Konferencja Naukowa

DZIAŁALNOŚĆ W ZAKRESIE CYBERBEZPIECZEŃSTWA. ASPEKTY PRAWNE, ORGANIZACYJNE I TECHNICZNE

Warszawa, 7 sierpnia 2020 r., godz. 10.00-14.00

Platforma komunikacyjna PTI - MS Teams PTI

Zwiększanie efektywności kształcenia: Gra komputerowa Cyberbezpieczeństwo w administracji

Konrad Radomiński

Uniwersytet Kardynała Stefana Wyszyńskiego

Postępująca informatyzacja administracji szanse i zagrożenia

- Ułatwienie społeczeństwu dostępu do zasobów i usług administracji.
  - Dostęp do rejestrów prowadzonych w systemach teleinfromartycznych
  - Możliwość załatwienia wielu spraw, m.in. podatkowych czy wyborczych bez wychodzenia z domu.
- Zwiększenie efektywności pracy administracji.
  - Wiele usług odbywa się automatycznie, dzięki interoperacyjności systemów, dzięki czemu urzędy mają więcej czasu na wykonywanie tych obowiązków do których potrzebny jest człowiek.
- Zwiększone ryzyko.
  - Dane obywateli utrwalone w postaci cyfrowej i dostępne przez Internet mogą być bardziej podatne na wycieki czy kradzieże, przez:
    - Zaniedbania na szczeblu organizacji.
    - Zaniedbania poszczególnych pracowników.

Najwyższa Izba Kontroli o bezpieczeństwie informacji w jednostkach samorządu terytorialnego

- *Kontrole NIK **już w 2014 r. i 2016 r. ujawniły istotne nieprawidłowości** w zapewnieniu bezpieczeństwa systemów informatycznych i zgromadzonych w nich danych o obywatelach. Brak było systemowego podejścia kierowników urzędów do zarządzania bezpieczeństwem informacji oraz właściwego zabezpieczania danych będących w posiadaniu urzędów.* **Pomimo upływu kilku lat nadal nie nastąpiła poprawa w tym zakresie…***
- **70%** skontrolowanych w 2018 r. j.s.t. w wyniku kontroli bezpieczeństwa danych oceniono **negatywnie**,
- Wśród pozostałych **30%** ocenionych pozytywnie, **stwierdzono nieprawidłowości**.

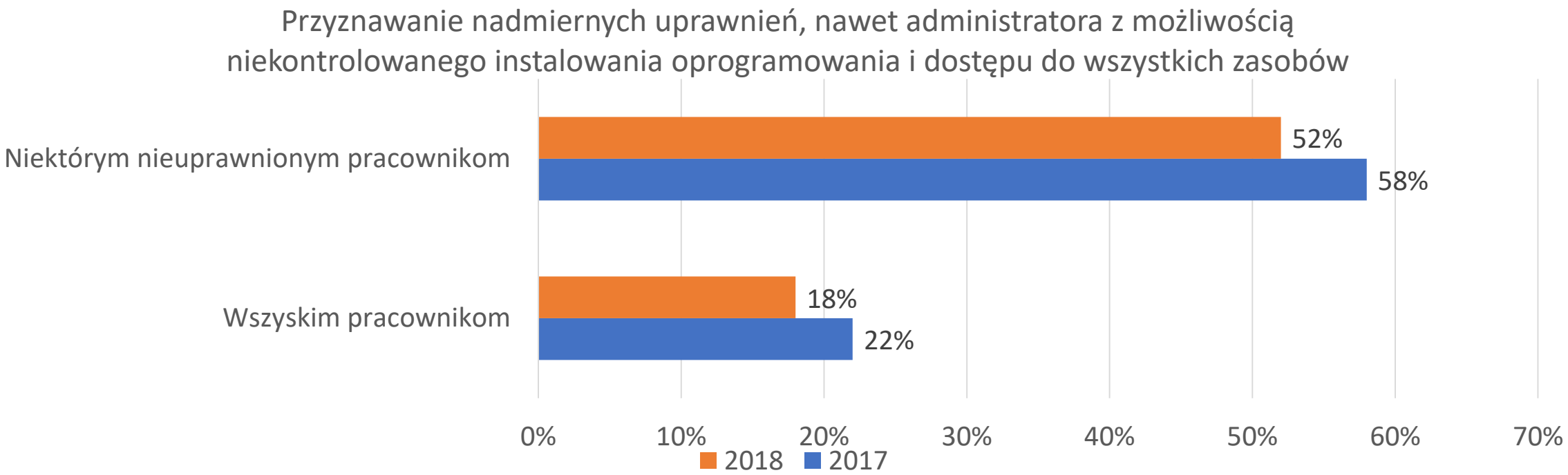
Raport NIK o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego z dnia 10.05.2019 r. – raport za rok 2018.

Najwyższa Izba Kontroli o szkoleniach z zakresu bezpieczeństwa informacji w jednostkach samorządu terytorialnego

- W kontrolowanych j.s.t. skupiano się przede wszystkim na wymogach z RODO, pomijając kwestię bezpieczeństwa informacji.

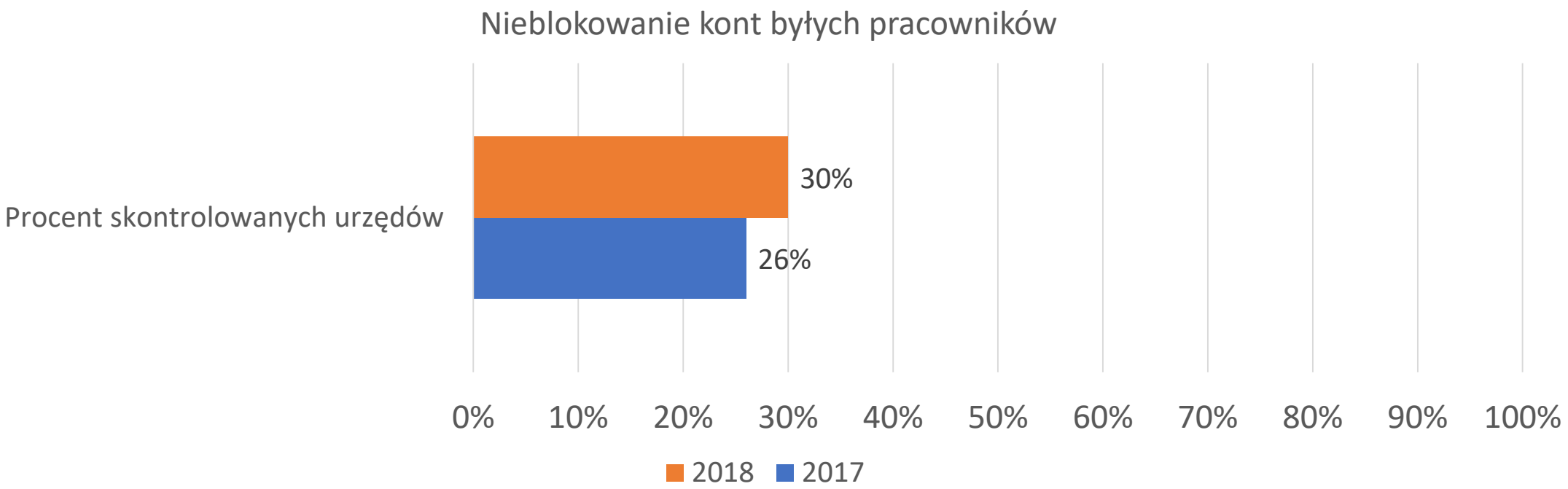
Źródło: Raport NIK *o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego* z dnia 10.05.2019 r.– raport za rok 2018. Raport NIK *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne* z dnia 06.11.2018 r. raport za rok 2017.

