Biuro Financial & Specialty Lines Grupy MAK

Ubezpieczenie Cyber

Ubezpieczenie Cyber mylnie kojarzone jest jako produkt związany wyłącznie z odpowiedzialnością za naruszenie prywatności. Pamiętajmy, że **wyciek danych osobowych nie jest jedynym ryzykiem**, 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.

Warto również mieć na uwadze, że w związku z implementacją Dyrektywy NIS2, poszerzy się 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?**

W ramach jednaj polisy, możesz zadbać aż o trzy obszary ważne dla Twojej organizacji:

Straty własne, w tym:

- utracony zysk oraz dodatkowe koszty działalności wynikające z zakłóceń w działaniu systemów informatycznych,
- koszty informatyki śledczej, koszty obrony dobrego imienia (PR),
- koszty wymuszeń.

Odpowiedzialność administracyjną, w tym:

- koszty obrony w postępowaniu administracyjnym przed UODO,
- zwrot kar administracyjnych nakładanych na Spółkę w przypadku naruszenia RODO, NIS1/2, DORA.

Odpowiedzialność cywilną względem osób trzecich:

- odszkodowania zasądzone w związku z wyciekiem lub utratą danych,
- koszty obrony.

Dobrze skonstruowana polisa Cyber to nie tylko umowa ubezpieczenia, ale także **realny dostęp do usług prewencyjnych.** To codzienne wsparcie dla Pracowników w ochronie przed cyberzagrożeniami – od edukacji po praktyczne narzędzia zwiększające bezpieczeństwo.

Kogo chroni **ubezpieczenie cyber?**

spółkę lub inny podmiot

pracowników

członków władz spółki

spadkobierców, współmałżonków osób wskazanych powyżej, w zakresie w jakim bezpośrednio wobec nich skierowano roszczenie w związku z działaniem, błędem lub zaniechaniem popełnionym przez osobę lub podmiot wskazany powyżej

Kiedy przydaje się **ubezpieczenie cyber?**

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 pomagającego w opracowaniu 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.

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.

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.

Jakie są **wymogi ubezpieczycieli?**

- **MFA dla zdalnego połączenia z siecią** (np. poprzez vpn)
- **MFA dla poczty email** odseparowane max cotygodniowe backupy (offsite, a najlepiej offline)
- **antywirus i firewall** regularnie updateowany (najlepiej żeby był też EDR)
- **rozsądna polityka** dotycząca praw administratora
- **separacja IT/OT** (jeżeli występuje OT)

Kontakt

Agata Żbikowska
Dyrektor Biura Financial & Specialty Lines Grupy MAK

agata.zbikowska@makubezpieczenia.pl

GRUPA MAK