MATERIAŁ PRASOWY

**Ochrona biznesu przed cyberatakami dzięki ubezpieczeniu ryzyka cybernetycznego i prywatności**

**W szybko zmieniającym się cyfrowym środowisku liczba zagrożeń cybernetycznych i wycieków danych bardzo wzrosła. Według danych Cybersecurity Ventures, koszty związane z cyberprzestępczością mają do 2025 roku wzrosnąć do 10,5 biliona dolarów rocznie.**

W miarę jak rośnie częstotliwość i złożoność tych ataków, sama świadomość strategii zapobiegawczych przestała być już wystarczająca. Konieczne stały się działania proaktywne, mające na celu zapewnienie bezpieczeństwa zarówno osobom prywatnym, jak i firmom. Nawet przy odpowiednim przygotowaniu i zachowaniu czujności, nieprzewidywalny charakter zagrożeń cybernetycznych może prowadzić do znaczących strat, które dotykają nas wszystkich. Wzrastające nieustannie ryzyko związane z cyberprzestępczością i ochroną prywatności spowodowało konieczność stworzenia rozwiązania wspierającego przedsiębiorstwo w przypadku ataku cybernetycznego: ubezpieczenia ryzyk cybernetycznych i prywatności.

*Colonnade oferuje przyszłościowe rozwiązanie ubezpieczeniowe dostosowane do zagrożeń wynikających z wycieków danych i naruszeń. W oferowanych pakietach klienci otrzymają nie tylko ochronę ubezpieczeniową, ale także kompleksowy zestaw specjalistycznych usług. Te zasoby są dostępne, gdy kryzys uderza niespodziewanie, stanowiąc pomoc w nawigowaniu przez zawiłości wyzwań związanych z cyberprzestępczością. Nasi klienci korzystają z wiedzy doświadczonych profesjonalistów od ochrony danych, specjalistów od bezpieczeństwa IT i ekspertów prawnych specjalizujących się w ochronie danych* - zaznaczył Juliusz Małyszko, Lider Praktyki Cyber.

**Rozumienie ryzyk związanych z cyberprzestępczością i prywatnością**

W erze, w której dane stały się życiodajną siłą organizacji, ryzyka związane z prywatnością wplątały się w struktury codziennych operacji. Każde przedsiębiorstwo, niezależnie od swojej wielkości, boryka się z zawsze obecnym wyzwaniem związanym z przetwarzaniem danych elektronicznych przechowywanych na komputerach, serwerach lub w szerokich przestrzeniach Internetu. Dane, zarówno te poufne, jak i osobiste, przechodzą przez wirtualne kanały, podczas gdy procesy digitalizacji i archiwizacji dokumentów fizycznych wymagają wzmożonej czujności.

Proces zarządzania danymi, czy poprzez tradycyjne systemy oparte na papierze, czy te nowoczesne oparte na chmurze, niesie w sobie ryzyko ochrony danych. Firmy stają się podatne na zakłócające ataki, takie jak blokada usług (DoS, DDoS) lub wtargnięcia oparte na sieci, które zagrażają działalności operacyjnej. W rosnącej przestrzeni cyfrowej ryzyka związane z urządzeniami mobilnymi, systemami IT i przestrzenią wirtualną stają się coraz bardziej złożone. Współczesne przedsiębiorstwa priorytetowo traktują zabezpieczanie systemów komputerowych, sieci oraz bezcennych danych, które przechowują, odzwierciedlając przełomową zmianę od ochrony aktywów materialnych do zabezpieczania obszarów cyfrowych.

**Potencjalne czynniki ryzyka**

• Czynnik ludzki: błędy i zaniedbania wynikające z podejmowanych działań

• Słabe punkty w organizacji: niedoskonałe procesy i luki w strukturach firmy

• Ryzyka związane z bezpieczeństwem informacji: wyzwania wynikające z zarządzania poufnymi informacjami

• Celowe ataki: intencjonalne działania hakerów wprowadzające znaczące ryzyko

• Luki związane z outsourcingiem: powierzenie zarządzania danymi podmiotom zewnętrznym

Jak pokazują przykłady z działalności Colonnade, łatwo o popełnienie błędu.

**Przykład 1**

Wielkość ubezpieczonej firmy: mała

Działalność gospodarcza ubezpieczonej firmy: produkcja portfeli

Typ ataku: błąd pracownika

Opis: Pomyłka pracownika doprowadziła do poważnego wycieku danych ubezpieczonego. W niefortunnym zdarzeniu pracownik pomyłkowo wysłał e-mail do niezamierzonego odbiorcy z załącznikiem bazy danych zawierającej poufne dane klientów. Chociaż odbiorca natychmiast usunął e-mail, ubezpieczony był zobowiązany poinformować swoich klientów o incydencie w ramach środków ostrożności.

Skutki finansowe wyniosły od 2 600 do 13 000 euro. Ubezpieczenie ryzyka cybernetycznego pokryło koszty powiadomienia klientów, przy czym udział własny to jedyny koszt poniesiony przez ubezpieczonego.

