- 68,9 proc. polskich firm potwierdza zanotowanie cyberincydentu - to wzrost o niemal 5 proc. w porównaniu z danymi sprzed roku.
- 82,8 proc. odpowiedziało, że zabezpieczanie danych informatycznych w firmie jest ważne.
- Aż 72,2 proc. uczestników badania przyznało, że zapłaciłoby okup w przypadku ataku typu ransomware.
- Najbardziej zagrożone cyberatakami: sektor bankowy i finansowy, branża medyczna, administracja i instytucje publiczne.

Wystąpienie cyberincydentu potwierdza już 68,9 proc. polskich przedsiębiorstw. I choć, jak wskazują wyniki najnowszego Raportu VECTO: „Cyberbezpieczeństwo w polskich firmach 2023", świadomość cyberzagrożeń wzrasta, to wciąż zbyt wolno przekłada się ona na realne działania w obszarze ochrony danych systemów IT. W zakresie świadomości istniejących rozwiązań zabezpieczających infrastrukturę informatyczną, respondenci mają dość konserwatywne podejście, a przygotowanie procedur na wypadek ataku hakerskiego deklaruje zaledwie 26,4 proc. badanych firm. W przypadku wystąpienia incydentu ransomware, 72,2 proc. respondentów badania rozważyłoby zapłacenie okupu. Wśród branż szczególnie narażonych na cyberataki są: sektor bankowy i finansowy, branża medyczna i instytucje administracji publicznej.

VECTO publikuje swój coroczny Raport: Cyberbezpieczeństwo w polskich firmach już po raz szósty. To ważny dokument wpisujący się w konieczność budowania świadomości cyberzagrożeń i diagnozowania gotowości polskich firm i instytucji do stawiania czoła współczesnym cyberwyzwaniom. Szczególnie, że najnowsza edycja Raportu potwierdza ogólnodostępne dane, dotyczące wyraźnego wzrostu incydentów, publikowane przez CERT Polska. Przypomnijmy, w 2022 r. do CERT Polska wpłynęło ponad 322 tys. zgłoszeń, o skutkowało obsłużeniem 39 tys. incydentów. To ponad 34 proc. wzrost zarejestrowanych incydentów w zestawieniu z 2021 r., zaś liczba wszystkich zgłoszeń wzrosła o blisko 178 proc. Dane te wprost korespondują ze statystykami globalnymi. Ubiegły rok na świecie był po raz kolejny rekordowy pod względem cyberataków – ich liczba wzrosła aż o 38 proc. Według autorów Raportu, doświadczenia cyberataku potwierdza już 68,9 proc. polskich firm, a zatem o 5 proc. więcej względem roku poprzedniego. Konsekwentny wzrost ryzyka ataków

wynika również z czynników geopolitycznych i trwających obecnie kryzysów, które bez wątpienia zachęciły cyberprzestępców do większej aktywności w naszej części Europy.

W rankingu NCSI zajmujemy 11. lokatę wśród wszystkich państw, które w najbliższym czasie będą zmagały się z rosnącą liczbą cyberincydentów. Potwierdzeniem dla wyników naszego badania oraz dostępnych ekspertyz są liczne, spektakularne ataki na polskie firmy i instytucje, których świadkami byliśmy w tym i mijających latach. „Pandemia, wojna w Ukrainie, aktywność Chin na arenie międzynarodowej i ich konflikt gospodarczy z USA, których w ostatnich latach świadkami jesteśmy, stanowiły istotny impuls dla dynamicznego wzrostu zagrożeń w obszarze cyberbezpieczeństwa. Coraz groźniejsze incydenty, tak dotkliwie doświadczające firmy na całym świecie, stają się również przykrą rzeczywistością dla wielu polskich firm. Poprzednie edycje Raportu VECTO niezbicie dowodziły, że skala zagrożeń jest niezmiennie w tendencji rosnącej, kreśląc pesymistyczne perspektywy dla przedsiębiorstw wielu branż i instytucji publicznych" – mówi Jakub Wychowański, prezes zarządu VECTO, spółki wdrażającej rozwiązania w zakresie cyberbezpieczeństwa i ochrony danych.

