Sajtóközlemény
2019. április 30.

A kiberkockázatok nagyobb veszélyt jelentenek, mint a katasztrófák

Az egyre gyakoribb adatvédelmi támadások minden vállalkozás számára komoly üzleti kockázatot jelentek. A nagyvállalatok túlnyomó része felkészült az új típusú biztonsági kockázatokra, de vajon milyen lehetőségeik vannak a mikro-, kis- és középvállalkozásoknak arra, hogy megvédjék informatikai rendszereiket és biztosítsák az adatbiztonságot egy esetleges hacker támadás esetén?

Nagyobb kárt okoznak a kibertámadások, mint a természeti katasztrófák

Az Allianz év elején publikált kockázati barométere szerint súlyos adatvédelmi incidensek, jelentős kibertámadások miatt bekövetkező hálózatkiesések, valamint megszigorított adatvédelmi előírások állítják újabb kihívás elé a vállalatokat. Becslések szerint a kiber**bűncselekmények** ma már évi 600 milliárd dolláros kárt okoznak globálisan, míg 2014-ben ez évi 445 milliárd dollár volt[1]. Ez háromszor annyi, mint a természeti katasztrófák által okozott kár (10 éves átlagban 208 milliárd dollár)[2]. Ennek oka egyrészről az, hogy a bűnözők egyre innovatívabb módszereket vetnek be az adatlopásra, csalásokra és zsarolásra, illetve nő az országok és a hozzájuk köthető hackercsoportok által jelentett kiberveszély.

Egyre kifinomultabb módszerekkel támadnak a hackerek

A hackerek leggyakrabban a kritikus infrastrukturális szolgáltatókat célozzák meg, értékes adatokat és üzleti titkokat tulajdonítanak el a vállalatoktól. Az is egyre jellemzőbb, hogy a kiberbiztonsági események nyomán peres ügyekre – így értékpapírokkal kapcsolatos és fogyasztói csoportperekre kerül sor. Az adatvédelmi incidensek és az informatikai leállások emellett súlyos felelősségbiztosítási következményekkel is járhatnak, ha az érintett adatalany kártérítést követel a vállalattól.

Adatvédelmi incidensek

A GDPR az EU adatvédelmi rendelete 2018. május 25-től jelentősen megváltoztatta az adatkezelési szabályokat Magyarországon is. Az új rendelet egységes adatkezelési szabályozást határozott meg az unió területére, és ezzel együtt a vállalatok és szervezetek felelőssége, valamint az adatvédelemmel kapcsolatos üzleti kockázatok is megnőttek. A rendelkezés magas bírságokkal kényszeríti ki a biztonságos adatkezelést és sok más mellett olyan esetet is szabályoz, amikor például egy hackertámadás következtében személyes adatok kikerülnek az adatkezelő rendszeréből, vagy ha egy rendszerhiba miatt azok megsemmisülnek. A szabályozás szerint adatvédelmi incidensnek minősül minden olyan esemény, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Ennek értelmében a személyes adatokat tartalmazó

[1] Center for Strategic and International Studies, Economic Impact of Cybercrime – No Slowing Down (Stratégiai és Nemzetközi Tanulmányok Központ: A kiberbűnözés hatása – nincs megállás)

[2] Swiss Re, Preliminary sigma estimates for 2018 (Előzetes valószínűségi becslések a 2018-as évre)

laptop, vagy telefon elvesztése, vagy akár a téves címre küldött email is adatvédelmi kockázatot rejt.

Statisztikák

Az Európai Bizottság hivatalos statisztikái szerint a GDPR hatálybalépésétől, 2018. május 25-től 2019. január végéig terjedő időszakban 41 502 adatkezeléssel kapcsolatos incidenst jelentettek az Európai Unióban a különböző adatkezelő szervezetek, vállalkozások, és eddig egyelőre 91 esetben szabtak ki bírságot az illetékes hatóságok. A legtöbb esetet Hollandiában, Németországban és az Egyesült Királyságban regisztrálták (12 600, 15 400 és 10 600).

Magyarországon az incidens bejelentésekből 2018. május 25-től mintegy 200 érkezett a NAIH-hoz, ezek harmada téves címre küldött küldemény miatt érkezett be, 10 százaléknál jogellenesen tettek közzé valamit, hasonló arányban volt, hogy valaki jogellenesen ismert meg adatokat, de 3 százalékban különböző adathordozók elveszítése miatt is a hatósághoz fordultak. A NAIH elnöke szerint ebből is látszik, hogy az adatvédelmi incidensek legtöbbször emberi mulasztásra vezethetőek vissza, például amikor valaki véletlenül rányom a mindenkinek elküld gombra a levelezésében.

Digitális üzleti és adatvédelmi biztosítás

Az Allianz Cégmester vállalkozásbiztosítás, egy komplex biztosítási csomag, amely a leggyakoribb kockázatokra való vagyon és felelősségbiztosítások mellett a kiberkockázatokra, az adatvédelmi incidensekkel, adatlopással kapcsolatban felmerülő károkra és bírságokra is fedezetet kínál. Az Allianz Cégmester vállalkozásbiztosítás gyorsan és egyszerűen, akár online is megkötheto és rugalmasan alakítható fedezeteket tartalmaz az olyan kisvállalkozások számára is, amelyek telephelyi összvagyonának biztosítási összege maximum 100 millió Ft, éves bruttó árbevétele maximum 400 millió Ft, és maximum 10 főt foglalkoztatnak.

További információ:

Zsámboki Olivia
Marketing és kommunikációs osztály
Allianz Hungária Zrt.
Tel.: +36-1-451-9205
Mob.: +36 30 974 5117
1087 Budapest Könyves K. krt. 48-52.
e-mail: olivia.zsamboki@allianz.hu

Keszthelyi Lívia
Marketing és kommunikációs osztály
Allianz Hungária Zrt.
1087 Budapest Könyves K. krt. 48-52.
Tel.: +36-1-451- 6273
Mob.: +36 30 843 7889
e-mail: livia.keszthelyi@allianz.hu