Wybrane nieprawidłowości na szczeblu organizacyjnym



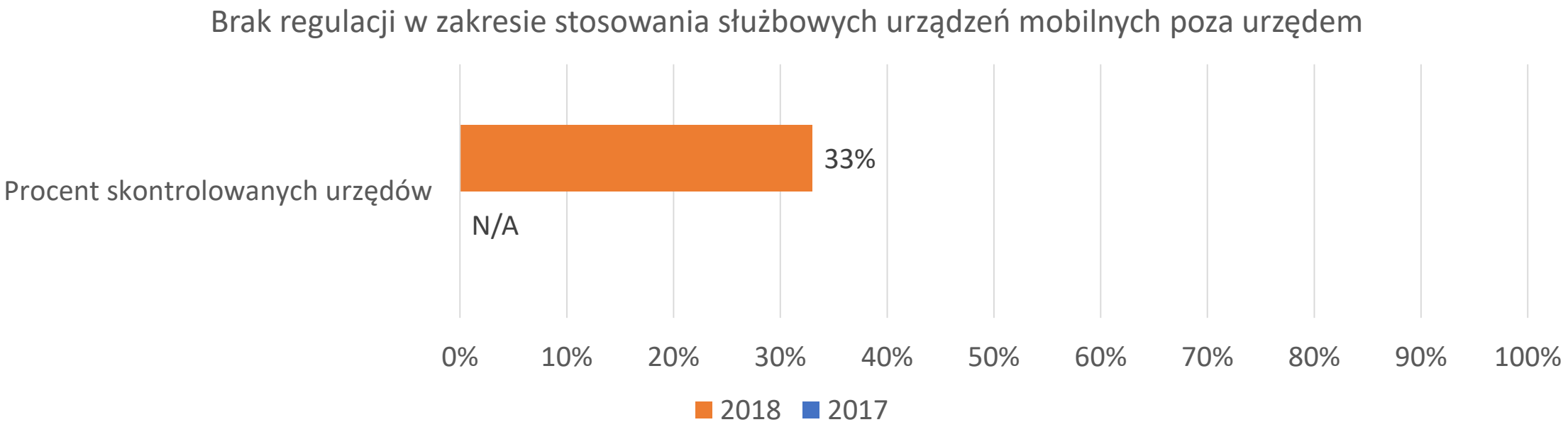
Raport NIK *o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego* z dnia 10.05.2019 r.– raport za rok 2018.
Raport NIK *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne* z dnia 06.11.2018 r. raport za rok 2017.
https://niebezpiecznik.pl/post/sekrety-drukarek-i-kserokopiarek/

Wybrane nieprawidłowości na szczeblu organizacyjnym



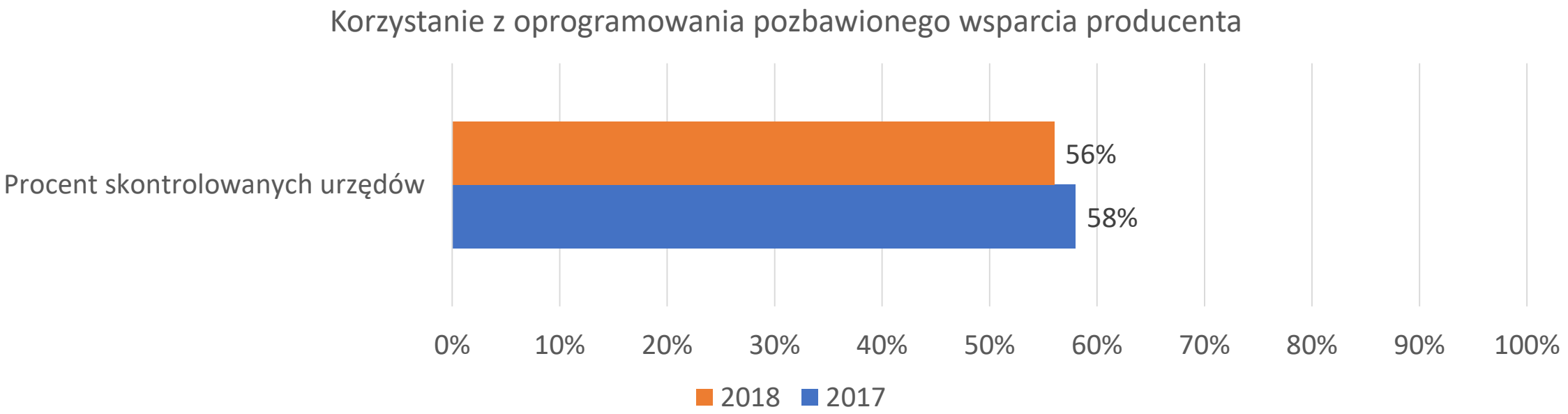
Raport NIK *o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego* z dnia 10.05.2019 r.– raport za rok 2018.
Raport NIK *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne* z dnia 06.11.2018 r. raport za rok 2017.
https://niebezpiecznik.pl/post/sekrety-drukarek-i-kserokopiarek/

