NIK o pracy zdalnej w urzędach

Kategoria: Aktualności
Opublikowano: wtorek, 26, lipiec 2022 12:12
Ewelina Kocemba
Odsłony: 1202

W marcu 2020 roku stan epidemii Covid-19 postawił instytucje publiczne w bardzo trudnej sytuacji. Z jednej strony zapewnienie pracownikom bezpieczeństwa, a z drugiej urzędom ciągłości funkcjonowania wymusiło natychmiastową zmianę organizacji pracy, co stwarzało nowe zagrożenia dla gromadzonych i przetwarzanych w tych instytucjach danych.

Kontrola przeprowadzona przez NIK pokazała, że mimo obowiązujących przepisów od stycznia 2020 r. do grudnia 2021 r. w połowie kontrolowanych urzędów nie wprowadzono systemu zarządzania bezpieczeństwem informacji podczas pracy na odległość. Regulacje, które tam obowiązywały, dotyczyły jedynie danych osobowych. Część instytucji nie przestrzegała nawet własnych zasad związanych z pracą na indywidualnych kontach systemu operacyjnego, szyfrowaniem twardych dysków służbowych komputerów czy postępowaniem z zewnętrznymi nośnikami danych.

Kancelaria Prezesa Rady Ministrów, która z powodu likwidacji resortu pełni także obowiązki Ministerstwa Cyfryzacji, nie monitorowała ani skali wprowadzenia w instytucjach publicznych pracy na odległość, ani tego, w jakim stopniu zapewniono tam bezpieczeństwo przetwarzanym mobilnie danym.

Poza kancelarią premiera, kontrola NIK objęła także 10 instytucji w Warmińsko-Mazurskiem: Wojewódzki Urząd Ochrony Zabytków, Wojewódzki Inspektorat Farmaceutyczny i Izbę Administracji Skarbowej w Olsztynie, a także 5 urzędów gmin i 2 urzędy powiatowe. Jednym z kryteriów wyboru tych instytucji były informacje dotyczące zakresu pracy zdalnej w okresie od 8 marca 2020 r. do 31 marca 2021 r. zebrane przez Najwyższą Izbę Kontroli w 142 urzędach regionu. W niemal 50 z nich zdalnie pracowało ponad ¾ zatrudnionych tam osób. Uzyskane informacje pozwoliły również na określenie skali wykorzystania w tym czasie podczas pracy zdalnej komputerów służbowych i prywatnych.

Rekomendacje zamiast przepisów

Informacje są bezpieczne, jeśli ich gromadzenie odbywa się we właściwym miejscu, formie i czasie, a przekazywanie adresatom - w wyznaczonym terminie, za pomocą odpowiedniego kanału i w tajemnicy przed niepożądanymi odbiorcami. Minimalne wymagania w tym zakresie nakłada na instytucje publiczne, rządowe rozporządzenie z 2012 r. dotyczące Krajowych Ram Interoperacyjności.

Wynika z niego, że urzędy powinny zapewnić bezpieczeństwo wszystkim kategoriom przetwarzanych informacji, tymczasem kontrolowane przez NIK instytucje dbały przede wszystkim o bezpieczeństwo danych osobowych. W połowie skontrolowanych urzędów nie opracowano i nie wdrożono systemu zarządzania bezpieczeństwem informacji (SZBI), który powinien określać sposób postępowania właściwy dla każdego rodzaju przetwarzanych informacji.

Po ogłoszeniu stanu epidemii, kancelaria premiera opublikowała w internecie zalecenia w zakresie podniesienia poziomu bezpieczeństwa teleinformatycznego w administracji publicznej. Dotyczyły one m.in. korzystania z domowej sieci Wi-Fi, wdrożenia VPN, dwuskładnikowego uwierzytelniania, tworzenia kopii zapasowych, niekorzystania z publicznych otwartych sieci Wi-Fi oraz nieużywania prywatnych skrzynek pocztowych, czy grup na portalach społecznościowych do komunikacji firmowej, a także stosowania się do wytycznych pracodawcy i wykorzystywania w pracy zdalnej wyłącznie firmowego sprzętu – laptopów i telefonów. Były to jednak wyłącznie rekomendacje, które nie nakładały obowiązków ani na urzędy, ani na KPRM, ani na Pełnomocnika Rządu do spraw Cyberbezpieczeństwa. W efekcie kancelaria premiera w bardzo ograniczonym zakresie sprawdzała w jaki sposób instytucje publiczne korzystały z zaleceń (skontrolowała jedynie Ministerstwo Rodziny i Polityki Społecznej), nie

miała także informacji na temat skali wprowadzenia pracy zdalnej w urzędach i zapewnienia przez nie bezpieczeństwa informacjom przetwarzanym mobilnie.

Zdaniem NIK, gromadzenie przez kancelarią premiera danych na temat skali wprowadzenia w urzędach pracy zdalnej i mobilnego przetwarzania danych oraz zastosowanych przy tym rozwiązań technicznych i organizacyjnych mogłoby pomóc we wcześniejszym rozpoznaniu zagrożeń i formułowaniu dodatkowych ostrzeżeń oraz rekomendacji, a to podniosłoby poziom cyberbezpieczeństwa.

Z danych Departamentu Cyberbezpieczeństwa KPRM wynika, że w 2020 r. doszło do 388 incydentów bezpieczeństwa w administracji publicznej, a tylko do sierpnia 2021 r. do kolejnych 287. Informacje te są jednak niepełne, ponieważ Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy nie ma obowiązku przekazywania KPRM szczegółowych informacji o takich incydentach.

