Cyberpolisa od PZU to bezpieczeństwo twoich danych

Rozmowa z **Pauliną Borowiec** i **Piotrem Kruszyńskim**, koordynatorami ds. underwritingu w PZU

Aleksandra E. Wysocka: – Czy ryzyka cyber to wciąż miejska legenda, czy już twarda biznesowa rzeczywistość, z którą musi się liczyć każda firma?

Piotr Kruszyński: – To ryzyko, które już dawno wyszło z serwerowni i weszło na posiedzenia zarządów. Kiedyś cyber kojarzył się z wielkimi korporacjami, dziś jest codziennością także małych i średnich firm. Dodajmy do tego internet rzeczy, automatyzację biur i domów, a także naszą skłonność do karmienia narzędzi IT ogromnymi ilościami danych. To wszystko tworzy środowisko, które z bezpieczeństwem ma niewiele wspólnego.

Do tego dochodzi prawo. RODO i NIS2 nie tylko nakładają obowiązki ochrony danych, lecz także wprowadzają konieczność raportowania incydentów. A kary liczone od rocznych przychodów potrafią iść w miliony euro.

Żeby PZU w ogóle przygotowało ofertę, firma musi spełnić konkretne warunki. Jakie elementy są absolutnie nie do ominięcia?

Paulina Borowiec: – Najpierw patrzymy na fundamenty. Dla firm do 100 mln zł przychodów oznacza to komercyjną zaporę sieciową i antywirusa, a nie domowe, darmowe rozwiązania. Dalej kopie zapasowe trzymane w odizolowanym środowisku i instalowanie krytycznych poprawek w ciągu 30 dni. To naprawdę podstawy, bez których nie można mówić o jakiejkolwiek odporności.

W większych firmach wymagania rosną. Przy przychodach powyżej 50 mln zł zdalny dostęp musi być zabezpieczony MFA, czyli przynajmniej dwiema niezależnymi metodami autoryzacji.

A powyżej 100 mln zł przychodów dochodzi szyfrowanie danych, wyłączenie zdalnego pulpitu i ograniczenie uprawnień administratorów tylko do wybranych osób. Jeśli firma korzysta z wycofanego sprzętu albo ma środowisko produkcyjne połączone z IT, to również musi to uporządkować.

Firmy często reagują wzruszeniem ramion: „Co może się zdarzyć?". No więc – co się zdarza?

P.K.: – Na przykład atak na British Airways z 2018 r. Złośliwe oprogramowanie wgrane przez stronę przewoźnika doprowadziło do wycieku danych kilkuset tysięcy pasażerów, w tym numerów kart płatniczych. Brytyjski regulator wymierzył karę 183 mln funtów, potem obniżoną do 20 mln. Finansowe konsekwencje ataku malware były więc dla BA ogromne.

P.B.: – Albo WannaCry. Rok 2017, ponad 150 krajów zainfekowanych. Szpitale, uniwersytety, Deutsche Bank, Telefonica, FedEx. Luka w Windowsie, zaszyfrowane pliki, okup. Straty globalne sięgnęły 8 mld dol. A wszystko przez nieaktualny system.

Phishing kojarzy się nam z SMS-em do babci i wyłudzeniami „na wnuczka". Czy dla firm to naprawdę równie poważne zagrożenie?

P.K.: – Mamy bardzo spektakularny przykład pokazujący, że phishing nie jest „SMS-em do babci". Jeden cyberprzestępca z Litwy przez dwa lata podszywał się pod autentycznych dostawców Google i Facebooka. Wysyłał im faktury oraz dokumenty finansowe ze zmienionym numerem konta, podszywając się pod zaufanego dostawcę. W ten sposób wyprowadził łącznie ponad 100 mln dol. To nie była magia, tylko konsekwentne wykorzystanie jednego błędu: braku procedur weryfikacji płatności.

Załóżmy jednak, że firma odrobiła pracę domową. Co realnie dostaje w PZU?

P.K.: – Dla przedsiębiorstw z przychodami do 300 mln zł możemy praktycznie od ręki przygotować ofertę z sumą ubezpieczenia do 10 mln zł. Całość ochrony dostępna jest do wysokości limitu sumy ubezpieczenia, bez dzielenia jej na podlimity.

Kluczowe jest to, że klient nie zostaje sam. Oferujemy wsparcie incydent managera dostępnego 24/7 po polsku. To technicy, prawnicy i eksperci od komunikacji, którzy przeprowadzą firmę przez kryzys. Od pierwszych prób przywrócenia działania sieci, przez zgłoszenia do urzędów, aż po przygotowanie komunikatów dla klientów i mediów.

P.B.: – I ta ochrona nie jest wyłącznie dla korporacji. W MŚP każdy przetwarza dane, więc każdy jest potencjalnym celem. Co więcej, cyberprzestępcy zdają sobie sprawę, że w mniejszych firmach zabezpieczenia często są słabsze, więc atak na nie jest dla nich po prostu łatwiejszy.

W polisach zawsze ważne są wyłączenia. Jakie są te, o których klienci najczęściej nie wiedzą, a powinni?

P.K.: – Najważniejsze: ubezpieczenie cyber nie obejmuje szkód rzeczowych. Jeśli atak „spali" sprzęt, sama naprawa laptopa nie będzie pokryta, choć incydent może uruchomić inne elementy ochrony.

Druga kwestia to przelewy FTF. Jeśli firma nie stosuje procedur, nie weryfikuje zmiany numeru konta i nie szkoli pracowników, szkoda może być wyłączona. To fundamentalne: technologia nie zastąpi zdrowego rozsądku.

A które obszary w ubezpieczeniu cyber najczęściej budzą wątpliwości brokerów?

P.B.: – Zazwyczaj są to kwestie techniczne, dotyczące zabezpieczeń. Na przykład co to jest MFA, czyli uwierzytelnienie wieloskładnikowe, i czy rozwiązanie klienta spełnia to wymaganie. Albo czym się różnią systemy IT od OT – te pierwsze odpowiedzialne są za dane i aplikacje biznesowe, drugie za fizyczne procesy i urządzenia.

Brokerzy zgłaszają, że klienci mają problem z rozróżnieniem polisy cyber i OC IT. Czym te produkty się różnią?

P.B.: – To dwa różne ubezpieczenia. Ubezpieczenie cyber chroni firmę przed skutkami ataku w jej własnym środowisku. OC IT chroni klientów firmy informatycznej, gdy jej oprogramowanie lub sprzęt nie działa tak, jak powinien, a więc dotyczy odpowiedzialności względem osób trzecich za usługi i produkty IT.

P.K.: – Nasze OC zawodowe dla branży technologicznej obejmuje m.in. software house'y, firmy budujące sieci, dostawców cyberbezpieczeństwa i jednoosobowe działalności B2B. Świetnie uzupełnia polisę cyber. Jedno dotyczy tego, co firma „popsuje u klienta", drugie – tego, co wydarzy się wewnątrz niej.

Dziękuję za rozmowę.

Aleksandra E. Wysocka