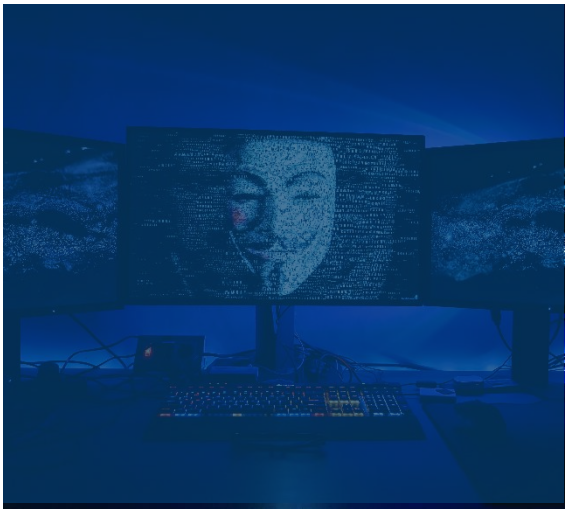
UBEZPIECZENIE CYBER



Ubezpieczenie Cyber mylnie kojarzone jest jako produkt związany wyłącznie z odpowiedzialnością za naruszenie prywatności. Pamiętajmy, że wyciek danych osobowych to nie jedyne ryzyko, z którym mierzą się dziś przedsiębiorstwa.
W rzeczywistości cyberprzestępcy coraz częściej atakują branże, które prawie w ogóle nie przechowują poufnych danych. Dziś to ataki ransomware, które zatrzymują działalność, czy też oszustwa związane z firmową pocztą e-mail, które skutkują przelewaniem płatności na fałszywe konta.
Dodatkowo, dyrektywa NIS2, której implementacja planowana jest na październik b.r. rozszerza krąg podmiotów objętych wymogami w ramach krajowego systemu cyberbezpieczeństwa, jak również zakres ich obowiązków. Za nieprzestrzeganie wymogów grozić będą m.in. wysokie kary administracyjne.

PRZED CZYM CHRONI UBEZPIECZENIE CYBER?

Ubezpieczenie cyber wychodzi naprzeciw rozwijającej się działalności cyberprzestępców i obejmuje:

- Utracony zysk oraz dodatkowe koszty działalności wynikające z zakłócenia systemów informatycznych.
- Koszty wymuszeń (w tym kwotę okupu).
- Koszty obrony w postępowaniu administracyjnym przed UODO oraz zwrot kar administracyjnych nakładanych na Spółkę w przypadku naruszenia RODO.
- Koszty obrony oraz zasądzone odszkodowania z tytułu odpowiedzialności cywilnej za wyciek lub utratę danych.
- Koszty zarządzania kryzysowego, takie jak np. koszty informatyki śledczej, koszty notyfikacji, koszty obrony dobrego imienia (PR).

KOGO I CO CHRONI UBEZPIECZENIE CYBER?

- Spółka lub inny podmiot.
- Członkowie władz spółki, dyrektorzy, kierownicy.
- Spadkobiercy i współmałżonkowie osób wskazanych powyżej, w zakresie w jakim bezpośrednio wobec niej skierowano roszczenie w związku z działaniem, błędem lub zaniechaniem popełnionym przez osobę lub przez podmiot wskazany powyżej.

PRZYKŁADY, KIEDY PRZYDAJE SIĘ **UBEZPIECZENIE CYBER**

#1 CYBER WYMUSZENIE

Dyrektor generalny organizacji telekomunikacyjnej otrzymuje wiadomość e-mail z żądaniem okupu w wysokości 500 000 EUR w bitcoinach w ciągu 24 godzin. W przeciwnym razie anonimowi hakerzy ujawnią wrażliwe informacje o Klientach i wyłączą krytyczne systemy biznesowe. Organizacja wynajmuje firmę zewnętrzną, która ustala, że zagrożenie jest realne i że uzyskano dostęp do ponad 50 000 poufnych danych Klientów.

Polisa Cyber pokryła m.in. koszty informatyki śledczej, koszty zarządzania kryzysowego/koszty wynajęcia zespołu PR pomagający w opracowaniu i strategii medialnej i kontroli narracji publicznej związanej z naruszeniem; monitoring kredytowy i koszty call center w celu odpowiedzi na zapytania od zaniepokojonych klientów; koszty obrony w postępowaniu administracyjnym.

#2 NARUSZENIE PRYWATNOŚCI

Atak typu spear phishing na pocztę elektroniczną pracowników pozwolił hakerom włamać się do systemów. W ten sposób uzyskali dostęp do danych uwierzytelniających logowanie oraz poufnych informacji handlowych dużej organizacji handlu detalicznego, w tym danych osobowych Klientów. Rekordy są sprzedawane w Dark Web, a szczegóły naruszenia zostają upublicznione. Klienci rozpoczynają postępowanie przeciwko organizacji.

Polisa Cyber pokryła m. in. koszty informatyki śledczej, koszty zarządzania kryzysowego/koszty PR, koszty notyfikacji Klientów oraz koszty obrony w postępowaniu administracyjnym.

#3 ZAKŁÓCENIE DZIAŁALNOŚCI SYSTEMU INFORMATYCZNEGO

Atak przeprowadza niezadowolony pracownik z wysokimi uprawnieniami i wiedzą na temat systemów informatycznych firmy produkcyjnej. Nadużywając swojej pozycji w organizacji, manipuluje danymi i pozoruje odmowę usług. Po uzyskaniu dostępu do systemów firmowych, pracownik metodycznie zmienia dane wejściowe, wpływając na funkcjonowanie linii produkcyjnej i skład wszystkich wytwarzanych towarów.

Polisa Cyber pokryła m. in. koszty informatyki śledczej oraz utracony w wyniku przestoju produkcyjnego zysk.

ZADBAJ O CYBERBEZPIECZENSTWO **I SKONTAKTUJ SIĘ Z NAMI**

Zespół Financial Lines STBU
e-mail: fl@stbu.pl