01/2021. számú iránymutatás

Az adatvédelmi incidensek bejelentésével kapcsolatos példákról

Elfogadás időpontja: 2021. december 14.

2.0. változat

Korábbi változatok

2.0. változat	2021. december 14.	Az iránymutatás nyilvános konzultációt követő elfogadása
1.0. változat	2021. január 14.	Az iránymutatás nyilvános konzultációra történő elfogadása

Tartalomjegyzék

AZ EURÓPAI ADATVÉDELMI TESTÜLET

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének e) pontjára,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére[1],

tekintettel eljárási szabályzatának 12. és 22. cikkére,

tekintettel az Európai Parlamentnek és a Tanácsnak címzett, a polgárok szerepe erősítésének és az EU digitális átállással kapcsolatos megközelítésének pillérét képező adatvédelem – az általános adatvédelmi rendelet alkalmazásának két éve című bizottsági közleményre[2],

ELFOGADTA A KÖVETKEZŐ IRÁNYMUTATÁST

1 BEVEZETÉS

1. Az általános adatvédelmi rendelet bizonyos esetekben bevezeti azt a követelményt, hogy az adatvédelmi incidenst be kell jelenteni az illetékes nemzeti felügyeleti hatóságnak (a továbbiakban: felügyeleti hatóság), és az adatvédelmi incidensről tájékoztatni kell az incidens által érintett egyéneket (33. és 34. cikk).

2. A 29. cikk szerinti munkacsoport 2017 októberében már elkészített egy *általános* iránymutatást az adatvédelmi incidensek bejelentéséről, kielemezve az általános adatvédelmi rendelet vonatkozó szakaszait (Iránymutatás az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről, a munkacsoport WP 250. számú iránymutatása) (a továbbiakban: a WP 250. számú iránymutatás)[3]. Jellege és időzítése miatt azonban ez az iránymutatás nem foglalkozott kellő részletességgel valamennyi gyakorlati kérdéssel. Ennek következtében felmerült egy *gyakorlatorientált, esettanulmányokat magában foglaló* útmutató szükségessége, amely felhasználná a felügyeleti hatóságok által az általános adatvédelmi rendelet alkalmazása óta szerzett tapasztalatokat.

3. E dokumentum célja, hogy kiegészítse a WP 250. számú iránymutatást és tükrözze az EGT felügyeleti hatóságainak az általános adatvédelmi rendelet hatálybalépése óta szerzett közös tapasztalatait. A

[1] A dokumentumban a „tagállamokra” való hivatkozásokat az „EGT-tagállamokra” való hivatkozásként kell értelmezni.

[2] COM(2020) 264 final, 2020. június 24.

[3] A 29. cikk szerinti munkacsoport WP 250. számú iránymutatása, rev.1, 2018. február 6., Iránymutatás az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről – az Európai Adatvédelmi Testület által elfogadva, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

dokumentum célja, hogy segítse az adatkezelőket annak eldöntésében, hogyan kezeljék az adatvédelmi incidenseket, és milyen tényezőket vegyenek figyelembe a kockázatértékelés során.

4. Az incidensek kezelésére irányuló bármilyen kísérlet első lépéseként az adatkezelőnek és adatfeldolgozónak fel kell tudnia ismerni az ilyen eseteket. Az általános adatvédelmi rendelet 4. cikkének 12. pontjában a következőképpen határozza meg az „adatvédelmi incidens” fogalmát: „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”.

5. A személyes adatok megsértése bejelentéséről szóló 03/2014 sz. véleményében[4] és a 29. cikk szerinti munkacsoport WP 250. számú iránymutatásában kifejtette, hogy az adatvédelmi incidensek az alábbi három jól ismert információbiztonsági elv szerint kategorizálhatók:

- „titoksértés”: személyes adatok jogosulatlan vagy véletlen közlése vagy az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés;
- „sértetlenségi adatsértés”: személyes adatok jogosulatlan vagy véletlen módosítása;
- „hozzáférhetőségi adatsértés”: a személyes adatokhoz való hozzáférés véletlen vagy jogosulatlan elvesztése vagy a személyes adatok véletlen vagy jogosulatlan megsemmisítése[5].

6. Az adatvédelmi incidenseknek különféle, jelentősen hátrányos hatásai lehetnek az egyénekre, ezek a hatások pedig fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek. Az általános adatvédelmi rendelet szerint ilyen kár lehet többek között a személyes adataik feletti rendelkezés elvesztése vagy a jogaik korlátozása, a hátrányos megkülönböztetés, a személyazonosság-lopás vagy a személyazonossággal való visszaélés, a pénzügyi veszteség, az álnevesítés engedély nélküli feloldása, a jó hírnév sérelme, valamint a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése. E körbe tartozhat még az egyéneket sújtó egyéb jelentős gazdasági vagy szociális hátrány is. Az adatkezelő egyik legfontosabb kötelezettsége, hogy értékelje az érintettek jogait és szabadságait érintő kockázatokat, és megfelelő technikai és szervezési intézkedéseket hajtson végre ezek kezelésére.