Wysokie koszty ransomware

Według różnych szacunków, codziennie powstaje ponad 316 tysięcy wariantów złośliwego oprogramowania. Już w 2022 roku przeciętny okup za odszyfrowanie danych kosztował polskie przedsiębiorstwa średnio 670 tys. zł., co często stanowi kwotę wielokrotnie wyższą, niż inwestycje w skuteczne rozwiązania chroniące firmową infrastrukturę IT. Podkreślić należy, że mówimy o uśrednionych kosztach ataków, wiemy bowiem o przypadkach strat liczonych w dziesiątkach milionów złotych. Jednak, jak wskazują wyniki Raportu, 72,2 proc. badanych firm rozważa zapłacenie okupu w przypadku wystąpienia incydentu ransomware, co wyraźnie wskazuje, że wiele firm czuje się bezbronnych w obliczu takiego zagrożenia. Może to wynikać m.in. z faktu, że zdecydowana większość firm nie posiada procedur bezpieczeństwa, które minimalizują zagrożenia wynikające z tzw. czynnika ludzkiego. Analitycy wskazują, że 60 proc. naruszeń systemów ma w sobie element inżynierii społecznej i wpływu oraz manipulacji wywieranych wprost na ludzi. To właśnie na błędach użytkowników przestępcy najczęściej opierają swoje działania i są w tym aspekcie brutalnie skuteczni. Co ciekawe, perspektywa zapłacenia okupu ulega zdecydowanej zmianie, gdyby atak ransomware dotyczył prywatnych danych użytkowników. W takim przypadku, aż 78,8 proc. respondentów jednoznacznie deklaruje brak gotowości do pertraktowania z przestępcami.

Zagrożone branże

Niezmiennie, większość respondentów badania, jako główne źródło cyberzagrożeń wskazuje nieznane grupy hakerów - 67,9 proc., ale warto zauważyć, że odsetek ten wzrósł o niecałe 7 proc. w skali roku. 12 na 100 ankietowanych uważa, że za cyberincydentami stać może nieuczciwa konkurencja, a niemal co piąty twierdzi, że obecni pracownicy. W kontekście wystąpienia cyberataku, zdecydowanie najwięcej badanych firm obawia się utraty bazy klientów i kontaktów (34,6 proc.), unikalnego know-how i własności intelektualnej (25,9 proc.), a także utraty kontroli nad stroną internetową (21,7 proc.). Rzadziej martwimy się o korespondencję firmową czy dokumentację (kolejno 11,2 proc. oraz 4,1 proc.). Możemy zatem wnioskować, że wiele z badanych firm identyfikuje swoje mocne strony w konkurencyjności, przede wszystkim opartej na wypracowanych relacjach z otoczeniem biznesowym, unikalności produktów i usług, kompetencjach pracowników, własnych technologiach czy patentach. Obawiamy się również efektów ataku na stronę internetową, co jest z pewnością związane z faktem, że coraz częściej jest to podstawowy kanał dotarcia do klientów i kontrahentów. Zmiany w porównaniu z badaniem z ubiegłego roku obserwujemy również w kontekście oceny respondentów branż, które są szczególnie narażone na działania cyberprzestępców. O ile wciąż uważamy, że widomo ataku hakerskiego to codzienność dla podmiotów sektora finansowego i bankowego (25,5 proc.) oraz sektor usług medycznych (20,7 proc.), to na trzecie miejsce awansowała administracja publiczna, która zanotowała wzrost wskazań z 7 proc. w 2022 roku do 18,1 proc. w tegorocznym badaniu.

Zdaniem ekspertów i obserwatorów rynku cyberbezpieczeństwa kolejne lata przyniosą dalsze wzrosty zagrożeń. Postępująca digitalizacja w każdym wymiarze biznesu i codziennego życia społeczeństw na całym świecie, które jak nigdy dotąd doświadczają zalet i wad niesionych pojęciem globalnej wioski, rozwijająca się technologia IoT, a nawet rozpalająca opinię publiczną dyskusja o przyszłości sztucznej inteligencji stanowić będą podatny grunt dla kreatywności i zwiększania skuteczności działań cyberprzestępców. To dość pesymistyczna perspektywa, którą wszyscy powinniśmy uwzględniać w definiowaniu najważniejszych wyzwań dla polskich przedsiębiorstw i instytucji w

nadchodzących latach.

„Analiza tegorocznych wyników badania VECTO wskazuje jednak, że świadomość zagrożeń rośnie. Nie możemy jednak zapominać, że w dużej mierze jest to nauka na błędach niemal 70 proc. polskich przedsiębiorstw, które potwierdziły wystąpienie ataków naruszających bezpieczeństwo i integralność danych. Dziś żadna firma, podmiot, instytucja, żaden indywidualny użytkownik sieci internetowej nie powinien zadawać sobie pytania czy jego infrastruktura IT zostanie zaatakowana. Właściwe pytanie brzmi bowiem: kiedy to nastąpi. Warto zatem wykorzystać czas, by się do tego doświadczenia stosownie przygotować. Tym bardziej, że innowacyjnych, skutecznych rozwiązań, a również ekspertów dysponujących odpowiednimi kompetencjami do ich wdrożenia na polskim rynku nie brakuje" – podsumowuje Jakub Wychowański.

Link do Raportu: https://vecto.pl/raport-2023

VECTO