iT w administracji
Miesięcznik informatyków i menedżerów IT sektora publicznego

nr 6 (163) czerwiec 2021 | www.itwadministracji.pl

Z urzędu do chmury

Przenoszenie danych, dostęp do narzędzi, zarządzanie usługami

ISSN 1898-3227
cena 36,00 zł (w tym 8% VAT)

Inwestycje w bezpieczeństwo są niewidoczne... do czasu

Analiza badań i statystyk wskazuje, że wiele firm i organizacji traktuje cyberbezpieczeństwo bez należytej atencji. Jednocześnie – jak czytamy w raporcie „Global Digital IQ" firmy PwC – jest ono postrzegane jako kluczowa kompetencja dla ponad 80% firm na świecie i dla blisko 60% w Polsce. Okazuje się, że jedynie w 18% zbadanych podmiotów dyrektor ds. bezpieczeństwa informacji uważany jest przez zarząd za jednego z liderów. Aż w 80% firm i organizacji brakuje regularnego raportowania o stanie bezpieczeństwa.

Praktycy zajmujący się bezpieczeństwem wskazują, że o ile zarządy polskich firm znają już wartość, jaką generuje stosowanie nowych technologii, i potrafią z powodzeniem wdrażać je do swojego biznesu, o tyle w dalszym ciągu nie doceniają wyzwań związanych z naruszeniami bezpieczeństwa, które towarzyszą tym technologiom. Gdy prezesi światowych przedsiębiorstw w ogromnej większości mówią o cyberbezpieczeństwie jako kompetencji o kluczowym znaczeniu dla funkcjonowania firmy, w Polsce działania w tym zakresie często ograniczają się do formalnego osiągania zgodności z regulacjami, związanymi zwłaszcza z ochroną danych osobowych.

Co istotne, ochrona informacji jest zadaniem nie tylko dla działów IT. Świadomość wartości informacji oraz sposobów ich wykradania przez cyberprzestępców zmusza do współodpowiedzialności na poziomie całej organizacji. Zapewnienie bezpieczeństwa to proces, który powinien być zainicjowany dobrze wykonanym audytem, uwzględniającym wskazania analizy ryzyka dla konkretnego przedsiębiorstwa. Często dopiero audyt uświadamia kierownictwu, na jakie niebezpieczeństwa narażona jest cała organizacja. Po analizie wyników audytu zabezpieczeń systemowych należy zastanowić się nad przygotowaniem i implementacją polityki bezpieczeństwa. Istotnym jej elementem jest przewidywanie problemów i zapewnienie ciągłości działania w razie zaistnienia sytuacji kryzysowej. Bezwzględnie konieczne jest zaplanowanie ochrony fizycznej organizacji, dostosowanej do krytyczności przechowywanych repozytoriów informacji. Wykonanie tych działań, niezbędnych dla prawidłowego zabezpieczenia informacji gromadzonych i przetwarzanych w przedsiębiorstwie, pozwoli dobrać odpowiednie narzędzia IT. Warto przy tym wszystkim pamiętać, że w zakresie bezpieczeństwa najsłabszym ogniwem jest najczęściej człowiek, trzeba więc też zadbać o odpowiednie szkolenia.

Dlaczego wciąż w wielu organizacjach brakuje poważnego traktowania zagadnień dotyczących cyberbezpieczeństwa, nawet na poziomie budowania świadomości zagrożeń (security awareness)? Odpowiedź jest prosta. Inwestycji w cyberbezpieczeństwo nie widać z poziomu potencjalnego ich zwrotu i zysku organizacji. Nie widać ich jednak do czasu pierwszego incydentu, który będzie miał konkretny wymiar finansowy.

Tylko specjaliści wiedzą, jak wiele podejmowanych jest prób ataku każdego dnia na różne systemy, urządzenia, sieci, a nawet na budynki czy fabryki. W czasach, w których praca w coraz większym stopniu odbywa się online, cyberbezpieczeństwo jest wyzwaniem dla każdej organizacji, chcącej funkcjonować w nowoczesnym świecie. Podczas naszych realizacji wielokrotnie – z pozytywnym skutkiem – przekonywaliśmy klientów do kompleksowego i profesjonalnego potraktowania zagadnień dotyczących bezpieczeństwa cyfrowego.

Robert Baranowski
wiceprezes zarządu NASK SA