7. Ennek megfelelően az általános adatvédelmi rendelet az adatkezelőket az alábbiakra kötelezi:

- nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket[6];
- értesíti a felügyeleti hatóságot az adatvédelmi incidensről, kivéve, ha az adatvédelmi incidens valószínűleg nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve[7];

---

[4] A 29. cikk szerinti munkacsoport WP 213. számú iránymutatása, 2014. március 25., 03/2014. sz. a személyes adatok megsértése bejelentéséről, 5. o., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

[5] Lásd: WP 250. számú iránymutatás, 7. o. – Figyelembe kell venni, hogy az adatvédelmi incidens egyszerre vagy együttesen egy vagy több kategóriát is érinthet.

[6] Az általános adatvédelmi rendelet 33. cikkének (5) bekezdése.

[7] Az általános adatvédelmi rendelet 33. cikkének (1) bekezdése.

- tájékoztatja az érintettet az adatvédelmi incidensről, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve[8].

8. Az adatvédelmi incidensek önmagukban is problémát jelentenek, de lehetnek egy sérülékeny, esetleg elavult adatbiztonsági rendszer tünetei is, illetve jelezhetik a rendszer hiányosságait is, amelyekkel foglalkozni kell. Általános igazságként mindig jobb az adatvédelmi incidenseket előzetes felkészüléssel megelőzni, hiszen számos következményük természetüknél fogva visszafordíthatatlan jellegű. Mielőtt az adatkezelő *teljes mértékben* fel tudja mérni a valamilyen formában elkövetett támadás által okozott adatvédelmi incidensből eredő kockázatot, azonosítani kell a probléma kiváltó okát annak megállapítása érdekében, hogy az incidenshez vezető sebezhetőségek továbbra is fennállnak-e, és ezért továbbra is kiaknázhatók-e. Az adatkezelő számos esetben képes azonosítani, hogy az incidens valószínűleg kockázatot eredményez, és ezért azt be kell jelenteni. Más esetekben a bejelentést nem kell elhalasztani addig, amíg az incidenssel kapcsolatos kockázat és hatás teljes körű felmérése meg nem történik, mivel a teljes körű kockázatértékelés a bejelentéssel párhuzamosan is megtörténhet, és az így szerzett információk további indokolatlan késedelem nélkül később részletekben is közölhetők a felügyeleti hatósággal[9].

9. Az incidenst akkor kell bejelenteni, ha az adatkezelő úgy véli, hogy az valószínűleg az érintett jogait és szabadságait érintő kockázattal jár. Az adatkezelőknek ezt az értékelést akkor kell elvégezniük, amikor tudomást szereznek az incidensről. Az adatkezelő nem várhat a részletes igazságügyi vizsgálatra és a (korai) kockázatmérséklő lépésekre, mielőtt felmérné, hogy az adatvédelmi incidens valószínűleg kockázattal jár-e vagy sem, és ezért azt be kell-e jelenteni.

10. Ha az adatkezelő saját maga a kockázatot valószínűtlennek ítéli meg, de kiderül, hogy a kockázat megvalósul, az illetékes felügyeleti hatóság élhet korrekciós hatáskörével és szankciókat alkalmazhat

11. Minden adatkezelőnek és adatfeldolgozónak rendelkeznie kell tervekkel, eljárásokkal az esetleges adatvédelmi incidensek kezelésére. A szervezeteknek egyértelmű függelmi rendszerekkel és a helyreállítási folyamat egyes szempontjaiért felelős személyekkel kell rendelkezniük

12. Az adatkezelők és az adatfeldolgozók számára is alapvető fontosságú, hogy az adatkezelő és az adatfeldolgozó munkatársai számára adatvédelmi kérdésekkel kapcsolatos képzést és tudatosságnövelést biztosítsanak, amely az adatvédelmi incidensek kezelésére összpontosít (az adatvédelmi incidensek azonosítása és a további teendők stb.). Ezt a képzést az adatkezelési tevékenység típusától és az adatkezelő méretétől függően rendszeresen meg kell ismételni, kitérve a legújabb trendekre és a kibertámadásokból vagy más biztonsági incidensekből származó figyelmeztetésekre.

