Rozmowa z **Michałem Chodą**, underwriterem PZU

Polisa cyber – ważne uzupełnienie polityki bezpieczeństwa cybernetycznego firmy

Aleksandra E. Wysocka: – Porozmawiamy o ryzykach cyber, których w tym zdalnym świecie jest coraz więcej. Jak to wygląda u polskich przedsiębiorców? Na co powinni oni szczególnie uważać, biorąc pod uwagę, że tak dużo procesów przebiega u nich zdalnie?

Michał Choda: – Bezpieczeństwo pracy zdalnej zależy od jakości i niezawodności połączenia z systemami IT. W PZU zwracamy szczególną uwagę na to, aby taka praca w przedsiębiorstwie ubezpieczonego była odpowiednio zabezpieczona, czy to przez szyfrowaną sieć VPN, czy przez dwupoziomowe uwierzytelnianie. Kładziemy na to nacisk podczas przeprowadzanej oceny ryzyka. Home office jest bardzo popularnym rozwiązaniem w czasie pandemii, jest też ogromną pokusą dla hakerów, którzy czyhają tylko na najsłabsze punkty w połączeniu. Prosty przykład: udostępnienie pulpitu może być dla nich łakomym kąskiem. Jeśli system nie jest odpowiednio zabezpieczony, ryzyko włamania jest bardzo wysokie.

Chciałbym też zwrócić uwagę na odpowiednią ochronę smartfonów czy tabletów, które są także naszymi narzędziami pracy. Wystarczy ochrona biometryczna lub po prostu dodatkowe hasło, by w razie kradzieży uniemożliwić dostęp do wrażliwych danych przechowywanych na urządzeniach mobilnych.

Czy praca zdalna i hybrydowa wpłynęły na liczbę cyberincydentów w polskich firmach? Jak przedsiębiorca powinien w ogóle na takie wydarzenie zareagować?

– Chociaż obserwujemy znaczny wzrost zarówno liczby samych incydentów, jak i wartości wynikających z nich szkód cyber, to przedsiębiorcy niechętnie przyznają się do tego, że

padli ofiarą ataku hakerskiego. Jest to bardzo niekorzystne, gdyż ukrywanie takich informacji znacznie utrudnia rzetelną ocenę ryzyka i wprowadzanie prewencyjnych rozwiązań umożliwiających wyeliminowanie niebezpieczeństw w przyszłości.

Rekomendujemy pełną transparentność w przypadku takich incydentów, co pozwala dokładniej ocenić ryzyka i ułatwia wprowadzenie rozwiązań umożliwiających zarządzanie nimi, a najlepiej ich wyeliminowanie.

Na co powinien zwrócić uwagę broker, który przygotowuje ofertę cyber dla swojego klienta?

– Najważniejsze są szczegółowe dane zebrane w kwestionariuszu. Na przykład odpowiedź na pytanie dotyczące wykonywania backupu danych nie powinna być ogólna i brzmieć lakonicznie „tak” albo „nie”.

Jako ubezpieczyciel powinniśmy wiedzieć, jak często wykonywane i testowane są backupy oraz w jaki sposób są przechowywane. Z takich odpowiedzi musimy uzyskać jak najwięcej przydatnych informacji.

> Najistotniejszym dla przedsiębiorcy z praktycznego punktu widzenia jest assistance. Nasz ekspert w pierwszej kolejności sprawdzi, co dokładnie wydarzyło się u klienta, z jakim atakiem czy wyciekiem danych mamy do czynienia, a następnie ustali plan dalszego działania, by jak najszybciej wyjść z sytuacji kryzysowej.

Jeżeli chodzi o Waszą ofertę w zakresie cyber, to który z elementów może być szczególnie istotny dla przedsiębiorców?

– W mojej ocenie najistotniejszym z praktycznego punktu widzenia jest assistance. W razie incydentu usługa ta zapewni klientowi PZU dostęp do infolinii działającej 24 h na dobę, 7 dni w tygodniu.

Nasz ekspert w pierwszej kolejności sprawdzi, co dokładnie wydarzyło się u klienta, z jakim atakiem czy wyciekiem danych mamy do czynienia, a następnie ustali plan dalszego działania, by jak najszybciej wyjść z sytuacji kryzysowej.

> Odpowiedź na pytanie dotyczące wykonywania backupu danych nie powinna być ogólna i brzmieć lakonicznie „tak” albo „nie”. Jako ubezpieczyciel powinniśmy wiedzieć, jak często wykonywane i testowane są backupy oraz w jaki sposób są przechowywane. Z takich odpowiedzi musimy uzyskać jak najwięcej przydatnych informacji.

Jeżeli problem jest poważny i zajdzie taka potrzeba, do współpracy będzie angażowana na przykład kancelaria prawna, agencja public relations czy informatyk śledczy, który doprowadzi system do stanu użytkowania.

Rozumiem, że innej ochrony potrzebuje mniejsza firma, a innej korporacja. Czy w Waszej ofercie jest takie zróżnicowanie produktowe?

– W PZU oferujemy klientom dwa ubezpieczenia cyber – dla małych i średnich podmiotów oraz dużych przedsiębiorstw. W pierwszym produkcie proces oceny ryzyka jest uproszczony, zaś w samej ofercie skupiamy się przede wszystkim na assistance, czyli pomocy ekspertów, a także na pokryciu części kosztów odtworzenia naruszonych danych lub strat wynikających z zakłócenia działalności. Dochodzi do tego ochrona OC, która zabezpieczy wszelkiego rodzaju roszczenia w stosunku do klienta wynikające z wycieku danych wrażliwych.

Dla największych podmiotów – w szczególności dla klientów z segmentu infrastruktury krytycznej – mamy przygotowany tzw. duży produkt. Kluczowym jego wyróżnikiem jest to, że klient może również ubezpieczyć szkody rzeczowe po cyberatakach. Przykładem takiej szkody może być wybuch, a następnie pożar w serwerowni klienta spowodowany bezpośrednio przez atak hakerski. To unikatowa oferta na polskim rynku. Warto też zwrócić uwagę na e-kradzież, czyli nieuczciwe transfery elektroniczne.

Rynek cyber jest bardzo dynamiczny. Niemal z każdym dniem przybywa nowych wirusów i zagrożeń, których nie jesteśmy w stanie przewidzieć. Pamiętajmy, że samo ubezpieczenie cyber nigdy nie może zastąpić systemu bezpieczeństwa po stronie klienta.

Ochrona ubezpieczeniowa wspiera w razie krytycznej sytuacji, nigdy nie może być substytutem polityki bezpieczeństwa cybernetycznego obowiązującej u danego klienta.

Dziękuję za rozmowę.

Aleksandra E. Wysocka