- Już niemal 40 proc. polskich firm zetknęło się ze zjawiskiem cyberprzestępczości.
- Tylko 14 proc. telefonów i mniej niż połowę komputerów służbowych zabezpieczamy programem antywirusowym.
- 70 proc. respondentów nie wie, jak zareagować w chwili stwierdzenia cyberzagrożenia.

VECTO ponownie zbadała polskie firmy pod kątem świadomości cyberzagrożeń i wdrażanych zabezpieczeń. Wnioski nie są optymistyczne. Choć już niemal 40 proc. przedsiębiorstw odnotowała incydenty zagrażające bezpieczeństwu danych, wciąż niewłaściwie je chronimy. Nie rozumiemy również, że urządzenia mobilne to dziś integralny element infrastruktury IT, który jednocześnie hakerzy coraz chętniej wykorzystują w swojej przestępczej działalności. Publikacja raportu VECTO związana jest z Dniem Bezpiecznego Internetu, który obchodzimy 5 lutego.

W 2018 r. liczba ataków hakerskich drastycznie wzrosła. Tylko w drugim kwartale skutki działań cyberprzestępców dotknęły 765 mln osób, co jasno pokazuje jak wielki jest to problem dla całego świata. Również dla polskich firm i pracowników. Internetowe włamania, kradzieże danych i tożsamości, blokowanie systemów IT – to dziś realne zagrożenia. Dotychczasowe przekonanie, że nasze przedsiębiorstwa nie są przedmiotem zainteresowania cybeprzestępców zostały brutalnie zweryfikowane stratami wynikającymi choćby z ataków ransomware, które skutecznie zablokowały dane wielu polskich firm w 2018 roku. Doszło również do kilku spektakularnych ataków grup hackerskich, włączając w to zeszłoroczny atak DDoS na Home.pl – największy w ponad 20 letniej historii potentata na rynku usług hostingowych w Polsce.

4 na 10 firm doświadczyło cyberincydentu naruszającego bezpieczeństwo IT
Jak wynika z raportu VECTO, już niemal 40 proc. polskich firm zetknęło się ze zjawiskiem cyberprzestępczości. „Respondenci potwierdzają, że kwestia zabezpieczeń danych firmowych jest istotna, ale świadomość ta nie przekłada się niestety na realne działania. Firmy wciąż naiwnie wierzą, że incydenty różnych form naruszenia integralności danych i systemów IT ich ominą. Według mnie jednak jest to tylko kwestią czasu. Do inżynierów VECTO codziennie zgłaszają się menedżerowie firm, których fundamentem polityki cyberbezpieczeństwa była właśnie taka wiara. Niestety, katalog działań naprawczych po ataku zwykle jest ograniczony i łączy się z poważnymi startami – finansowymi, operacyjnymi i wizerunkowymi.” – mówi Jakub Wychowański, członek zarządu VECTO. Już dziś wiemy, że koszty cyberataków w ujęciu globalnym w 2021 r. wyniosą ok. 6 bln dol. Oznacza to podwojenie poziomu notowanego w 2015 r. W zaledwie sześć lat. Wkrótce zatem koszty te będą czterokrotnie wyższe od wartości obecnego, światowego rynku e-commerce.

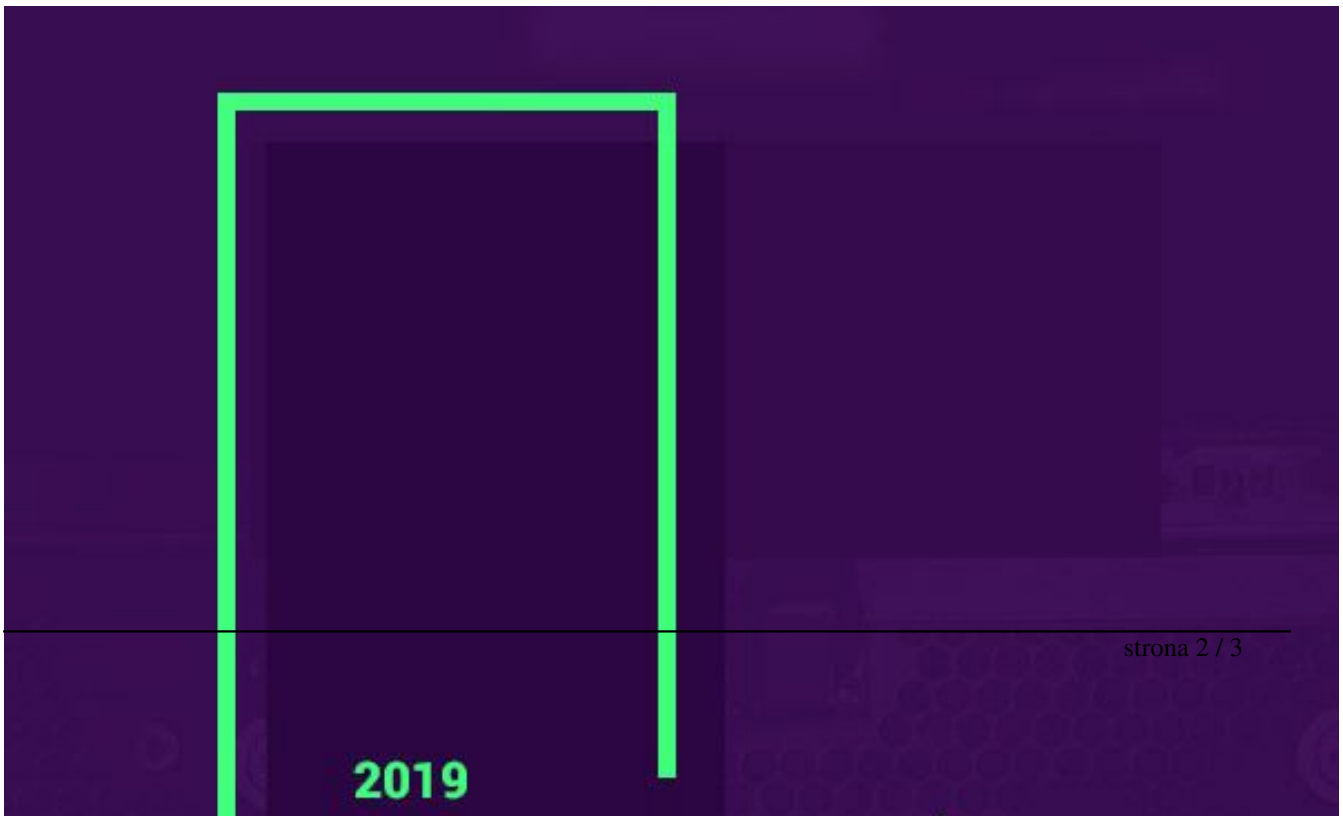
Brak inwestycji sprzyja cyberprzestępcom
Nic istnieją żadne przesłanki by móc sądzić, że w tych kosztach nie będą partycypowały polskie firmy. Szczególnie, gdy zdamy sobie sprawę z tego, że tylko co czwarte przedsiębiorstwo monitoruje zagrożenia związane z