13. Az elszámoltathatóság elve és a beépített adatvédelem koncepciója magában foglalhatna olyan elemzést, amely beépülne az adatkezelő és az adatfeldolgozó saját „Adatvédelmi incidensek kezelésére vonatkozó kézikönyvébe”, amelynek célja, hogy a művelet minden fő szakaszában tényeket állapítson meg az adatkezelés valamennyi szempontjára vonatkozóan. Egy ilyen, előzetesen elkészített kézikönyv sokkal gyorsabb információforrást biztosítana, amely lehetővé tenné az adatkezelők és adatfeldolgozók számára, hogy indokolatlan késedelem nélkül mérsékeljék a kockázatokat és teljesítsék a kötelezettségeiket. Ez biztosítaná, hogyha adatvédelmi incidensre kerülne sor, a szervezetben dolgozók tudnák, hogy mit kell

[8] Az általános adatvédelmi rendelet 34. cikkének (1) bekezdése.

[9] Az általános adatvédelmi rendelet 33. cikkének (4) bekezdése.

tenniük, és az incidenst nagyobb valószínűséggel gyorsabban kezelhető lenne, mintha nem lennének kockázatmérséklő intézkedések vagy tervek.

14. Bár az alábbiakban bemutatott esetek fiktívek, a felügyeleti hatóságok adatvédelmi incidensekkel kapcsolatos bejelentéseinek kollektív tapasztalataiból származó tipikus eseteken alapulnak. A bemutatott elemzések kifejezetten a vizsgált esetekre vonatkoznak, de azzal a céllal, hogy segítséget nyújtsanak az adatkezelőknek saját adatvédelmi incidenseik értékeléséhez. Az alább ismertetett esetek körülményeinek bármilyen változása eltérő vagy jelentősebb kockázati szintekkel járhat, és így eltérő vagy kiegészítő intézkedéseket tehet szükségessé. Ezek az iránymutatások az eseteket az incidensek bizonyos kategóriái szerint strukturálják (pl. zsarolóvírus-támadások). Az incidensek egyes kategóriájának kezelése során minden esetben szükség van bizonyos kockázatmérséklő intézkedésekre. Ezeket az intézkedéseket nem feltétlenül ismétlik meg minden egyes, azonos incidenskategóriába tartozó esetelemzésnél. Az azonos kategóriába tartozó esetek esetében csak a különbségek kerülnek meghatározásra. Ezért az olvasónak el kell olvasnia az incidens adott kategóriájához tartozó összes esetet, hogy azonosítsa és megkülönböztesse a meghozandó megfelelő intézkedéseket.

15. Az incidens belső dokumentálása az incidenssel kapcsolatos kockázatoktól független kötelezettség, amelyet minden egyes esetben el kell végezni. Az alábbiakban bemutatott esetek megpróbálnak némi felvilágosítást adni arról, hogy az incidenst be kell-e jelenteni a felügyeleti hatóságnak és közölni kell-e az érintettekkel.

2 ZSAROLÓVÍRUS

16. Az adatvédelmi incidens bejelentésének gyakori oka az adatkezelőt ért zsarolóvírus-támadás. Ezekben az esetekben egy rosszindulatú kód titkosítja a személyes adatokat, majd a támadó a visszafejtő kódért cserében váltságdíjat kér az adatkezelőtől. Az ilyen jellegű támadás általában hozzáférhetőségi adatsértésnek minősül, de gyakran előfordulhat titoksértés is.

2.1 01. sz. ESET: Zsarolóvírus megfelelő biztonsági mentéssel és kiszivárogtatás nélkül

Egy kis gyártóvállalat számítógépes rendszerei zsarolóvírus-támadásnak voltak kitéve; és az ezekben a rendszerekben tárolt adatokat titkosították. Az adatkezelő az inaktív adatokra is kiterjedő titkosítást alkalmazott, így a zsarolóprogram által elért valamennyi adatot titkosított formában tárolták egy korszerű titkosítási algoritmus segítségével. A támadás során a visszafejtő kulcs nem került veszélybe, azaz a támadó nem férhetett hozzá és közvetve sem használhatta fel azokat. Ennek következtében a támadó csak a titkosított személyes adatokhoz fért hozzá. Különösen nem érintette sem a vállalat e-mail rendszerét, sem az ahhoz való hozzáférésre használt ügyfélrendszereket. A vállalat egy külső kiberbiztonsági cég szakértelmét veszi igénybe az incidens kivizsgálásához. Rendelkezésre állnak a vállalattól kimenő valamennyi adatáramlást nyomon követő naplók (ideértve a kimenő e-maileket is). A naplók és a vállalat által telepített észlelő rendszerek által gyűjtött adatok elemzése után a külső kiberbiztonsági cég által támogatott belső vizsgálat *teljes bizonyossággal* megállapította, hogy az elkövető csak titkosította az adatokat, de nem szivárogtatta ki azokat. A naplók nem mutatnak kifelé irányuló adatáramlást a támadás időtartama alatt. Az incidens által érintett személyes adatok a vállalat ügyfeleire és alkalmazottaira vonatkoznak, összesen néhány tucat személyre. A biztonsági mentés gyorsan rendelkezésre állt, és az adatokat a támadás után néhány órával helyreállították. Az incidens semmilyen következménnyel nem járt az adatkezelő napi működésére. A munkavállalók fizetései és az ügyfelek kérelmeinek kezelése nem szenvedett késedelmet.