Wybrane nieprawidłowości na szczeblu organizacyjnym



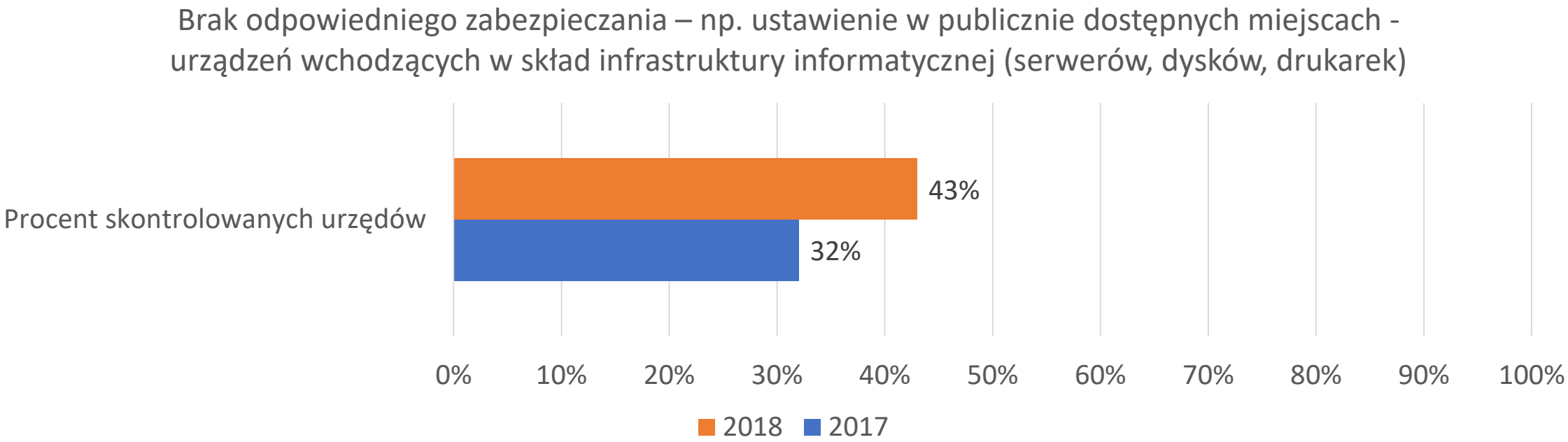
Raport NIK *o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego* z dnia 10.05.2019 r.– raport za rok 2018.
Raport NIK *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne* z dnia 06.11.2018 r. raport za rok 2017.
https://niebezpiecznik.pl/post/sekrety-drukarek-i-kserokopiarek/

Wybrane nieprawidłowości na szczeblu organizacyjnym



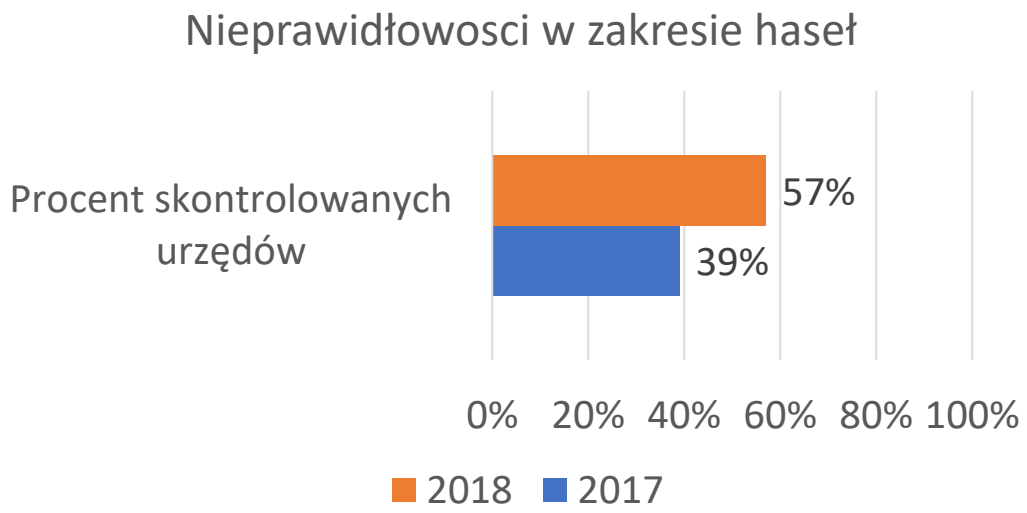
Raport NIK *o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego* z dnia 10.05.2019 r.– raport za rok 2018.
Raport NIK *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne* z dnia 06.11.2018 r. raport za rok 2017.
https://niebezpiecznik.pl/post/sekrety-drukarek-i-kserokopiarek/

Wybrane nieprawidłowości na szczeblu organizacyjnym



Raport NIK *o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego* z dnia 10.05.2019 r.– raport za rok 2018.
Raport NIK *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne* z dnia 06.11.2018 r. raport za rok 2017.
https://niebezpiecznik.pl/post/sekrety-drukarek-i-kserokopiarek/

Wybrane nieprawidłowości na szczeblu pracowników



- Brak haseł.
- Stosowanie zbyt krótkich, oczywistych, haseł.
- Niezmienianie haseł w określonych odstępach czasu

Raport NIK *o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego* z dnia 10.05.2019 r.– raport za rok 2018.
Raport NIK *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne* z dnia 06.11.2018 r. raport za rok 2017.

