- 64,17 proc. potwierdza cyberincydenty – to wzrost o 19 proc. w porównaniu z danymi sprzed roku.
- 92 proc. ankietowanych potwierdza korzystanie ze sprzętu firmowego do celów prywatnych.
- Mniej niż co druga firma korzysta ze wsparcia specjalistów w zakresie cyberbezpieczeństwa.
- Tylko 23,75 proc. ankietowanych potwierdza, że firmowa sieć w ich firmie nie jest prawidłowo zabezpieczona.
- Najbardziej zagrożone cyberatakami: sektor bankowy, medyczny, firmy farmaceutyczne.

Już prawie 65 proc. polskich firm zetknęło się z cyberincydentem zagrażającym bezpieczeństwu danych i systemów IT. Trwająca pandemia i zmieniające się modele prowadzenia biznesu generują zupełnie nowe zagrożenia. Tymczasem tylko 48 proc. rodzimych przedsiębiorstw korzysta ze wsparcia specjalistów w zakresie cyberbezpieczeństwa. Coraz powszechniejsza praca zdalna nie przełożyła się na wzrost inwestycji w ochronę danych, choć 92 proc. respondentów przyznało, że korzysta ze sprzętu firmowego do celów prywatnych. W ocenie Polaków, szkodliwego oprogramowania i aktywności hakerów powinny obawiać się przede wszystkim instytucje bankowe, podmioty służby zdrowia i firmy farmaceutyczne.

Raport: Cyberbezpieczeństwo w polskich firmach 2021 to już czwarta edycja badania, w którym VECTO analizuje stopień przygotowania i świadomość zagrożeń rodzimych przedsiębiorstw w zakresie ochrony danych i systemów IT. Wydarzenia ubiegłego roku, z oczywistych względów, skierowały atencję autorów opracowania na nowe obszary bezpieczeństwa danych. Koronawirus stał się bowiem katalizatorem głębokich przemian na wielu płaszczyznach. Wymusił zmiany organizacyjne, które w połączeniu z rozwojem takich technologii, jak AI, IoT, Big Data czy rozwiązań chmurowych, zrewolucjonizował model prowadzenia biznesu i spopularyzował koncept pracy zdalnej. Efektem tych zmian jest wyraźne zwiększenie ruchu w sieci, przesyłanych informacji, a także i czasu, jaki użytkownicy spędzają przed ekranami komputerów i urządzeń mobilnych.

„W cieniu szans, wynikających z digitalizacji i wzrostu udziału nowoczesnych technologii w biznesie, kryją się jednak zagrożenia. Cyberprzestępczość wkroczyła w swoją złotą erę, a jej skala rośnie w zastraszającym tempie. Światowe dane wskazują, że w ciągu doby notowanych jest ponad 17,5 mln cyberincydentów. Swoje żniwo zbiera wciąż oprogramowanie ransomware.

Polskie firmy również muszą być przygotowane na czarne scenariusze, albowiem nasz kraj już znalazła się w gronie 20 państw najbardziej narażonych na cyberataki” – mówi Jakub Wychowański, członek zarządu VECTO.

Cyberincydent już w 64 proc. polskich firm

Drastycznie, względem danych z lat ubiegłych wzrósł odsetek firm, które stały się celem cyberataku lub odnotowały incydenty zagrażające bezpieczeństwu systemów IT i integralności danych. 64,17 proc. firm potwierdziło odnotowanie zdarzenia, które stanowiło zagrożenie lub wprost doprowadziło do utraty lub zaszyfrowania danych firmowych. Oznacza to wzrost o 19 proc. względem danych za rok 2019. Trend ten, połączony z niewątpliwie rosnącą świadomością cyberzagrożeń wśród Polaków, znajduje odzwierciedlenie w odpowiedziach na pytanie: „Czy uważasz, że sieć w Twojej firmie jest prawidłowo zabezpieczona?". O ile w poprzednich edycjach odpowiedź „tak" uzyskała 44 proc., o tyle w raporcie za 2020 rok odsetek ten wyraźnie spadł do poziomu 23,75 proc. Wzrosła za to liczba odpowiedzi „nie" oraz „trudno powiedzieć", notując kolejno 32,5 proc. i 35,42 proc.

Koresponduje to również ze wzrostem odsetku przedsiębiorstw, które nie korzystają z usług specjalistów w dziedzinie bezpieczeństwa danych – z 46 proc. w 2019 roku do niemal 52 proc. w 2020 roku. Deklarację korzystania ze specjalistów w zakresie cyberbezpieczeństwa złożyło łącznie 48,33 proc. badanych firm, z tego 26,25 proc. dysponuje tego typu kompetencjami inhouse, a 22,08 firm zleca obsługę obszaru ochrony systemów i danych IT na zewnątrz.

