UBEZPIECZENIA OD CYBEZAGROŻEŃ - NOWA SZANSA W CYBERBEZPIECZEŃSTWIE?

Uważamy, że klienci powinni inwestować w różnego rodzaju rozwiązania technologiczne, a samo ubezpieczenie powinno być uzupełnieniem szeroko rozumianej ochrony - mówią w rozmowie z Cyberdefence24 eksperci z firmy ERGO Hestia przybliżając nam rynek ubezpieczeń od cyberzagrożeń.

Jak wygląda sektor ubezpieczeń od cyberzagrożeń w Polsce i jak prezentuje się on na tle innych państw. Czy wiedzą Państwo ilu klientów w Polsce korzysta z takich ubezpieczeń? Ilu klientów korzysta z Państwa rozwiązań?

Rynek cyberubezpieczeń w Polsce jest na etapie rozwoju. Obecnie ubezpieczenia od cyberzagrożeń oferuje kilka towarzystw. Dla porównania na świecie, głównie w USA i Wielkiej Brytanii, rynek jest bardzo rozwinięty, a jednorazowe składki z ubezpieczenia przekraczają czasami 100 mln USD rocznie (dotyczy USA). Na polskim rynku nie prowadzi się jeszcze statystyk dotyczących ilości polis od cyberzagrożeń.

Czy prowadzą państwo współpracę z takimi firmami jak Exatel czy Comarch w celu analizy, budowy oraz zabezpieczenia infrastruktury? Czy są to może inne prywatne firmy, które zapewniają odpowiednie zaplecze technologiczne dla Państwa klientów?

Jako Grupa ERGO Hestia posiadamy kompetencje m.in. w zakresie analizy, budowy oraz zabezpieczenia infrastruktury. Tego typu usługi świadczy spółka ekspercka Hestia Loss Control, która m.in. prowadzi szkolenia, tworzy polityki bezpieczeństwa i plany ciągłości działania czy przeprowadza testy penetracyjne zasobów IT. Dodatkowo Hestia Loss Control jest w stanie wspierać swoich klientów i doradzać im w zakresie bezpieczeństwa teleinformatycznego. Dodatkowo jako ERGO Hestia współpracujemy z firmą zewnętrzną w zakresie informatyki śledczej.

Czy współpracują Państwo z rządowymi instytucjami oraz CERTAmi?

Dotychczas nie współpracowaliśmy z instytucjami rządowymi, natomiast jak najbardziej współpracujemy z firmami sektora prywatnego.

Czy Państwa zdaniem oprócz inwestowania w odpowiednie ubezpieczenia od cyberzagrożeń firmy powinny w równym stopniu inwestować w rozwiązania technologiczne oraz realizować zadania edukacyjne własnych pracowników?

Uważamy, że klienci powinni inwestować w różnego rodzaju rozwiązania technologiczne, a samo ubezpieczenie powinno być uzupełnieniem szeroko rozumianej ochrony. Dlatego jako towarzystwo ubezpieczeń w ramach ochrony oferujemy naszym klientom wsparcie w zakresie podnoszenia świadomości zagrożeń cybernetycznych, jakie mogą spotkać ich pracowników.

Czy mogą podzielić się Państwo przykładami z życia? Oczywiście bez podawania żadnych danych charakterystycznych dla firm, ale przykładem, w którym Państwa ubezpieczenie np. uratowało firmę przed bankructwem.

Nie mamy jeszcze przypadków szkód u naszych klientów. W tym miejscu warto też podkreślić, że nasze ubezpieczenie nie chroni przed bankructwem. Ubezpieczenie cyber ERGO Hestii dotyczy przede wszystkim kosztów, które może ponieść klient w związku z utratą lub uszkodzeniem danych elektronicznych (dane, oprogramowanie). Należą do nich np. koszty odtworzenia danych czy też koszty zakupu nowego oprogramowania.

Eksperci zgodzili się na analizę kilku scenariuszów przygotowanych na potrzeby tej publikacji, poniżej przedstawiamy zmyślone scenariusze, które jednak naszym zdaniem mogły by mieć miejsce w realnym życiu.

W firmie X szef bardzo dba o szkolenia cyberbezpieczeństwa, każdy z pracowników zanim zacznie pracę przy komputerze przechodzi obowiązkowe szkolenie. Firma w dodatku posiada odpowiednie i najnowsze mechanizmy zabezpieczające ja przed atakami. Dla spokoju ducha szef przekonał zarząd, że potrzebne jest firmie ubezpieczenie obejmujące obszar cyberbezpieczeństwa. Firma staję się obiektem ataku phishingowego. Jeden z użytkowników nieświadomie otwiera wiadomość e-mail przesłaną do niego na prywatną skrzynkę, do której ma dostęp w pracy. Sieć firmy zostaję zarażona, hakerzy włamują się do sieci, wykradają dane, część dostępu do komputerów szyfrują dzięki wirusom ransomware. Jak w takim wypadku będzie działać ubezpieczenie? Do rozważenia także podam inny wariant, w którym, ten sam e-mail zostaję wysłany na skrzynkę firmową - efekty są podobne.

