MATERIAŁ
MARKETINGOWY

PZU Cyber

Ubezpieczenie od ryzyk cybernetycznych i związanych z RODO

POMOC I OCHRONA W RAZIE ZDARZEŃ CYBERNETYCZNYCH I PRZYPADKÓW NARUSZENIA DANYCH

Rozwój technologii idzie w parze z rozwojem zagrożeń, które czekają na nas w sieci. W świecie nowoczesnych technologii, dostępności Internetu oraz powszechności korzystania z komputerów w codziennym biznesie cyberataki są nieuniknione. Nasze bezpieczeństwo jest zagrożone już nie tylko w świecie realnym, ale przede wszystkim w wirtualnym. Korzystanie z systemów komputerowych znacznie zwiększa podatność firm na zagrożenia cybernetyczne i naruszenia danych. Niezaplanowane przerwy w działaniu komputerów i infrastruktury IT, spowodowane np. złośliwym oprogramowaniem czy atakami hakerskimi, skutkują często stratami, które mogą doprowadzić nawet do upadłości firmy. Jednym z rozwiązań, zwiększających bezpieczeństwo finansowe w obliczu wskazanych zagrożeń, jest ochrona ubezpieczeniowa, która zapewnia pomoc renomowanych, międzynarodowych ekspertów działających lokalnie – tam gdzie Twój biznes.

Zagrożenia cybernetyczne i ich skutki

Złośliwe oprogramowanie (malware)

Malware to różnego rodzaju szkodliwe programy, które usiłują zainfekować komputer lub urządzenie mobilne. Hakerzy wykorzystują je do różnych celów — wykradania danych osobowych, haseł i pieniędzy oraz blokowania dostępu do urządzeń.

Do szczególnie uciążliwych należą:

- **wirusy komputerowe** – złośliwe programy lub kody, które zarażają programy i pliki, kopiując się samodzielnie,
- **ransomware** – program, którego celem jest wymuszenie okupu. Po uruchomieniu na urządzeniu szyfruje dane i wyświetla żądanie zapłaty za odzyskanie danych. Jednak nawet zapłata okupu nie daje gwarancji zwrotu danych. Niektóre programy ransomware mogą też szyfrować dyski sieciowe i dane w chmurze.

Przykład
Pracownik wszedł na zainfekowaną stronę internetową, z której pobrał dokument i otworzył pozornie nieszkodliwy plik. Następnego dnia zamówienia magazynowe i kasy sklepowe zaczęły działać nieprawidłowo, a sprzedaż została zatrzymana w wyniku awarii sieci. Część plików została zaszyfrowana przez oprogramowanie ransomware.

Phishing

Oszustwo polegające na podszywaniu się pod innych w celu kradzieży danych od ofiary, najczęściej informacji dostępowych, np. loginu i hasła do systemów firmowych, lub nakłonienia do pewnych działań. Oszuści często wysyłają podszywającą się pod wiarygodną wiadomość e-mail, która udaje komunikat od autentycznej instytucji lub osoby, i nakłaniają do otworzenia zainfekowanego pliku lub strony internetowej.

Przykład
Pracownik otrzymał wiadomość pochodzącą rzekomo od działu IT z prośbą o zalogowanie się na nowej stronie dostępowej do poczty. Nie zwracając specjalnie uwagi na treść wiadomości, kliknął w odnośnik i wpisał swoje dane dostępowe. Okazało się, że haker uzyskał dostęp do skrzynki pocztowej pracownika, w której znajdowały się poufne dane klientów. Haker groził sprzedaniem tych danych w Internecie, jeżeli nie zostanie zapłacony mu okup.

Atak blokujący dostęp (atak DoS i DDoS)

Zmasowany atak na system komputerowy lub usługę sieciową, polegający na wysyłaniu ogromnej liczby zleceń (prób połączeń z systemem, operacji), którego celem jest zablokowanie działania systemu firmy ofiary przez zajęcie wszystkich wolnych zasobów. Atak blokujący dostęp pochodzi z jednego źródła lub z wielu, np. z urządzeń „zombie", zarażonych wcześniej przez złośliwe oprogramowanie (malware) i sterowanych przez napastnika.