17. Ebben az esetben az „adatvédelmi incidens” fogalmából a következő elemek valósultak meg: a biztonság sérülése a tárolt személyes adatok jogellenes megváltoztatását és az azokhoz való jogosulatlan hozzáférést eredményezte.

2.1.1 01. sz. ESET – Előzetes intézkedések és kockázatértékelés

18. Mint minden külső szereplő által jelentett kockázat esetében, a zsarolóvírus-támadás sikerének valószínűsége drasztikusan csökkenthető az adatellenőrzési környezet biztonságának szigorításával. Az ilyen incidensek többsége megelőzhető a megfelelő szervezeti, fizikai és technológiai biztonsági intézkedések megtételével. Ilyen intézkedés például a hibajavító csomagok megfelelő kezelése (patch management) és a rosszindulatú szoftverek észlelésére szolgáló megfelelő rendszer használata. A megfelelő és különálló biztonsági mentés segít enyhíteni egy esetleges sikeres támadás következményeit. Emellett a munkavállalók biztonsági oktatására, képzésére és tudatosságának növelésére irányuló program segít megelőzni és felismerni az ilyen jellegű támadásokat. (A javasolt intézkedések listája a 2.5. szakaszban található.) Ezen intézkedések közül az egyik legfontosabb a hibajavító csomagok megfelelő kezelése (patch management), amely biztosítja, hogy a rendszerek naprakészek legyenek, és a telepített rendszerek minden ismert sebezhetősége kijavításra kerüljön. Ez az egyik legfontosabb intézkedés, mivel a zsarolóvírus-támadások többsége jól ismert sebezhetőségeket használ ki.

19. A kockázatok értékelése során az adatkezelőnek ki kell vizsgálnia az incidenst, és azonosítania kell a rosszindulatú kód típusát, hogy megértse a támadás lehetséges következményeit. A figyelembe veendő kockázatok között szerepel annak kockázata, hogy az adatok kiszivárogtatására úgy került sor, hogy a rendszerek naplóiban ennek nem maradt nyoma.

20. Ebben a példában a támadó hozzáfért személyes adatokhoz, és a titkosított formában személyes adatokat tartalmazó rejtjelezett szöveg titkossága sérült. Az esetlegesen kiszivárogtatott adatokat azonban az elkövető – legalábbis egyelőre – nem tudja elolvasni vagy felhasználni. Az adatkezelő által alkalmazott titkosítási technika megfelel a legkorszerűbb technikai követelményeknek. A visszafejtő kulcsot nem törték fel, és feltehetően más módon sem lehetett megfejteni. Következésképpen a természetes személyek jogait és szabadságait érintő titoktartási kockázatok minimálisra csökkennek, hacsak a rejtjelfejtés fejlődése nem teszi a titkosított adatokat a jövőben értelmezhetővé.

21. Az adatkezelőnek mérlegelnie kell, hogy az incidens milyen kockázatot jelent az egyének számára[10]. Ebben az esetben úgy tűnik, hogy az érintettek jogait és szabadságait érintő kockázatok a személyes adatok hozzáférhetőségének hiányából erednek, és a személyes adatok bizalmas jellege nem sérül[11]. Ebben a

[10] A „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a 29. cikk szerinti munkacsoport „Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában »valószínűsíthetően magas kockázattal jár«-e” című dokumentumát, WP 248. rev. 01, – az Európai Adatvédelmi Testület által elfogadva, https://ec.europa.eu/newsroom/article29/items/611236, 9. o.

[11] Technikai értelemben az adatok titkosítása magában foglalja az eredeti adatokhoz való „hozzáférést”, és a zsarolóvírusok esetében az eredeti adatok törlését – a titkosításhoz és az eredeti adatok törléséhez a zsarolóvírus kódjának hozzá kell férnie az adatokhoz. A támadó a törlés előtt készíthet másolatot az eredeti adatokról, de a személyes adatok nem mindig kerülnek kinyerésre. Az adatkezelő vizsgálatának előrehaladtával olyan új információk kerülhetnek napvilágra, amelyek ezt az értékelést megváltoztatják. A személyes adatok jogellenes megsérülését, elvesztését, módosítását, másnak jogosulatlanul tudomására jutását vagy az érintett biztonsági kockázatát eredményező hozzáférés az adatok értelmezése nélkül is ugyanolyan súlyos lehet, mint a személyes adatok értelmezésével történő hozzáférés.

példában az incidens hátrányos hatásait az incidens bekövetkezte után viszonylag hamar sikerült enyhíteni. A megfelelő biztonsági mentési rendszer[12] mérsékli az incidens hatásait, és ebben az esetben az adatkezelő hatékonyan tudta kihasználni azt.

