SKUTECZNA OCHRONA PRZED CYBERATAKIEM

Nie ryzykuj bez potrzeby. Cyberzagrożenia są wszędzie, ale możesz się przed nimi zabezpieczyć. Nawet, jeśli do ataku dojdzie, możesz otrzymać szybką pomoc.

Z roku na rok fala cyberataków przybiera na sile. Hakerzy polują na wrażliwe informacje i próbują wymuszać okup. Problemem może być także zwykły wyciek danych na skutek błędu pracownika. Zagrożenia czają się wszędzie, a wiele firm nie ma nawet podstawowej wiedzy o własnym poziomie bezpieczeństwa. – Często rozmawiamy z przedsiębiorstwami, które nie potrafią nam podać szczegółów rozwiązań związanych z bezpieczeństwem krytycznych systemów – mówi Monika Ściuba, koordynator ds. Underwritingu w PZU.

WIELE DO ZROBIENIA

Jak tłumaczy Monika Ściuba, jakość ochrony polskich firm poprawia się. Przykładowo, dziś praktycznie nie ma firm, które nie miałyby antywirusów czy firewalli. Co więcej, wiele z nich dba o to, by zabezpieczenia były aktualne. Z tym jeszcze do niedawna były problemy. Firmy są także zainteresowane nowymi narzędziami takimi jak systemy do badania stopnia ochrony strony internetowej.

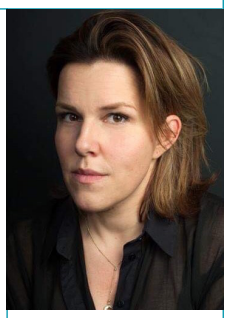
PZU oferuje np. bezpłatną usługę PZU Cyber Raport. To projekt przygotowany we współpracy ze startupem w ramach programu #PZUReadyForStartups. Raport dostępny jest dla wszystkich (nie tylko klientów PZU) i pozwala wygenerować zestawienie podatności na zagrożenia cybernetyczne oraz ocenić ryzyko i koszty ich wystąpienia.

Wciąż jednak jest wiele do zrobienia w kwestii ochrony danych przez cyberatakami. Przykładowo wiele firm dba o to, by posiadać kopie zapasowe swoich systemów czy plików, ale często zapomina o ich odpowiednim zabezpieczeniu lub regularnej aktualizacji. Wyzwaniem jest wciąż praca zdalna i brak wieloskładnikowego uwierzytelniania dostępu do systemów firmowych. – Widzę poprawę, ale wciąż zarządzający firmami nie zdają sobie sprawy, jak kosztowne mogą być same incydenty, nie mówiąc już o kosztach przerw w funkcjonowaniu firmy – tłumaczy Ściuba.

Proste zablokowanie systemu rodzi nie tylko konieczność jego odblokowania (a to sporo kosztuje nawet, jeśli nie zapłacimy hakerom), ale także paraliżuje działalność firmy. Same koszty zgodnego z prawem zawiadomienia osób, których dane wyciekły mogą wynieść kilkaset tysięcy złotych. – Nie każda firma zatrudnia prawników, którzy potrafią zarządzać zdarzeniami cybernetycznymi. Koszt zatrudnienia takich osób może być spory, a to najłatwiejszy scenariusz – dodaje. Prosty błąd, który doprowadził do umieszczenia wrażliwych danych w internecie, sprowadził na jedną z polskich firm wiele problemów. – Sprawa trwała rok i musiała zostać zgłoszona do UODO. Prezes urzędu nie nałożył ostatecznie kary. Firma korzystała z pomocy specjalistów w ramach ubezpieczenia ryzyk cybernetycznych. Dzięki temu nie poniosła kosztów prawników, kosztów prowadzenia sprawy oraz kosztów zatrudnienia informatyków śledczych, którzy przez cały czas wyjaśniania incydentu współpracowali z ubezpieczonym i PUODO oraz pomogli wypracować zasady bezpieczeństwa na przyszłość – komentuje Monika Ściuba.

UBEZPIECZENIE W ŚWIECIE CYFROWYM

Na rynku jest jednak narzędzie, które może pomóc w takich sytuacjach. To ubezpieczenie od cyberzagrożeń. Jego koszt zaczyna się od kilkuset złotych i zależy od skali biznesu i potencjalnego ryzyka. To nie jest wysoka kwota, biorąc pod uwagę nie tylko proces obsługi szkód, ale także sam koszt zarządzania incydentem. Bo praca informatyków, którzy próbują uratować sytuację w firmie kosztuje, nie mówiąc już o kosztach prawników.



MONIKA ŚCIUBA
koordynator ds. Underwritingu w PZU

– W PZU oferujemy klientom ubezpieczenia cyber – dla małych i średnich podmiotów oraz dużych przedsiębiorstw. W pierwszym produkcie proces oceny ryzyka jest uproszczony, w samej ofercie skupiamy się na zarządzeniu zdarzeniem cybernetycznym, czyli pomocy ekspertów i na pokryciu kosztów odtworzenia naruszonych danych lub strat wynikających z zakłócenia działalności. Dochodzi do tego ochrona OC, która zabezpieczy wszelkiego rodzaju roszczenia w stosunku do klienta wynikające z wycieku danych wrażliwych. Dla największych podmiotów – w szczególności dla klientów z segmentu infrastruktury krytycznej – mamy przygotowany tzw. duży produkt. Kluczowym jego wyróżnikiem jest to, że klient może również ubezpieczyć szkody rzeczowe po cyberatakach. Przykładem takiej szkody może być wybuch, a następnie pożar w serwerowni klienta spowodowany bezpośrednio przez atak hakerski. Jest to coś unikatowego na rynku polskim. Warto też zwrócić uwagę na e-kradzież, czyli nieuczciwe transfery elektroniczne – mówi Monika Ściuba.

– Jeśli zdajemy sobie sprawę, że istnieje ryzyko, to musimy się na nie przygotować. Nie musimy być zaatakowani, by mieć problemy. Wystarczy błąd ludzki taki jak ujawnienie danych klientów – uściśla przedstawicielka PZU.

PZU dla ubezpieczonych firm oferuje też dostęp do specjalnej infolinii 24h na dobę 7 dni w tygodniu. W razie incydentu klient może uzyskać pomoc incydent menedżera. Specjalista sprawdzi, co dokładnie wydarzyło się u klienta i ustali plan działania tak, by jak najszybciej wyjść z sytuacji kryzysowej. Jeżeli skala ataku tego wymaga, możliwe jest wsparcie i pomoc kancelarii prawnej, agencji public relations czy informatyka śledczego.