CyberRED – KOMPLEKSOWE UBEZPIECZENIE RYZYK ZWIĄZANYCH Z NARUSZENIEM CYBERBEZPIECZEŃSTWA

Już teraz zadbaj o cyfrowe bezpieczeństwo Twojej firmy!

W związku z szybkim rozwojem technologicznym oraz przeniesieniem części usług do internetu, zapewnienie bezpieczeństwa cyfrowego stało się kluczowym wyzwaniem dla przedsiębiorców na całym świecie. Niestety, mimo świadomości zagrożenia codziennie słyszymy o nowych atakach i incydentach, które niosą ze sobą poważne konsekwencje, a często decydują nawet o być albo nie być danej firmy.

Dlatego chcemy zwrócić Twoją uwagę na to, że:

wiadomość e-mail to najpopularniejsze źródło rozprzestrzeniania złośliwego oprogramowania

kwoty okupu, jakich żądają hakerzy w związku z atakiem typu ransomware, sięgają nawet **kilkudziesięciu milionów dolarów**

najbardziej kosztownym skutkiem cyberincydentów są **przerwanie i blokada działalności**

w przypadku wycieku danych kara nałożona na podstawie przepisów RODO może wynieść aż **20 milionów euro** lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa

Odpowiedz sobie na pytanie
– czy Twoja firma jest na to odpowiednio przygotowana?

Zabezpiecz się, korzystając z CyberRED, w ramach którego oferujemy m.in.:

- szeroki zakres ubezpieczenia, a w nim aż 10 sekcji do wyboru
- wsparcie w reakcji na incydent, świadczone przez naszego partnera – eksperta z obszaru cyberbezpieczeństwa, wraz z infolinią dostępną całodobowo, 7 dni w tygodniu (SOC oraz CSIR)
- pomoc w łagodzeniu skutków ataku oraz pokrycie straty wynikającej z przerwy w działalności
- wsparcie prawne i finansowe w przypadku naruszenia przepisów RODO
- badanie zasadności oraz pokrycie kierowanych przeciwko Twojej firmie roszczeń
- pokrycie kosztów odbudowy wizerunku
- ochronę również w przypadku ataku cyberterrorystycznego
- jasne i przejrzyste warunki ubezpieczenia

We współpracy z naszym partnerem, oferujemy dostęp do:

SECURITY OPERATIONS CENTER (SOC) – weryfikującego, czy Twoja firma padła ofiarą incydentu:

- call center w trybie 24/7
- analiza zgłoszeń i incydentów
- wydawanie rekomendacji dot. dalszych działań po incydencie

CYBER SECURITY INCIDENT RESPONSE (CSIR) – pomagającego usunąć skutki incydentu:

- koordynacja działań
- zdalna reakcja na incydenty oraz reakcja w miejscu ich wystąpienia
- wdrożenie środków zaradczych
- analiza śledcza artefaktów cyfrowych oraz przygotowanie materiałów dowodowych na potrzeby procesu sądowego

CyberRED w praktyce – historie z życia wzięte

Oferowany przez nas zakres ubezpieczenia został skonstruowany tak, aby chronić Twoją firmę przed realnymi skutkami zagrożeń cyfrowego świata.

BŁĄD PRACOWNIKA

W wyniku prostego błędu ludzkiego zaufany pracownik Twojego sklepu internetowego upublicznił niezaszyfrowaną bazę klientów, zawierającą m.in. dane osobowe oraz numery ich kart płatniczych. Efektem tego były liczne pozwy cywilne od samych poszkodowanych, a na domiar złego UODO wszczął wobec Ciebie postępowanie i nałożył na Twoją firmę karę administracyjną. Niestety, ze względu na informacje opublikowane na ten temat w internecie ucierpiała również reputacja sklepu.

