COLONNADE
A FAIRFAX COMPANY

Ismerje meg
"VIRTUÁLIS VÉDŐHÁLÓ"
CYBER ÉS ADATVÉDELMI
felelősségbiztosításunkat!

A karanténhelyzet mind a vállalatokat, mind a munkavállalókat számos kihívás elé állítja. Azon cégek, amelyek a munkavégzést otthoni környezetbe tudták helyezni, szembesültek azzal az IT feladattal, hogy a munkatársak rendelkezésére bocsátott eszközök és a cég személyes és üzleti adatai megfelelő biztonságban helyezzék. Sok helyen korábban is rendszer volt a részleges otthoni munkavégzés, de a teljes cég távoli működésének biztosítása más szabályozást igényel. Vajon megfelelőek-e a biztonsági intézkedések a kiadott laptopoknál? Felkészítették-e a dolgozókat arra, hogyan őrizzék meg a céges adatvagyon sérthetetlenséget?

A távoli munkavégzéshez összeállítottunk néhány jótanácsot.

A legnagyobb felkészülés ellenére sem érezhetjük magunkat 100 %-os biztonságban, hiszen a kényszerű home office-ban a céges hálózatnak, eszközöknek és felhasználóiknak a korábbinál kevésbé védett környezetben kell kezelniük a potenciálisan érzékeny vállalati adatokat. Számos vállalatirányítási programot, online platformot használunk, e-mailezünk, bízunk a felhőtechnológiában. A Nemzeti Kibervédelmi Intézet (NKI) figyelmeztetést adott ki arról, hogy február óta itthon is megnövekedett az adathalász és az álhírterjesztő tevékenység. A céges rendszerek a home office üzemmódban még a szokásosnál is sebezhetőbbek. A hackertámadások, adatlopások száma folyamatosan nő, célpont lehet bármely cég tevékenységtől, mérettől, felkészültségtől függetlenül. A vállalt szerződéses kötelezettségeket azonban a járvány ellenére is teljesíteni kell. A körültekintő felkészülés ellenére is történhetnek adatvédelmi incidensek és az emberi hibázás lehetősége mindig megmarad. Egy hibának komoly anyagi következményei lehetnek, a pénzügyi kockázatok pedig biztosíthatók.

A kialakult helyzetre 8 pontos biztosítási védelmi csomagot alakítottunk ki, amellyel csökkenthetők a pénzügyi ráfordítások. Az egyszerű eljárással köthető biztosításunkkal a „home office" üzemmódból fakadó, fokozott kockázatnövekedésre gondoltunk. Szélesebb körben, elérhető díjon juthatnak alapfedezetekhez ügyfeleink, és védelmet nyújtunk a későbbi, normál üzleti környezetben is.

MILYEN ESETEKBEN NYÚJTUNK BIZTOSÍTÁSI VÉDELMET?

Néhány példa a teljesség igénye nélkül:

1. SZEMÉLYES ADATOK VÉDELME

Még mindig GDPR... Téves e-mail, eltévedt csatolmányok, ellopott eszközök, stb.

2. VÁLLALATI ADATOK VÉDELME

Az üzleti adat érték!

3. HÁLÓZATBIZTONSÁG

Szoftver, kód vagy vírus a tárolt szoftverekben és adatokban sérülést okoz, vagy azok működését megakadályozza.

4. PROAKTÍV SZAKÉRTŐI SZOLGÁLTATÁSOK

Feltételezett adatszivárgás. A fenyegetettség miatt meg kell bizonyosodni arról, hogy a cég információi, adatbázisai nem kerültek illetéktelen kezekbe.

5. A TÁRSASÁG JÓ HÍRNEVÉNEK VÉDELME

Az adatsértés azonnali beavatkozást igényel, az óra ketyeg, a cégbe vetett bizalom megrendülhet, partnerek, üzletfelek pártolhatnak el.

6. ADATALANYOK ÉRTESÍTÉSE

Az illetéktelen kezekbe került információval rosszhiszemű visszaélés történhet, személyiségi jogsértést eredményezhet.

7. ELEKTRONIKUS ADATOK HELYREÁLLÍTÁSA

A biztonsági mentés és az elveszett adatok visszaállítása komoly ráfordítást vagy erőforrás mozgósítást igényel.

8. ADATKEZELÉSSEL KAPCSOLATOS BÍRSÁGOK

Bejelentés, incidens nyomán az adatvédelmi hatóság a lefolytatott vizsgálat során jogsértésre hivatkozva bírságot szabhat ki.

MILYEN SZOLGÁLTATÁSRA SZÁMÍTHAT?

A személyes adatsérelem visszaélésekhez vezethet, esetlegesen **kártérítési kötelezettséget** jelenthet. Magánszemélyek és vállalatok polgári pert is indíthatnak tényleges veszteségük, természetes személyek személyiségi jogsérelem címen is érvényesíthetik jogaikat.
Bizonyított személyes hátrány kompenzálására **sérelmi díj** megfizetésére is kötelezhető a cég. Egy szerencsétlen eset a cég reputációját hosszú időre visszavetheti, lényeges, hogy **PR szakértő** segítse a megfelelő kommunikációt ilyenkor. Az adatszivárgás kezelésének költségei magasak, a biztosító által felkért **IT biztonsági és adatvédelmi szakértő, szakjogász** hatékonyan tud megfelelő intézkedéseket javasolni a cégnek.
A feltételezett jogsértésnek utána kell járni, az esetleges hatósági eljárás során bírságot is kiszabhatnak.
"VIRTUÁLIS VÉDŐHÁLÓ" Cyber és adatvédelmi biztosításunkkal csökkenthetők az incidensek által okozott veszteségek.

KIS MULASZTÁSSAL NAGY KÁROK KELETKEZHETNEK, KIS RÁFORDÍTÁSSAL NAGY VESZTESÉGEK KOMPENZÁLHATÓK!

FONTOS TUDNIVALÓK:
Ezt a biztosítást azon cégek számára kínáljuk, amelyek a lehető legtöbbet tettek már az IT biztonság terén. A kulcspontokon végigvezetjük Önt, elvárt felkészülésként, **a tényleges állapotról nyilatkozni is kell szerződéskötéskor**. Az ajánlaton ezek a „GDPR megfelelés" kérdéssor mellett az I. „Alapfeltételek" felsorolásban szerepelnek. A különösen érzékeny adatok kezelőivel ezzel a típusú egyszerűsített eljárással nem tudunk szerződni, de egyedi kockázatfelméréssel rendelkezésükre állunk. Már folyamatban levő ügyekre nem lehet biztosítást kötni, a korábbi esetekről információt kérünk. Ez a termék egy cégre köthető, nem vonhatók be a kiszervezett tevékenységet végző alvállalkozók, illetve anya, társ,- és leányvállalatok. Az egyszerűsített ajánlaton szereplő kártérítési mértéken felül is tudunk védelmet nyújtani, továbbra is értékesítjük a bővebb fedezeteket tartalmazó „GDPR" és „Cyber" adatvédelmi termékeinket.

LÁTOGASSON EL WEBOLDALUNKRA, VAGY KÉRJE BIZTOSÍTÁSKÖZVETÍTŐ SEGÍTSÉGÉT!

www.gdpr-biztositas.hu

Tájékoztatónk általános jellegű, nem minősül ajánlattételnek és nem helyettesíti a biztosítási feltételeket.

COLONNADE
A FAIRFAX COMPANY