

Kiberbiztonság a cégvezetők szemszögéből

Ahogy vállalkozásunkat folyamatosan fejlesztjük és növeljük, egyre fontosabbá válik a kiberbiztonság. De miért? Van egyáltalán bármilyen jelentősége az üzleti siker szempontjából? Nos, a válasz egyszerű. A kiberbiztonság minden vállalkozás alapvető elemévé kellene, hogy váljon, függetlenül a méretétől vagy az iparágától. Miért pont a cégvezetőknek kellene ezzel foglalkozniuk? Konkrétan nem biztos, hogy a cégvezető feladata, az alábbiakban viszont megfogalmaztam öt érvet, ami a döntéshozók bevonása nélkül megvalósíthatatlan, ezért tartom nagyon fontosnak a cégvezetés képzését és tájékoztatását a kiberbiztonság területén.

Üzleti hírnév megőrzése: Ügyfeleink és partnereink megbíznak bennünk. Nagyon fontos, hogy megőrizzük ezt a bizalmat. Egy sikeres kibertámadás nemcsak az adatvédelmet fenyegeti, hanem a hírnevünket is, ráadásul az üzleti partnereinknek is kellemetlenséget okozhatunk.

Pénzügyi károk minimalizálása: A kibertámadásoknak jelentős pénzügyi következményei lehetnek, például jogi követelések vagy helyreállítási költségek. A megfelelő kiberbiztonsági intézkedések segíthetnek minimalizálni ezeket a károkat.

Jogszabályoknak való megfelelés: Számos jogszabály vonatkozik az adatvédelemre és a kiberbiztonságra, amelyeket be kell tartani. Ha nem teszünk eleget ezeknek a követelményeknek, akkor jogi problémák és büntetések várhatók.

Üzleti folytonosság biztosítása: A kibertámadások jelentős zavart okozhatnak a vállalat működésében. Fontos, hogy megfelelő védelmi intézkedéseket hozzunk annak érdekében, hogy üzleti folytonosságunkat megőrizzük.

Versenylőny megtartása: A megfelelő kiberbiztonsági intézkedések bevezetése lehetőséget nyújthat a versenylőny megszerzésére a piacon. Ügyfeleink és partnereink egyre inkább elvárják a magas szintű adatvédelmet és kiberbiztonságot.

A fentiekből egyértelműen látszik, hogy ez nem egy egyszeri feladat, ezért az EU is foglalkozik a témával. 2024-ben Magyarországon is elindul az úgynevezett NIS2 (Network and Information Security Directive 2), ami a tagállamokat az információs és hálózatbiztonság megerősítésére kötelezi. Ez a gyakorlatban azt jelenti, hogy minden magyarországi szolgáltatónak, szervezetnek és vállalatnak önellenőrzést kell tartani, hogy érintett-e a NIS2 –ben, illetve ha igen akkor 2024.06.30-ig nyilvántartásba kell kerülnie a cégnek, amit a cégkapun keresztül tehetünk meg. (23/2023. (XII. 19.) SZTFH rendelet az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról)

Fontos, hogy akkor is van feladatunk, ha nem vagyunk érintettek közvetlenül a NIS2-ben! Amennyiben beszállítója vagy bármilyen üzleti kapcsolatban vagyunk egy NIS2-ben nyilvántartott céggel, akkor nekünk is közvetett feladatunk lesznek. Az érintett szervezet a Kibertantv. 19. §(5) bekezdése szerint szerződésben fogja rögzíteni, hogy a közreműködőnek meg kell felelnie a biztonsági céloknak (egészen pontosan 19. §(1)-(3)ra vonatkozni).

Az alábbiakban felsorolok pár intézkedést, amit egy kisvállalkozásnak is meg kell fontolnia.

Tudatosság növelése: Fontos, hogy a kisvállalkozások megértsék az NIS2 követelményeit és hogyan érintik azok őket. Ez magában foglalhatja az irányelv áttekintését és az esetleges változtatások hatásainak elemzését a vállalkozásra.

Rizikóelemzés: A kisvállalkozásoknak érdemes felmérniük az információs és hálózatbiztonságot érintő lehetséges kockázatokat és sebezhetőségeket. Ezek alapján ki kell dolgozniuk egy megfelelő védelmi stratégiát. (Itt jegyzem meg, hogy már a GDPR irányelvek bevezetésénél is kellett volna foglalkozni az IT biztonsággal!)

Biztonsági intézkedések bevezetése: A vállalkozásnak meg kell fontolnia biztonsági intézkedések bevezetését, mint például tűzfalak, vírusirtó szoftverek, biztonsági mentések és a hálózati védelem.

Alkalmazottak képzése: Nagyon fontos, hogy a vállalkozás alkalmazottai tisztában legyenek az információs biztonsági elvekkel és legyenek képesek azokat betartani a mindennapi munkájuk során.

Együttműködés más szervezetekkel: Ha lehetséges, érdemes együttműködni más vállalkozásokkal vagy szakértőkkel, hogy megosszák az információt és a legjobb gyakorlatokat átvegyük az információs biztonság terén.

Most már egyértelműen látszik, hogy a cégvezetőknek és a cégvezetésnek fontos szerepe van abban, hogy megértsék és prioritásként kezeljék ezt a kérdést vállalkozásukban. A megfelelő intézkedések meghozatalával nemcsak ügyfeleinket és partnereinket védjük meg, hanem vállalkozásunk hosszú távú stabilitását is biztosítjuk.

Hajdara Gábor