W cyberubezpieczeniach kryzys czy rozwój?

W 2020 r. po raz pierwszy usłyszeliśmy, że nadchodzi poważny kryzys ubezpieczeń ryzyk cyber. Mimo niekorzystnej narracji rynku zainteresowanie tą linią ubezpieczeń wcale nie zmalało.

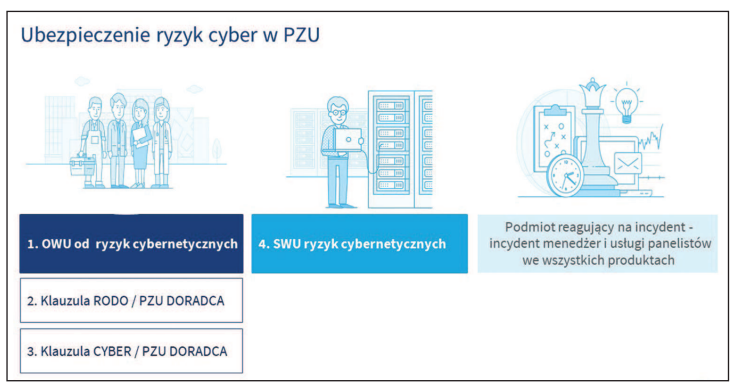
Skąd ten kryzys?

Temat kryzysu ubezpieczeń cyber wywołały dwa czynniki. Pierwszy wynika bezpośrednio ze wzrostu liczby zdarzeń cybernetycznych na świecie i przede wszystkim większej niż kiedykolwiek skali zdarzeń typu ransomware, czyli złośliwego oprogramowania, które uniemożliwia odczyt zapisanych w systemie danych, a następnie żąda okupu za przywrócenie dostępu.

Problem dotknął również naszego kraju. Zgodnie z raportem o stanie bezpieczeństwa cyberprzestrzeni w Polsce za 2020 r., opublikowanym przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, liczba zgłoszeń, które zostały zakwalifikowane jako zdarzenia dotyczące potencjalnego wystąpienia incydentu, wzrosła w 2020 r. o 8% w porównaniu z 2019 r. i wyniosła 246 107. Natomiast liczba zdarzeń, które zostały zarejestrowane w 2020 r. jako faktyczny incydent, wyniosła 23 308 i wzrosła aż o 88% w porównaniu z 2019 r.

Drugą przyczyną kryzysu i rewizji podejścia reasekuratorów były niekorzystne wyniki ubezpieczycieli oferujących polisy ryzyk cybernetycznych na amerykańskim rynku za 2020 r.

Dane opublikowane przez NAIC (National Association of Insurance Commissioners) wskazują, że rynek ubezpieczeń cyber wUSA wzrósł w 2020 r. o 29,1% w porównaniu z 2019 r., przy czym TOP3 ubezpieczycieli ryzyk cyber na tym rynku (z łącznym udziałem w rynku na poziomie 33,6%) zanotowało za 2020 r. wskaźniki szkodowości odpowiednio 61%, 98,2%, 100,6%.



Nie taki kryzys straszny

Konsekwencje powyższego wydawały się dość oczywiste: brak pojemności na rynku i koszt ubezpieczeń cyber tak duży, że klientów nie będzie na nie stać. Tymczasem rynek zareagował całkiem dojrzale. Na wieść o zmianie uwarunkowań część reasekuratorów wycofała się ze swojej dotychczasowej polityki i zrewidowała podejście do oferowania niektórych zakresów ochrony, np. zakresu ransomware. Inni postanowili podnieść ceny, jednak tylko niektórzy dosyć drastycznie.

Natomiast co najważniejsze, wszyscy, którzy zostali na rynku ubezpieczeń cyber, w tym również PZU, zaostrzyli zasady oceny ryzyka i akceptacji przyjmowania umów do portfela.

Co przyniesie kolejny rok?

Rozwój ryzyk cyber, w ślad za rewolucją przemysłową i fuzją technologii, jest nieunikniony. Podobnie jak zrewidowanie podejścia do zakresu ubezpieczenia ryzyka ransomware i innych ryzyk będących na styku ubezpieczeń „crime".

Regulatorzy mówią wprost o swoim zaangażowaniu w opracowywanie nowych sposobów monitorowania rozwijającego się rynku, po to aby lepiej przeciwdziałać ryzyku cyber, pokazując w ten sposób, że to ważny i perspektywiczny rynek.

Wyzwaniem rynku na 2022 r. będzie rozpoczęcie prac nad określeniem minimalnych standardów zabezpieczeń. Katalog dobrych praktyk w zakresie oceny ryzyka cyber to przecież coś, na co wszyscy czekamy.

Monika Ściuba
koordynator ds. underwritingu PZU SA i TUW PZUW

Jakie skutki może zrodzić przejęcie jednej skrzynki e-mail w organizacji?

Podczas ostatniego wydarzenia organizowanego przez „Gazetę Ubezpieczeniową" prezentowałem przypadek opisujący konsekwencje przejęcia skrzynki e-mail prezesa małej spółki IT przez nieuprawnione osoby.

