



Postępująca cyfryzacja polskich przedsiębiorstw oraz rosnący trend hybrydowych systemów pracy, dla których impulsem rozwoju stała się pandemia, przełożyły się bezpośrednio na wzrost cyberzagrożeń. Już niemal 70 proc. rodzimych firm potwierdza odnotowanie incydentów naruszających bezpieczeństwo danych. To znacząca różnica względem ubiegłorocznych wyników Raportu – o ponad 8 punktów procentowych. Tegoroczny Raport VECTO podsumowuje piątą już edycję badania diagnozującego stan świadomości cyberzagrożeń oraz stosowane w polskich firmach rozwiązania w zakresie bezpieczeństwa IT.

Według szacunków, do 2025 roku globalne skutki cyberincydentów kosztować będą poszkodowane firmy i instytucje ok. 10,5 bln dolarów rocznie. Przekonanie, że udział w tej zawrotnej kwocie ominie polskie firmy jest irracjonalne. Jak wynika z Raportu VECTO już 69,93 proc. rodzimych przedsiębiorstw musiało zmierzyć się z różnymi formami ataków. Z pewnością, część firm, które stanęły w obliczu konieczności poniesienia kosztów utraty dostępu do zasobów IT zdecydowała o konieczności zakończenia działalności. Straty wynikające z opóźnienia procesów, czy odbudowy infrastruktury i baz danych często przewyższają wartość oczekiwanego przez cyberprzestępców okupu. Ten z kolei, według Webroot Brightcloud Threat, w 2021 roku wyniósł średnio w skali globalnej 233 817 USD – i był o 30 proc. wyższy, niż w 2020 r. Nie istnieją obecnie rzetelne dane, które wskazywałyby średnią wartość okupu płaconego przez polskie firmy. Można jednak przyjąć, że wiele z nich nie ma oporów przed pertraktowaniem z przestępcami, bowiem 60 proc. badanych przez VECTO podmiotów potwierdziło, że byłoby skłonnych zapłacić okup za odzyskanie zaszyfrowanych lub skradzionych danych.

„Warto podkreślić, że inwestycja w zabezpieczenie danych nie tylko jest mniej kosztowna niż wartość oczekiwanego przez hakerów okupu, ale przede wszystkim radykalnie zmniejsza ryzyko wystąpienia cyberincydentu i innych zagrożeń dla prawidłowego funkcjonowania firmowej infrastruktury IT. Na szczęście przedsiębiorstw, które odpowiedzialnie podchodzą do kwestii bezpieczeństwa informatycznego jest coraz więcej, o czym może świadczyć również fakt, że w 2021 roku rynek ochrony przed cyfrowymi zagrożeniami wzrósł o 10 proc. a prognozy na 2022 przewidują dalsze wzmocnienie tego trendu” – mówi Jakub Wychowański, prezes zarządu VECTO.

Jak się zabezpieczamy?

Polskie firmy, według opinii 38 proc. respondentów badania VECTO, nie monitorują zagrożeń wynikających z cyberprzestępczości. Przeciwnego zdania jest co 4 ankietowany, zaś 35 proc. przyznało, że nie ma wiedzy na temat podejmowanych przez pracodawcę działań w tym zakresie. Zważywszy jednak na fakt, że tylko 14,68 proc. firm ma przygotowany scenariusz postępowania w przypadku wystąpienia incydentu naruszającego bezpieczeństwo danych, można wnioskować, że choć świadomość rośnie, to nie przekłada się ona na realne działania prewencyjne lub strategię minimalizacji kosztów skutecznie przeprowadzonych ataków. Odsetek firm przyznających, że takich procedur nie

wdrożono wyniósł 39 proc., odpowiedź „nie wiem” wskazało aż 45,84 proc. ankietowanych. Nieznajomość procedur dotyczących postępowania po naruszeniu integralności danych skłania do wniosku, że w przytłaczającej większości firm takie procedury nie istnieją lub są źle komunikowane pracownikom.