- Ustawianie ekranów w sposób umożliwiający obsługiwanym osobom wgląd do wyświetlanych danych
- Pozostawiania kart autoryzujących bez należytej ochrony.
- Kradzieże danych lub środków finansowych na skutek:
  - Podłączania nieautoryzowanych urządzeń zewnętrznych.
  - Ataków socjotechnicznych wyłudzających np. hasła – m.in. Phishing.
  - Złośliwego oprogramowania przemycanego w mailach – w plikach udających znane popularne pliki np. tekstowe.
  - Blokowania komputerów służbowych dla wyłudzenia okupu.
  - Podłączania służbowych telefonów do fałszywych „publicznych” ładowarek USB.
  - Podsłuchów infekujących urządzenia w momencie odwiedzenia niezaufanych stron WWW.

Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań, Cyfrowa Polska 2019; Raport PwC „Cyber-ruletka po polsku. Dlaczego firmy z cyberprzestępcami liczą na szczęście”, https://wyborcza.pl/1,155287,20436215,znalazles-pendrive-a-uwazaj-moze-byc-zainfekowany.html,
Raport CSRIT o stanie bezpieczeństwa cyberprzestrzeni RP w 2018 r.

„Wiedza jest, umiejętności nie ma”

- Wielu nieprawidłowości można było uniknąć gdyby pracownicy mieli okazję przećwiczyć zdobytą na szkoleniach **wiedzę** w praktyce – czyli gdyby zdobyli **umiejętności**.
- Nabywanie umiejętności musi odbywać się w **warunkach bezpiecznych**, gdzie błąd nie spowoduje np. wycieku danych.
- Najlepszym sposobem jest przećwiczenie swojej wiedzy w wirtualnym środowisku, symulującym sytuacje, z którymi pracownik może spotkać się w świecie rzeczywistym, tj. w **edukacyjnej grze wideo.**

Zasadność stosowania gier w edukacji pracowników

- **76%** użytkowników Internetu gra w Gry.
- Spośród nich **51%** to osoby zatrudnione na stałe, a **12%** to osoby zatrudnione tymczasowo – razem osoby pracujące stanowią aż **63%** graczy.
  - Jedynie 10% stanowią osoby bezrobotne, pozostałe 27% stanowią osoby bierne zawodowo tj. dzieci, niepracujący studenci i osoby zajmujące się domem.
- **61%** graczy to osoby między 25 a 45 rokiem życia a zatem ponad połowa wszystkich graczy przypada na około **59%** wszystkich osób aktywnych zawodowo i pracujących.
  - Doliczając do tego grupę między 46 a 55 rokiem życia, która stanowi **14%** graczy, to grupa wiekowa 25-55 będzie stanowiła aż **76%** graczy, która będzie przypadał na około **73%** wszystkich osób aktywnych zawodowo i pracujących.
- W badaniach graczy jako oddzielną zbadano grupę *Silver Gamers* czyli Internautów między 56 a 65 rokiem życia. Spośród tych osób aż **52%** osób to gracze. Grupa ta stanowić może minimum **18%** wszystkich osób aktywnych zawodowo i pracujących.

Źródła danych: https://polishgamers.com/pgr/polish-gamers-research-2019/general-information-about-our-study/

http://swaid.stat.gov.pl/RynekPracy_dashboards/Raporty_predefiniowane/RAP_DBD_RPRA_2.aspx

Grywalizacja

- Wykorzystywanie najbardziej lubianych przez graczy i skutecznych z punktu widzenia psychologii behawioralnej mechanizmów znanych z gier lub gier jako takich dla podnoszenia efektywności działań podejmowanych w świecie rzeczywistym.
- Od wielu lat znajduje zastosowanie m.in. w:
  - **Marketingu** – np. różnego rodzaju programy lojalnościowe (użytkownik zbiera punkty, aby wchodzić na wyższy poziom i móc odebrać lepsze zniżki czy nawet nagrody.
  - **Zarządzaniu zasobami ludzkimi** – stawianie przed pracownikami stopniowo coraz trudniejszych zadań (wraz z rozwojem), rywalizacja – np. *leaderboardy*
  - **e-Learningu** – wykorzystanie prostych gier do nauki np. języków, odznaki na platformie Moodle.