W ramach ubezpieczenia pokryjemy koszty odtworzenia i przywrócenia danych, jesteśmy także w stanie pokryć koszty odblokowania dostępu do danych oraz koszty informatyki śledczej. Do tego dochodzą koszty dodatkowe tj. koszty przeznaczone na public relations czy koszty powiadomienia klientów o utracie ich danych. W przypadku kosztów dodatkowych katalog jest otwarty i od klienta zależy, jak wykorzysta przyznany limit odpowiedzialności. Nie pokrywamy kosztów okupu.

Pracownik tej samej idealnej firmyX posiadającej odpowiedni poziom cyberbezpieczeństwa, wysyła przypadkiem na zły adres e-mail hasła dostępowe do ważnej części sieci. Ktoś przechwytuje e-mail, lub nawet sam odbiorca sprzedaje go na czarnym rynku i następuje włamanie do sieci firmowej.

Ubezpieczenie obejmuje takie zdarzenia jak: atak hakerski i wirus komputerowy. Poprzez atak hakerski rozumiemy złamanie zabezpieczeń i uzyskanie dostępu do danych. Jeśli pracownik wykorzystał swoje uprawnienia systemowe do kradzieży danych, wtedy nie zachodzi odpowiedzialność ubezpieczyciela, gdyż firma dała pracownikowi odpowiednie uprawnienia. Jeśli pracownik nie ma dostępu do danych i uzyska dostęp poprzez złamanie zabezpieczeń, wtedy przyjmujemy odpowiedzialność. Jeśli dostęp do danych uzyska osoba nieuprawniona (nie będąca pracownikiem lub pracownik bez uprawnień), wtedy odpowiedzialność istnieje, bez znaczenia w jaki sposób uzyskał dostęp.

Hakerzy namierzyli jednego z pracowników firmy X, on nieświadomy zabrał ze sobą do domu urządzenie firmowe, zabezpieczone, dostał pozwolenie na pracę zdalną na laptopie. Po powrocie do siedziby firmy hakerzy, będący już obecni na komputerze pracownika udając działanie pracownika włamują się do sieci. Nikt nie jest świadomy ataku, ponieważ wszystkie systemy monitorujące uznały działania hakerów za tzw. prawdziwy-fałsz.

Istnieje odpowiedzialność, ponieważ mamy do czynienia z włamaniem do systemu przez nieuprawniony dostęp, z wykorzystaniem zabezpieczonego urządzenia firmowego. Pomimo tego, że firma posiada mechanizmy zabezpieczające infrastrukturę teleinformatyczną, w tym urządzenia końcowe swoich pracowników (tablet, komputer), a mimo to dojdzie do włamania przez hakera lub zainfekowania złośliwym oprogramowaniem, wtedy ubezpieczyciel przyjmie odpowiedzialność. Posiadanie zabezpieczeń nie wyłącza odpowiedzialności towarzystwa ubezpieczeń. Jednocześnie warto pamiętać, że posiadane zabezpieczenia mają wpływ na ocenę ryzyka* przed zawarciem polisy (ocena ryzyka decyduje, czy ubezpieczenie zostanie zawarte, czy też nie) oraz wysokość składki ubezpieczeniowej.

***Ocena ryzyka przeprowadzana jest na podstawie kwestionariusza oceny ryzyka przygotowanego we współpracy z Hestia Loss Control oraz na podstawie przeprowadzanych testów penetracyjnych infrastruktury teleinformatycznej.**

Haker podszywa się pod szefa firmy. Wysyła do pracownika niższego szczebla, który odpowiada za część finansów w firmie, że pilnie potrzebuje pewnej kwoty pieniędzy. Utknął na lotnisku, nie ma dostępu do telefonu oraz jego karty zostały zablokowane. Pracownik nie znający szefa, sprawdza, że faktycznie jego szef istotnie nazywa się tak jak podaje to haker w fałszywej wiadomości e-mail. Jednak pracownik nigdy nie miał bezpośredniej styczności ze swoim szefem, nie zna jego adresu e-mail, ani numeru konta, które zostały przesłane w wiadomości e-mail lub przekazane telefonicznie.

O ile taka sytuacja w ogóle miałaby miejsce (gdyż trudno nam sobie wyobrazić, aby osoba odpowiedzialna za finanse firmy nie znała szefa) ubezpieczenie nie pokrywa kradzieży pieniędzy (kradzież z konta, przelew na inne, podstawione konto).

Eksperci firmy Ergo Hestia – Tomasz Dolata ERGO Hestia, Dariusz Włodarczyk Hestia Loss Control.

Czytaj też: [Cyber- ubezpieczenia - wyzwania i szanse]