W ocenie respondentów badania, najskuteczniejszą metodą ochrony przed cyberzagrożeniami są programy antywirusowe. Taką odpowiedź wskazało 76,21 proc. ankietowanych. Względem ubiegłorocznego badania wzrósł również odsetek wskazujących rozwiązania z zakresu backup’u danych – 12,13 proc. Szkolenia wskazało 6,65 proc, procedury bezpieczeństwa zaś 3,11 proc. Połowa wszystkich użytkowników komputerów służbowych przyznała, że sprzęt jest zabezpieczony programem antywirusowym (49,59 proc.), a na 10,84 proc. urządzeń jest zainstalowane również rozwiązanie zapewniające automatyczny backup. Z haseł dostępu korzysta 29 proc. respondentów. Brak jakichkolwiek zabezpieczeń deklaruje tylko 1,73 proc. pytanym.

Pandemia i praca zdalna wymusza inwestycje w IT

Częstsze wykorzystanie hybrydowych modeli pracy i pracy zdalnej przekłada się bezpośrednio na wzrost deklarowanych inwestycji w infrastrukturę IT. Trend ten obserwujemy od początku pandemii i w ostatnim roku został on utrzymany. 83 proc. ankietowanych potwierdza, że ich firmy inwestują w rozwiązania zapewniające zachowanie ciągłości pracy i procesów. Czterokrotnie wzrósł również (względem danych z poprzedniego raportu) odsetek ankietowanych (48,51 proc.), którzy przyznali, że ich firma wdrożyła dodatkowe zabezpieczenia dla pracujących zdalnie. Dynamika ta koresponduje również ze świadomością ankietowanych, że pandemia i wynikająca z niej weryfikacja dotychczasowych systemów pracy zwiększa ryzyko wystąpienia cyberataku. Tego zdania jest 88 proc. respondentów. Z tezą tą nie zgadza się 4,51 proc. uczestników badania.

Dotkliwe skutki cyberataku

Zapytaliśmy naszych respondentów, w jakich obszarach upatrują najbardziej dotkliwych skutków ataku. Choć, podobnie jak w roku ubiegłym, najwięcej osób wskazało uszczerbek w bazie i relacjach z kontrahentami (29,89 proc.) i niebezpieczeństwie utraty unikalnego know-how i własności intelektualnej (24,78 proc.), to zanotowaliśmy znaczący wzrost udziału odpowiedzi „korespondencja firmowa” – z 3,75 proc. w 2021 roku do 17,44 proc. obecnie. Respondenci mogą zatem być obserwatorami kłopotów z wyciekiem maili urzędników państwowych i doceniamą niebezpieczeństwa, w tym wizerunkowe, wynikające z tego typu zdarzeń. Badani obawiają się również utraty dokumentacji przedsiębiorstwa (8,91 proc.) i przejęcia kontroli nad stroną internetową (17,10 proc.).

„W kontekście polskich firm, wyniki Raportu wskazują wyraźnie, że postęp technologiczny wyprzedza świadomość zagrożeń. Bez wątpienia należy docenić rodzimy biznes za zmiany, które dokonały się na przestrzeni ostatnich pięciu lat, od kiedy opublikowaliśmy pierwszą edycję naszego Raportu. Pamiętajmy jednak, że wyścig trwa, a cyberprzestępcy w ostatnich latach nie odpoczywali. Przeciwnie, wciąż powiększają i urozmaicają arsenał swoich możliwości, a rosnąca liczba ataków dowodzi, że są w swojej działalności niezwykle skuteczni. To, w jakim stopniu ich aktywność dotknie polskie firmy w głównej mierze zależy od naszej gotowości i podjętych działań prewencyjnych. Parafrazując znane powiedzenie, chcąc prowadzić satysfakcjonującą działalność biznesową, musimy szykować się na cyberwojnę” – dodaje Jakub Wychowański.

Więcej o wynikach badania polskich przedsiębiorstw w Raporcie:

<https://vecto.pl/doc/Vecto-Cyberbezpieczenstwo-polskich-firm-2022.pdf>

VECTO