Adatvédelmi incidens – amikor elindul a 72 óra



Egy rossz címzett, egy elveszett laptop vagy egy feltört postafiók is lehet adatvédelmi incidens. A kérdés nem az, hogy megtörténik-e, hanem az, hogy mikor és a vállalkozás kellően felkészült-e rá.

Valós helyzet – amikor megtörténik

Egy figyelmetlen munkatárs véletlenül rossz címzettnek küld egy érzékeny ügyféllistát, vagy egy zsarolóvírus titkosítja a számítógépeket. Mielőtt legyintenénk rá, hogy ezek kizárólag informatikai problémák, jó ha tudjuk, ha személyes adatok biztonsága is sérül, adatvédelmi incidens is bekövetkezik. Ebbe a kategóriába tartozik az adatok véletlen vagy jogellenes megsemmisülése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés.

Mit tegyünk?

A GDPR 33. cikke alapján az adatkezelőnek az incidenst haladéktalanul, indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával a tudomásszerzést követően be kell jelentenie a felügyeleti hatóságnak, ha az valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Magyarországon a bejelentés a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) felé teljesíthető.

Természetesen a 72 órás időkorlát nem azt jelenti, hogy ennyi idő van kivizsgálni az incidenst, és minden részletre kiterjedően feltárni a körülményeket. A bejelentés szakaszosan is teljesíthető és később kiegészíthető, hiszen sok adat csak később, szakértők bevonásával állapítható meg. Magas kockázat esetén az érintetteket is indokolatlan késedelem nélkül tájékoztatni kell. Minden adatvédelmi incidenst dokumentálni kell akkor is, ha végül nem szükséges a hatóság felé bejelenteni.

Nemzetközi példa – egy hiányzó védelmi intézkedés ára

A brit adatvédelmi hatóság (ICO) 2025. márciusában 3,07 millió font bírságot szabott ki az Advanced Computer Software Group Ltd.-re. A 2022-es zsarolóvírus-támadás során a támadók egy olyan ügyfélfiókon keresztül jutottak be a rendszerbe, amelynél nem alkalmaztak többtényezős hitelesítést (MFA). Az ICO közlése szerint a biztonsági hiányosságok 79 404 ember személyes adatait tették kockára. A történet a kisebb vállalkozások számára is fontos tanulság: a hozzáférés-védelem, a frissítések, a mentések és az incidenskezelési folyamat nem „nagyvállalati luxus”, és ezen a ponton kapcsolódik össze az adatvédelem és az infromációbiztonság.

Mik az első lépések ?

Észlelés és korlátozás: Mindenképpen meg kell állítani a további károkozást, de meg is kell őrizni a vizsgálathoz szükséges bizonyítékokat.

Értékelés: Meg kell határozni, milyen adatokat érint az incidens, hány érintett van és milyen lehetséges következmények lehetnek.

Dokumentálás: Rögzíteni kell a tudomásszerzés időpontját, a körülményeket, a döntéseket és a megtett intézkedéseket.

Bejelentés: Kockázattal járó incidensnél főszabály szerint 72 órán belül bejelentést kell tenni a NAIH felé.

Érintettek és megelőzés: Magas kockázat esetén tájékoztatni kell az érintetteket, majd be kell építeni a tanulságokat a működésbe, szükség szerint oktatást kell tartani.

Az adatvédelmi incidensek túlnyomó része nem rosszindulatú támadás, hanem egyszerű emberi hiba következménye: egy téves címzett, egy elveszett adathordozó vagy egy nem megfelelően kezelt hozzáférési jogosultság is elegendő. Éppen ezért a technikai védelem mellett legalább ilyen fontos a munkatársak megfelelő felkészítése és az egyértelmű belső eljárások kialakítása. Egy jól működő incidenskezelési folyamat segítségével a vállalkozás már az első órákban képes felmérni a helyzet súlyosságát és meghozni a szükséges döntéseket. A gyors és dokumentált reagálás nemcsak a GDPR-kötelezettségek teljesítését segíti, hanem jelentősen csökkentheti az incidensből eredő pénzügyi, működési és reputációs károkat is.

Adatvédelmi önellenőrzés

- ☐ Van írásos incidenskezelési eljárásrend?
- ☐ Kijelölték, ki felel az incidens értékeléséért és a szükséges bejelentésért?
- ☐ A munkatársak tudják, mit kell azonnal jelenteniük és kinek?
- ☐ Ismerik a 72 órás határidőt és a NAIH bejelentési folyamatát?
- ☐ Minden incidenst dokumentálnak, még a be nem jelentendő eseteket is?
- ☐ A fontos felhasználói fiókoknál alkalmaznak többtényezős hitelesítést (MFA)?
- ☐ Rendszeresen készül biztonsági mentés, és ellenőrzik annak visszaállíthatóságát?

Szabó Péter

Források és további információ

NAIH – Adatvédelmi incidensek (GDPR): https://www.naih.hu/adatvedelmi-incidensek-gdpr

NAIH – Adatvédelmi Incidensbejelentő Rendszer: https://naih.hu/adatvedelmi-incidensbejelento-rendszer

EDPB – Data breaches, SME data protection guide: https://www.edpb.europa.eu/sme/assess-the-risks/data-breaches_en

EDPB – Guidelines 9/2022 on personal data breach notification: https://www.edpb.europa.eu/documents/guideline/guidelines-92022-on-personal-data-breach-notification-under-gdpr_en

EDPB – Template for personal data breach notification (2026): https://www.edpb.europa.eu/public-consultations/template-for-personal-data-breach-notification_en

ICO – Advanced Computer Software Group Limited, monetary penalty (2025): https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited