Your World First

Hackertámadás az ünnepekre – az adatvédelmi incidensek kezelésének legújabb gyakorlata

Dr. Necz Dániel LL.M.

Adatbiztonság – teljes védelem?

- Adatkezelőre és adatfeldolgozóra is vonatkozik

- Fogalma nem meghatározott, csak **példálózó felsorolást** ad a GDPR a megfelelő szervezési és technikai intézkedésekre

Adatbiztonsági intézkedések fajtái

Kockázatértékelés – módszertana alapjául szolgálhat az ISO 27000, ide tartozhatnak továbbá penetrációs tesztek, sérülékenységi vizsgálatok, etikus hacker vizsgálatok

Személyzettel kapcsolatos intézkedések (például: tréning, e-learning)

Fizikai biztonság biztosítása (például: beléptetőrendszer, clean-desk policy)

Menedzsment és szervezeti intézkedések (például: döntéshozatal szabályozása)

IT biztonság biztosítása a szervezet sajátosságai szerint (például: IP log management, IT és kommunikációs rendszer megfigyelése – munkavállalók jogainak betartásával!)

Incidenskezelés – az adatbiztonsági stratégia szerves része

Adatvédelmi incidens: „*a biztonság olyan sérülése, 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*”

Az incidenskezelési stratégia az adatvédelmi incidensek megakadályozását, kezelését célozza

Idetartozik különösen:

Incidenskezelési „task force” kijelölése, feladatainak megszervezése

Incidens kezelési szabályzat és a munkavállalók erről való felvilágosítása

A meglévő intézkedések felülvizsgálata, a biztonsági rések „befoltozása”

GDPR - Adatbiztonság

Incidens kezelési szabályzat

- Döntéshozatali eljárásrend meghatározása
- Jelentési eljárásrend meghatározása, jelentési kötelezettségek előírása
- Incidens kezelési feladatok meghatározása
- Szakértő bevonás esetkörei és szabályai
- Incidens nyilvántartás vezetés szabályai
- Kommunikációs levél minták elkészítése
- Incidens észlelés eszközrendszerének meghatározása
- Felelősségek meghatározása

Rosszindulatú támadások kezelése

- Hackertámadás, zsarolóvírus, adatszivárgás = adatvédelmi incidens
- Ha valószínűsíthetően kockázattal jár az érintettekre, jelenteni kell az adatvédelmi hatóságnak
- Ha valószínűsíthetően magas kockázattal jár az érintettekre, az érintetteket is tájékoztatni kell! – kivéve, ha olyan intézkedéseket hoztak, amellyel az adatokat értelmezhetetlenné teszik, a magas kockázatot kiküszöbölték, illetve ha az érintetteket nem lehet egyedileg tájékoztatni (pl. sajtóban, honlapon történő tájékoztatás)
- Egyes szolgáltatók esetén egyéb hatóságokat is értesíteni kell, így
  - Hírközlési szolgáltatók: Nemzeti Média és Hírközlési Hatóság;
  - Online piactér, felhőszolgáltató, keresőszolgáltató: Nemzetbiztonsági Szakszolgálat

Rosszindulatú támadások az adatvédelmi hatóság gyakorlatában I.

Magyar adatvédelmi hatóság – 11.000.000,-Ft. adatvédelmi bírság

Mi történt?	A NAIH szerint…
Egy hacker hozzáfért és közzétette az interneten a szervezet weboldalának sérülékenységeire vonatkozó információkat és a támadáshoz használt parancsot. Az adatbázis több mint 6.000 személy adatait tartalmazta. A sérülékenységet a szervezet weboldalát érintő átirányítási hiba okozta. A támadó az általa használt parancsot nyilvánosságra hozta, a parancs segítségével, IT szempontból alacsonyan képzett személyek számára is lehetőség nyílt arra, hogy az adatbázisból adatokat szerezhessenek.	· Az adatbázis és a jelszavak titkosításához használt technológia megfelelő szintű védelmet kell nyújtson a rosszindulatú dekódolási technikákkal szemben. A jelszavak titkosításához használt MD5 algoritmus nem megfelelő. · Az incidens kockázatos akkor is, ha az adatok nem naprakészek vagy teszt adatbázis részei. · Azonosító adatokhoz (pl. név, e-mail, felhasználónév, jelszó) való hozzáférés önmagában is magas kockázat. · Megfelelő jelszó komplexitást validáló algoritmusokat kell használni, amelyek kikényszerítik a megfelelő hosszúságú és speciális karaktert tartalmazó jelszavakat. A NAIH csupa kisbetűből álló jelszót is talált.

Tanulság:	A társaságoknak felül kell vizsgálniuk az adatbiztonsági intézkedéseiket és az adatvédelmi incidenseket kezelő eljárásaikat.

