NIK. W samorządach ochrona danych osobowych bez ochrony

Kategoria: Aktualności
Opublikowano: czwartek, 22, luty 2024 09:17
Joanna Gryboś-Chechelska

Wieloletnie zaniedbania dotyczące ochrony danych osobowych, nieświadomość zagrożeń, brak jednoznacznych wytycznych, używanie domen publicznych bez stosownych umów gwarantujący bezpieczeństwo – to w ocenie NIK sprawia, że podstawowe elementy systemu ochrony danych osobowych w jednostkach samorządowych były nieskuteczne. NIK rekomenduje szybką potrzebę zmian. Najwyższa Izba Kontroli szacuje, że skala nieprawidłowości może dotyczyć kilkunastu tysięcy publicznych instytucji. Biorąc pod uwagę skalę problemu, NIK rozszerza postępowanie kontrolne na wszystkie samorządy w kraju i dokonuje rozpoznania w innych sferach działalności publicznej.

W ostatnim czasie Najwyższa Izba Kontroli z niepokojem obserwuje rosnącą liczbę doniesień medialnych na temat nieodpowiedniego postępowania urzędników państwowych związanego z tak podstawowym elementem bezpieczeństwa, jak korzystanie do celów służbowych z adresów mailowych w publicznych domenach i przetwarzanie danych osobowych za ich pośrednictwem. Aby potwierdzić lub wyeliminować ryzyko zagrożeń systemowych dla odpowiedniej ochrony danych osobowych NIK podjęła się kontroli, której celem było szybkie wyeliminowanie ewentualnych nieprawidłowości. Kontrolę oparto o kilka założeń strategicznych, m.in. o: efektywność postępowania kontrolnego, współpracę z interesariuszami w trakcie czynności kontrolnych, oczekiwanie działań naprawczych już w trakcie czynności kontrolnych oraz nastawienie kontroli na możliwie szybką zmianę porządku publicznego w kontrolowanym obszarze.

NIK skontrolowała 12 jednostek samorządu terytorialnego w województwie podlaskim. Sprawdzono jak zapewniana jest ochrona i prawidłowość przetwarzania danych, w tym danych osobowych gromadzonych w formie elektronicznej przez jednostki samorządu terytorialnego oraz podległe im jednostki organizacyjne na stronach internetowych, poczcie elektronicznej oraz w związku z odbywającymi się sesjami organów uchwałodawczych.

Najważniejsze ustalenia kontroli

Kontrola wykazała wieloletnie zaniedbania związane z ochroną danych osobowych, nieświadomość zagrożeń, brak jednoznacznych wytycznych – wybrane elementy systemu ochrony danych osobowych w jednostkach samorządowych były złym stanie. W rezultacie kontroli prowadzonych przez inspektorów NIK wyeliminowano korzystanie (niekiedy kilkunastoletnie) z adresów mailowych utworzonych w domenach komercyjnych bez zawarcia wymaganych rozporządzeniem RODO umów powierzenia przetwarzania danych osobowych. Zmieniono adresy mailowe w 45 jednostkach samorządowych, w tym m.in. w trzech urzędach, ośmiu instytucjach kultury, 10 ośrodkach pomocy społecznej oraz 15 placówkach oświatowych. Łącznie zrezygnowano z używania blisko 250 adresów mailowych wykorzystywanych do celów służbowych, a zlokalizowanych na domenach komercyjnych bez zawarcia stosownych umów gwarantujących odpowiedni poziom bezpieczeństwa.

Analiza szczegółowa wykazała, że w skrzynkach e-mailowych w sposób nieprawidłowy przetwarzano takie rodzaje danych jak: dane osobowe osób fizycznych (imiona, nazwiska, adresy, numery PESEL, numery telefonów), dane o ich stanie zdrowia (m.in. wyniki badań lekarskich), dane o korzystaniu ze świadczeń opieki społecznej, dane o zatrudnieniu i wysokości wynagrodzenia oraz dane o sytuacji rodzinnej (m.in. opisy diagnoz w poradniach psychologiczno-pedagogicznych). Usunięto ponad 1,3 tys. dokumentów z Biuletynów Informacji Publicznej – były to oświadczenia majątkowe, których okres publikacji wynosi sześć lat, a niektóre z nich dotyczyły roku 2002. Ponadto w siedmiu samorządach zmieniono zasady transmitowania i publikowania posiedzeń organów stanowiących. Pierwotnie były transmitowane na niezabezpieczonych portalach społecznościowych.

