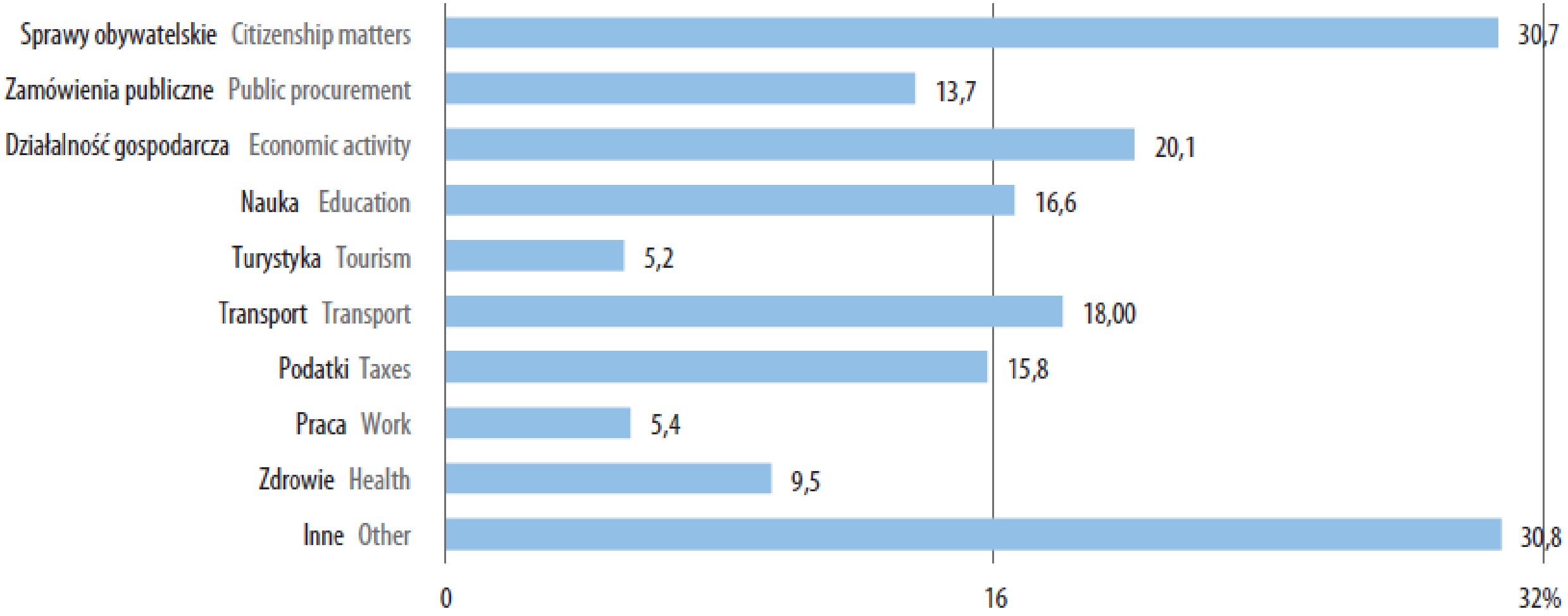
Public administration units providing citizens services via Internet by type of units



