8 na 10 firm deklaruje gotowość zapłaty okupu w przypadku ataku ransomware!

Eksperci VECTO opublikowali właśnie siódmą edycję raportu VECTO: „Cyberbezpieczeństwo w polskich firmach 2024". To coroczna, szczegółowa analiza świadomości zagrożeń i stosowanych przez polskie przedsiębiorstwa rozwiązań w obszarze ochrony danych IT, a także najważniejszych trendów w dziedzinie cyberbezpieczeństwa. Badanie potwierdza, że w kontekście wzrostu skali cyberzagrożeń, przedsiębiorstwa i instytucje muszą podejmować intensywne działania, związane z zabezpieczeniem infrastruktury informatycznej oraz rozwijaniem kompetencji tzw. czynnika ludzkiego. W przeciwnym razie ciężko będzie im sprostać wszystkim wyzwaniom, które przyniesie cyfrowa przyszłość i geopolityczne napięcia w naszej części Europy.

Autorzy Raportu VECTO alarmują - niemal 74 proc. polskich firm potwierdza wystąpienie cyberincydentu, który mógł naruszyć integralność danych. Ponad 79 proc. przedsiębiorstw deklaruje gotowość zapłacenia okupu w przypadku ataku ransomware. Jednocześnie tylko 28 proc. firm uważa, że infrastruktura IT w ich firmach jest prawidłowo zabezpieczona. To tylko kilka z wielu zaskakujących danych, które przynosi siódma już edycja Raportu. Eksperci VECTO podkreślają, że w polskiej przestrzeni informatycznej największe zagrożenia to phishing, ransomware, błędy ludzkie i nieodpowiednia ochrona urządzeń mobilnych. To one w głównej mierze odpowiadały za liczne incydenty, których doświadczały w 2024 roku polskie firmy i instytucje. Odnotowane i potwierdzone cyberzdarzenia stanowią bezsporny dowód na to, że cyberprzestępcy atakują dziś nie tylko duże i średnie korporacje, ale również małe podmioty i instytucje publiczne. Gromadzone analizy, w tym statystyki prezentowane przez CERT Polska kreślą pesymistyczny obrazy aktualnego stanu rzeczy - skala zagrożeń rośnie lawinowo, a cyberprzestępcy coraz częściej, wykorzystując kompilację technologii i praktyk manipulacyjnych, atakują zarówno przedsiębiorstwa, jak i indywidualnych

użytkowników.

Respondenci badania VECTO wyróżniają branżę finansową, medyczną oraz administrację publiczną, jako potencjalnie najbardziej narażone na cyberataki. Sektor finansowy zresztą od lat pozostaje głównym celem cyberprzestępców, ze względu na gromadzone dane wrażliwe oraz przypuszczalnie wysokie straty finansowe. Od okresu pandemii, corocznie obserwujemy również spektakularne ataki na branżę medyczną, zarówno lokalnie, jak i globalnie. Administracja publiczna i jednostki zarządzające tzw. infrastrukturą krytyczną także odnotowują znaczący wzrost cyberincydentów, co może być związane ze szczególną sytuacją geopolityczną naszej części Europy. Zwłaszcza, że nie brakuje dziś dowodów, że za częścią z nich stały międzynarodowe grupy cyberprzestępców, zwykle inspirowanych i finansowanych przez rządy obcych państw. W porównaniu z danymi z zeszłorocznej edycji Raportu, wzrosła liczba incydentów w sektorze e-commerce oraz małych przedsiębiorstw i mikrofirm, dla których najczęściej barierą kompleksowego zabezpieczenia i niezbędnej modernizacji infrastruktury IT są ograniczone środki inwestycyjne.

„Przez Polskę przetacza się aktualnie front cyberkonfliktu. Cyberprzestępcy atakują coraz skuteczniej i na coraz większą skalę, a rodzime firmy i instytucje, w tym zarządzające infrastrukturą krytyczną, znajdują się w centrum tych wydarzeń. Wierzymy, że nasz raport dostarczy polskim przedsiębiorstwom praktycznych wskazówek i danych, które pomogą im skuteczniej identyfikować zagrożenia, zapobiegać incydentom oraz chronić swoje informatyczne zasoby. Tylko poprzez inwestycje w nowoczesne technologie, rozwój kompetencji każdego użytkownika firmowej sieci IT i podnoszenie świadomości na wszystkich szczeblach organizacji możemy stworzyć realne zabezpieczenia przeciwko eskalującym dziś zagrożeniom” – podkreśla Jakub Wychowański, Prezes Zarządu VECTO.

VECTO działa na polskim rynku od 2008 roku. Spółka dostarcza i wdraża systemy informatyczne oraz świadczy usługi outsourcingu IT dla firm. Specjalizuje się w kompleksowym zabezpieczaniu danych oraz projektowaniu efektywnych narzędzi backupu. VECTO jest autorem corocznego raportu „Cyberbezpieczeństwo w polskich firmach”, stanowiącego analizę świadomości zagrożeń i rozwiązań w zakresie bezpieczeństwa i ochrony danych, stosowanych przez polskie firmy. Eksperci spółki prowadzą również bezpłatne webinary w ramach cyklu Vtorki Technologiczne, podczas których dzielą się wiedzą i kompetencjami w obszarze IT oraz cyberbezpieczeństwa.

Pełna wersja raportu jest dostępna pod adresem: https://vecto.pl/raport-2024

VECTO