aut. Tomasz Fastyn 28.07.2016

RAPORT: ZALEDWIE 23 PROC. PRZEDSIĘBIORSTW JEST WSTANIE OBRONIĆ SIĘ PRZED WYCIEKIEM DANYCH

Ponad trzy czwarte firm nie potrafi poradzić sobie z wyciekiem wrażliwych danych, według firmy WinMagic, która przeprowadziła ankietę wśród 250 menadżerów IT oraz tysiąca pracowników z działów IT. Nieco ponad 40 proc. pracowników twierdzi nadal że głównym organem w firmie odpowiedzialnym za cyberbezpieczeństwo jest właśnie dział informatyczny.

Może to wynikać z jednej strony z nieprzystosowania firm do samej tematyki cyberbezpieczeństwa, z drugiej znów strony z organizacji działów bezpieczeństwa wewnątrz samych struktur działów informatycznych. Jednak odpowiedzialność całego działu za bezpieczeństwo informatyczne nie jest według ekspertów rozważnym podejściem osób na stanowiskach menadżerskich. Jak wynika z badania, około 25 proc. kierowników działu IT poleca korzystanie pracownikom z urządzeń prywatnych do pracy z ważnymi dokumentami firmy.

Mimo, że wtedy osoby odpowiedzialne za cyberbezpieczeństwo nie mają żadnej kontroli na urządzeniami pracowników, co może doprowadzić do włamania hakerskiego, wyniesienia wrażliwych danych na pamięci laptopa lub wielu innych. Jeżeli administrator jest wstanie zarządzać połączeniami oraz operacjami wykonywanymi na laptopach, komputerach a nawet telefonach służbowych to może przeciwdziałać niektórym wydarzeniom bezpieczeństwa. Niecałe 40 proc. menadżerów nie widzi także nic złego w dostępie do działów o ograniczonym dostępie za pomocą urządzeń prywatnych pracowników.

W ankiecie potwierdzają się także badania przeprowadzone choćby przez instytut Ponemon, w którym uznano, że 70 proc. przypadków naruszenie bezpieczeństwa sieci wynikało z niedbalstwa pracowników niskiego i średniego szczebla. Jednak w ankiecie WinMagic, zagrożenie ze strony pracowników dla integralności infrastruktury wskazało 24 proc. pracowników działu IT, wyżej znajdowali się tylko hakerzy. Nie znamy dokładnej skali zjawiska jaka miała miejsca w firmach, jednak 17 proc. pracowników przyznało się do otwarcia załącznika z nieznanego adresu. Realna skala zjawiska może być inna. W dodatku korzystając z niezabezpieczonych prywatywnych urządzeń występuję ryzyko narażenia sieci na niebezpieczeństwo.

Czytaj też: Sektor medyczny jest najbardziej narażony na ataki