22. Az érintettekre gyakorolt következmények súlyosságát illetően csak csekély következményeket lehetett megállapítani, mivel az érintett adatokat néhány órán belül helyreállították, az incidens nem járt következményekkel az adatkezelő napi működésére nézve, és nem volt jelentős hatással az érintettekre sem (pl. a munkavállalók fizetései vagy az ügyfelek kérelmeinek kezelése).

2.1.2 01. sz. ESET – Mérséklés és kötelezettségek

23. Biztonsági mentés nélkül az adatkezelő kevés intézkedést tud tenni a személyes adatok elvesztésének orvoslására, és az adatokat újra össze kell gyűjteni. Ebben a konkrét esetben azonban a támadás hatásait hatékonyan meg lehetett fékezni azzal, hogy az összes veszélyeztetett rendszert visszaállították egy olyan tiszta állapotba, amelyről ismert, hogy nem tartalmaz rosszindulatú kódokat, továbbá kijavították a sebezhetőségeket, és a támadást követően gyorsan helyreállították az érintett adatokat. Biztonsági mentés nélkül az adatok elvesznek, és a súlyosság fokozódhat, mivel az egyéneket érintő kockázatok vagy hatások is növekedhetnek.

24. Az incidens elemzésekor kulcsfontosságú változó, hogy az azonnal rendelkezésre álló biztonsági mentésből mikor került sor az adok hatékony helyreállítására. A veszélyeztetett adatok helyreállítására fordítható megfelelő időkeret meghatározása a szóban forgó incidens egyedi körülményeitől függ. Az általános adatvédelmi rendelet értelmében az adatvédelmi incidenseket indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órán belül be kell jelenteni. Ezért megállapítható, hogy a 72 órás határidő túllépése semmi esetben sem tanácsos, de magas kockázattal járó esetek esetén még e határidő betartása is elégtelennek tekinthető.

25. Ebben az esetben az adatkezelő egy részletes hatásvizsgálatot és az incidenskezelési folyamatot követően megállapította, hogy az incidens valószínűleg nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, ezért nincs szükség az érintettek tájékoztatására, és az incidenst nem szükséges bejelenteni az adatvédelmi hatóságnál sem. Ugyanakkor, mint minden incidenst, azt a 33. cikk (5) bekezdésével összhangban nyilván kell tartani. Előfordulhat, hogy a szervezetnek szüksége lehet arra is (vagy a későbbiekben a felügyeleti hatóság arra kötelezheti), hogy frissítse és javítsa a személyes adatok szervezeti és technikai biztonságkezelését és a kockázatcsökkentő intézkedéseket és eljárásokat. E frissítés és helyreállítás keretében a szervezetnek alaposan ki kell vizsgálnia az incidenst, és azonosítania kell az okokat és az elkövető által alkalmazott módszereket annak érdekében, hogy a jövőben meg lehessen előzni a hasonló eseményeket.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	X	X

[12] A biztonsági mentési eljárásoknak strukturáltnak, következetesnek és megismételhetőnek kell lenniük. A biztonsági mentési eljárások példái a 3-2-1 módszer és a nagyapa-apa-fiú módszer. Minden módszert minden esetben meg kell vizsgálni a lefedettség hatékonysága és az adatok helyreállításának időpontja tekintetében. A rendszer integritásának biztosítása érdekében a tesztelést bizonyos időközönként és különösen az adatkezelési műveletben vagy annak körülményeiben bekövetkező változások esetén meg kell ismételni.

2.2 02. sz. ESET: Zsarolóvírus megfelelő biztonsági mentés nélkül

Egy mezőgazdasági vállalat által használt számítógépek egyike zsarolóvírus-támadásnak volt kitéve, és az adatait a támadó titkosította. A vállalat egy külső kiberbiztonsági cég szakértelmét veszi igénybe hálózata ellenőrzéséhez. Rendelkezésre állnak a vállalattól kimenő valamennyi adatáramlást nyomon követő naplók (ideértve a kimenő e-maileket is). A naplók és az egyéb észlelő rendszerek által gyűjtött adatok elemzése után a kiberbiztonsági cég által támogatott belső vizsgálat megállapította, hogy az elkövető csak titkosította az adatokat,anélkül, hogy kiszivárogtatta volna azokat. A naplók nem mutatnak kifelé irányuló adatáramlást a támadás időtartama alatt. Az incidens által érintett személyes adatok a vállalat ügyfeleire és alkalmazottaira vonatkoznak, összesen néhány tucat személyre. Az incidens az adatok különleges kategóriáit nem érintette. Elektronikus formában nem állt rendelkezésre biztonsági mentés. Az adatok többségét papíralapú biztonsági mentésekből helyreállították. Az adatok helyreállítása 5 munkanapot vett igénybe, ami kisebb késedelmekhez vezetett a megrendelések ügyfeleknek történő kézbesítése során.