Bezpieczeństwo danych

Wprowadzenie w urzędach pracy na odległość wymagało zapewnienia pracownikom narzędzi umożliwiających zdalnie wykonywanie zadań, a także aktualizacji systemów zarządzania bezpieczeństwem danych. Część kontrolowanych przez NIK instytucji nie była przygotowana do natychmiastowego wprowadzenia takich zmian.

Początkowo koncentrowano się głównie na zapewnieniu pracownikom dystansu społecznego i ograniczeniu kontaktów między nimi. Wprowadzono system rotacyjny, zgodnie z którym poszczególne grupy pracowały na zmianę - jeden dzień w formie stacjonarnej i jeden dzień w formie zdalnej, ale bez dostępu do systemów teleinformatycznych. Ponieważ kontrolowane instytucje nie były gotowe do wprowadzenia rozwiązań technicznych umożliwiających taki dostęp, praca zdalna urzędników polegała na udziale w konferencjach i szkoleniach oraz na opracowywaniu ogólnych dokumentów, bez dostępu do wewnętrznych sieci instytucji.

W 2020 r. w 10 kontrolowanych przez NIK urzędach z inicjatywy pracodawcy zdalnie pracowało niemal 73% zatrudnionych tam osób, na własną prośbę - 9,5%. W kolejnym roku pandemii te proporcje wyglądały już zdecydowanie inaczej - 47,5% zatrudnionych pracowało zdalnie na polecenie pracodawcy, na swój wniosek 12,5%. W badanym okresie także niektóre osoby objęte kwarantanną lub izolacją wykonywały swoje obowiązki na odległość.

Podstawowymi kanałami przesyłania informacji niezbędnych do wykonywania zadań na odległość były: poczta elektroniczna oraz szyfrowane połączenie VPN umożliwiające dostęp do pulpitu zdalnego komputerów stacjonarnych znajdujących się w urzędach.

Przesyłanie załączników zawierających informacje chronione (dane osobowe) wymagało szyfrowania i zabezpieczenia hasłem, które należało przekazać adresatowi innym kanałem łączności (np. za pośrednictwem telefonu, SMS). W trzech urzędach dopuszczono możliwość wykorzystywania w celach służbowych także prywatnych kont mailowych, a w dwóch z nich określono warunki jakie należało spełnić, aby z tej możliwości można było korzystać. Jednym z nich było uzyskanie pisemnej zgody administratora danych lub administratora systemów informatycznych. Takich warunków nie określono w Urzędzie Ochrony Zabytków w Olsztynie.

Kategoria: Aktualności
Opublikowano: wtorek, 26, lipiec 2022 12:12
Ewelina Kocemba
Odsłony: 1202

W przypadku informacji przetwarzanych podczas pracy zdalnej za pomocą szyfrowanych kanałów VPN w pięciu urzędach dopuszczono stosowanie jedynie sprzętu służbowego. W pięciu pozostałych instytucjach można było korzystać także z prywatnych komputerów, ale po spełnieniu określonych wymagań. Przed dopuszczeniem takiego sprzętu do nawiązywania połączeń VPN z zasobami informatycznymi urzędów konieczna była aktualizacja systemu operacyjnego, zainstalowanie programu antywirusowego, stosowanie indywidualnego konta i hasła zgodnego z przyjętą w urzędach polityką.

Czy zastosowane w kontrolowanych urzędach rozwiązania dotyczące bezpieczeństwa informacji w pracy zdalnej przyniosły oczekiwane efekty? Na pewno wpłynęły na podniesienie poziomu bezpieczeństwa, jednak trudno ocenić w jakim stopniu, ponieważ kierownicy tych instytucji nie dysponowali rzetelną oceną skuteczności wprowadzonych rozwiązań. Tylko trzy na 10 urzędów przeprowadziły w badanym okresie zewnętrzny audyt bezpieczeństwa systemów informatycznych. Część jednostek zleciła audyt wewnętrzny i uwzględniała jego wyniki w przeprowadzanych analizach ryzyka. Dwa urzędy nie przeprowadziły żadnego przeglądu w tym zakresie.

NIK ma także zastrzeżenia do szkoleń organizowanych przez kontrolowane instytucje. Zdaniem Izby, ich pracownicy nie mieli pełnej wiedzy o zagrożeniach dotyczących bezpieczeństwa informacji w pracy na odległość i o sposobach zapobiegania skutkom tych zagrożeń. Informacje na ten temat zdobywano głównie dzięki samokształceniu, m.in. poprzez udostępnione przez pracodawców materiały. Jedynie dwie instytucje zorganizowały szkolenia na temat bezpiecznego łączenia się z siecią wewnętrzną urzędu, dwie kolejne w całym badanym okresie nie przeprowadziły żadnego. Poprzestano tam jedynie na instruowaniu tych pracowników, którzy odbierali sprzęt do pracy zdalnej.

Wnioski NIK

Do ministra właściwego do spraw informatyzacji:

- Pozyskiwanie od jednostek administracji publicznej informacji o skali wykorzystania systemów teleinformatycznych w pracy zdalnej i o stosowaniu wydanych przez ministra zaleceń i rekomendacji.

Do jednostek administracji publicznej:

- Dokonanie przez jednostki administracji publicznej przeglądu regulacji wewnętrznych w obszarze bezpieczeństwa informacji i zmodyfikowanie ich tak, aby nie ograniczały się one wyłącznie do ochrony danych osobowych.

Źródło: NIK