Bezpieczne dane, bezpieczny biznes.
Ubezpieczenie cyber i OC IT w praktyce pytania i odpowiedzi

1. Prosimy o podanie przykładów zdarzeń mających miejsce w Polsce.

Posługujemy się przykładami szkód zagranicznych z dwóch względów - po pierwsze chcemy uniknąć podawania szczegółów szkód, które łatwo będzie zidentyfikować i przypisać do konkretnego klienta, a po drugie ubezpieczenie ryzyk cybernetycznych to jednak specyficzny produkt i informacje o incydentach, zakresie pokrycia i wysokości odszkodowania mogą być potencjalnie zachętą dla cyberprzestępców do atakowania naszych krajowych klientów.

2. Z czego wynika tak duża liczba cyberataków w Polsce?

Możemy wymienić tu kilka przyczyn, ale najważniejszą jest geopolityka i specyficzne położenie Polski na mapie świata. Duża część ataków jest przeprowadzana przez prorosyjskie grupy hakerskie, celem wywołania destabilizacji regionu. Co więcej jesteśmy ważnym krajem tranzytowym dla wojsk NATO i dostaw dla Ukrainy, co powoduje, że ataki na naszą infrastrukturę są częstsze. Poza tym mamy coraz mocniej scyfryzowaną administrację i usługi publiczne czy sektor finansowy - to też powoduje zwiększoną aktywność cyberprzestępców.

3. Co to znaczy, że kopie zapasowe należy przechowywać w odizolowanym środowisku? Czy to musi być offline?

Środowisko przechowywania kopii zapasowych nie musi być offline. Może to być również np. chmura. Natomiast musi to być środowisko oddzielone od reszty systemu IT klienta. Tu oczywiście chodzi o to, aby w razie ataku i utraty danych, móc je w miarę szybko odzyskać z kopii zapasowych. Jeśli kopie zapasowe nie będą oddzielone od reszty systemu to w przypadku ataku one również mogą ulec zaszyfrowaniu i staną się bezużyteczne.

4. Czy wszystkie dane osobowe muszą być szyfrowane? Czy wystarczy szyfrowanie na serwerach? Czy kopie zapasowe również muszą być szyfrowane?

Tak, szyfrować należy wszystkie dane. Zarówno te w spoczynku, czyli np. na dyskach czy serwerach, ale również dane w czasie transmisji z sieci czy do niej. Kopie zapasowe również powinny być szyfrowane, ponieważ w przypadku ataku one również, tak jak reszta danych, mogą dostać się w niepowołane ręce.

5. Czy w sytuacji, gdy Klient nie zgłaszał dotychczas szkód, istnieje możliwość zaoferowania ochrony wstecznej?

Jak najbardziej możemy w takim przypadku zaproponować pokrycie wsteczne dla ubezpieczonego.

6. Jaka wielkość obrotu procentowego na rynku USA/Kanada wyłącza możliwość złożenia oferty PZU?

Standardowa oferta przeznaczona jest dla podmiotów, których roczny przychód z USA nie przekracza 25% całości przychodu. Natomiast uzyskiwanie wyższego przychodu nie wyłącza możliwości złożenia oferty, w takim przypadku przeprowadzamy dodatkową ocenę ryzyka i jeśli będzie ona pozytywna to również możemy złożyć ofertę.

7. Czy jednostki samorządu terytorialnego (JST) mogą skorzystać z oferty ubezpieczeniowej PZU w zakresie ubezpieczenia ryzyk cybernetycznych?

Tak, oczywiście tak jak w pozostałych przypadkach badamy zabezpieczenia klienta oraz podstawowe parametry dotyczące danych osobowych. Jeżeli JST spełnia wymagania dot. bezpieczeństwa sieci to jak najbardziej składamy oferty.

PZU DLA BIZNESU KORPORACYJNEGO

8. Czy w ramach ubezpieczenia od ryzyk cybernetycznych pokrywany jest utracony zysk?

Tak, zgodnie z zakresem wskazanym w pkt 1.2. OWU od ryzyk cybernetycznych.