2.2.1 02. sz. ESET – Előzetes intézkedések és kockázatértékelés

26. Az adatkezelőnek a 2.1. részben és a 2.9. szakaszban említett előzetes intézkedésekkel azonos intézkedéseket kellett volna hoznia. A fő különbség az előző esethez képest az elektronikus biztonsági mentés és az inaktív adatokra is kiterjedő titkosítás hiánya. Ez meghatározó különbségeket eredményez a következő lépésekben.

27. A kockázatok értékelése során az adatkezelőnek ki kell vizsgálnia a behatolás módszerét, és azonosítania kell a rosszindulatú kód típusát, hogy megértse a támadás lehetséges következményeit. Ebben a példában a zsarolóvírus anélkül titkosította a személyes adatokat, hogy azokat kiszivárogtatta volna. Ezért úgy tűnik, hogy az érintettek jogait és szabadságait érintő kockázatok a személyes adatok hozzáférhetőségének hiányából erednek, és a személyes adatok bizalmas jellege nem sérül. A kockázat meghatározásához elengedhetetlen a tűzfal naplóinak és ennek következményeinek alapos kivizsgálása. Az adatkezelőnek kérésre be kell mutatnia e vizsgálatok ténymegállapításait.

28. Az adatkezelőnek szem előtt kell tartania, hogy ha a támadás kifinomultabb, a rosszindulatú szoftver képes a naplófájlok szerkesztésére és a nyom eltávolítására. Így – tekintettel arra, hogy a naplóbejegyzéseket nem továbbítják vagy másolják egy központi naplószerverre – az adatkezelő akkor sem állíthatja, hogy a naplóbejegyzés hiánya bizonyítja a kiszivárgás hiányát, ha egy alapos vizsgálat azt mutatta ki, hogy a támadó nem szivárogtatott ki személyes adatokat, ezért a titoksértés valószínűsége nem zárható ki teljesen.

29. Az adatkezelőnek fel kell mérnie az incidens kockázatait[13], ha az adatokhoz a támadó hozzáfért. A kockázatértékelés során az adatkezelőnek figyelembe kell vennie az incidensben érintett személyes adatok jellegét, érzékenységét, mennyiségét és kontextusát is. Ebben az esetben a személyes adatok különleges kategóriái nem érintettek, és a sérült adatok mennyisége és az érintettek száma alacsony.

30. A jogosulatlan hozzáférésre vonatkozó pontos információk gyűjtése kulcsfontosságú a kockázati szint meghatározásához és az újabb vagy folytatólagos támadás megelőzéséhez. Ha az adatokat kimásolták volna az adatbázisból, az nyilvánvalóan kockázatnövelő tényező lett volna. Ha bizonytalanok a jogosulatlan

[13] A „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

hozzáférés részletei, a rosszabb forgatókönyvet kell mérlegelni és a kockázatot ennek megfelelően kell értékelni.

31. A biztonsági mentési adatbázis hiánya kockázatnövelő tényezőnek tekinthető, attól függően, hogy milyen súlyos következményekkel jár az érintettek számára az adatok hozzáférhetőségének hiánya.

2.2.2 02. sz. ESET – Mérséklés és kötelezettségek

32. Biztonsági mentés nélkül az adatkezelő kevés intézkedést tud tenni a személyes adatok elvesztésének orvoslására, és az adatokat újra össze kell gyűjteni, kivéve, ha valamilyen más forrásból (pl. rendeléseket visszaigazoló e-mailek) ezek hozzáférhetők. Biztonsági mentés nélkül az adatok elveszhetnek, és ennek súlyossága az egyénekre gyakorolt hatástól függ.

33. Az adatok helyreállítása nem jelenthet túlzottan nagy problémát[14], ha az adatok papíron még mindig rendelkezésre állnak. Ugyanakkor az elektronikus biztonsági adatbázis hiánya miatt a felügyeleti hatóság értesítése szükségesnek tekintendő, mivel az adatok helyreállítása időbe telt, és ez késedelmet okozhat a megrendelések ügyfeleknek történő kézbesítésében, továbbá a metaadatok jelentős része (pl. naplók, időbélyegzők) nem feltétlenül lesz visszakereshető.

34. Az érintettek tájékoztatása az incidensről attól is függhet, hogy a személyes adatok mennyi ideig nem hozzáférhetők, és hogy ez milyen nehézségeket okozhat az adatkezelő működésében (pl. késedelem a munkavállalói fizetések átutalásában). Mivel ezek a fizetési és szállítási késedelmek pénzügyi veszteséget okozhatnak azon személyek számára, akiknek az adatai sérültek, azzal is lehet érvelni, hogy az incidens valószínűleg magas kockázattal jár. Emellett nem biztos, hogy elkerülhető az érintettek tájékoztatása, ha a titkosított adatok helyreállításához szükség van a közreműködésükre.