European Commission

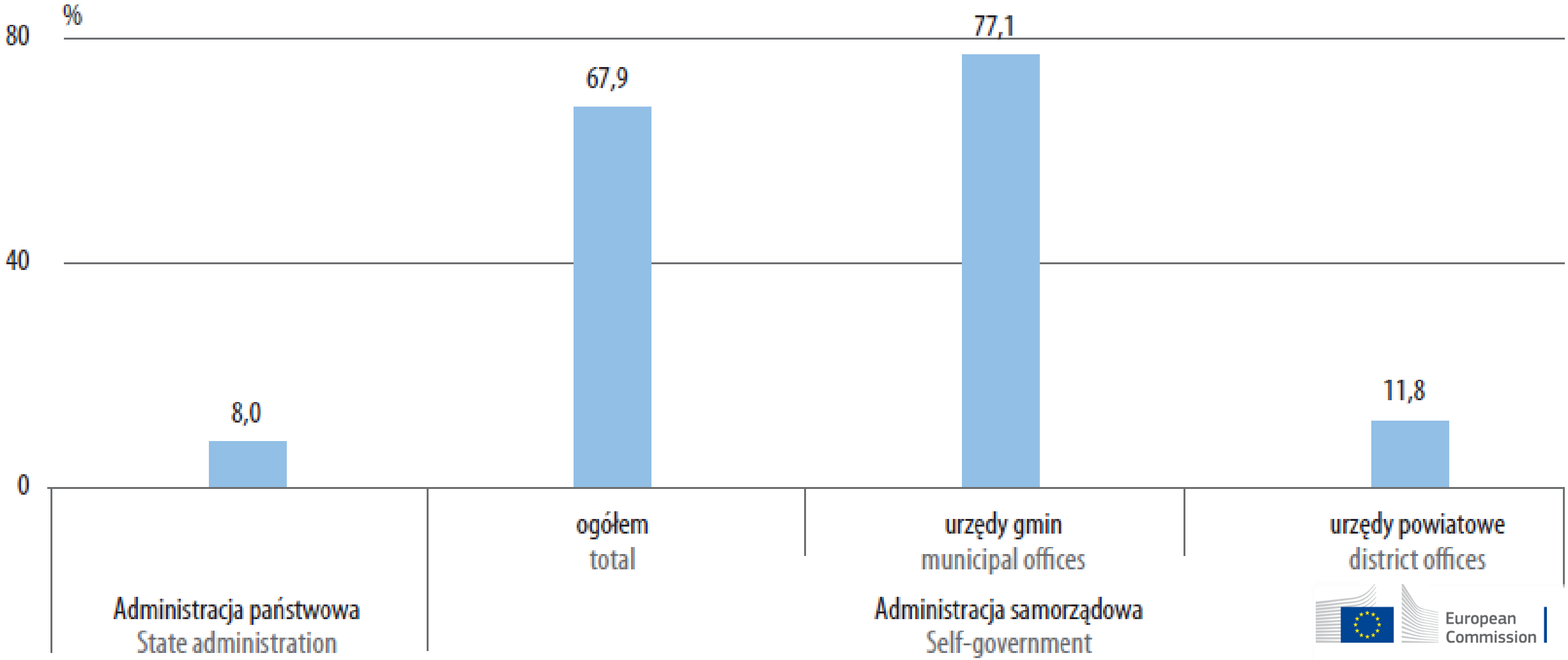
Jednostki administracji samorządowej świadczące usługi elektroniczne na poziomie interakcji dwukierunkowej według obszarów usług (w % jednostek administracji samorządowej świadczących usługi elektroniczne) w 2018 r.

Self-government administration units providing electronic services at the level of two-way interaction by service area (in % of self-government administration units providing electronic services) in 2018



Jednostki administracji publicznej umożliwiające składanie wniosku „Rodzina 500+” według rodzaju jednostki w 2018 r.

Public administration units enabling the submission of the "Family 500+" application by type of unit in 2018