Dlaczego opisywałem, wydawałoby się, trywialny przypadek incydentu?

Ponieważ taka sytuacja może dotknąć każdego z nas, zarówno prywatnie, jak i zawodowo, i może doprowadzić do prawdziwych dramatów. Najczęściej nie dlatego, że ktoś świadomie chciał zadać sobie trud i spędził wiele godzin, aby znaleźć sposób na dostanie się do naszej poczty.

Jeżeli używamy tego samego hasła do wielu serwisów, to wystarczy, że z jednego z nich wyciekną nasze dane logowania. Potem już tylko wystarczy użyć tego samego hasła w wielu innych serwisach i mamy dostęp do czyjejś prywatnej skrzynki, konta na Facebooku czy też, o zgrozo, konta bankowego. Z tym ostatnim na szczęście trochę trudniej, bo systemy bankowe są zobligowane do weryfikacji użytkowników poprzez tak zwane wieloskładnikowe uwierzytelnienie.

Jeżeli ktoś używa prostego hasła, składającego się z kilku znaków, to nie trzeba nawet skanować wycieków danych, wystarczą narzędzia „siłowego łamania haseł", odpowiednia moc obliczeniowa i proste hasło łamie się w sekundy. Co gorsza, najczęściej robią to automaty, a nie ludzie.

Jeżeli już dojdzie do incydentu, to co powinniśmy zrobić?

Jeżeli dotyczy to naszej skrzynki prywatnej, powinniśmy zmienić hasło i jeżeli jest to możliwe, aktywować wieloskładnikowe uwierzytelnienie. Warto założyć, że dane z naszej skrzynki e-mail zostały skopiowane i mogą zostać wykorzystane na różne sposoby. Dlatego nieodzowny jest przegląd wszystkich e-maili, wyszukanie haseł, skanów dowodów osobistych, informacji do logowania, umów, wszystkich innych poufnych danych, które mogą się znaleźć w rękach osób o złych intencjach.

Jeżeli wyciek danych mógł narazić osoby trzecie, np. przyjaciół czy rodzinę, to powinniśmy ich o tym poinformować. Wiem, że to jest żmudne i kosztowne, ale jeżeli tego nie zrobimy, jest spora szansa, że nasze zaniedbanie zostanie bezwzględnie wykorzystane. Optymalnym rozwiązaniem jest oczywiście zlecenie pomocy wyspecjalizowanej firmie, nie jest to jednak ani proste, ani tanie.

W przypadku przejęcia firmowej skrzynki e-mail powinniśmy ten fakt zgłosić niezwłocznie osobom z IT lub działu bezpieczeństwa. Ukrywanie tego faktu może narazić całą organizację na dużo większe konsekwencje.

Hakerzy po przejęciu danego konta w organizacji sprawdzają, do jakich systemów mogą się jeszcze zalogować z wykorzystaniem tego samego hasła. Co gorsza, mogą też wykorzystać przejętą skrzynkę e-mail w celu ataków socjotechnicznych na waszych współpracowników.

Jakie mogą być potencjalne skutki incydentu?

To zależy, do czego wasze przejęte konto e-mail zostanie użyte. Nie warto jednak liczyć, że posłużycie tylko do wysyłki spamu. Im dłużej hakerzy mają dostęp do skrzynki, tym większe szkody mogą poczynić. Jeżeli skrzynka zawiera dużo cennych informacji, może być wykorzystana wielokrotnie w wielu różnych formach ataków.

Pośrednicy ubezpieczeniowi są wymarzonym celem ataków, szczególnie te osoby, przez które przechodzi wiele formularzy oceny ryzyka dla ubezpieczeń cyber. Praktyka rynkowa pokazuje, że większość formularzy jest wysyłana pomiędzy klientami a TU bez szyfrowania. Haker przejmuje skrzynkę brokera i ma wielu klientów na widelcu!

Jak uchronić się przed powyżej opisanymi sytuacjami?

Starałem się ten temat przybliżyć w swojej prezentacji podczas ostatniego webinaru. W tym miejscu chciałbym podzielić się jednym przykładem. Jakieś dwa lata temu brałem udział w szkoleniu z cyberbezpieczeństwa dla organizacji zajmującej się logistyką. W szkoleniu wzięło udział ok. 30 osób. Podczas szkolenia poruszyliśmy temat używania „menedżerów haseł". Tego typu oprogramowania pomagają w bezpiecznym przechowywaniu i tworzeniu haseł oraz zarządzaniu nimi.

Tak się złożyło, że po roku miałem spotkanie z tą samą grupą osób. I co się okazało? Z całej grupy tylko dwie osoby zadeklarowały, że używają menedżerów haseł, w tym jedna dlatego, że miała incydent cyber.

Życzę sobie i Państwu, aby z wiedzą wyniesioną z naszego ostatniego webinaru było inaczej!

Tomasz Gaj
prezes zarządu Findia