35. Ez az eset példaként szolgál az érintettek jogaira és szabadságaira nézve kockázatot jelentő, de a magas kockázatot el nem érő zsarolóvírus-támadásra. A támadást a 33. cikk (5) bekezdésével összhangban nyilván kell tartani, és a 33. cikk (1) bekezdésével összhangban be kell jelenteni a felügyeleti hatóságnak. Előfordulhat, hogy a szervezetnek szüksége lehet arra is (vagy a felügyeleti hatóság arra kötelezheti), hogy frissítse és javítsa a személyes adatok szervezeti és technikai biztonságkezelését és a kockázatcsökkentő intézkedéseket és eljárásokat.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	X

[14] Ez a személyes adatok összetettségétől és szerkezetétől függ. A legösszetettebb forgatókönyvek esetében az adatok integritásának helyreállítása, a metaadatokkal való összhang, az adatstruktúrákon belüli helyes kapcsolatok biztosítása és az adatok pontosságának ellenőrzése jelentős erőforrásokat és erőfeszítéseket igényelhet.

2.3 03. sz. ESET: Zsarolóvírus biztonsági mentéssel és kiszivárogtatás nélkül egy kórházban

Egy kórház/egészségügyi központ információs rendszere zsarolóvírus-támadásnak volt kitéve, és az adatok jelentős részét a támadó titkosította. A vállalat egy külső kiberbiztonsági cég szakértelmét veszi igénybe hálózata ellenőrzéséhez. Rendelkezésre állnak a vállalattól kimenő valamennyi adatáramlást nyomon követő naplók (ideértve a kimenő e-maileket is). A naplók és az egyéb észlelő rendszerek által gyűjtött adatok elemzése után a kiberbiztonsági cég által támogatott belső vizsgálat megállapította, hogy az elkövető csak titkosította az adatokat, de nem szivárogtatta ki azokat. A naplók nem mutatnak kifelé irányuló adatáramlást a támadás időtartama alatt. Az incidens által érintett személyes adatok az alkalmazottakra és betegekre vonatkoznak, ami több ezer személyt jelent. Elektronikus formában rendelkezésre álltak biztonsági mentések. Az adatok nagy részét sikerült helyreállítani, de ez a művelet 2 munkanapig tartott, és jelentős késedelmekhez vezetett a betegek kezelésében, mivel műtéteket kellett törölni/elhalasztani, és a rendszerek hozzáférhetetlensége miatt csökkent a szolgáltatási szint.

2.3.1 03. sz. ESET – Előzetes intézkedések és kockázatértékelés

36. Az adatkezelőnek a 2.1. részben és a 2.5. szakaszban említett előzetes intézkedésekkel azonos intézkedéseket kellett volna hoznia. A fő különbség az előző esethez képest az, hogy az érintettek jelentős részét érintő következmények nagyon súlyosak[15].

37. A sérült adatok mennyisége és az érintettek száma magas, mivel a kórházak általában nagy mennyiségű adatot dolgoznak fel. Az adatok hozzáférhetetlensége az érintettek jelentős részére nagy hatással van. Ezen túlmenően a betegek adatainak bizalmas jellegére nézve fennáll egy magas súlyosságú fennmaradó kockázat.

38. Fontos az incidens típusa, illetve az incidensben érintett személyes adatok jellege, érzékenysége és mennyisége. Annak ellenére, hogy az adatokról biztonsági mentés készült, és azokat néhány nap alatt helyre lehetett állítani, továbbra is fennáll a magas kockázat, mert az érintettekre gyakorolt következmények súlyosak voltak az adatoknak a támadás pillanatában és az azt követő napokban való hozzáférhetetlensége miatt.

2.3.2 03. sz. ESET – Mérséklés és kötelezettségek

39. A felügyeleti hatóság értesítése szükségesnek tekintendő, mivel személyes adatok különleges kategóriái érintettek, és az adatok helyreállítása hosszú időt vehet igénybe, ami jelentős késedelmet okozhat a betegellátásban. Az érintettek tájékoztatása az incidensről a betegekre gyakorolt hatás miatt szükséges, még a titkosított adatok helyreállítása után is. Bár az elmúlt évek során a kórházban kezelt valamennyi betegre vonatkozó adatokat titkosították, de a támadás csak azokat a betegeket érintette, akiknek a kórházi kezelését a számítógépes rendszer elérhetetlensége idejére ütemezték. Az adatkezelőnek közvetlenül e betegeket kell tájékoztatnia az adatvédelmi incidensről. A 34. cikk (3) bekezdésének c) pontjában foglalt kivétel miatt nem feltétlenül szükséges a többi beteg közvetlen tájékoztatása, akik közül előfordulhat, hogy néhányan nem is jártak a kórházban több mint húsz éve. Ilyen esetekben az érintetteket nyilvánosan közzétett információk[16]

[15] A „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

[16] Az általános adatvédelmi rendelet (86) preambulumbekezdése kimondja, hogy „*Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal,*

útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását. Ebben az esetben a kórháznak nyilvánosságra kell hoznia a zsarolóvírus-támadást és annak hatásait.