Przykład
Hakerzy przeprowadzili atak DDoS na serwery kwiaciarni internetowej. Atak polegał na wysłaniu w ciągu minuty milionów żądań wyświetleń strony internetowej, na której zamawia się kwiaty. Brak możliwości sprzedaży przez tydzień spowodował znaczącą utratę dochodów.

Naruszenie bezpieczeństwa danych, np. kradzież, wyciek danych, zgubienie dokumentów

To np. sytuacja, gdy pracownik niechcący wyśle e-mail z widoczną pełną listą adresów odbiorców, zaginie dokumentacja medyczna pacjentów przychodni, nieuczciwy pracownik wykradnie dane finansowe klientów Twojej firmy czy hakerzy skradną dane klientów z Twojej bazy.

Przykład
Nieuczciwy pracownik wykradł ponad 700 danych osobowych klientów, w tym nazwiska, adresy i dane kontaktowe, numery PESEL. Okazało się, że dane zostały dostarczone nowemu pracodawcy. Ponieważ jest to zdarzenie powodujące naruszenie RODO, zawiadomienie musiało zostać przekazane do Prezesa Urzędu Ochrony Danych i zainteresowanych osób, których dane dotyczą.

Jakie mogą być skutki zdarzeń cybernetycznych

- Blokada, awaria czy wyłączenie komputerów i innych urządzeń firmowych.
- Spowolnienie działania lub zablokowanie sieci komputerowej firmy.
- Kradzież i sprzedaż wrażliwych danych przedsiębiorstwa.
- Zaszyfrowanie danych i żądanie okupu za ich odzyskanie.
- Pozyskanie przez osoby trzecie dostępu do tajnych dokumentów firmy.
- Utrata danych klientów, pracowników, kontrahentów.
- Przerwa w prowadzeniu działalności (przestój firmy) i związana z tym utrata dochodów.
- Naruszenie reputacji firmy.

Zakres ubezpieczenia od ryzyk cybernetycznych

Nasze ubezpieczanie chroni Cię m.in. przed skutkami ataków cybernetycznych i zobowiązaniami wynikającymi z naruszenia przepisów dotyczących prywatności, m.in. rozporządzenia o ochronie danych (RODO). Zapewnimy Ci szybką pomoc w sytuacji kryzysowej.

Pokryjemy koszty roszczeń (np. odszkodowań, zadośćuczynień, kar i grzywien – w granicach dozwolonych przez prawo), które są do Ciebie kierowane i które powstały w wyniku:

- naruszenia prywatności, w tym danych osobowych,
- naruszenia praw autorskich, prawa własności przemysłowej, prawa do firmy lub prawa do domeny internetowej,
- plagiatu, piractwa, przywłaszczenia lub kradzieży koncepcji,
- naruszenia dobrego imienia (zniesławienia, pomówienia, podważenia reputacji biznesowej),
- naruszenia obowiązku zachowania poufności,
- przekazania dalej wirusa lub innego złośliwego oprogramowania.

Pokryjemy koszty związane z naprawą szkód spowodowanych naruszeniem danych lub zagrożeniem bezpieczeństwa sieci, np. koszty:

- informatyków śledczych,
- obsługi prawnej,
- odzyskania danych, które zostały przypadkowo usunięte, uszkodzone, zniszczone lub zaszyfrowane przez wirusa lub oprogramowanie ransomware,
- związane z cybernetycznym wymuszeniem (żądaniem okupu),
- zawiadomienia (np. związane z obowiązkiem informacyjnym RODO),
- ochrony dobrego imienia (działania PR),
- monitorowania transakcji (na wypadek nieuprawnionego posłużenia się danymi Twoich klientów, w tym kartami płatniczymi – tzw. kradzieży tożsamości).

