

## Ubezpieczenie ryzyk cybernetycznych

Każda Firma duża, średnia czy mała narażona jest na atak cybernetyczny, ale nie każda Firma jest w stanie udźwignąć finansowo skutki tego ataku.

Naszym zdaniem Ubezpieczeni powinno pokrywać skutki finansowe ataku - cyber ataku na systemy informatyczne ubezpieczającego niezależnie od daty wykonania pierwotnego ataku.

Powinno obejmować ochroną ubezpieczeniową Ubezpieczonego na wypadek włamania do jej systemu komputerowego, ataku hakerskiego, wycieku danych, zainstalowania złośliwego oprogramowania w sytuacji niewystarczającego zabezpieczenia systemu komputerowego, ochronę ubezpieczeniową na wypadek działalności przestępczej lub zwykłego zaniedbania ze strony pracowników Ubezpieczonego, pokrycie kosztów wyspecjalizowanych firm w informatyce śledczej, kancelarii prawnych oraz ekspertów ds. public relations w celu zminimalizowania negatywnego wpływu na wizerunek Ubezpieczonego.

Powinno ono również obejmować swoją odpowiedzialnością szkody wyrządzone osobom trzecim, gdy jesteśmy ( sprzęt Firmy ) jest wykorzystany do rozprzestrzeniania cyber ataku.

Wyróżniamy na rynku oferowaną konstrukcję umów opartą na doborze klauzul włączających i regulujących zakres ubezpieczenia budując w ten sposób modułami zakres ochrony. Stosowane są również warunki określające zakresy świadczeń, do których podstawiamy oprócz arkusza oceny ryzyka (wniosku) sumy odpowiedzialności, do których odpowiedzialność jest ustalana wg pogrupowanych sekcji.

Przykładowy zakres może obejmować zdarzenia:

Sekcja I: dane elektroniczne

1. koszty przywrócenia danych
2. koszty zakupu nowego oprogramowania
3. koszty odtworzenia danych
4. koszty usunięcia złośliwego oprogramowania

5. koszty przywrócenia dostępu do danych

Sekcja II: koszty dodatkowe m.in.:

1. koszty public relations w celu przywrócenia reputacji/wizerunku publicznego
2. koszty przeniesienia nie utraconych danych na inne serwery
3. koszty porady prawnej
4. koszty ograniczenia skutków utraty danych
5. utrata zysku w wyniku zakłócenia działania jakiegokolwiek sieci na skutek ataku
6. koszty obrony prawnej i odszkodowanie w przypadku utraty danych osobowych, ujawnienia informacji handlowej, korzystania z usług podwykonawców i bezpieczeństwa sieci,
7. kwoty odpowiadające wysokości kar administracyjnych za naruszenie danych (sankcje z tytułu naruszenia prawa ochrony danych),
8. honoraria z tytułu świadczenia usług prawnych oraz reprezentowania Ubezpieczonego przed organami władzy państwowej w związku z postępowaniem prowadzonym przez organ nadzoru,
9. honoraria z tytułu świadczenia przez specjalistów usług w zakresie informatyki śledczej,
10. honoraria z tytułu świadczenia usług przez niezależnych doradców, których celem jest ochrona reputacji spółki i osób fizycznych,
11. honoraria związane z zawiadomieniem osoby, której dotyczą dane,
12. honoraria związane z odzyskaniem danych elektronicznych, opcjonalnie do zakresu ochrony ubezpieczeniowej włączone mogą zostać:
13. działalność multimedialna, pokrycie szkód i kosztów obrony prawnej poniesionej wskutek naruszenia praw ochrony własności intelektualnej osoby trzeciej, w związku z treściami przekazywanymi za pośrednictwem mediów cyfrowych
14. próby wymuszenia, pokrycie kosztów niezależnych doradców, w celu ustalenia okoliczności szantażu, jak również kwoty okupu na rzecz osoby trzeciej grożącej ujawnieniem poufnych informacji bezprawnie uzyskanych z baz danych Ubezpieczonego
15. inne koszty nie wymienione wyżej

Sekcja III: odpowiedzialność cywilna

1. koszty odtworzenia danych u poszkodowanych (osób trzecich)

2. koszty przywrócenia danych u poszkodowanych (osób trzecich)
3. koszty przywrócenia systemu u poszkodowanych (osób trzecich)
4. koszty działania specjalistów z zakresu informatyki śledczej poniesione na poszukiwanie sprawcy ataku komputerowego
5. koszty postępowań i kar administracyjnych związanych z ochroną danych osobowych (GIODO) oraz ochroną prawa własności intelektualnej (Urząd Patentowy)
6. utracone korzyści poniesione przez osoby trzecie powstałe wskutek uszkodzenia, utraty danych lub powstałych w wyniku wycieku danych personalnych osób trzecich
7. inne koszty nie wymienione wyżej związane z zdarzeniem ubezpieczeniowym

Pytanie najczęściej zadawane przez Naszych klientów: ile kosztuje ubezpieczenie cyber ?

Odpowiedź na to pytanie możesz uzyskać po ustaleniu zakresu oczekiwanej ochrony, specyfiki branży w której działa Firma, sposobu i rodzaju stosowanych rozwiązań, zabezpieczeń informatycznych oraz innych czynników wpływających na ocenę ryzyka.

Broker Ubezpieczeniowy

www.abi.pl