Żeby elektronicznie znaczyło bezpiecznie

2019-05-10 07:00:00

NIK o zarządzaniu bezpieczeństwem informacji w jednostkach samorządu terytorialnego

Dane gromadzone i przetwarzane w bazach i systemach komputerowych urzędów gmin i miast, a także w starostwach są słabo chronione. Niestety urzędnicy nie przywiązują dostatecznej wagi do tego aby zapewnić ich bezpieczeństwo. Najwyższa Izba Kontroli podkreśla, że pomimo upływu kilku lat w urzędach nie nastąpiła poprawa w tym obszarze. Rodzi to uzasadnione obawy o bezpieczeństwo danych obywateli, zwłaszcza, że coraz więcej spraw załatwianych jest drogą elektroniczną, a administracja publiczna gromadzi i przetwarza coraz więcej danych w postaci elektronicznej.

W Polsce można zaobserwować stały wzrost zainteresowanie obywateli elektroniczną formą załatwiania spraw w urzędach. Jednocześnie oczekiwania społeczne co do ułatwienia i przyspieszenia załatwienia spraw powodują, że instytucje publiczne wykorzystują je w coraz szerszym zakresie. Obywatele oczekują nie tylko usprawnień w zakresie funkcjonowania e-administracji, lecz także zapewnienia, że wszelkie dane posiadane przez administrację publiczną są właściwie zabezpieczone przed dostępem osób nieupoważnionych.

Źródło: opracowanie własne NIK na podstawie wyników kontroli.

Dlatego **zapewnienie bezpieczeństwa przetwarzania informacji w urzędzie staje się jednym z najistotniejszych wyzwań stojących przed administracją publiczną. Niewłaściwe zarządzanie bezpieczeństwem informacji może doprowadzić do wycieku, utraty lub sfałszowania danych posiadanych przez urząd**. Możliwy jest także całkowity paraliż pracy urzędu.

Zgodnie z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności (rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. - dotyczące minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych), **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. Wymagania w zakresie zapewnienia ochrony danych osobowych zostały określone w nowym unijnym rozporządzeniu RODO, które weszło w życie w dniu 25 maja 2018 roku. Tym samym przepisy dotyczące ochrony danych osobowych dla wszystkich państw członkowskich zostały ujednolicone. Celem RODO było m.in. unowocześnienie regulacji o ochronie danych osobowych, które obowiązywały od 1995 r. i w dobie szybko postępującej cyfryzacji miały coraz mniejsze zastosowanie praktyczne. Jednocześnie RODO zostało zredagowane tak, aby było zawsze aktualne niezależnie od rozwoju technologii. Ochrona danych osobowych wymaga zaprojektowania w urzędzie całego systemu tej ochrony, w tym ustanowienia procedur dla wszystkich procesów gromadzenia, przechowywania i korzystania z danych osobowych, w tym przetwarzanych w systemach informatycznych.

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

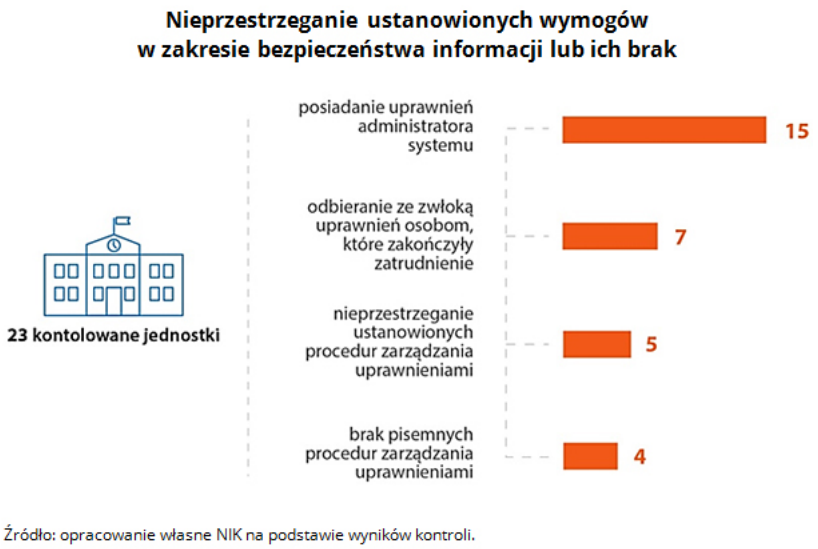
- w ciągu dwóch lat (2013-2014) hakerzy okradli pięć polskich gmin, w tym gminę Jaworzno na prawie milion złotych;
- w 2014 r. wyciekły dane dzieci z przemyskiego Urzędu Miejskiego;
- w 2017 r. z Urzędu Miasta Łodzi wyciekły dane z tzw. deklaracji śmieciowych, przez co bez problemu można było poznać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