**Przykład 2**

Wielkość ubezpieczonej firmy: duża

Działalność gospodarcza ubezpieczonej firmy: produkcja urządzeń komputerowych

Typ ataku: system antywirusowy pokonany przez najnowszy wirus

Opis: Nowe zagrożenie cybernetyczne zakłóciło działalność w renomowanym przedsiębiorstwie produkującym urządzenia komputerowe. Hakerzy zdołali przełamać nowoczesny system informatyczny ubezpieczonego za pomocą złośliwego oprogramowania, co wymusiło zawieszenie wszystkich działań produkcyjnych przez dwa tygodnie. Przez ten czas proces objął badanie, czyszczenie serwerów, oprogramowania oraz komputerów przez ekspertów. W celu naprawy rozległych szkód, roszczenie ubezpieczonego zostało podzielone na dwie kategorie: po pierwsze, znaczne koszty związane ze specjalistycznym śledztwem i bezpiecznym przeniesieniem danych na nowy sprzęt; po drugie, znaczące przerwy w działalności, które trwały ponad 14 dni, aż do pełnej odbudowy infrastruktury IT.

Skutki finansowe tego incydentu wyniosły od 130 000 do 260 000 euro. Wszechstronne ubezpieczenie ryzyk cybernetycznych pokryło wszystkie wydatki związane z usługami ekspertów i zminimalizowało straty netto ze sprzedaży, przy czym udział własny to jedyny koszt poniesiony przez ubezpieczonego.

**Adresowanie ryzyka związanego z cyberprzestępczością i prywatnością**

Współczesne zagrożenia dla systemów informatycznych odzwierciedlają niebezpieczeństwa dotyczące aktywów materialnych. Konsekwencje incydentu cybernetycznego mogą być bardzo poważne. Ubezpieczenie cybernetyczne Colonnade zaprojektowano, aby poradzić sobie z zawiłymi reakcjami łańcuchowymi takich kryzysów, łagodząc ich rozległe skutki. Poniżej znajduje się przykładowy scenariusz, który podkreśla wieloaspektowy charakter tych wyzwań w ramach przedsiębiorstwa:

• Wyciek danych: poufne dane biznesowe lub osobiste są nielegalnie ujawniane, co niszczy zaufanie i reputację.

• Zarządzanie kryzysowe działu IT: szybka reakcja ze strony działu IT jest niezbędna do przywrócenia normalnej działalności, jednocześnie utrzymując operacje biznesowe.

• Łagodzenie kryzysu poprzez działania PR: szybka reakcja na wiadomości o wycieku danych łagodzi szkody reputacyjne zaostrzone przez zasięg mediów społecznościowych.

• Skutki finansowe: konsekwencje finansowe incydentu zakłócają regularne operacje biznesowe.

• Zamieszanie w zarządzaniu: nieprzewidziane incydenty stwarzają wyzwania na poziomie zarządzania.

**Przewagi i zalety ubezpieczeń ryzyk cybernetycznych i prywatności**

Ubezpieczenie ryzyk cybernetycznych i prywatność wykracza poza konwencjonalne paradygmaty ochrony, obejmując wielowymiarowe aspekty naruszeń danych, wycieków i ich konsekwencji. Zakres oferty obejmuje ochronę finansową, wsparcie w zachowaniu reputacji korporacyjnej, łagodzenie negatywnych wpływów na systemy IT oraz synergiczną ochronę ubezpieczeniową wraz z ekspertyzą doradczą, a także ekspertyzy śledcze, odzyskiwanie utraconych danych elektronicznych, ponowne zbieranie, replikację i pokrycie kosztów ich odzyskiwania.

Ubezpieczenie ryzyk cybernetycznych i prywatności oferuje uniwersalne rozwiązanie dostępne dla przedsiębiorstw każdej wielkości i ze wszystkich branż. Niezależnie od charakteru, podmioty podatne na opisane wyzwalacze - czy to kradzieże danych, zakłócenia sieci czy inne - mogą skorzystać z ochrony zapewnianej przez to ubezpieczenie. W świecie naznaczonym niepewnością, jedna prawda pozostaje niezachwiana: cyberodporność stanowi fundament, na którym budowane jest solidne przedsiębiorstwo.

\*\*\*

## Kontakt dla mediów

Sandra Olechnowicz

sandra.olechnowicz@corepr.pl

tel. 603 782 077

**Colonnade Insurance S.A. jest spółką ubezpieczeń majątkowych i osobowych (non-life) zarejestrowaną w Luksemburgu, należącą do grupy Fairfax i utworzoną w celu strategicznego rozszerzenia działalności ubezpieczeniowej Fairfax w Europie Środkowej i Wschodniej. Posiada licencję na oferowanie 17 z 18 ustawowych grup ubezpieczeń majątkowych i osobowych (z wyjątkiem grupy 10 – OC posiadaczy pojazdów mechanicznych). Uprawnia do prowadzenia działalności we wszystkich krajach członkowskich UE w ramach swobody świadczenia usług. Działalność Colonnade wspierają wiodący światowi reasekuratorzy o najsilniejszej pozycji finansowej, między innymi Swiss Re, Hanover Re, Munich Re, SCOR and Everest Re, Aspen Re, syndykat Lloyd's. Firma powadzi działalność przez oddziały w Bułgarii, Czechach, na Węgrzech, w Rumunii, Polsce, Słowacji oraz przez spółkę w Ukrainie, korzystając z pomocy zespołu ponad 600 doświadczonych specjalistów. Oferuje produkty dla klientów indywidualnych i korporacyjnych i od 2017 r. lat posiada rating A- nadany przez AM Best. Kapitał zakładowy wynosi 9 500 000 EUR.**