Rosszindulatú támadások az adatvédelmi hatóság gyakorlatában II.

Illetéktelen behatolás a Marriott szállodalánc adatbázisába; 99 millió fontos tervezett bírság

Mi történt?	A brit hatóság válasza…
A Marriott szállodaláncot ért adathalász támadás következtében számos adat szivárgott ki a szállodalánc világszinten kb. 339 millió vendég adatait tartalmazó adatbázisából, melyből kb. 30 millióan az Európai Gazdasági Közösséget alkotó 31 ország valamelyikének területén laknak. A vizsgálat szerint az adatok veszélybe kerülése akkorra vezethető vissza, amikor a Starwood szállodalánc adatbázisait 2014-ben feltörték. 2016-ban a Marriott felvásárolta a Starwoodot, de az ügyfelek adatinak kiszivárgására csak 2018-ban derült fény.	Az ICO vizsgálata alapján a Marriott nem járt el kellő körültekintéssel a Starwood (adatvédelmi) átvilágítása során amikor felvásárolta a szállodaláncot, és informatikai rendszereit sem erősítette meg kellő mértékben.

Tanulság:	A vállalatok felelőssége az általuk kezelt adatok biztonságáért arányban áll az adatkezeléssel érintettek számával, ez pedig az esetlegesen kiszabott bírság összegének megállapítására is hatással van.

Rosszindulatú támadások az adatvédelmi hatóság gyakorlatában III.

Illetéktelen behatolás a British Airways adatbázisába, 500 000 ügyfél személyes adataihoz volt illetékteleneknek hozzáférése; a nem megfelelő biztonsági rendszerek miatt a bírság tervezett összege: 183 390 000 font

Mi történt?	A brit hatóság válasza…
Adathalász támadás érte a British Airways légitársaságot, amely kb. 500.000 ügyfelet érintett. Vizsgálata során a brit adatvédelmi hatóság (ICO) azt találta, hogy a nem megfelelő adatbiztonsági intézkedések miatt olyan adatok szivárogtak ki, mint a bejelentkezési adatok, bankkártya számok, foglalási adatok, nevek és címek.	Bár a British Airways az incidenst követően együttműködött a hatósággal és fejlesztéseket is eszközölt a biztonsági rendszerein, az ICO 183 390 000 font összegű bírságot helyezett kilátásba, amely a légitársaság 2018. évi összbevételének 1,5 %-a. Ez lenne (és vélhetően lesz is) az ICO által adatvédelmi szabályok megsértéséért mindezidáig kiszabott legnagyobb összegű bírság.

Tanulság:	A vállalatok felelőssége az általuk kezelt adatok biztonságáért arányban áll az adatkezeléssel érintettek számával, ez pedig az esetlegesen kiszabott bírság összegének megállapítására is hatással van.

Rosszindulatú támadások az adatvédelmi hatóság gyakorlatában IV.

Nem megfelelő adatbiztonsági intézkedések egy bolgár banknál – nincs támadás, csak annak a lehetősége

Mi történt?	The bolgár adatvédelmi hatóság szerint:
Egy bolgár bank 33 492 ügyfelének személyes adatait hagyta megfelelő védelem nélkül. Az ügyet egy harmadik fél általi bejelentés robbantotta ki, miután jelezte, hogy hozzáfér a bank ügyfeleinek adataihoz. A belső vizsgálat nem derített fényt illetéktelen behatolásokra, és az adatok kiszivárgása is inkább papíralapú adathordozón volt lehetséges, mint elektronikus úton.	A bolgár adatvédelmi hatóság úgy döntött, hogy a bank nem tette meg a megfelelő technikai és szervezési lépéseket annak érdekében, hogy az ügyfelek és harmadik személyek adatait megfelelő védelemben részesítsék, ezért 511 200 eurós bírságot szabott ki.

Tanulság:	Az adatfeldolgozóknak és az adatkezelőknek olyan technikai és szervezeti struktúrát kell kialakítaniuk, valamint ezek hatékonyságát folyamatosan vizsgálniuk, amely alkalmas arra, hogy az általuk kezelt adatoktól függően minimalizálják az azokhoz fűződő kockázatokat, mert ennek elmulasztása esetén még tényleges behatolás nélkül is komoly bírsággal nézhetnek szembe.

Tanulságok

Az adatbiztonsági szint folyamatos garantálása megfelelő adatbiztonsági intézkedésekkel

Nem csak informatikai feladat, emberi hiba kockázata is jelentős (

Megfelelő biztonsági mentési gyakorlat a támadások egyes típusai esetén különösen hasznos lehet (pl. zsarolóvírusok)

Azonnali reagálás, hatékony hatósági együttműködés esetén elkerülhetők a bírságok

Necz Dániel
Ügyvéd

T +36 1 505 4906
E daniel.necz@cms-cmno.com