mieć dostęp do kluczowych systemów w firmie. Wystarczy zainfekować ich sieć wi-fi, by przestępcy mogli umieścić złośliwe oprogramowanie na serwerach służbowych. Są na to sposoby, ale pracownicy i tak muszą być czujni.

Najlepszym wyjściem są szkolenia. Nawet najlepsze systemy zawiodą, jeśli nasz pracownik otworzy e-mail o dziwnym tytule: „Książę z Nigerii chce ci dać 10 milionów dolarów" i kliknie w załącznik. Ataki są także bardziej wyrafinowane, np. podszywanie się pod kontrahentów wysyłających zapytania ofertowe z zainfekowanymi plikami Excela.

Po drugie – zabezpiecz systemy. Niezależnie od tego, z jakiej technologii korzystamy ani jakie urządzenia wykorzystujemy, trzeba mieć aktualne oprogramowanie i jednocześnie zapewniać dodatkowe poziomy ochrony. Tu musimy zdać się na wsparcie ekspertów – czy to wewnętrznych w firmie, czy tych zewnętrznych. Dobrym rozwiązaniem jest także wykorzystanie zewnętrznych audytorów, którzy zbadają odporność naszej firmy na ataki i potencjalnie wskażą miejsca, które musimy poprawić.

OFIARĄ ATAKU MOŻE STAĆ SIĘ KAŻDY. PROBLEM POLEGA NA TYM, ŻE WIĘKSZOŚĆ Z NICH JEST ZAUTOMATYZOWANA. NAWET JEŚLI PROWADZISZ MAŁĄ FIRMĘ, MOŻESZ STRACIĆ DOSTĘP DO BAZ DANYCH LUB SERWERÓW ALBO DANE KLIENTÓW TRAFIĄ DO INTERNETU. OGRANICZ TO RYZYKO!

GRZEGORZ WASZKIEWICZ
broker ubezpieczeniowy, członek zarządu Krajowego Biura Obsługi Roszczeń Ubezpieczeniowych, twórca marki: BezpieczenstwowBiznesie.pl

UBEZPIECZENIE OD CYBERZAGROŻEŃ

Czy firma może zabezpieczyć się przed atakiem cyberprzestępców? Niestety, nie sposób uniknąć ataku, ale można zabezpieczyć się przed negatywnymi skutkami takiego zdarzenia. Wraz ze wzrostem pracy zdalnej wzrasta też prawdopodobieństwo popełnienia błędu przez pracowników oraz niespodziewanych awarii technicznych. Utrata danych czy odpowiedzialność za ich nieuprawnione wykorzystanie, czyli naruszenie standardów bezpieczeństwa prywatności czy przechowywania danych, będzie wiązać się zawsze z poważnymi stratami finansowymi. Wynikają one np. z konieczności zapłaty odszkodowań na rzecz osób poszkodowanych i kar na rzecz organów nadzoru (Urząd Ochrony Danych Osobowych).

Podstawowym zadaniem polisy od cyberataków jest ochrona na wypadek przerwy w prowadzeniu działalności spowodowanej awarią systemu komputerowego firmy. Ubezpieczyciel pokrywa koszty odzyskania utraconych danych elektronicznych, zakupu nowego czy usunięcia złośliwego oprogramowania. Firma ubezpieczeniowa wypłaca odpowiednie środki, gdy cyberprzestępca przeprowadzi atak komputerowy na serwery i zablokuje dostęp do danych, wskutek czego nastąpi wstrzymanie działalności przedsiębiorstwa. Towarzystwa ubezpieczeniowe oferują w ramach polis nie tylko zwrot poniesionych kosztów przywrócenia danych czy kosztów porady prawnej, ale również finansowanie tzw. informatyki śledczej. Pokrywają koszty związane ze wsparciem w komunikacji kryzysowej oraz zewnętrznego doradztwa IT. Ubezpieczyciele oferują również zwrot kosztów związanych z usługami public relations mającymi na celu przywrócenie dobrego imienia organizacji po ataku. Dodatkowo w zakres ten wchodzą koszty przeniesienia zachowanych danych na nowe serwery.

Cena ubezpieczenia zawsze jest uzależniona od poziomu ryzyka, branży, liczby pracowników (użytkowników systemu) czy ilości danych, które znajdują się w zasobach firmy. Już podczas wnioskowania o ofertę, widząc pytania, dana firma może zweryfikować poziom swoich zabezpieczeń i procedur bezpieczeństwa. Ubezpieczenie Cyber można zakupić bezpośrednio u ubezpieczyciela. Jednak skorzystanie z doradztwa niezależnego brokera daje szanse na dostosowanie polisy i jej warunków do oczekiwań konkretnej firmy.