cyberprzestępczością. 44 proc. ankietowanych uważa, że nie potrzebuje wsparcia pracownika (wewnętrznego lub zewnętrznego), który pomógłby zarządzać ryzykiem wynikającym z sieciowych incydentów. Oszczędności są tu kluczowym argumentem. „W mojej ocenie jest to błędna strategia, albowiem konieczność inwestowania w obszar IT wymusza postęp cywilizacyjny oraz wciąż rosnący udział rozwiązań internetowych w dosłownie każdej działalności biznesowej. Coraz więcej firm generuje swoją wartość w oparciu o zasoby niematerialne, jak programy, czy bazy danych, zatem wizja ich utraty powinna być wystarczającym motywatorem do skutecznych metod ich zabezpieczenia." – mówi Jakub Wychowański. Ten kierunek potwierdzają trendy globalne. Zaczyna dominować podejście, iż lepiej inwestować w ochronę, niż później zmagać się ze skutkami wycieku danych czy wadliwie pracującymi systemami wstrzymującymi procesy. Zgodnie z raportem Global Market Insights poziom wydatków na bezpieczeństwo IT wzrośnie ze 120 mld dol. w roku 2017 do 300 mld dol. w 2024 r.

Przede wszystkim bądźmy ostrożni!
Tymczasem w Polsce, łącznie 70 proc. respondentów biorących udział w badaniu VECTO nie umie wskazać jasnych procedur postępowania po stwierdzeniu cyberataku lub przyznaje, że takich procedur w ich firmach po prostu nie ma. Gdy pojawia się realny problem i niezbędne jest podejmowanie racjonalnych, precyzyjnych kroków ograniczających straty, pracownicy nie wiedzą jak postępować. „To szczególnie zadziwiające, bowiem przygotowanie scenariuszy postępowania w przypadku naruszenia bezpieczeństwa danych nie jest kosztowne. Podobnie, jak realizacja szkoleń dla pracowników. Obserwujemy bezpośrednią korelację wzrostu bezpieczeństwa IT z przeprowadzonymi szkoleniami. Ludzie po prostu wiedzą, co może być realnym zagrożeniem w sieci, jak cyberprzestępcy wykorzystują ich nieostrożność. Mając tę wiedzę, możemy redukować ryzyka już na poziomie pierwszych prób naruszenia bezpieczeństwa IT." – dodaje Wychowański.

Cyfryzacja społeczna, jaka stała się udziałem polskich firm i instytucji tworzy nieograniczone wręcz możliwości rozwoju. „Otwierają się przed nami wszystkimi perspektywy nowych obszarów aktywności, skraca się dystans pomiędzy sprzedającym, a kupującym, dostawcą, a odbiorcą towarów i usług. Dziś możemy zarządzać biznesem z dowolnego miejsca na świecie, definiować cele dla zespołów, projektować procesy, rozliczać projekty. Operujemy coraz większymi plikami danych, streamujemy efekty swojej pracy i wiele obszarów życia codziennego. Nie wolno nam jednak zapominać, że nowe szanse przynoszą również nowe zagrożenia. Przecieramy szlaki do realizacji biznesowych marzeń i ambicji, ale gdzieś w cybernetycznym cieniu kryją się ci, którzy te same cele chcą osiągać drogami na skróty." – przestrzega Wychowański.

Link do raportu „Cyberbezpieczeństwo w polskich firmach 2018":
https://vecto.pl/doc/Vecto-Cyberbezpieczenstwo-polskich-firm-2019.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 2018 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.
VECTO jest autorem raportu „Cyberbezpieczeństwo w polskich firmach 2018", stanowiącego analizę świadomości zagrożeń i rozwiązań w zakresie bezpieczeństwa i ochrony danych, stosowanych przez polskie firmy.

VECTO
press box