

Badanie VMware: ponad jedna trzecia dużych polskich firm spodziewa się poważnego cyberataku w ciągu najbliższych trzech miesięcy

Polska, Warszawa, 25 maja 2016 r. — VMware Inc., światowy lider w dziedzinie infrastruktury chmury obliczeniowej oraz mobilności biznesu, publikuje wyniki badań przeprowadzonych w marcu 2016 roku przez TNS Polska w dużych polskich przedsiębiorstwach. Jak wynika z badań, ponad jedna trzecia (36 proc.) firm spodziewa się poważnego cyberataku w ciągu najbliższych trzech miesięcy.

- Pomimo tego, że prawie trzy czwarte (71 proc.) pracowników uważa, że firmowe działy IT nie są w stanie zapewnić skutecznej ochrony przed cyberatakami, jedynie 4 proc. decydentów IT jest świadomych konieczności utworzenia stanowiska Administratora Bezpieczeństwa Informacji (Data Protection Officer). Jednocześnie 18 proc. badanych decydentów IT jest przekonanych, że takie stanowisko już funkcjonuje w ich organizacjach.

Istniejące podatności wymagają nowego podejścia do kwestii bezpieczeństwa

Polskie firmy w coraz większym stopniu są narażone na poważne naruszenia prywatności oraz wyciek informacji. Obecne metody zabezpieczeń coraz częściej okazują się nieskuteczne wobec stale zmieniających się oraz coraz bardziej złożonych zagrożeń istniejących w cyfrowym świecie biznesu. 70 proc. 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 znacznie szybciej niż mechanizmy obrony.

- Rozbieżność między opiniami pracowników i decydentów IT stanowi wyzwanie dla organizacji, które stoją w obliczu zmian, które niesie ze sobą cyfrowa transformacja biznesu. Przedsiębiorstwa muszą zacząć kłaść nacisk na wypracowanie odpowiednich mechanizmów, które pozwolą im na skuteczną ochronę reputacji i które umożliwią utrzymanie zaufania klientów. Aktualnie pracownicy mają dostęp do danych i aplikacji z każdego miejsca i z poziomu wielu różnych urzędzeń, a to wymaga zerwania z tradycyjnym podejściem do kwestii bezpieczeństwa IT, które dziś już nie wystarcza do zapewnienia skutecznej ochrony – mówi Paweł Korzec, Systems Engineering Manager – Eastern Europe, VMware

Pracownicy muszą być zaangażowani w kwestie utrzymania cyberbezpieczeństwa

Przebadani decydenci IT wśród najbardziej znaczących wewnętrznych przyczyn istniejących trudności w utrzymaniu wysokiego poziomu cyberbezpieczeństwa uznali pracowników, którzy lekceważą procedury bezpieczeństwa lub nie są odpowiednio przeszkoleni (55 proc.).

- Niniejsze badanie pokazuje także działania, które podejmują pracownicy w celu zwiększenia produktywności. Ponad połowa (56 proc.) badanych pracowników używa własnego urządzenia do uzyskania dostępu do danych służbowych, ponieważ jest lepsze niż to, które zostało zapewnione przez dział IT.
- Jednocześnie trzy czwarte (75 proc.) otwarcie przyznaje, że byliby gotowi na świadome podjęcie ryzyka związanego z naruszeniem bezpieczeństwa organizacji na rzecz zwiększenia efektywności wykonywanej pracy.

O badaniu

Badanie zostało przeprowadzone w marcu 2016 roku przez agencję badawczą TNS Polska na próbie 50 decydentów IT oraz 100 pracowników w firmach działających w Polsce oraz zatrudniających powyżej 250 osób. Zastosowana metodologia obejmowała wywiady telefoniczne (CATI) oraz ankiety przeprowadzone online (CAWI).