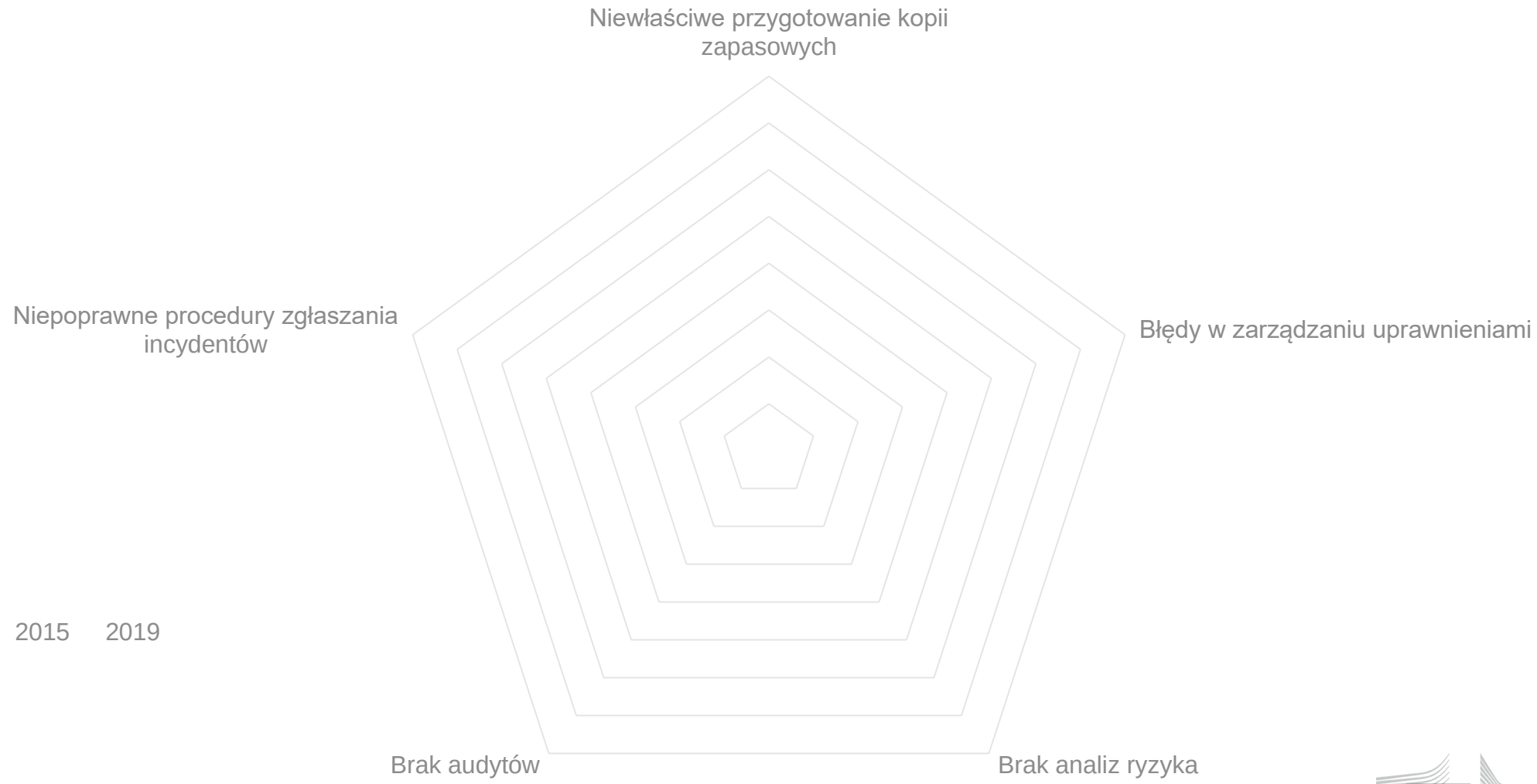
European Commission

Diagnoza NIK

- **Brak systemowego podejścia do zapewnienia bezpieczeństwa informacji** w JST;
- **Mała świadomość problematyki cyberbezpieczeństwa**, w tym obowiązujących przepisów prawa, szczególnie w odniesieniu do kierownictwa małych gmin wiejskich i miejsko-wiejskich;
- **Jeśli świadomość w tym zakresie istnieje**, to często nie wiadomo co zrobić aby zapewnić cyberbezpieczeństwo na wymaganym poziomie;
- **Nawet jeśli wiadomo co i jak** można zrobić w zakresie cyberbezpieczeństwa, to brakuje ludzi i środków finansowych.