Zagrożenia? Hakerzy i my sami!

Za cyberincydenty winimy przede wszystkim nieznane grupy hakerów (62 proc.). Podobnie jak w latach poprzednich ta odpowiedź była wskazywana najczęściej w kontekście pytania o źródła zagrożeń bezpieczeństwa IT. Na drugim miejscu uplasowaliśmy samych siebie – obecni pracownicy, w ocenie 24,58 proc. respondentów, odpowiadają za naruszenie integralności systemów informatycznych. 11,25 proc. wskazało nieuczciwą konkurencję.

Praca zdalna – dodatkowe zabezpieczenia w zaledwie co 10 firmie

Skalę potencjalnych niebezpieczeństw obrazują kolejne dane. Aż 91,67 proc. naszych ankietowanych stwierdziło, że dostęp do firmowej infrastruktury IT,
w tym komputerów, smartfonów, tabletów ma od 90 do 100 proc. wszystkich pracowników. Choć ogromna część zatrudnionych pracuje do dziś zdalnie, to w aż 88 proc. badanych firm nie wprowadzono żadnych dodatkowych zabezpieczeń dla pracowników w trybie home office. Jedynie 12 proc. ankietowanych przedsiębiorstw podjęło takie działania. Dane są zaskakujące, gdy skonfrontujemy je z analizą odpowiedzi na pytanie, czy wspomniana praca zdalna w dobie koronawirusa zwiększa ryzyko wystąpienia cyberzagrożeń. Twierdząco odpowiedziało aż 82 proc. badanych firm.

Polskie firmy łatwym celem?

„W polskich przedsiębiorstwach wciąż pokutuje przeświadczenie, że nie są one interesującym celem ataków. Jednakże w katalogu firm i instytucji, którym przyszło się zmierzyć w ubiegłym roku z konsekwencjami cyberataków, nie znajdujemy wyłącznie podmiotów z pierwszych stron gazet. Znane marki wśród ofiar cyberprzestępców to jedynie czubek góry lodowej. Na jej fundament, niewidoczny pod powierzchnią oceanu szkodliwego oprogramowania, ransomware, szpiegostwa gospodarczego, phishingu i wielu innych narzędzi cyberprzestępców, składa się dramat małych i średnich firm. Setki polskich przedsiębiorstw i tysiące użytkowników codziennie zdaje sobie sprawę, że nie dostrzegli w porę zagrożeń dzisiejszego cyberświata" – mówi Jakub Wychowański.

Tymczasem rynek jest pełen interesujących rozwiązań, które pozwalają skutecznie przygotować się na ewentualność naruszenia integralności danych. Nie zawsze są to narzędzia kosztowne, choć i te, oferowane dziś w modelu subskrypcyjnym, nie są nieosiągalne dla podmiotów o mniejszych możliwościach finansowych. „Doświadczenia na polskim rynku, a także wyraźne trendy globalne powinny być wystarczającą rekomendacją dla każdego odpowiedzialnego przedsiębiorcy i zachętą do weryfikacji dotychczasowej strategii zabezpieczenia danych i infrastruktury IT. Tylko dbając o bezpieczeństwo firmowych danych i zasobów informatycznych, możemy skutecznie zadbać o przyszłość naszego biznesu" – podsumowuje Jakub Wychowański.

Link do Raportu:

https://vecto.pl/doc/Vecto-Cyberbezpieczenstwo-polskich-firm-2021.pdf

VECTO sp. z o.o. działa od 2008 roku. Firma łączy kilkudziesięcioletnie doświadczenie kadry kierowniczej z potencjałem młodego zespołu, który rozumie realia rynku IT i wyzwania stojące przed firmami i instytucjami wobec dynamicznie zmieniającej się technologii.
Spółka dostarcza i wdraża systemy informatyczne oraz świadczy usługi outsourcingu IT dla firm. Oferuje kompleksowe rozwiązania zabezpieczania danych oraz backupu w oparciu o produkty renomowanej firmy DELL EMC. Wszystkie prace wdrożeniowe wykonuje zespół certyfikowanych, doświadczonych inżynierów.
W 2021 roku, VECTO została uhonorowana prestiżowym tytułem Diamentu Forbesa. Nagroda ta przyznawana jest firmom, które w ciągu ostatnich trzech lat rozwijały się najszybciej i osiągnęły największy wzrost. Wśród najważniejszych kryteriów znalazły się również takie elementy, jak wartość majątku, wiarygodność biznesowa i brak negatywnych zdarzeń prawnych. Za rzetelne opracowanie wyników odpowiada redakcja magazynu Forbes oraz wywiadownia gospodarcza Bisnode Polska. W 2019 i 2020, roku, spółka znalazła się wśród laureatów Gazel Biznesu, przyznawanych przez redakcję dziennika Puls Biznesu.
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.

VECTO