**Blisko 92 proc. urzędów w Polsce nadal ma papierowy system zarządzania dokumentacją**

**Prowadzona przez NIK kontrola e-administracji lokalnej wykazała, że jedynie pojedyncze urzędy w Polsce wdrożyły elektroniczny obieg dokumentacji, a w dalszym ciągu, aż w 9 na 10 jednostkach dokumentacja funkcjonuje w tradycyjnej, papierowej formie[1]. Według ekspertów, w strukturze wszystkich wycieków danych, instytucje publiczne stanowią ponad 30 proc. odnotowanych przypadków[2]. Zarówno informatyzacja polskich urzędów, jak i ochrona istniejącej już papierowej dokumentacji nie wygląda najlepiej. W wielu placówkach brakuje podstawowej Polityki Bezpieczeństwa Informacji, a nieprawidłowości związane z bezpieczeństwem informacji stwierdzono w ponad 80 proc. zbadanych jednostek[3]. Szansą na rozwój e-administracji są fundusze unijne na lata 2014-2020, a jakie szanse na większe bezpieczeństwo mają nasze dokumenty na papierze?**

*„Ostatnimi czasy dużo mówi się w mediach i nie tylko o cyfryzacji społeczeństwa, o projektach e-zdrowie, e-administracja, jednak jak wynika z ostatniej kontroli przeprowadzonej przez Najwyższą Izbę Kontroli, ponad 90 proc. urzędów nadal ma tradycyjny, papierowy system zarządzania dokumentacją. Nikogo nie powinno to dziwić, ponieważ pomimo tego, że informatyzacja w Polsce postępuje, to całkowite wykluczenie papierowego obiegu dokumentów, zwłaszcza w jednostkach tak specyficznych jak urzędy, jest na chwilę obecną po prostu nierealne. W tym zakresie powinniśmy postawić na synergię działań. Jednoczesne unowocześnianie jednostek administracyjnych pod kątem wykorzystania nowych technologii oraz kompleksowa i przede wszystkim zgodna z obowiązującymi standardami bezpieczeństwa informacji obsługa istniejącej już papierowej dokumentacji jest najrozsądniejszym rozwiązaniem”* – komentuje Marcin Sobaniec, ekspert HSM Polska.

Mimo obowiązującej od październiku 2012 normy DIN 66399, wciąż brakuje wiedzy na temat zastosowania elementarnych zasad bezpieczeństwa informacji w codziennym życiu. Norma DIN 66399 (źródło: www.din66399.pl) jest dedykowana osobom odpowiedzialnym za bezpieczeństwo danych w firmie oraz osobom zaangażowanym w proces utylizacji. Określa ona wymagania dla procesów niszczenia oraz poszczególnych jego etapów. Norma definiuje trzy różne metody w zakresie niszczenia nośników danych. Każda z nich wymaga zdefiniowania i udokumentowania organizacji, personelu oraz poszczególnych etapów procesów. Często wyciek poufnych informacji to efekt niewiedzy lub zwykłego niedbalstwa osób, które mają z nimi do czynienia. Dlatego warto edukować pracowników w kwestii bezpieczeństwa danych.

*„W wynikach kontroli NIK niepokoić może fakt, że w wielu placówkach brakuje tak podstawowych rozwiązań jak Polityka Bezpieczeństwa Informacji, a w 8 na 10 placówek wykryto nieprawidłowości związane z bezpieczeństwem informacji. Badania ekspertów mówią o tym, że ponad 50 proc. wycieków poufnych danych następuje z winy pracowników*[*[4]*](http://#_ftn4)*. Wynikają one przede wszystkim z niewiedzy i zaniedbań. Edukacja kadr i budowanie świadomości zagrożeń, jakie niesie za sobą ryzyko nieprzestrzegania norm bezpieczeństwa informacji – te dwa czynniki powinny być kluczowym elementem procesu poprawy bezpieczeństwa w polskich urzędach. Powinniśmy także zwrócić uwagę na proces niszczenia dokumentacji zawierającej poufne dane. Najlepiej, jeśli odbywa się on wewnątrz organizacji, wtedy ryzyko wycieku jest zdecydowanie najmniejsze. Wykorzystywane do tego powinny być nowoczesne niszczarki, spełniające normy bezpieczeństwa, w szczególności. DIN66399. Takie niszczarki zapewniają całkowitą utylizację papierowych i cyfrowych nośników danych. Niemożliwe jest ich późniejsze odtworzenie. Natomiast do całego procesu powinna być dedykowana specjalnie przeszkolona osoba”* – podsumowuje Marcin Sobaniec, ekspert HSM Polska.

Poufne i tajne dokumenty zapisane na nośnikach optycznych, magnetycznych czy elektronicznych podlegają takiej samej ochronie, jak informacje zapisane na papierze. Z racji ilości zapisanych na nich danych, winny podlegać szczególnej ochronie. Po ich zdezaktualizowaniu należy je zniszczyć za pomocą odpowiedniej, gwarantującej pewność i bezpieczeństwo technologii. Należy także ograniczyć możliwość wypływu tego typu nośników poza struktury organizacji. Niszczenie elektronicznie przechowywanych danych bezpośrednio w miejscu ich powstawania jest najlepszym sposobem zapewnienia bezpieczeństwa. Dzięki temu mamy większą pewność, że wrażliwe informacje nie wyciekną. Trzeba pamiętać o tym, że zlecanie tego zadania podmiotom zewnętrznym zawsze wiąże się z ryzykiem ingerencji osób trzecich.

[[1]](http://#_ftnref1) Najwyższa Izba Kontroli

[[2]](http://#_ftnref2) Global Data Leakage Report

[[3]](http://#_ftnref3) Najwyższa Izba Kontroli

[[4]](http://#_ftnref4) Global Data Leakage Report