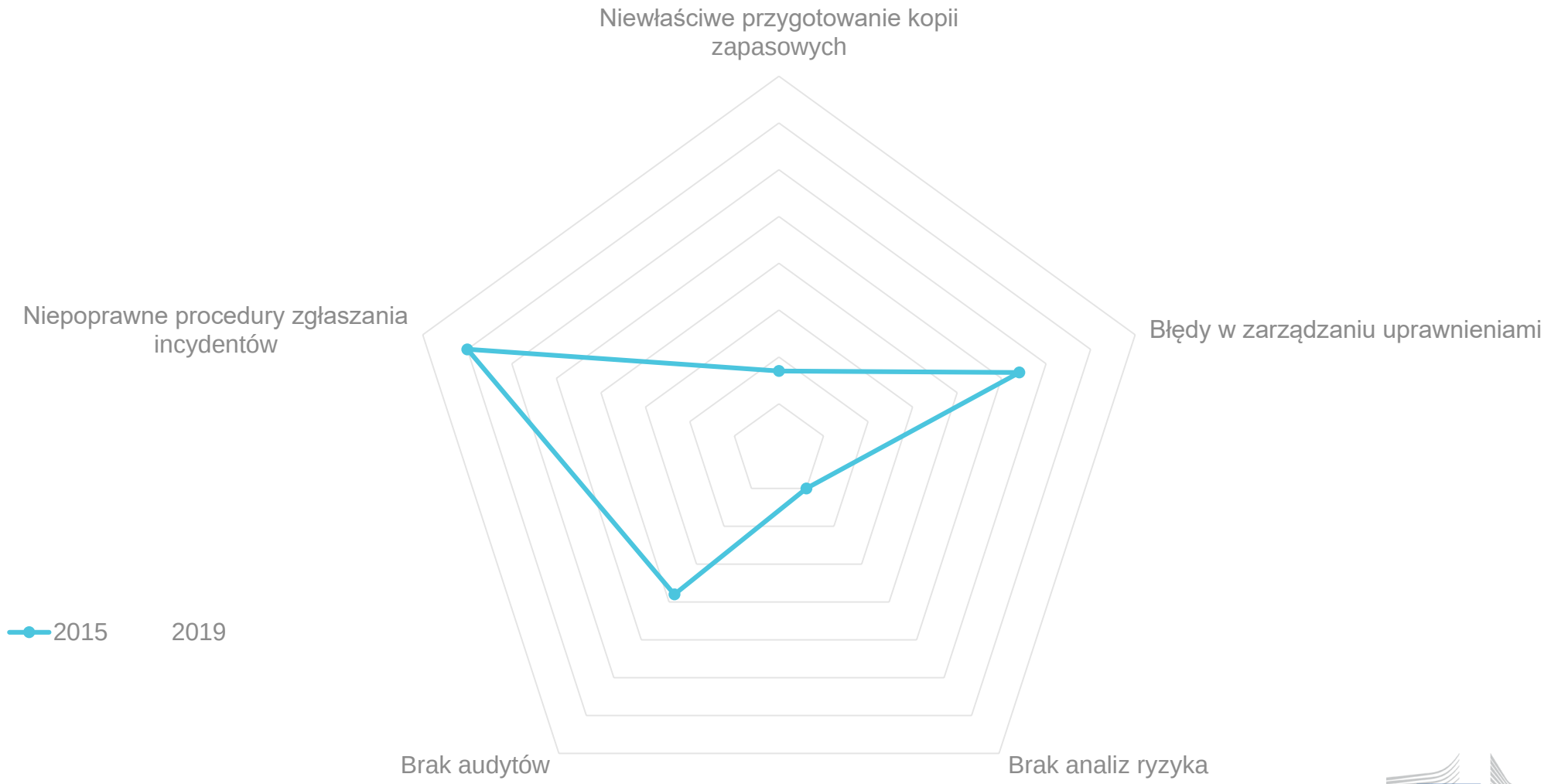
European Commission

Problemy zidentyfikowane przez NIK



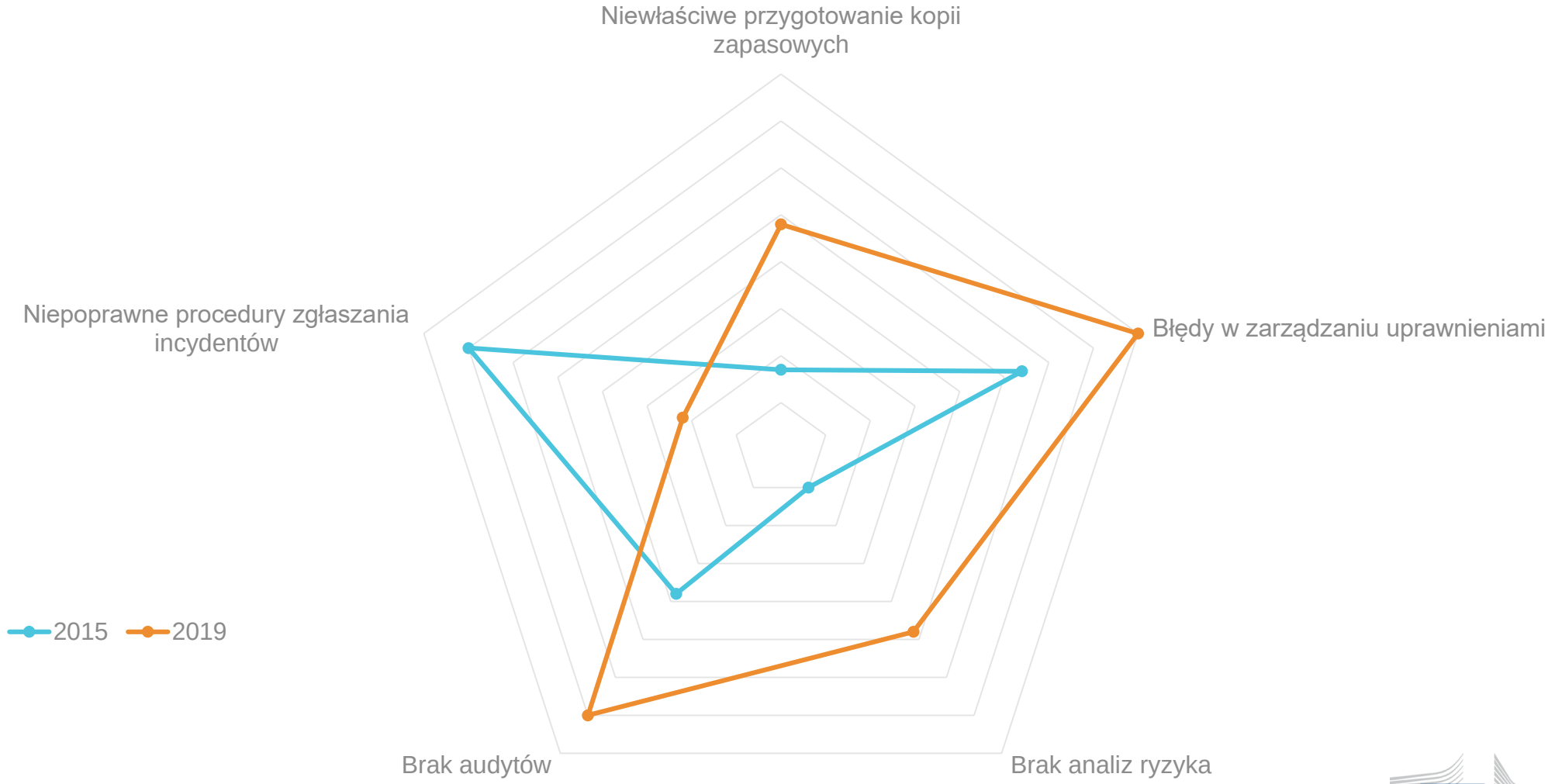
European Commission

Problemy zidentyfikowane przez NIK



European Commission

Problemy zidentyfikowane przez NIK



European Commission

Kościerzyna

Historia o braku zabezpieczeń

European Commission

Zaszyfrowane pliki i żądanie okupu

- Gmina Kościerzyna została zaatakowana szkodliwym oprogramowaniem szyfrującym pliki i żądającym okupu za ich odszyfrowanie.
- Uniemożliwia to korzystanie z systemów IT – w efekcie z usług publicznych.
- Przestępcy często żądają okupu w kryptowalutach.
- Atakują małe podmioty, bo tam są słabsze zabezpieczenia.
- Zaszyfrowanych plików nie da się odszyfrować bez klucza. Znane klucze są dostępne m.in. na stronie NoMoreRansom.

Dlaczego doszło do incydentu?

- **Brak świadomości**
  - m.in. brak wiedzy o KSC, brak wiedzy o KRI
- **Brak przygotowania i zabezpieczeń**
  - m.in. brak ograniczeń korzystania z Internetu przez pracowników
- **Brak wiedzy jak reagować**
  - doszło do częściowego zatarcia śladów

Dotknięte systemy

- **Podatnicy oraz e-Deklaracje**
- **Dane GOPS** - dane klientów, 500+, 300+, zasiłki celowe, wywiady rodzinne
- **Księgowość** - dane klientów urzędu