Najważniejsze ustalenia kontroli

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 zabezpieczenia danych będących w posiadaniu urzędów. **Pomimo upływu kilku lat nadal nie nastąpiła poprawa w tym zakresie, co rodzi obawy o bezpieczeństwo danych, zwłaszcza, że coraz więcej spraw obywateli załatwianych jest drogą elektroniczną, a administracja publiczna gromadzi i przetwarza coraz więcej danych w postaci elektronicznej.** W ocenie NIK, **blisko 70 proc. skontrolowanych urzędów** (16 z 23 urzędów) **nie radziło sobie z zapewnieniem bezpieczeństwa przetwarzania informacji, co Izba oceniła negatywnie.**

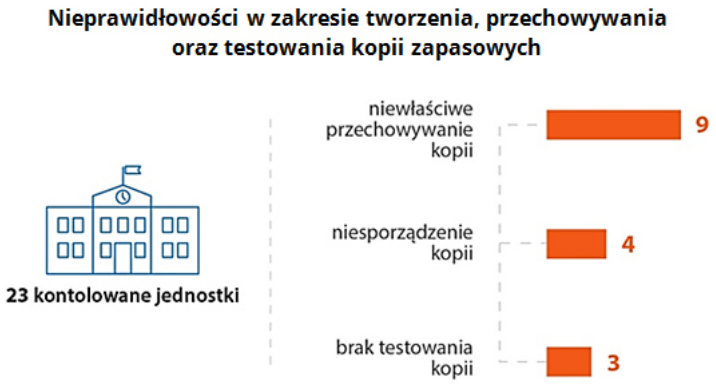
Kontrolerzy NIK stwierdzili, że **w ponad 60 proc. badanych urzędów brakowało systemowego podejścia do zapewnienia bezpieczeństwa informacji**, gdyż opracowane w tych jednostkach regulacje dotyczyły głównie danych osobowych i nie obejmowały bezpieczeństwa innych informacji. W szczególności w urzędach tych nie ustanowiono polityk bezpieczeństwa informacji. Ponadto stwierdzono, że **w prawie 3/4 kontrolowanych urzędów brak było pełnej i aktualnej informacji o posiadanych zasobach informatycznych służących do przetwarzania danych**, co oznacza, że w przypadku wystąpienia poważnej awarii lub innego zdarzenia losowego (takiego jak zalanie, pożar czy kradzież), utrudnione będzie szybkie odtworzenie infrastruktury i zapewnienie ciągłości świadczenia usług dla obywateli.

Kontrola NIK wykazała, że w części urzędów nie przestrzegano obowiązujących zasad mających na celu zwiększenie bezpieczeństwa przetwarzania danych. **W ponad 80 proc. skontrolowanych urzędów wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych.**



Źródło: opracowanie własne NIK na podstawie wyników kontroli.

W zakresie uzyskiwania dostępu do systemów informatycznych, w ponad połowie kontrolowanych urzędów (57 proc.) ustanowione zasady nie były przestrzegane, np. użytkownicy używali haseł do systemów informatycznych krótszych niż wymagane. Również w ponad połowie jednostek **wykorzystywano komputery z zainstalowanym systemem operacyjnym bez wsparcia producenta.** Wykorzystywanie w działalności urzędu oprogramowania nieposiadającego wsparcia producenta znacząco obniża poziom bezpieczeństwa informatycznego i zdaniem NIK należy dążyć do jak najszybszej wymiany takiego oprogramowania na nowsze, posiadające wsparcie techniczne. **Stwierdzono też nieprawidłowości w zakresie tworzenia, przechowywania oraz weryfikacji kopii zapasowych danych.**



Źródło: opracowanie własne NIK na podstawie ustaleń kontroli.

