NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Główne problemy związane z bezpieczeństwem informacji w JST

dr Marcin Adamczyk

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

- W 2014 r. Najwyższa Izba Kontroli badała wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności (dalej jako KRI). W ponad 87% skontrolowanych urzędów miejskich stwierdzono nieprawidłowości.
- NIK w 2019 r. ponownie dokonuje kontroli w zakresie zarzadzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego i ponownie kontrola nie napawa optymizmem.
- Czy coś się zmięło w 2021 r.?

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Podmioty realizujące zadnia publiczne mają obowiązek opracować, ustanowić i wdrożyć, a następnie monitorować i przekładać oraz doskonalić system zarzadzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji, co wynika wprost z rozporządzenia KRI.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Główne problemy:

- ✓ brak systemowego podejścia do zapewnienia bezpieczeństwa informacji;
- ✓ problematyka bezpieczeństwa informacji nie może być swoistym „złem koniecznym”, z jakim trzeba się mierzyć;
- ✓ brak było pełnej i aktualnej informacji o posiadany zasobach informatycznych służących do przetwarzania danych;
- ✓ brak analizy ryzyka;
- ✓ brak obligatoryjnego corocznego audytu z zakresu bezpieczeństwa informacji.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Problemy z ochroną danych osobowych

- niedostosowanie uregulowań wewnętrznych w zakresie ochrony danych do przepisów RODO.
- Inspektor Ochrony Danych Osobowych źle wskazany - dlaczego m.in. sekretarz, sekretarka, kadrowa, nie mogą pełnić funkcji inspektora danych osobowych? => zob. Wytyczne grupy roboczej art. 29 WP.

Błędy w zakresie zarządzania uprawnieniami użytkowników systemów informatycznych

- ✓ brak opracowania i wdrożenia pisemnych procedur zarządzania uprawnieniami użytkowników w systemach informatycznych,
- ✓ brak dezaktywacji kont pracowników, którzy zakończyli zatrudnienie,
- ✓ posiadanie uprawnień administratora systemu na komputerach użytkowanych przez poszczególnych pracowników niebędących administratorami (zdarzały się jednostki, gdzie wszyscy pracownicy mieli takie uprawnienia),
- ✓ brak przestrzegania ustanowionych zasad dostępu do systemów informatycznych (używano zbyt krótkich haseł niż określone w wymaganiach),

- ✓ brak w umowach dotyczących zakupu lub serwisowania sprzętu komputerowego (oprogramowania) zapisów gwarantujących poufność informacji uzyskanych przez wykonawców,
- ✓ brak wykorzystywania wsparcia producenta systemu operacyjnego wykorzystywanego w użytkowanych komputerach,
- ✓ nieprawidłowości związane z niesporządzaniem kopii zapasowej, niewłaściwym przechowywaniu kopii zapasowej oraz braku sprawdzenia prawidłowości sporządzonych kopii,
- ✓ inne ….

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Podstawowe zasady bezpieczeństwa przetwarzanych danych

Zasada nr 1

Jeśli jakaś osoba jest w stanie namówić cię do uruchomienia jego programu w twoim komputerze, nie jest to już twój komputer.

- oprogramowanie w pracy musi być zatwierdzone przez odpowiednią osobę,
- pracownik musi mieć świadomość, iż sam nie może decydować o tym co i kiedy zainstalować w systemie,
- system ochrony danych osobowych musi w jasny sposób ustalać zakres kompetencji i odpowiedzialności konkretnych osób.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Zasada nr 2

Jeśli jakaś osoba może zmienić system operacyjny w twoim komputerze, nie jest to już twój komputer.

- podobnie jak w zasadzie nr 1, trzeba ustalić zakres kompetencji i odpowiedzialności konkretnych osób w systemie ochrony danych,
- w zasadzie poruszona jest większa skala zjawiska, która dotyczy nie tylko zmiany pojedynczego programu, ale całego systemu operacyjnego.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Zasada nr 3

Jeśli jakaś osoba ma ograniczony dostęp fizyczny do twojego komputera, to nie jest to już twój komputer.

