Finał badania: Cyberbezpieczeństwo w polskich firmach 2018

Polskie firmy mają świadomość cyberzagrożeń, ale niechętnie inwestują w rozwiązania zwiększające bezpieczeństwo danych i systemów informatycznych. Pokutuje przeświadczenie, że szkodliwa działalność hakerów koncentruje się wyłącznie na dużych, globalnych firmach. Tymczasem cyberataku doświadczyło aż 54,5 proc. ankietowanych – wynika z opublikowanego przez VECTO raportu „Cyberbezpieczeństwo polskich firm 2018".

O powadze ryzyk związanych z cyberprzestępczością nikogo nie trzeba dziś przekonywać. Skala działalności hackerów przybiera na sile i coraz częściej słyszymy o jej szkodliwości również w Polsce. Wystarczy przypomnieć zeszłoroczne żniwa, jakie zebrały ataki typu ransomware, szyfrujące dane w polskich firmach. Powagę sytuacji zaczęły doceniać również polskie instytucje rządowe – w zeszłym roku, w obliczu szalejącego w naszej części Europy wirusa Petya, ówczesna premier Beata Szydło po raz pierwszy w historii powołała Rządowy Zespół Zarządzania Kryzysowego. Tę rosnącą świadomość cyberzagrożeń potwierdza raport VECTO. Zdaniem niemal 85 proc. badanych, kwestia zabezpieczania firmowych danych jest istotna. Na tym jednak kończą się dobre wiadomości. Choć polskie firmy przyglądają się kwestiom zabezpieczeń przed nowymi zagrożeniami z cyfrowej przestrzeni, to jedynie 33,6 proc. ankietowanych oceniło poziom zabezpieczeń w swoich firmach jako prawidłowe. Przeciwnego zdania było aż 38 proc. respondentów. Podczas, gdy na świecie firmy bardzo szybko zwiększają wydatki na modernizację systemów informatycznych i wszelkiego rodzaju zabezpieczeń, w Polsce niestety dominuje postawa oczekiwania. Praktyka bardzo nierozsądna, jeśli wyobrazimy sobie naszą firmę, w której wskutek ataku hackera tracimy kontrolę nad zasobami lub całym procesem produkcyjnym. Paraliż operacyjny może skutkować ogromnymi kosztami, a utrata wszystkich danych unicestwić marzenia o naszym biznesowym sukcesie.

„Zdaniem ponad 83 proc. ankietowanych, atak cyberprzestępców na system informatyczny może wpłynąć na

funkcjonowanie przedsiębiorstwa. Tymczasem 61 proc. z nich stwierdziło, że nie korzysta z usług specjalistów od bezpieczeństwa. Widać zatem zadziwiającą niekonsekwencję i igranie z ogniem. Takie podejście można oczywiście tłumaczyć oszczędnościami, ale w przypadku - zwłaszcza firm dużych - to także przykład niefrasobliwości i niedoceniania zagrożenia." – mówi Jakub Wychowański z VECTO.

Smartfon słabym ogniwem

Tymczasem analitycy zgodnie oceniają, że hakerzy poczynają sobie coraz odważniej i uderzają w coraz to nowe sektory gospodarki. Nasze rodzime przedsiębiorstwa już kilka razy przekonały się o dokuczliwości tego typu zdarzeń, choć zmasowane akcje na wielką skalę póki co nasz rodzimy biznes omijają. Niestety taki stan rzeczy może się długo nie utrzymać, a polskie firmy, będące przecież częścią globalnego systemu informatycznego są w większości, jak się okazuje, bezbronne. Uniknąć strat będzie coraz trudniej, bowiem hackerzy nie ustają w kreatywnym poszukiwaniu słabych stron naszych systemów informatycznych. Cyberprzestępcy są stale jeden krok przed nami i wyciągają wnioski z obserwacji ludzkich zachowań. Dlatego coraz częstszym źródłem problemów jest nieostrożne korzystanie ze smartfonów i tabletów, które przez wielu użytkowników traktowane są jako podręczne komputery. Zapominamy, że w ich przypadku również musimy stosować określone zabezpieczenia. Chronimy nasze służbowe komputery, czy serwery, jednak aż 72 proc. z wszystkich wykrytych w 2017 roku zagrożeń dotyczyło właśnie urządzeń mobilnych. Co 10 sekund pojawia się nowa odmiana złośliwego oprogramowania atakującego system Android, zwiększając niebezpieczeństwo zainfekowania aż o 50 proc. względem ubiegłego roku. „Przeprowadzane przez VECTO audyty wskazują, że większość polskich firm wciąż nie rozumie, że telefon podłączony do firmowej sieci wi-fi może stanowić furtkę, przez którą cyberprzestępcy dokonują ingerencji w system IT, kradną lub szyfrują dane, niszczą zasoby informatyczne." – przestrzega Wychowański.

Zaufanie klientów bezcenne

Autorzy badania zapytali ankietowanych o biznesowe konsekwencje ewentualnych ataków hackerskich. Ciekawostką jest fakt, że najwyższej ocenioną odpowiedzią
(4,2 pkt) była obawa o znaczne osłabienie wizerunku oraz zaufania. Nieco niższy wynik (4,1 pkt.) uzyskała odpowiedź wskazująca, że atak może doprowadzić do strat
finansowych firmy. Taki rozkład odpowiedzi – choć różnice są wciąż niewielkie – pokazuje, że w mentalności polskich przedsiębiorstw doszło do poważnej przemiany. Potencjalne straty wizerunkowe ocenione zostały bowiem jako bardziej dotkliwe, niż spadek przychodów. Widać zarówno przedsiębiorcy, jak i pracownicy zrozumieli już, że straty finansowe można odrobić łatwiej, niż pozbyć się rys na wizerunku i zaufaniu klientów i partnerów biznesowych.

„Cyberbezpieczeństwo to jeden z absolutnych globalnych priorytetów na 2018 r. i polskie firmy również powinny podchodzić do tej problematyki z należytą atencją. Trzeba podejmować działania profilaktyczne, zabezpieczać dane i eliminować słabe ogniwa systemów informatycznych. Jeśli zaczniemy działać dopiero po wystąpieniu ataków, na reakcję będzie za późno, a finalnie może to doprowadzić firmę nawet do likwidacji. Polskie przedsiębiorstwa muszą zrozumieć, że świadomie lub nie, uczestniczą po prostu w wojnie, tylko że cyfrowej i w wirtualnym świecie, choć często za prawdziwe pieniądze." – podsumowuje Jakub Wychowański.

Więcej informacji:
Raport (PDF): http://vecto.pl/raport

VECTO sp. z o.o. działa od 2008 roku. Forma 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.

VECTO
press box