Zrekompensujemy utratę zysku Twojego przedsiębiorstwa oraz wydatki niezbędne do podtrzymania działalności firmy:

- utracony zysk netto oraz wydatki niezbędne do podtrzymania działalności Twojej firmy z powodu nieupoważnionego dostępu, błędu operatora, ataku poprzez odmowę dostępu czy wprowadzenia złośliwego oprogramowania,
- koszty i wydatki, które poniosłeś, aby uniknąć lub zmniejszyć rozmiary skutków awarii systemu komputerowego lub zakłóceń sieci informatycznej,
- koszty wykrycia i zmniejszenia zakłóceń lub pogorszenia bezpieczeństwa sieci informatycznej oraz koszty ustalenia i utrwalenia dowodów tej szkody.

Pokryjemy koszty kar i oceny PCI związane z naruszeniem standardów bezpieczeństwa PCI podczas przetwarzania danych kart płatniczych.

Standardy bezpieczeństwa PCI obowiązują firmy (niezależnie od ich wielkości i kwoty transakcji), które akceptują płatności kartami kredytowymi i debetowym. Każda firma, która przechowuje, przetwarza i/lub przesyła numery kart płatniczych, powinna zapewnić zgodność obsługi transakcji ze standardem PCI DSS.

Pomagamy szybko i profesjonalnie

Nasza pomoc dostępna jest 24 godziny na dobę, 365 dni w roku.

Skontaktuj się z Centrum Pomocy

Jeśli potrzebujesz pomocy, to dzięki ubezpieczeniu w PZU możesz się z nami skontaktować telefonicznie lub e-mailowo o każdej porze dnia i nocy. Dane kontaktowe znajdziesz w swojej polisie.

Podaj potrzebne informacje

Nasi konsultanci zbiorą podstawowe dane o zdarzeniu i przekażą Twoje zgłoszenie do eksperta z odpowiedniego zespołu reagowania.

Przygotujemy plan działania i udzielimy wstępnej pomocy

Skontaktuje się z Tobą nasz ekspert z zespołu reagowania na incydenty, który przekaże Ci pierwsze wskazówki oraz przygotuje plan działania najbardziej korzystny dla Twojej firmy.

Zorganizujemy pomoc ekspertów

Dzięki ekspertom, z którymi stale współpracujemy, pomożemy Ci w usunięciu skutków powstałej szkody – odzyskasz płynność w działalności biznesowej i zminimalizujesz negatywne skutki zdarzenia.

Nasi eksperci:

- zatrzymają atak oraz przywrócą dane i systemy informatyczne Twoje firmy,
- zapobiegną przerwaniu działalności firmy z powodu ataku cybernetycznego czy innego zdarzenia,
- zapewnią pomoc prawną w zakresie roszczeń odszkodowawczych,
- zorganizują działania PR, jeśli Twoja marka została poszkodowana w wyniku ataku cybernetycznego.

Nasi partnerzy

W przypadku ataku cybernetycznego lub naruszenia bezpieczeństwa danych ważna jest szybka i profesjonalna pomoc. Współpracujemy z renomowanymi międzynarodowymi partnerami, którzy działają też lokalnie – tam gdzie Twój biznes. Nasi partnerzy to m.in.:

Zarządzanie incydentami

Crawford

Public relations

FLEISHMANHILLARD FISHBURN

Eksperci IT

F-Secure

Grant Thornton

Kancelarie prawne

CMS Law.Tax

大成 DENTONS

DLA PIPER

DZP więcej niż prawo

Główne korzyści z ubezpieczenia

Uzupełnienie zabezpieczeń systemów

Nawet najbardziej zaawansowane zabezpieczenia nie zapewniają w 100% bezpieczeństwa sieci. Złośliwe oprogramowanie szuka słabych punktów systemów i często znajduje luki, które nie zostały jeszcze zaktualizowane. Coraz częściej, gdy trudno jest dostać się zdalnie do sieci przedsiębiorcy, hakerzy próbują wykorzystywać błędy ludzi, stosując rozmaite chwyty socjotechniczne.

