

Tomasz Salachna
Centrum Usług Publicznych
Sieć Badawcza ŁUKASIEWICZ – Instytut Technik Innowacyjnych
EMAG

Aspekty cyberbezpieczeństwa w jednostkach samorządu terytorialnego

23. Konferencja
Miasta w Internecie



Podstawową misją Instytutu Technik Innowacyjnych EMAG jest:

- przewodzenie badań i prac rozwojowych w obszarach szeroko rozumianej informatyki,
przystosowywanie ich wyników do nowych zastosowań,
inicjowanie problemów badawczych w środowiskach spoza sfery nauki, o aplikacyjnym charakterze,
opracowywanie innowacyjnych rozwiązań,
doskonalenie istniejących urządzeń, technologii i systemów przyczyniających się do poprawy efektywności procesów produkcyjnych, wzrostu bezpieczeństwa pracy, jakości życia,
utrzymanie i doskonalenie infrastruktury badawczej i laboratoryjnej służących rozwojowi nauki w obszarach:
- gospodarka – kierunek Przemysł 4.0,
 - **administracja publiczna,**
 - **bezpieczeństwo państwa,**
 - Internet rzeczy,
 - prospołecznych – przeciw wykluczeniu społecznemu.

Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria (KS03C)

Uczestnikami projektu są jednostki naukowo – badawcze funkcjonujące pod nadzorem Ministra Cyfryzacji a mianowicie:

Instytut Łączności – Państwowy Instytut Badawczy (IŁ – PIB)

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB)

Instytut Technik Innowacyjnych EMAG (ITI EMAG).

Jednostki te stworzą system oceny i certyfikacji bezpieczeństwa i prywatności produktów i usług teleinformatycznych, w odpowiedzi m.in. na inicjatywę Komisji Europejskiej mającą na celu utworzenie Europejskich Ram Certyfikacji Bezpieczeństwa i Prywatności dla produktów i usług (zaproponowany w projekcie rozporządzenia Cybersecurity Act).

Samorząd terytorialny – sytuacja krytyczna

Obecnie (stan na 01.01.2019)

Polska dzieli się na:

- 16 województw
- **314 powiatów**
- 66 miast na prawach powiatu
- **2 477 gmin**
 - 302 miejskich w tym:
 - 638 miejsko-wiejskich
 - **1 537 wiejskich**

Regulacje prawne dotyczące ochrony danych osobowych w jednostkach samorządu terytorialnego

Wymóg prawny:

Krajowe Ramy Interoperacyjności Art.20

Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

RODO – UODO w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. IOD – Art. 37

Krajowy System Cyberbezpieczeństwa – „Obowiązki podmiotów publicznych” Art. 21-25, Art. 21, pkt 3. „...możliwość powołania osoby do kontaktu z CSIRT NASK...”



Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego

KAP.430.020.2018

Nr ewidencyjny: P/18/006

Data publikacji: **2019-05-10**

Dział tematyczny: administracja publiczna

Rzeczywisty obraz stanu cyberbezpieczeństwa w samorządach

- Brak systemowego podejścia do zapewnienia bezpieczeństwa informacji
- Brak analiz ryzyka i nieprowadzenie audytów bezpieczeństwa informacji
- Nieprzestrzeganie ustanowionych wymogów w zakresie bezpieczeństwa informacji
- Brak poprawy w zapewnieniu bezpieczeństwa informacji w urzędach j.s.t
kontrole NIK w latach 2014-2016 ujawniły nieprawidłowości w zapewnieniu bezpieczeństwa systemów informatycznych
- **Wdrażanie RODO a zapewnienie bezpieczeństwa informacji** –
Nieprzestrzeganie wymogów dotyczących bezpieczeństwa informacji wynikające z obowiązującego od 2012 r. KRI.
- **Niekompletne procedury ochrony danych** – w 61% urzędach NIK stwierdził brak systemowego podejścia dla zapewnienia bezpieczeństwa informacji, o którym mowa w §20 ust. 1 KRI – nie ustanowiono polityk bezpieczeństwa informacji.

Rzeczywisty obraz stanu cyberbezpieczeństwa w samorządach

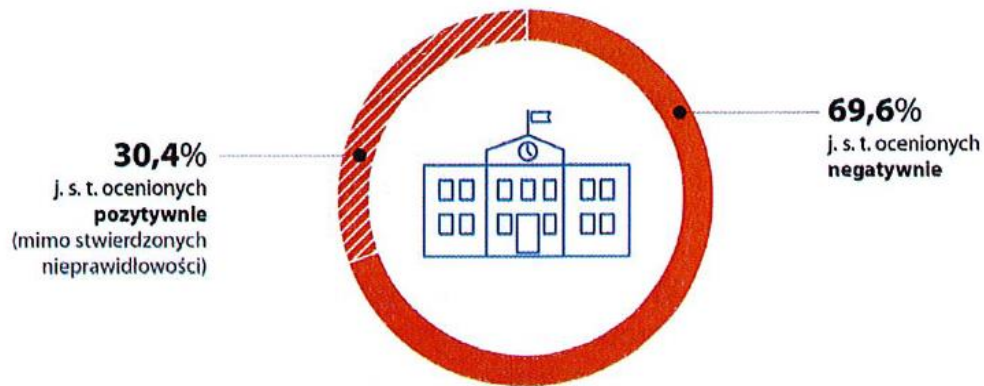
- Niedostosowanie wewnętrznych regulacji do przepisów RODO.
- Realizacja przez IODO innych zadań, mogących wywoływać konflikt interesów – *Art.38 ust.6 RODO*
- Brak informacji lub niepełna informacja o posiadanych zasobach informatycznych – *w 74% skontrolowanych urzędach nie utrzymywano aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania – niezgodne z §20 ust.2 pkt. 2 KRI*
- *Niewłaściwe zarządzanie uprawnieniami użytkowników systemów informatycznych.*
- *Stosowanie niewłaściwych haseł do systemów.*
- *Nieustanowienie zasad pracy mobilnej.*
- *Niewłaściwie zabezpieczenie danych zgromadzonych na urządzeniach mobilnych – w 70% skontrolowanych urzędach nie stosowano szyfrowania dysków twardych komputerów przenośnych.*

Rzeczywisty obraz stanu cyberbezpieczeństwa w samorządach

- Niewłaściwe zabezpieczenie serwerowni – niezgodne z § 20 ust. 2, pkt 9 KRI
- Brak zapisów w zakresie zachowania poufności informacji w umowach serwisowych – w 52% skontrolowanych urzędach stwierdzono niezgodność z § 20 ust.2, pkt 10 KRI
- Wykorzystywanie oprogramowania nieposiadającego wsparcia producenta – w 56% urzędach stwierdzono niezgodność § 20, ust. 2, pkt 2, lit. a i f KRI
- Niewłaściwe tworzenie kopii zapasowych.
- Brak okresowych analiz ryzyka.
- Nieprzeprowadzanie audytów bezpieczeństwa informacji – w 70% skontrolowanych urzędach stwierdzono niezgodność z § 20, ust. 2, pkt 14 KRI

Rzeczywisty obraz stanu cyberbezpieczeństwa w samorządach

Rodzaje ocen kontrolowanej działalności wykonywanej w badanych j.s.t. [%]



Źródło: Opracowanie własne NIK

Rzeczywisty obraz stanu cyberbezpieczeństwa w samorządach

- Cyberbezpieczeństwo nie jest priorytetem w prognozach finansowych. Brak pozycji w budżetach, a nawet klasyfikacji budżetowej.
- Zagadnienia bezpieczeństwa powierzone są wyłącznie komórkom IT.
- Brak regulacji i standardów co do minimalnego wymaganego poziomu cyberbezpieczeństwa – certyfikacja.
- Brak szacowania ryzyka związanego z posiadaniem danych o istotnym znaczeniu dla funkcjonowania j.s.t.
- Brak możliwości oceny poziomu zabezpieczeń przez decydentów, brak audytów.
- Trudne pozyskanie i utrzymanie specjalistów cyberbezpieczeństwa.
- Brak planów szkoleniowych.
- Minimalne zabezpieczenie (Firewall i Antywirus), które nie pozwalają na neutralizację zaawansowanych cyberataków.

Rzeczywisty obraz stanu cyberbezpieczeństwa w samorządach

O tym jak ważne jest właściwe zabezpieczenie informacji gromadzonych w jednostkach samorządu terytorialnego świadczą przypadki ich utraty nagłośnione przez media w ostatnich latach:

- w ciągu dwóch lat (2013-2014) hakerzy **okradli** pięć polskich gmin, w tym gminę Jaworzno **na prawie milion złotych**;
- w 2014 r. wyciekły dane dzieci z przemyskiego Urzędu Miejskiego;
- w 2017 r. z Urzędu Miasta Łodzi wyciekły dane z tzw. deklaracji śmieciowych, przez co bez problemu można było poznać dane właścicieli łódzkich nieruchomości;
- w 2018 r. wyciekły dane części posiadaczy Karty Krakowskiej.