Kategoria: Aktualności
Opublikowano: czwartek, 22, luty 2024 09:17
Joanna Gryboś-Chechelska
Odsłony: 882

Wielka skala nieprawidłowości w skontrolowanych jednostkach samorządu terytorialnego i gminnych oraz powiatowych jednostkach organizacyjnych wymusiła przeprowadzenie w Najwyższej Izbie Kontroli analizy powszechnego problemu wymagającego natychmiastowej reakcji samorządowców w całym kraju. Analiza ta pokazuje bardzo wysokie prawdopodobieństwo wystąpienia podobnych nieprawidłowości w kilkunastu tysiącach jednostek publicznych w całym kraju, które codziennie wymieniają korespondencję za pośrednictwem skrzynek mailowych, korzystając przy tym z hostingu i domen komercyjnych. Z analizy wynika, że 43% placówek oświatowych, 32% publicznych zakładów opieki zdrowotnej oraz 28% ośrodków pomocy społecznej na co dzień wykorzystuje główne adresy mailowe w domenach komercyjnych np. wp.pl, poczta.onet.pl, gmail.com. Może to nie tylko świadczyć o braku zawarcia z właścicielami tych domen stosownych umów zabezpieczających administratorów danych osobowych przed bezpodstawnym przetwarzaniem, ale również może powodować niskie zaufanie do instytucji publicznych.

Ryzyka stwierdzono również w przypadku ośrodków kultury, bibliotek, powiatowych inspektorów nadzoru budowlanego, powiatowych stacji sanitarno-epidemiologicznych, domów pomocy społecznej, powiatowych centrów pomocy rodzinie, przychodni psychologiczno-pedagogicznych, centrów usług wspólnych i innych.

Biorąc pod uwagę ustalenia kontroli oraz fakt, że oprócz głównych adresów mailowych przypisanych do jednostki, niejednokrotnie pracownicy tych instytucji publicznych również użytkowali adresy mailowe w domenach komercyjnych jako adresy służbowe, Najwyższa Izba Kontroli szacuje, że skala nieprawidłowości może dotyczyć kilkunastu tysięcy publicznych instytucji oraz kilkudziesięciu tysięcy adresów mailowych, które nie powinny być wykorzystywane do celów służbowych. Wskazuje to na ryzyko, że dziennie na takie adresy mailowe może wpływać tysiące wiadomości, w tym część z nich zawierających dane osobowe szczególnie chronione. Stąd też postępowanie kontrolne rozszerzone zostanie na wszystkie jednostki samorządowe w kraju. Ma ono wyeliminować nieprawidłowości i zagwarantować pozytywne zmiany w usługach publicznych, w całym sektorze samorządowym. Znamienne jest, że niejednokrotnie jednostki samorządowe na nieodpowiednio zabezpieczone adresy mailowe otrzymywały wiadomości z ministerstw, organów nadzoru oraz instytucji nadrzędnych, co wskazuje na powszechną niską świadomość o stosowaniu bezpiecznych narzędzi i instrumentów w sposób odpowiedni zabezpieczających dane osobowe obywateli.

Oprócz jednostek samorządowych Najwyższa Izba Kontroli prowadzi rozpoznanie dotyczące innych branż i resortów. Dane uzyskane z dziewięciu sądów apelacyjnych wskazują, że problem może dotyczyć korespondowania za pośrednictwem poczty elektronicznej z biegłymi sądowymi, którzy podają adresy mailowe znajdujące się na bezpłatnych domenach komercyjnych, co może świadczyć o dużym ryzyku, że nie zawarli oni umowy przetwarzania danych osobowych z właścicielem domeny, tłumaczami przysięgłymi, ławnikami, mediatorami i kuratorami sądowymi.

Komunikacja służbowa powinna odbywać się za pomocą dedykowanej do tego skrzynki mailowej. Korzystanie z prywatnej skrzynki pocztowej w celach służbowych nie należy do dobrych praktyk bezpieczeństwa.

Najwyższa Izba Kontroli zdiagnozowała systemowy charakter nieprawidłowości w dziedzinie ochrony i przetwarzania danych, w tym danych osobowych w jednostkach samorządowych. Dlatego kontrola będzie rozszerzona o wszystkie jednostki samorządu terytorialnego w Polsce.

Kategoria: Aktualności
Opublikowano: czwartek, 22, luty 2024 09:17
Joanna Gryboś-Chechelska
Odsłony: 882

Dobre wzorce można czerpać z zagranicy. Dla przykładu w Austrii wszystkie jednostki samorządowe korzystają z domeny gv.at: w Czechach i Portugalii instytucje publiczne mają obowiązek korzystania z własnych wykupionych domen; na Malcie natomiast instytucje samorządowe korzystają z domen rządowych.

Źródło: NIK