Uzupełnienie standardowej ochrony ubezpieczeniowej Twojej firmy

Standardowe ubezpieczenia dla firm nie chronią przed skutkami cyberataków i przypadkami naruszenia danych. Ubezpieczenie od ryzyk cybernetycznych zostało specjalnie zaprojektowane tak, aby wyeliminować luki w ochronie ubezpieczeniowej firm i zapewnić przedsiębiorcom ochronę przed zagrożeniami cybernetycznymi oraz szybką pomoc w razie zdarzenia.

Międzynarodowi partnerzy, lokalna pomoc

Ataki cybernetyczne zdarzają się codziennie na całym świecie. Pomoc naszych ekspertów dostępna jest 24 godziny na dobę, 365 dni w roku. W razie problemów szybko przywrócimy działanie Twojej firmy. Będzie to możliwe dzięki naszej współpracy ze światowymi ekspertami w dziedzinie obsługi zdarzeń cybernetycznych. Teraz będą mogli pomóc także Tobie.

Pokrycie kosztów związanych ze zdarzeniem cybernetycznym

Odpowiedzialność, jaka wynika z utraty lub niewłaściwego wykorzystania danych wrażliwych, to tylko jeden z potencjalnych skutków zdarzenia cybernetycznego. Pozostałe to przerwanie działalności czy koszty odzyskiwania danych oraz przywrócenia dobrej reputacji firmy. Nasze ubezpieczenie pomoże Ci pokryć te – często niemałe – wydatki.

Finansowe zabezpieczenie w przypadku naruszenia danych osobowych

Administratorzy danych osobowych oraz firmy przetwarzające dane w ich imieniu narażone są na ryzyko kosztów nie tylko kar administracyjnych. Analizując zagrożenia takiej działalności, należy uwzględnić koszty cyberataków, zadośćuczynień, odszkodowań, utrzymania reputacji, przestojów w działalności, koszty zarządzania całym incydentem oraz koszty poinformowania osób, których dane zostały naruszone. Obecnie nie istnieją rozwiązania chroniące całkowicie przed naruszeniem bezpieczeństwa przetwarzanych danych, istnieje jednak rozwiązanie finansowe – zabezpieczenie się na okoliczność kosztów odpowiednią polisą od ryzyk cybernetycznych.

Uzupełnienie istniejących zespołów IT

Ubezpieczenie cybernetyczne nie podważa skuteczności zespołów bezpieczeństwa IT, z którymi już współpracuje Twoja firma. Takie ubezpieczenie uzupełnia ich umiejętności i dodatkowo chroni Twój biznes przed nieznanymi dotąd zagrożeniami. Ponadto jeśli w wyniku ataku cybernetycznego Twoja firma będzie miała przerwę w działalności, a w efekcie utracisz spodziewany zysk, ubezpieczenie pozwoli Ci zrekompensować tę stratę.

Nie musisz być celem, by zostać zaatakowanym

Ataki cybernetyczne mogą rozprzestrzeniać się za pośrednictwem e-maili od Twoich klientów, dostawców lub outsourcingu technologii. Może to mieć znaczący wpływ na Twoją firmę. Wcale nie musi być ona celem ataku, wystarczy, że będzie nim Twój dostawca hostingu, serwerów czy miejsca w chmurze. Sytuacja taka powoduje, że również dane Twojej firmy nie będą bezpieczne.

Ochrona dla każdej firmy i branży

Cyberprzestępstwa mogą mieć wpływ na każdą firmę, niezależnie od jej wielkości i branży, w której działa. Koszty ataku cybernetycznego czy wycieku danych zawsze są wysokie. Odpowiednie ubezpieczenie pozwoli szybko poradzić sobie z atakiem i jego skutkami (także finansowymi i wizerunkowymi).

5 wskazówek, które wzmocnią bezpieczeństwo firmy

Stosuj poniższe wskazówki i zwiększ bezpieczeństwo swojej firmy. Pamiętaj, że do ubezpieczenia wymagamy używania programu antywirusowego i zapory sieciowej oraz tworzenia kopii zapasowych istotnych danych.

