**Nieprzestrzeganie zasad zagraża danym rządowym**

**Według najnowszych badań instytucje, które powinny dawać przykład należytej ochrony wrażliwych danych, same nie spełniają wymaganych standardów.**

Przejmując nowe technologie, agencje rządowe starają się również wdrażać zasady odpowiedzialne za bezpieczeństwo danych. Jednak aż 80% z nich czuje się „podatnymi na zagrożenia”, a ponad jedna trzecia – „wyjątkowo zagrożonymi”.

Badania Thalesa pokazują, że prawie wszystkie (98%) agencje federalne wykorzystują wrażliwe dane w – ulegającym stałym przekształceniom – środowisku cyfrowym. W grę wchodzą tu takie technologie, jak magazynowanie i przetwarzanie danych w chmurze, big data, płatności mobilne, media społecznościowe, blockchain i internet rzeczy (IoT). Jednak mniej niż jedna trzecia respondentów korzysta w tych środowiskach z szyfrowania danych, które stanowi podstawę zabezpieczenia poufnych informacji – wynika z raportu.

W ramach swoich wysiłków, związanych z rewolucją cyfrową, agencje rządowe przechodzą stopniowo do środowisk wielochmurowych. 66% respondentów wykorzystuje 26 lub więcej aplikacji typu „oprogramowanie jako usługa” (ang. Software-as-s-Service – SaaS), a 41% – „platforma jako usługa” (ang. Platform-as-a-Service – PaaS). 78% przechowuje i przetwarza poufne dane w chmurze. Jak można się było spodziewać, wiele agencji wymienia „złożoność” jako główną przeszkodę w stosowaniu odpowiednich zabezpieczeń chroniących dane.

Biorąc pod uwagę, że ponad połowa (60%) agencji doznała już naruszenia, a więcej niż jedna trzecia (35%) była w ubiegłym roku celem ataku, wyniki niepokoją jeszcze bardziej. Według ankietowanych, trzy stojące przed nimi zadania o najwyższym priorytecie, to zarządzanie kryzysem po naruszeniu danych (30%), rozwiązywanie problemów dotyczących zgodności i prywatności danych (27%) oraz unikanie kar za naruszenie danych (24%). Warto odnotować, że jedna czwarta agencji nie przeprowadziła w ubiegłym roku audytu zgodności.

- *Ponieważ prewencja znajduje się na samym końcu – uporządkowanej według priorytetów – listy wydatków, agencje rządowe nie mają środków do obrony przed atakami hakerskimi, które coraz częściej wymierzone są w duże organizacje, w tym (ostatnio) w infrastrukturę krytyczną* - **wyjaśnia Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe** (www.bitdefender.pl).