- **Rejestry dłużników** - podatkowych i alimentacyjnych
- **Kadry i płace** - wypłaty dla pracowników urzędu, szkół, GOPS, etc.
- **Dane klientów zakładu komunalnego** - wodociągi, kanalizacja, mieszkania komunalne, dłużnicy

Konsekwencje incydentu

- Opóźnienia w wypłatach pensji
- Opóźnienia w wypłatach świadczeń
- Obniżona ściągalność podatków lokalnych (istotny dochód gminy)
- Utrata bazy dłużników gminy
- Utrata danych do projektów, w tym unijnych
- Ryzyko niezłożenia sprawozdań (miesięcznych i rocznego)
- Odpowiedzialność prawna z tytułu RODO, dyscypliny finansów publicznych, karnoskarbowa

Inne miasto

Historia o ignorowaniu problemu

Opis incydentu

- Przebieg podobny jak w Kościerzynie – zostały zaatakowane podobne systemy urzędu.
- Różnica – przez brak współpracy z ekspertami, incydent trwał o wiele dłużej (miesiące zamiast dni lub tygodni).
- Urząd próbował poradzić sobie sam, bez pomocy ekspertów (np. z PWCyber)

Skutki

- Lokalna policja zabezpieczyła sprzęt, a nie dane.
- Nie mieli zapasowego sprzętu.
- Przywracanie systemów na tej samej kopii zapasowej powodowało ich wielokrotne szyfrowanie.
- Nie zablokowali kanału wycieku danych i podczas prac naprawczych dane były wyciągane przez przestępców.
- Zamiast podnieść system przez weekend, podnosili go przez 3 miesiące.