Używaj programu antywirusowego i zapory sieciowej – zainstaluj oprogramowanie antywirusowe i zaporę sieciową (firewall), aby chronić systemy i sieci. Aktualizuj bazę sygnatur wirusowych najczęściej, jak to możliwe.

Twórz kopie zapasowe istotnych danych – kopie zapasowe powinny być tworzone przynajmniej co 7 dni.

Istotnymi danymi dla Twojej działalności mogą być bazy danych, które przechowujesz w swoich komputerach, telefonach, na dyskach i serwerach z bazami danych klientów czy wznowień. Kopię zapasową przechowuj na oddzielnym nośniku (np. zewnętrznym dysku twardym, pendrivie) lub w chmurze.

Szyfruj urządzenia mobilne i dyski firmowe – upewnij się, że urządzenia mobilne, takie jak: laptopy, telefony komórkowe, dyski przenośne, są odpowiednio zabezpieczone. Stosuj hasła, zabezpieczenia biometryczne, blokady i szyfruj dyski. Używaj do tego unikalnych haseł.

Przyjmujesz płatności kartą? Upewnij się, że robisz to prawidłowo – przestrzegaj standardów bezpieczeństwa danych kart płatniczych PCI DSS. Zobowiązuje Cię do tego umowa z operatorem płatności.

Zadbaj o ochronę ubezpieczeniową – dzięki ubezpieczeniu zapewnimy Ci pomoc i ochronę w razie zdarzeń cybernetycznych i przypadków naruszenia danych.

Nasi specjaliści pomagają zarówno w przypadku zewnętrznych ataków cybernetycznych, jak i w przypadku wewnętrznych incydentów wywołanych np. przez Twoich pracowników czy systemy, których używasz.

Oblicz, czy warto mieć ubezpieczenie od ryzyk cybernetycznych

1. Wyceń jeden dzień braku działalności Twojej firmy – policz utracone przychody, niezrealizowane zamówienia lub usługi, straty wynikające z przerwania procesu produkcji.
2. Pomnóż to przez liczbę dni potrzebnych na ponowne uruchomienie działalności i poprawę tego, co zawiodło, żeby sytuacja się nie powtórzyła.
3. Dodaj straty, jakie możesz ponieść w wyniku utraty danych, np. Twoich klientów.
4. Dodaj koszt strat wizerunkowych Twojej firmy, czyli koszty obsługi specjalistów PR.
5. Policz, ile będzie Cię kosztować odzyskanie utraconej pozycji na rynku. I dodaj tę kwotę do reszty.

Prawie połowa firm traci

44%
firm poniosło straty finansowe na skutek cyberataków

21%
padło ofiarą zaszyfrowania dysku przez ransomware

20%
średnich i dużych firm **nie ma ani jednego pracownika** ds. cyberbezpieczeństwa

8%
przebadanych firm jest dojrzałych pod względem bezpieczeństwa informacji

Źródło: Raport PwC Polska pt. „Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście”.

84%
firm najbardziej obawia się pojedynczych hakerów. Na kolejnych miejscach znalazły się zorganizowane grupy cyberprzestępcze oraz cyberterroryści (odpowiednio dla 58% i 57% respondentów). Blisko co druga firma (54%) obawia się działań niezadowolonych lub podkupionych pracowników.

Cyberataki pozostają powszechnym zjawiskiem wśród firm prowadzących działalność w Polsce. W 2018 roku **przynajmniej jeden cyberincydent odnotowało blisko 70% ankietowanych** przedsiębiorstw.

Czynnik ludzki jest największym wyzwaniem dla firm **(63%)** w zapewnieniu oczekiwanego poziomu zabezpieczeń. Brak wykształconej kadry jest większym problem niż zbyt mały budżet **(61%)**.

Złośliwe oprogramowanie – szpiegujące oraz szyfrujące dane (ransomware), a także kradzież danych przez pracowników są dla firm największymi zagrożeniami.

Źródło: Raport KPMG Polska pt. „Barometr cyberbezpieczeństwa. W obronie przed cyberatakami”.

801 102 102 pzu.pl
Opłata zgodna z taryfą operatora