9. Która firma obsługuje Call Center w przypadku zgłoszeń szkód związanych z ryzykiem cybernetycznym?

Obsługę Call Center dla szkód z ryzyk cybernetycznych realizuje firma Crawford Polska.

10. Jakie minimalne wymagania w zakresie zabezpieczeń musi spełnić Klient, aby uzyskać ochronę ubezpieczeniową?

Są one zależne od wielkości przedsiębiorstwa, a dokładnie od wysokości osiąganych przychodów. Dla podmiotów z przychodami do 100 mln PLN są to: przeznaczone do użytku komercyjnego zapora sieciowa i antywirus, kopie zapasowe w izolowanym środowisku, instalowanie poprawek krytycznych w ciągu maksymalnie 30 dni, zabezpieczenie zdalnego dostępu do sieci poprzez MFA oraz zachowywanie standardów kart płatniczych (jeśli to dotyczy ubezpieczonego). Dla podmiotów z przychodami pomiędzy 100 a 300 mln PLN dodatkowo jest to szyfrowanie danych, wyłączenie protokołu RDP, ograniczenie uprawnień administratorów do konkretnych osób i wdrożone protokoły dot. poczty elektronicznej. Jeśli ubezpieczony korzysta ze sprzętu lub oprogramowania wycofanego z eksploatacji to powinno być ono izolowanie od sieci. To samo dot. środowiska produkcyjnego - powinno być ono odizolowane od środowiska IT.

11. Czy ubezpieczenie ryzyk cybernetycznych obejmuje kary administracyjne wynikające z regulacji DORA i NIS2, a jeśli tak - w jakich sytuacjach?

To zależy o jakich karach dokładnie mówimy. Triggerem odpowiedzialności administracyjnej w ubezpieczeniu ryzyk cybernetycznych jest naruszenie danych, naruszenie prywatności, czyli ubezpieczenie ryzyk cybernetycznych to nie jest ubezpieczenie odpowiedzialności administracyjnej w szerokim sensie. DORA i NIS2 nakładają kary administracyjne szeroko, różnego rodzaju, w tym te związane np. z zarządzaniem przedsiębiorstwem (np. za niewdrożeniem przepisów czy braku zgodności z regulacjami). A zatem co do zasady pokrywać będziemy kary związane z tymi regulacjami, o ile są one wynikiem cyber incydentu u naszego klienta. Samo niespełnienie warunków dyrektywy nie jest przesłanką do pokrycia takiej kary w ramach ubezpieczenia cyber.

12. Co oznacza dokładnie zapora sieciowa do użytku komercyjnego?

Zapora sieciowa do użytku komercyjnego (ang. commercial firewall) to urządzenie lub oprogramowanie zaprojektowane specjalnie z myślą o ochronie sieci firmowej, organizacyjnej lub instytucjonalnej. Różni się od zapory do użytku domowego przede wszystkim zakresem funkcji, skalowalnością, wydajnością i wsparciem technicznym. Zazwyczaj taka zapora jest wprost przeznaczona do pracy w środowisku biznesowym, obsługuje większą liczbę użytkowników i urządzeń, oferuje zaawansowane funkcje oraz ma wsparcie techniczne i częste aktualizacje. Charakter zapory jest zazwyczaj określony w licencji lub ofercie producenta.

13. Jakie branże PZU uznaje za trudne/nieakceptowalne w kontekście ubezpieczenia OC zawodowe dla IT?

Takimi branżami mogą być m.in. działalność zawodowa IT w obszarze technologii lotniczych i ruchu lotniczego, usługi IT dla branży hazardowej i gier losowych, działalność związana ze stronami tylko dla dorosłych, czy też portale randkowe i społecznościowe.

14. Czy szkody cyber są objęte w OC?

To zależy jak rozumiemy szkodę cyber, ale przyjmując, iż u poszkodowanego dochodzi do szkody objętej ubezpieczeniem ryzyk cybernetycznych, która to wynikałaby np. z jakichś zaniedbań lub błędów po stronie firmy informatycznej obsługującej tego poszkodowanego i te błędy/ zaniedbania doprowadziłby do powstania szkody cyber, to można by było rozważać taką sytuację również w kontekście ubezpieczenia OC zawodowego IT firmy informatycznej – oczywiście z uwzględnieniem warunków OWU oraz ewentualnych postanowień dodatkowych polisy.

15. Czy dostawcy zewnętrzni, którzy korzystają ze zdalnego dostępu również są objęci wymogiem MFA?

Tak, jak najbardziej. Zdalny dostęp do sieci jest jednym z najbardziej wrażliwych punktów całej sieci, dlatego należy szczególnie zadbać o jego zabezpieczenie. Dotyczy to również dostępu dla zewnętrznych dostawców.

16. Czy ubezpieczenie OC zawodowej chroni błędy w kodzie lub konfiguracji systemów?

Tak, ubezpieczenie, zgodnie z warunkami OWU, może chronić szkody powstałe wskutek błędów w kodzie lub błędnej konfiguracji systemów. Tego typu scenariusz jest dość powszechnym przypadkiem. Oczywiście, istotne jest właściwe zgłoszenie działalności do ubezpieczenia.

17. Czy ubezpieczenie obejmuje szkody powstałe w wyniku rażącego niedbalstwa ubezpieczonego?

Tak, zgodnie z warunkami OWU § 3 ust. 2 zakres ochrony ubezpieczeniowej obejmuje również odpowiedzialność za szkody powstałe wskutek rażącego niedbalstwa ubezpieczonego.

18. Czy programista prowadzący jednoosobową działalność gospodarczą może skorzystać z ubezpieczenia odpowiedzialności cywilnej zawodowej dla IT?

Tak, jak najbardziej jesteśmy zainteresowani klientami z tego segmentu.

19. Jak ustalany jest zakres działalności zawodowej objętej ochroną w ofercie lub polisie ubezpieczeniowej?

Na podstawie informacji uzyskanych w toku oceny ryzyka – czy to w oparciu o kwestionariusz oceny ryzyka, czy też zapytanie brokerskie, w ofercie/ polisie precyzyjnie wskazujemy zakres działalności zawodowej Ubezpieczonego, podobnie jak w innych ubezpieczenia odpowiedzialności cywilnej.

20. Czy dostępna jest anglojęzyczna wersja warunków ubezpieczenia OC dla branży IT?

Aktualnie produkt OC dla branży IT jest w fazie wdrożenia, dlatego anglojęzyczna wersja warunków nie jest jeszcze dostępna. Planujemy jej udostępnienie w najbliższym czasie.

21. Czy programiści zajmujący się automatyką przemysłową mogą skorzystać z ubezpieczenia odpowiedzialności cywilnej zawodowej dla IT?

Tak, aczkolwiek w zależności od tego jaki to będzie przemysł i jaka automatyka, możemy potrzebować dodatkowych informacji do oceny ryzyka.

22. Czy celowe działanie pracownika lub wykonawcy świadczącego usługi informatyczne u klienta, skutkujące incydentem cyber (np. utrata dostępu, wyciek danych) będzie objęte ubezpieczeniem w zakresie ubezpieczenia ryzyk cybernetycznych?

W zakresie ubezpieczenia ryzyk cybernetycznych – co do zasady wina umyślna pracownika nie jest wyłączona z zakresu ubezpieczenia. Oczywiście działanie to musiałby skutkować powstaniem zdarzenia cybernetycznego. Każdorazowo badane są również okoliczności powstania szkody, zapisy OWU i umowy ubezpieczenia. Wyłączona jest natomiast wina umyślna członków władz ubezpieczonego.

W kontekście ubezpieczenia OC zawodowej IT – ubezpieczenie generalnie wyłącza szkody wyrządzone umyślnie.