COLONNADE
A FAIRFAX COMPANY

TÁJÉKOZTATÓ

Cyber károk fedezetére vonatkozó kiterjesztés vagyonbiztosításokhoz

Legújabb Cyber kiterjesztésünkkel a vagyonbiztosítással rendelkező ügyfeleink részére kínálunk biztosítási megoldást a leggyakrabban előforduló, cyber támadás által előidézett károkra:

HÁLÓZATKIESÉS

Cyber támadás miatt bekövetkező üzemszünet során elszenvedett bevételkiesésre vonatkozó fedezet,

- *Például egy támadás miatt a termelést vezérlő számítógépek hozzáférhetetlenné válnak, és a termelés leáll.*

ADATHELYREÁLLÍTÁS

Egy cyber támadás során elveszett adatok biztonsági mentésből történő helyreállítását fedezi.

- *Például a biztosított által kezelt adatok egy része megsemmisül.*

"BRICKING"

Elektronikus eszközök működésképtelenné válására vonatkozó fedezet.

- *A biztosított belső hálózatára kapcsolt elektronikus eszközei egy cyber támadás következtében működésképtelenné válhatnak anélkül, hogy rajtuk fizikai sérülés keletkezne. Például egy külső hálózati behatolás során a biztosított egyik számítógépének operációs rendszerét olyan módon befolyásolják, hogy a számítógép használhatatlanná válik.*

ZSAROLÁS

Cyber támadással megvalósított zsarolás fedezete – a követelt pénzösszegre és/vagy a szakértői költségekre vonatkozó fedezet.

- *A biztosított által kezelt adatok egy részét illetéktelenek hozzáférhetetlenné teszik, és a zsarolók a hozzáférést bizonyos pénzösszeg megfizetésétől teszik függővé.*

IT SZAKÉRTŐI DÍJ

A Cyber támadással kapcsolatban igénybe vett informatikai szakértők díja.

- *A cyber támadással kapcsolatos körülmények vizsgálatának és a további támadások kiküszöbölésének érdekében tett szakértői intézkedések költsége.*

MINIMUMKÖVETELMÉNYEK:

A Cyber kiterjesztés könnyű hozzáférhetőségét kívánjuk biztosítani azzal, hogy annak megkötéséhez nincs szükség előzetes kérdőív kitöltésére, és az ügyfeleknek a teljes Cyber fedezethez képest lényegesen alacsonyabb technikai elvárásoknak kell megfelelniük.

- ✓ Rendelkezzenek biztonsági mentésekkel
- ✓ Megfelelő vírusvédelem és tűzfalak használata
- ✓ Fehasználónévvel és jelszóval védett hálózati hozzáférési pontok
- ✓ Kizárólag a fejlesztők által támogatott szoftverek használata

KIKNEK KÍNÁLJUK?

Azoknak a jelenlegi és leendő, vagyonbiztosítással rendelkező ügyfeleinknek kínáljuk, akik:

- **árbevétele az 5 milliárd forintot nem haladja meg;**
- **még nem rendelkeznek meglévő Cyber vagy GDPR biztosítással.**

LIMITOPCIÓK:

- 10.000.000 Ft (önrész: 100.000 Ft)
- 25.000.000 Ft (önrész: 200.000 Ft)
- 50.000.000 Ft (önrész: 300.000 Ft)

A „Bricking” fedezetet 5.000.000 Ft szublimittel kínáljuk.
A biztosítás díja az ügyfél árbevételétől, tevékenységétől és az igényelt limitopciótól függően hozzávetőlegesen 50.000 és 300.000 forint között mozog.

A kiterjesztés minden esetben csak a meglévő (vagy azzal egyidejűleg megkötött) vagyonbiztosítással együtt értelmezhető: a kiterjesztés feltétele a vagyonbiztosítás szerződési feltételéhez kapcsolódik, a termék illeszkedik a vagyonbiztosításban meghatározott biztosítási időszakhoz, illetve osztja a vagyonbiztosítás sorsát.

MEGTÖRTÉNT ESETEK

Mikor lehet hasznos egy cyber támadásokra kiterjedő biztosítás?

1 Hálózatkiesés fedezet

Egy termelőüzem számítógépes rendszerébe történő illetéktelen behatolás következtében a vállalatnak le kellett állítania gyártósorait, amíg a biztonsági hibát el nem hárítják. Az érintett adatok felmérése és elkülönítése, valamint a biztonsági hiba azonosítása 3 napot vett igénybe. Az üzemleállás több mint 48 millió forintos bevételkiesést okozott a társaságnak.

2 Adathelyreállítás fedezet

Egy cég alkalmazottja adathalász e-mailben szereplő linkre kattintva egy hamisított bejelentkezési oldalon megadta a társaság belső rendszereibe történő hozzáféréshez megkövetelt felhasználónevet és jelszót. A bejelentkezési adatok birtokában külső támadók bizalmas adatokat távolítottak el a társaság számítógépes rendszereiből. Az adatoknak az elkülönített szerveren található biztonsági másolatokból történő visszaállítása, azoknak a társasági rendszerekbe történő visszaintegrálása több mint 15 millió forintos IT szakértői költséget jelentett a társaságnak.

3 Zsarolás fedezet

Egy társaság zsarolóvírus áldozata lett, amely a vállalat hálózati rendszerein belül terjedt, ezzel számos személyi számítógépet és szervert megfertőzve. A vírus következtében a társaság működése szempontjából kulcsfontosságú adatok és rendszerek váltak hozzáférhetetlenné. A zsaroló 30 millió forintnak megfelelő összegű bitcoin megfizetésétől tette függővé az adatok újbóli hozzáférhetővé tételét.

4 "Bricking" fedezet

Egy külső hálózati behatolás során egy támadó hozzáfért egy társaság belső hálózatait használó számítógépekhez és gyártó berendezésekhez, és azok operációs rendszerének kerneljét olyan mértékben módosította, hogy a gépek processzora, memóriája, és azok fájlrendszere hozzáférhetetlenné, a gépek pedig használhatatlanná váltak. A gépek pótlásának költségei meghaladták a 4 millió forintot

BŐVEBB INFORMÁCIÓ:

vagyon@colonnade.hu