Z ustaleń kontroli wynika, że **w 1/3 badanych urzędów nie określono szczegółowych zasad i procedur korzystania przez pracowników z urządzeń przenośnych poza ich siedzibami**, gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Co więcej **w aż 70 proc. urzędów nie szyfrowano dysków twardych komputerów przenośnych**. W efekcie w razie ich utraty, rosło ryzyko nieuprawnionego dostępu do danych zgromadzonych na tych urządzeniach.

W wielu skontrolowanych urzędach miast i gmin, a także w starostwach nie dostrzegano występujących zagrożeń. W prawie połowie jednostek nie dokonywano analiz ryzyka, a w 70 proc. nie przeprowadzono obowiązkowego corocznego audytu z zakresu bezpieczeństwa informacji. **Zdaniem NIK brak cyklicznych analiz ryzyka i nieprowadzenie audytów bezpieczeństwa nie pozwalał urzędnikom na identyfikację istotnych zagrożeń w zakresie bezpieczeństwa informacji, a także na ustanowienie odpowiednich zabezpieczeń ograniczających**

możliwość ich wystąpienia.

Ponadto kontrolerzy NIK w 1/4 urzędów stwierdzili niedostosowanie uregulowań wewnętrznych w zakresie ochrony danych osobowych do przepisów RODO. Z kolei w 1/5 urzędów osoby pełniące funkcję Inspektora Ochrony Danych wykonywały inne zadania i obowiązki, które mogły powodować konflikt interesów.

Wyniki kontroli NIK wskazują, że **o ile w urzędach w większości podjęto działania w celu dostosowania do RODO, to w dalszym ciągu często nie są przestrzegane wymogi dotyczące bezpieczeństwa informacji, które wynikają z obowiązującego od 2012 roku rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI). W opinii NIK, nie jest możliwe zapewnienie wysokiego poziomu ochrony danych osobowych bez zachowania właściwego bezpieczeństwa informacji w systemach informatycznych.**

W związku z ustaleniami kontroli NIK, dotyczącymi działań jednostek samorządu terytorialnego związanych z zapewnieniem wdrożenia niektórych wymogów RODO, **informacja o wynikach tej kontroli została przekazana nie tylko Ministrowi Cyfryzacji, ale także Prezesowi Urzędu Ochrony Danych Osobowych.**

Wnioski

Do starostów, prezydentów miast, burmistrzów i wójtów o:
- prowadzenie okresowych analiz ryzyka utraty integralności, poufności lub dostępności informacji (zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI);
- opracowanie i wdrożenie oraz aktualizowanie Systemu Zarządzania Bezpieczeństwem Informacji (zgodnie z § 20 ust. 1 rozporządzenia KRI);
- prowadzenie aktualnej i kompletnej elektronicznej ewidencji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację (zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI);
- wdrożenie rozwiązań zapewniających odpowiednie zabezpieczenie pomieszczeń serwerowni (zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI);
- zapewnienie prowadzenia przynajmniej raz w roku okresowego audytu wewnętrznego z zakresu bezpieczeństwa informacji (zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI);
- zapewnienie dokumentowania procesu nadawania uprawnień użytkowników systemów informatycznych;
- przyznawanie pracownikom urzędów uprawnień w systemach informatycznych adekwatnych do realizowanych zadań (zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI);
- dostosowanie uregulowań wewnętrznych w zakresie danych osobowych do wymogów RODO;
- prowadzenie rejestru czynności przetwarzania danych (o którym mowa w art. 30 RODO);
- przeprowadzenie analizy i oceny procesów przetwarzania danych (o których mowa w art. 32 ust. 1 RODO). Do wojewodów:

W opinii NIK, konieczne jest aby wojewodowie objęli kontrolami większą liczbę urzędów jednostek samorządu terytorialnego w zakresie zapewnienia bezpieczeństwa informacji dla systemów teleinformatycznych oraz rejestrów publicznych.

Do Ministra Cyfryzacji:

Zdaniem NIK, istnieje potrzeba szerokiego promowania/informowania organów administracji o wymogach w zakresie bezpieczeństwa informacji określonych w rozporządzeniu KRI i ich wpływie na zapewnienie ochrony danych osobowych.