- powyższa zasada zwraca uwagę na bezpieczeństwo fizyczne pomieszczeń oraz urządzeń w nich się znajdujących,
- realizacja zasady poprzez wdrożenie rozwiązań o charakterze organizacyjnym (ograniczenie dostępu do obszaru przetwarzania danych) oraz technicznym (systemy kontroli dostępu).

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Zasada nr 4

Jeśli jakaś osoba może umieścić program w twojej witrynie sieci Web, nie jest to już twoja witryna sieci Web.

- powyższa zasada prowadzi do podobnych wniosków praktycznych jak wcześniejsze, jednakże na pierwszy plan wysuwa konieczność należytego zabezpieczenia własnej strony www,
- należy stosować wysoki poziom bezpieczeństwa, gdy przynajmniej jedno urządzenie systemu informatycznego połączone jest z siecią publiczną,
- instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych powinna regulować sposób zabezpieczenia systemu informatycznego przed różnego rodzaju oprogramowaniami, które umożliwiają do niego dostęp.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Zasada nr 5

Słabe hasła obracają wniwecz silne zabezpieczenia.

- w przypadku systemów informatycznych warto wdrożyć zabezpieczenie w miarę jednorodne, zwłaszcza iż faktyczny poziom zabezpieczeń wyznaczany jest przez jego najsłabszy element,
- zasada ta znajduje odzwierciedlenie w przepisach rozporządzenia, regulując kwestie mechanizmów kontroli dostępu do danych przetwarzanych przy użyciu systemu informatycznego.

Top 25 najczęściej używanych haseł:

1. **123456** (bez zmian) 2. **password** (bez zmian) 3. **12345678** (1 pozycja wyżej)
4. **qwerty** (1 pozycja wyżej) 5. **12345** (2 pozycje niżej) 6. **123456789** (bez zmian)
7. **football** (3 pozycje wyżej) 8. **1234** (1 pozycja niżej) 9. **1234567** (2 pozycje wyżej)
10. **baseball** (2 pozycje niżej) 11. **welcome** (nowe) 12. **1234567890** (nowe)
13. **abc123** (1 pozycja wyżej) 14. **111111** (1 pozycja wyżej) 15. **1qaz2wsx** (nowe)
16. **dragon** (7 pozycji niżej) 17. **master** (2 pozycje wyżej) 18. **monkey** (6 pozycji niżej)
19. **letmein** (6 pozycji niżej) 20. **login** (nowe) 21. **princess** (nowe)
22. **qwertyuiop** (nowe) 23. **solo** (nowe) 24. **passw0rd** (nowe)
25. **starwars** (nowe)

Pamiętaj o polityce haseł, metodach uwierzytelniania, sposobach ataków na hasła, podwójnym uwierzytelnianiu…

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Zasada nr 6

Komputer jest na tyle bezpieczny, na ile można ufać administratorowi.

- zasada kładzie nacisk na element osobowy, który wiąże się z ochroną danych osobowych,
- zasada „ograniczonego zaufania” w stosunku do osoby, która zajmuje się zasobami informatycznymi,
- pamiętać trzeba o dokumentowaniu czynności podejmowanych przez konkretne osoby, którym powierzono takie zadania,
- zmiana administratora nie powinna paraliżować działania organizacji,
- warto pamiętać o konieczności dokonania zmian, np. zmiana haseł administracyjnych w przypadku zmiany osoby administratora.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Zasada nr 7

Zaszyfrowane dane są bezpieczne, o ile bezpieczny jest klucz szyfrowania.