Na taką okoliczność warto wybrać następujące SEKCJE, które obejmują m.in.:

SEKCJA I

REAKCJA NA INCYDENT I NARUSZENIE OCHRONY DANYCH OSOBOWYCH

- wynagrodzenie ekspertów badających incydent
- poinformowanie poszkodowanych o wycieku ich danych
- usługi monitorowania sieci pod kątem pozyskania danych oraz ochrony przed wyłudzeniami
- koszty pomocy prawnej w postępowaniach przed organami państwowymi
- pokrycie nałożonych na Twoją firmę kar administracyjnych

SEKCJA IV

OCHRONA REPUTACJI

- pokrycie honorarium ekspertów z zakresu public relations opracowujących strategię i podejmujących działania w obronie reputacji firmy
- wynagrodzenie kancelarii prawnej reprezentującej Twoje interesy w sporach o naruszenie reputacji firmy (np. niesłuszne oskarżenie w mediach) w związku z zaistniałym incydentem

SEKCJA VII

NARUSZENIE STANDARDÓW BEZPIECZEŃSTWA BRANŻY KART PŁATNICZYCH (PCI-DSS)

- pokrycie kar pieniężnych nałożonych na Twoją firmę w związku z naruszeniem standardów PCI-DSS
- pokrycie kosztów ponownej certyfikacji PCI-DSS
- pokrycie kosztów wystawienia nowych kart płatniczych

SEKCJA VIII

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE DANYCH OSOBOWYCH

- pokrycie odszkodowania należnego poszkodowanym w wyniku wycieku danych
- wynagrodzenie kancelarii prawnej, wynajętej do obrony przed powyższymi roszczeniami

ZŁOŚLIWE OPROGRAMOWANIE

W wyniku zainfekowania złośliwym oprogramowaniem typu ransomware zablokowany został dostęp do głównego systemu informatycznego Twojej firmy, a także usunięto z niego wszystkie faktury VAT z ostatniego miesiąca. W zamian za odblokowanie autorzy ataku żądają okupu w kryptowalucie. Dodatkowo, aby zwiększyć pole rażenia, cyberprzestępcy, podszywając się pod pracownika Twojej firmy, rozesłali do wszystkich kontrahentów wiadomość e-mail z zainfekowanym załącznikiem, zawierającym to samo złośliwe oprogramowanie, które rozniosło się również na ich komputery.

Na taką okoliczność warto wybrać następujące SEKCJE, które obejmują m.in.:

SEKCJA II

DZIAŁANIA NAPRAWCZE

- pokrycie wynagrodzenia ekspertów zajmujących się odzyskiwaniem danych
- wynagrodzenie ekspertów zajmujących się odblokowaniem systemu
- identyfikacja trwale uszkodzonych danych
- odtworzenie trwale uszkodzonych faktur z wersji papierowych

SEKCJA III

PRZERWANIE DZIAŁALNOŚCI

- pokrycie straty w zyskach, jaką Twoja firma poniosła w związku z blokadą systemu
- zwiększone koszty prowadzenia działalności

SEKCJA V

WYMUSZENIE

- wynagrodzenie ekspertów z zakresu informatyki śledczej (IT forensic)
- pokrycie kwoty żądanego okupu (za zgodą organów ścigania)

SEKCJA IX

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE BEZPIECZEŃSTWA SIECI

- pokrycie odszkodowania zasądzonego na rzecz poszkodowanego, który utracił dostęp do swoich danych lub systemu z Twojej winy
- honorarium kancelarii prawnej zatrudnionej do obrony Twojej firmy przed wspomnianymi roszczeniami

ATAK HAKERSKI

Aby osłabić konkurencję, inna firma działająca na tym samym rynku zleciła dokonanie ataku hakerskiego wycelowanego w Twoją działalność. Chcąc wyrządzić jak najwięcej szkód, cyberprzestępcy weszli w posiadanie danych dostępowych do rachunku bankowego Twojego przedsiębiorstwa, po czym dokonali nieautoryzowanej transakcji, wyprowadzając z niego wszystkie środki. Chcąc dodatkowo zrazić do Twojej firmy zaufanego kontrahenta, za pomocą mediów społecznościowych opublikowali obraźliwy tekst naruszający publicznie dobre imię prezesa tej firmy, okraszony zdjęciem, do którego nie posiadałeś praw autorskich.

Na taką okoliczność warto wybrać następujące SEKCJE, które obejmują m.in.:

SEKCJA VI

CYBERPRZESTĘPSTWA

- pokrycie wartości niedających się odzyskać kwot, których zostałeś pozbawiony w wyniku incydentu

SEKCJA X

ODPOWIEDZIALNOŚĆ ZA TREŚCI ROZPOWSZECHNIANE W INTERNECIE

- pokrycie odszkodowania należnego za naruszenie odpowiednio - dobrego imienia oraz praw autorskich
- wynagrodzenie kancelarii prawnej, wynajętej do obrony przed roszczeniami związanymi z treściami rozpowszechnionymi w internecie