NIK: Państwowe systemy ochrony danych nie zapewniają ich bezpieczeństwa

Chaos związany z brakiem planowania, opieszałość i niewystarczające środki finansowe przeznaczane na system ochrony danych – to główne zarzuty jakie stawiają kontrolerzy Najwyższej Izby Kontroli (NIK). Alarmują: państwowe systemy ochrony danych nie zapewniają ich bezpieczeństwa, a informacje o milionach Polaków łatwo mogą trafić w niepowołane ręce.

Kontrolą NIK objęto: Ministerstwo Skarbu Państwa, Ministerstwo Spraw Wewnętrznych, Ministerstwo Sprawiedliwości, Komendę Główną Straży Granicznej, Narodowy Fundusz Zdrowia oraz Kasę Rolniczego Ubezpieczenia Społecznego. Raport dotyczy okresu od 1 stycznia 2014 roku do 1 października 2015 roku.

Chodzi o dane zgromadzone w systemach informatycznych, wykorzystywanych do realizacji istotnych zadań publicznych. Procesy zapewnienia bezpieczeństwa informacji realizowane były w sposób chaotyczny i – wobec braku procedur – intuicyjny.

– *NIK stwierdziła także ograniczoną wiedzę kierownictwa jednostek w zakresie konieczności ochrony bezpieczeństwa informacji i wymogów z tym związanych. Ze wszystkich skontrolowanych jednostek KRUS był jedyną instytucją, w której formalnie wdrożono system zarządzania bezpieczeństwem, w przeciwieństwie do pozostałych jednostek wprowadzono wszystkie procesy wymagane dla zapewnienia bezpieczeństwa danych. Kontrolowane jednostki w ograniczonym zakresie wykorzystywały metody identyfikacji, monitorowania i zapobiegania ryzyku związanemu z bezpieczeństwem informacji przetwarzanych w systemach teleinformatycznych* – mówi Krzysztof Kwiatkowski, prezes NIK.

W raporcie wskazano, że w ograniczonym zakresie wykorzystywano metody identyfikacji, monitorowania i zapobiegania ryzyku związanemu z bezpieczeństwem informacji przetwarzanych w systemach teleinformatycznych. Zwrócono uwagę, że istniała duża dysproporcja pomiędzy działaniami podejmowanymi dla ochrony poszczególnych grup informacji. Chodzi o informacje objęte ustawową ochroną (niejawne i dane osobowe) oraz innych informacji, których ochrona nie została wprost usankcjonowana w przepisach, ale które są istotne z punktu widzenia prawidłowej realizacji podstawowych zadań kontrolowanych instytucji.

„W jednostkach kontrolowanych brak było świadomości, że oprócz informacji, których wymóg ochrony zapisany jest wprost w przepisach prawa istnieją także inne informacje, równie ważne, o których ochronę każda jednostka powinna zadbać samodzielnie. W przeciwieństwie do normatywnie określonych wymogów dla ochrony informacji niejawnych i danych osobowych, zidentyfikowanie wszelkich innych, istotnych informacji oraz wybór metod ich chronienia jest praktycznie pozostawiony w gestii ich posiadacza" – czytamy w raporcie.

NIK ujawnia, że w żadnej z kontrolowanej instytucji nie określono precyzyjnie zakresu odpowiedzialności poszczególnych osób za zapewnienie bezpieczeństwa danych, co prowadziło do sporów kompetencyjnych. „W większości kontrolowanych jednostek zagadnienia dotyczące bezpieczeństwa informacji znajdowały się wyłącznie w gestii komórek bezpośrednio odpowiedzialnych za systemy informatyczne. Skutkowało to ograniczeniem faktycznego zakresu ochrony informacji jedynie do systemów informatycznych i nośników danych" – dodano.

Mimo że we wszystkich skontrolowanych instytucjach przeprowadzano audyty bezpieczeństwa a ich wnioski

trafiały do ich kierownictwa, to zalecenia wynikające z audytów nie były realizowane. Jak wskazuje NIK, istotnym problemem był jednak brak konsekwencji i zaangażowania kierownictw kontrolowanych podmiotów publicznych.

To kolejna z kontroli NIK dotyczących obszaru bezpieczeństwa systemów teleinformatycznych i przechowywanych w nich danych. W 2015 oku Izba opublikowana informację o wynikach kontroli pt. „Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej", w której która wykazała, że państwo polskie nie jest przygotowane do walki z zagrożeniami występującymi w cyberprzestrzeni.

IK

Fot. www.freeimages.com