- konieczność istnienia kompatybilności między stosowanymi zabezpieczeniami,
- środek zabezpieczający nie może utrudniać nam dostępu do informacji,
- poufność,
- dostępność informacji.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Zasada nr 8

Przestarzały skaner wirusów jest niewiele lepszy niż brak jakiegokolwiek skanera

- każdy sposób zabezpieczenia, który jest przestarzały, nie może chronić należycie posiadanych informacji,
- pokładanie ufności w zabezpieczenie, które nie chroni, może przesłaniać grożące niebezpieczeństwa,
- administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Zasada nr 9

Całkowita anonimowość nie jest praktyczna, ani w życiu, ani w sieci Web.

- zapewnienie poufności przetwarzanych danych jest tylko elementem systemu ochrony danych osobowych,
- pełna poufność może w sposób znaczący utrudniać realizację zadań administratora danych np. stosowanie bardzo mocnych haseł, które są trudne do zapamiętania (np. ich długość), co powoduje, iż informatyk w celu między innymi odblokowania dostępu do systemu poszczególnym użytkownikom musi korzystać z haseł administracyjnych.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Nie czekaj biernie na kontrolę, incydent, czy niepożądane działania.

Sprawdź m.in. (i wyciągnij z weryfikacji wnioski):

- ✓ czy jest pełny spis zasobów informatycznych służących do przetwarzania danych, w tym zidentyfikowanie wszystkich zbiorów danych posiadanych przez urząd;
- ✓ czy był audyt powdrożeniowy RODO (sprawdź m.in. dostosowanie uregulowań wewnętrznych w zakresie ochrony danych osobowych do RODO);
- ✓ sprawdź, czy inspektor ochrony danych osobowych nie wykonuje innych czynności mogących powodować konflikt interesów, o jakim mowa w art. 38 ust. 6 RODO (a jeśli wykonuje inne zadania, należy przeprowadzić odpowiednią analizę stanowiska, z której będzie wynikało, że nie ma takiego konfliktu);
- ✓ jaki jest kontakt z IOD, czy nie potrzebujesz regulaminu funkcjonowania (w tym kontaktu z IOD);
- ✓ kto odpowiada w jednostce za analizę ryzyka, kiedy była robiona i czy była aktualizowana;
- ✓ kiedy przeprowadzony był audyt z zakresu bezpieczeństw a informacji (ma być nie rzadziej niż raz do roku);

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Sprawdź m.in. (i wyciągnij z weryfikacji wnioski):

- ✓ czy przestrzegane są zasady dotyczące wykorzystania systemów informatycznych (nadawanie i odbieranie uprawnień, przestrzeganie wewnętrznej polityki haseł);
- ✓ czy są wdrożone (i przestrzegane) zasady i procedury wykorzystywania urządzeń mobilnych oraz pracy na odległość;
- ✓ do czego wykorzystywane są adresy poczty służbowej (służbowe dane na prywatnej skrzynce powinny być traktowane jako wynoszenie dokumentów z pracy z wszystkimi konsekwencjami);
- ✓ umowy na zakup sprzętu komputerowego (oprogramowania), czy zwierają zapisy gwarantujące zapewnienie poufności informacji uzyskiwanych przez wykonawcę;
- ✓ czy w komputerach wykorzystywanych w pracy system operacyjny ma aktywne wsparcie producenta;
- ✓ kiedy w jednostce wykonywano kopię zapasową posiadanych danych, gdzie jest ona przechowywana oraz sprawdzenie możliwości jej wykorzystania;

- Za zarzadzanie bezpieczeństwem informacji odpowiada kierownictwo podmiotu publicznego.
- Zapewnienie bezpieczeństwa informacji wymaga kompleksowych działań.
- Konieczna jest zmiana podejścia do tych działań i przede wszystkim zrozumienie ich wagi w tym potencjalnych zagrożeń z tym związanych oraz odpowiedzialności, jaką trzeba będzie ponieść w przypadku wystąpienia zdarzeń niepożądanych, powstałych w związku z brakiem wdrożenia odpowiednich procedur i zabezpieczeń.

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Dziękuję za uwagę.

dr Marcin Adamczyk

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

ul. Zielona 18, 90-601 Łódź tel. 42 633 10 70