vmware

Cyberbezpieczeństwo wymaga nowego podejścia

Przeprowadzone w Polsce badania VMware ujawniły rozbieżność między zarządami a decydentami IT w zakresie określenia strategii cyberbezpieczeństwa organizacji. To, w połączeniu z koniecznością zarządzania rosnącą liczbą aplikacji, urządzeń i lokalizacji wymaga ponownego przemyślenia bezpieczeństwa cyfrowego.

Nieświadomy zarząd

Badania unaoczniły różnice między decydentami IT a biznesem:

28%

decydentów IT uważa, że:

kierownictwo wyższego szczebla powinno ponosić odpowiedzialność za wycieki danych.

71%

pracowników sądzi, że firmowe działy IT nie są w stanie zapewnić skutecznej ochrony przed cyberatakami.

Jednocześnie

90%

decydentów IT uważa, że działy zajmujące się ochroną danych nie ujawniają incydentów z zakresu bezpieczeństwa IT przed zarządem.

58%

decydentów IT postrzega ochronę danych jako jeden z najważniejszych priorytetów biznesowych.

Wzrastający poziom zagrożeń

Powyższa rozbieżność opinii pracowników i decydentów IT, w połączeniu ze złożonością coraz bardziej cyfrowego świata biznesu, oznacza potrzebę przemyślenia podejścia do kwestii cyberbezpieczeństwa:

70%

decydentów IT w Polsce jest zdania, że jedną z największych słabości ich organizacji (z perspektywy możliwego ataku cybernetycznego) jest fakt, że

zagrożenia ewoluują i rozprzestrzeniają się znaczenie szybciej niż mechanizmy obrony.

Ponad jedna trzecia (37%)

firm spodziewa się poważnego cyberataku w ciągu najbliższych

3 miesięcy

Roczny koszt naruszeń bezpieczeństwa wynosi

$445 mld*

i rośnie szybciej niż rosną wydatki na IT.

Zachowania pracowników

Ludzie i procesy są zagrożeniem na równi z technologią:

55%

decydentów IT wśród najbardziej znaczących wewnętrznych przyczyn istniejących trudności w utrzymaniu wysokiego poziomu cyberbezpieczeństwa uznało pracowników, którzy lekceważą procedury bezpieczeństwa lub nie są odpowiednio przeszkoleni.

Tylko 4% decydentów IT uważa, że kompetencje pracowników działów IT w zakresie cyberbezpieczeństwa są na dostatecznym poziomie.

Trzy czwarte

75%

pracowników otwarcie przyznaje, że byliby gotowi na świadome podjęcie

ryzyka związanego z naruszeniem bezpieczeństwa organizacji

na rzecz zwiększenia efektywności wykonywanej pracy.

Ponad połowa

56%

badanych pracowników używa **własnego urządzenia do uzyskania dostępu do danych służbowych, ponieważ jest lepsze niż to, które zostało zapewnione przez dział IT.**

5 sposobów na poprawę cyberbezpieczeństwa

Zadbaj o płynny przepływ informacji między działami IT i wyższą kadrą kierowniczą – dzięki temu wszyscy będą mieli pełny ogląd sytuacji.

Aby skutecznie chronić markę i utrzymać zaufanie klientów, upewnij się, że w razie wystąpienia naruszeń, możesz na nie szybko zareagować.

Upewnij się, że twoi podwładni znają reguły bezpieczeństwa i rozumieją zagrożenia, jakie płyną z niestosowania się do nich.

Oferując pracownikom mobilne narzędzia pracy, zapewnij ich całościową ochronę.

Wbuduj architekturę bezpieczeństwa zdefiniowaną programowo w infrastrukturę IT, by podnieść bezpieczeństwo od wewnątrz.

*Źródło: Center for Strategic and International Studies (CSIS)

O VMware

VMware (NYSE: VMW), światowy lider w dziedzinie infrastruktury chmury obliczeniowej i mobilności dla biznesu, ułatwia klientom cyfrową transformację ich przedsiębiorstw poprzez wprowadzanie do biznesu i IT rozwiązań definiowanych programowo.

Dzięki stworzonej przez VMware architekturze One Cloud, Any Application, Any Device organizacje mogą w nieograniczony sposób zwiększać wykorzystanie mobilności, wyróżniać się na tle konkurencji i szybciej reagować na pojawiające się w biznesie szanse. Takie możliwości dają im nowoczesne aplikacje udostępniane z chmury hybrydowej oraz zaawansowane rozwiązania cyberbezpieczeństwa, chroniące ich markę i poziom zaufania klientów. W 2015 r. firma VMware zanotowała przychód 6,6 mld USD, obsługując 500 tys. klientów oraz współpracując z 75 tys. partnerów na całym świecie. Więcej informacji na stronie www.vmware.com/pl

vmware NSX

vmware