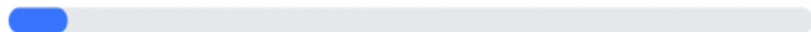
Źródło: <http://samorząd.pap.pl> 2019-05-10

Czy Polska jest przygotowana na cyberatak?

Wyniki ankiety <http://securak.pl> luty 2019

Facebook (głosowało około 3000 osób!)

Czy Polska jest przygotowana na cyberatak?



5% tak

95% nie ✓

Ta ankieta zakończyła się.

Liczba głosów: 3 tys.

Twitter (głosowało 308 osób):

Przypięty tweet



Sekurak @Sekurak · 2 lut

Czy Polska jest przygotowana na cyberatak?

6% tak

94% nie

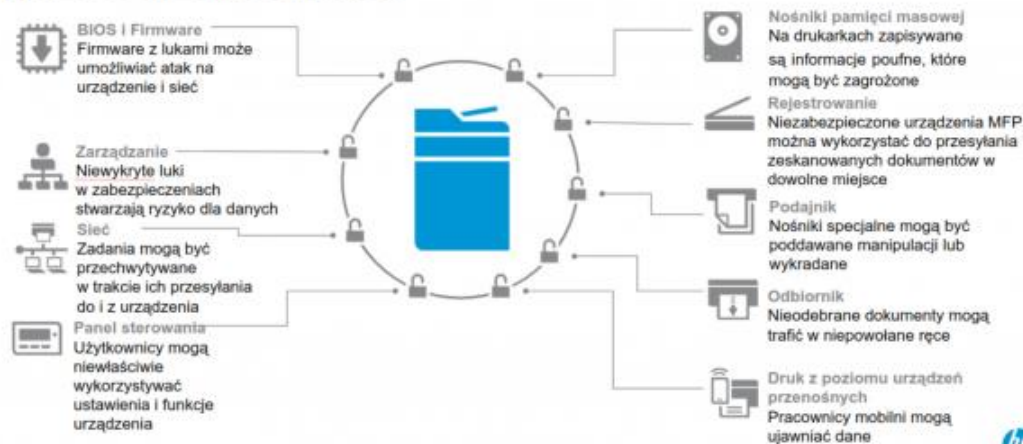
308 głosów • Wyniki końcowe

Zapomniana strefa w procedurach ochronnych



Serwis sprzątający - to też pracownicy
Mało tego - to pracownicy, którzy mają często tak samo łatwy dostęp do firmowej dokumentacji, co „biurowi”.

Typowe luki w zabezpieczeniach rozwiązań do druku i przetwarzania obrazu



Drukarki sieciowe to w większości organizacji najsłabszy punkt w systemie bezpieczeństwa informatycznego.

Dzieje się tak po części z winy producentów oraz po części w wyniku zaniedbań administratorów.

Najślabsze ogniwo w łańcuchu cyberbezpieczeństwa – człowiek



Informatyk w urzędzie



Najsłabsze ogniwo w łańcuchu cyberbezpieczeństwa

Przyczyny:

- Niewiedza.
- Obawy związane z ośmieszeniem się przed personelem.
- Rutyna.
- Brak wdrożonych procedur i ich kontroli.
- Brak uwarunkowań finansowych.
- Brak związania się z jednostką.

Najślabsze ogniwo w łańcuchu cyberbezpieczeństwa – panaceum

Wdrożenie metodyki - HUMAN FIREWALL

- Stałe podnoszenie kwalifikacji oraz świadomości w dziedzinie cyberbezpieczeństwa wśród wszystkich pracowników urzędów poprzez uruchomienie **ogólnopolskiego programu edukacyjnego dla samorządów**.
- Przeprowadzanie okresowych ćwiczeń dla całego personelu (nie tylko IT, ale osób decyzyjnych, sekretarek, kierowców).
- Przeprowadzania kontrolowanych cyberataków, których celem jest opracowanie procedur pozwalających na utrzymanie ciągłości działania systemów informatycznych.

Najsłabsze ogniwo w łańcuchu cyberbezpieczeństwa – panaceum

Ogólnopolski Program Edukacyjny dla Samorządów

- Stowarzyszenie "Miasta w Internecie"
- Instytut Technik Innowacyjnych EMAG
- Naukowa i Akademicka Sieć Komputerowa NASK



“

To, czego szukamy
w naszych ofiarach,
to przede
wszystkim
zaufanie.

KEVIN MITNICK

Najstynniejszy haker na świecie

BUSINESS
INSIDER
POLSKA

Tomasz Salachna
Centrum Usług Publicznych
Sieć Badawcza ŁUKASIEWICZ – Instytut Technik Innowacyjnych EMAG