Założenia gry edukacyjnej

- Stworzona na urządzenia mobilne!
  - Wybrało je 57% badanych graczy.
  - Korzysta się z nich najczęściej – 44% badanych graczy – dla *zabicia czasu.*
- Stworzona również na PC:
  - Ponieważ takim sprzętem najczęściej dysponują organizacje.
  - Często osobom starszym wygodniej jest korzystać z aplikacji na komputerze, m.in. ze względu na wielkość i przejrzystość wyświetlanych elementów
  - Nie jako aplikacja wymagająca pobrania i instalacji – aby uniknąć potencjalnych kolizji z procedurami bezpieczeństwa w organizacji.
  - **Jako aplikacja przeglądarkowa** – uruchamiana po zalogowaniu się na stronie gry. – aby ułatwić dostęp do gry.
  - Gry uruchamiane na komputerze są najczęściej wykorzystywane (41% badanych) dla celów edukacyjnych.
- Zapewniająca możliwość *crossplay* czyli możliwości wspólnej gry graczy z urządzeń mobilnych i PC – np. wspólny ranking wyników.

Założenia gry edukacyjnej

- Prosta i przejrzysta warstwa audiowizualna.
- Prosta mechanika gry.
  - w grze edukacyjnej nie powinno wymagać się od graczy wykazywania się refleksem i umiejętnością gry pod presją czasu.
- Rosnący poziom trudności zadań wplecionych w fabułę gry.
  - zadania stawiane przed graczem (kolejne umiejętności do nabycia) powinny być stopniowo coraz trudniejsze i złożone, tak aby pracownik nabywał nowe umiejętności krok po kroku (z możliwością powrotu do już nabytych).
- Możliwość dostosowania fabuły do wymań wewnętrznych procedur odbiorcy
  - np. w zakresie haseł.

Założenia gry edukacyjnej

- Powinna zawierać mechanizmy, które z gier rozrywkowych zaczerpnięto – w ramach zjawiska grywalizacji – do realnego świata!
  - **Fabuła z określonym celem głównym**.
    - Np. uratowanie urzędu przed złowrogim *crackerem* – w ramach celu pracownik będzie wykonywał kolejne zadania uczące go kolejnych niezbędnych umiejętności.
  - **Natychmiastowy feedback**
    - Gra musi Informować gracza co zrobił dobrze (np. przez gratulacje) a co źle i dlaczego.
  - **Nagradzanie gracza –**
    - np. przydzielanie punktów za prawidłowe rozwiązywanie zadań i systematyczne logowanie, umożliwiające:
      - Wprowadzenia rankingu graczy
      - Odblokowywania elementów wewnątrz gry np. elementów personalizacji.
      - Zdobywanie osiągnięć widocznych na profilu gracza.
- Reasumując gra edukacyjna powinna być zaprojektowana tak aby:
  - Faktycznie, a nie tylko teoretycznie, była ciekawszą alternatywą dla wielogodzinnych szkoleń.
  - Zachęcała graczy do jak najczęstszego grania czyli uczenia się.

Przykłady wdrożeń gier edukacyjnych w biznesie.

- **IBM's Innov8 –** gra ucząca zarządzania procesami biznesowymi, w której gracz wcielał się w szefa firmy IT i miał za zadanie prowadzić interesy z innymi przedsiębiorcami.
- **Wall Street Survivors –** gra ucząca podstawowych działań na rynku finansowym.
- **"Stepping Up to Management" –** gra stworzona przez **Xerox's**, pozwalająca pracownikom nabyć umiejętności niezbędne na ich stanowisku pracy oraz porównywać swoje wyniki ze współpracownikami.

Przykład wdrożenia gry edukacyjnej dla pracowników: Fabryki Volkswagen-a w Poznaniu

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Społeczny

Pilotażowe demo projektu UKSW *Cyberbezpieczeństwo w administracji. Gra edukacyjna.*

Dziękuję za uwagę

k.radominski@uksw.edu.pl