Orzysz

Mały incydent, poważne konsekwencje

European Commission

Defacement

- Defacement to rodzaj ataku polegający na podmianie treści na stronie internetowej.
- Zazwyczaj jest to atak prowadzony przez tzw. haktywistów, czyli osoby chcące przekazać określony komunikat ideologiczny (np. polityczny lub społeczny).
- Może też służyć jako narzędzie dezinformacji.

Amerykanie „chwalą” pobyt w Drawsku. „Jedyne czym mogą strzelić to gumki od majtek”

POLSKA I ŚWIAT | 2020-05-24 19:45 | INFORMACYJNA AGENCJA RADIOWA

587f68b545434.p

Zgodnie ze wspólną decyzją Ministerstwa Obrony Narodowej i Departamentu Obrony USA od 5 do 19 czerwca odbędzie się zmodyfikowane polsko - amerykańskie ćwiczenie DEFENDER-Europe 20 Plus. W trakcie ćwiczenia sprawdzona zostanie zdolność współpracy polskich i amerykańskich żołnierzy w ramach wspólnej operacji bojowej.

REPUBLIKA

RAPORTY TV REPUBLIKA | Poland Daily | WIDEO

Portal Republika: To nie był rosyjski atak hakerski. Redakcja jest autorem publikacji

M.N.

14:37 27 maja 2020

Minęła 20 / tvp.info/screenshot

Redakcja portalu Republika podwierdza, że jest autorem publikacji o tytule: Amerykanie „chwalą” pobyt w Drawsku. „Jedyne czym mogą strzelić to gumki od majtek”. Takie same artykuły umieszczone zostały na stronach Telewizji Republika, Radia Szczecin, portalu Olsztyn24.pl, na stronie gminy Orzysz.

European Commission

Poważne skutki

- Strona internetowa urzędu może zostać wykorzystana do szerzenia fałszywych informacji.
- Informacje mogą być przekazywane dalej, wzmacniając przekaz, używając strony urzędu jako wiarygodnego źródła informacji.
  - W przypadku Orzysza, zostały zaatakowane też inne strony m.in. Olsztyn24.com, RadioSzczecin.pl, ePoznan.pl, Niezależna.pl i strona TV Republika.
- Utrata zaufania może mieć poważne skutki dla działania urzędu.

Pewien urząd

Historia o kłopotliwych przetargach

European Commission

Utrata plików

- Przestępcy dostali się do systemów IT pewnego urzędu. Serwer z bazami danych geodezji i kartografii został zaszyfrowany. Łącznie zaszyfrowano ok. 2 TB danych.
- Policja w ramach czynności operacyjnych zajęła sprzęt, uniemożliwiając dokonywanie jakichkolwiek czynności, które mogłyby zmierzać do odzyskania bazy danych.
- Dane były niedostępne przez kilka miesięcy.

Wątpliwe rozwiązanie

- *„Przedmiotem zamówienia jest odzyskanie zaszyfrowanych baz danych (…). Odzyskanie polega na całkowitym odszyfrowaniu danych oraz konwersji danych do bazy wynikowej, która będzie mogła zostać skutecznie zaimportowana do systemu geodezyjnego (…).”*
- Wartość przetargu przekroczyła **pół miliona złotych** przeniesionych z innej części budżetowej.
- Czy podmiot wyłoniony w przetargu był naprawdę w stanie odzyskać dane?

Wnioski

Lepiej zapobiegać niż leczyć

European Commission

Co należy robić?

- Przygotować się!
  - **Rozwiązania są już znane** – regularne kopie zapasowe, aktualizacja oprogramowania, segmentacja sieci, listy zabronionych stron, stosowanie zabezpieczeń…
  - Trzeba pozwolić ekspertom działać! **Bezpieczeństwo idzie z góry, nie z dołu!**
- Zgłaszać incydenty i współpracować z ekspertami.
- Koszty naprawy są wielokrotnie wyższe od zapobiegania.

Dziękuję za uwagę!

Slide 5: map, source: Wikipedia; Slide 23: pictures, source: gov.pl

European Commission