40. Ez az eset példaként szolgál az érintettek jogaira és szabadságaira nézve magas kockázatot jelentő zsarolóvírus-támadásra. A támadást a 33. cikk (5) bekezdésével összhangban nyilván kell tartani, a 33. cikk (1) bekezdésével összhangban be kell jelenteni a felügyeleti hatóságnak, valamint a 34. cikk (1) bekezdésével összhangban arról tájékoztatni kell az érintetteket. A szervezetnek továbbá frissítenie és javítania kell a személyes adatok szervezeti és technikai biztonságkezelését és a kockázatcsökkentő intézkedéseket és eljárásokat.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	✓

2.4 04. sz. ESET: Zsarolóvírus biztonsági mentés nélkül és kiszivárogtatással

Egy tömegközlekedési vállalat szoftvere zsarolóvírus-támadásnak volt kitéve, és adatait a támadó titkosította. A belső vizsgálat megállapításai szerint az elkövető nemcsak titkosította az adatokat, hanem ki is szivárogtatta azokat. A sérült adatok típusai közé tartoztak az ügyfelek és alkalmazottak, valamint a cég szolgáltatásait (pl. online jegyvásárlás) igénybe vevő több ezer ember személyes adatai. Az alapvető személyazonosító adatokon túl személyazonosító igazolványok számai és pénzügyi adatok, például hitelkártyaadatok is érintettek az incidensben. Létezett egy biztonsági adatbázis, de a támadó azt is titkosította.

2.4.1 04. sz. ESET – Előzetes intézkedések és kockázatértékelés

41. Az adatkezelőnek a 2.1. részben és a 2.5. szakaszban említett előzetes intézkedésekkel azonos intézkedéseket kellett volna hoznia. Bár volt biztonsági mentés, azt is érintette a támadás. Már ez az intézkedés is kérdéseket vet fel az adatkezelő előzetes informatikai biztonsági intézkedéseinek minőségével kapcsolatban, és ezt a vizsgálat során alaposan ki kell vizsgálni, mivel egy jól megtervezett biztonsági mentési rendszerben több biztonsági másolatot kell biztonságosan tárolni anélkül, hogy azokhoz a fő rendszerből hozzá lehetne férni, különben ezek is veszélybe kerülhetnek ugyanazon támadás során. A zsarolóvírus-támadások ráadásul napokig észrevétlenül maradhatnak, lassan titkosítva a ritkán használt adatokat. Ez több biztonsági mentést is használhatatlanná tehet, ezért rendszeresen biztonsági mentéseket kell készíteni és azokat elkülönítve kell tárolni. Ez növelné a helyreállítás valószínűségét, bár nagyobb adatveszteséggel járna.

és betartva az általa vagy más érintett hatóságok például bűnüldöző hatóságok által adott útmutatást. Például az érintettek sürgős tájékoztatása a kár közvetlen veszélyének mérsékléséhez szükséges, azonban annak megelőzése több időt igényelhet, hogy a folyamatos vagy azonos jellegű adatvédelmi incidens esetében megfelelő intézkedéseket kell végrehajtani".

42. Ez az incidens nemcsak az adatok hozzáférhetőségét, hanem a titkosságát is érinti, mivel a támadó módosíthatta és/vagy lemásolhatta az adatokat a szerverről. Ezért az ilyen típusú incidens magas kockázattal jár[17].

43. A személyes adatok jellege, érzékenysége és mennyisége tovább növeli a kockázatokat, mivel az érintett személyek száma magas, ahogyan az érintett személyes adatok teljes mennyisége is. Az alapvető személyazonosító adatokon túl személyazonosító okmányok és pénzügyi adatok, például hitelkártyaadatok is érintettek. Az ilyen típusú adatokat érintő adatvédelmi incidensek önmagukban is magas kockázatot jelentenek, és ha együttesen dolgozzák fel őket, akkor – többek között – személyazonosság-lopásra vagy csalásra is felhasználhatók.

44. Hibás szerverlogika vagy szervezeti ellenőrzés miatt a biztonsági mentések fájljait érintette a zsarolóvírus, ami megakadályozta az adatok helyreállítását és növelte a kockázatot.

45. Ez az adatvédelmi incidens magas kockázatot jelent az egyének jogaira és szabadságaira nézve, mivel valószínűleg mind anyagi (pl. pénzügyi veszteség, mivel a hitelkártyaadatok érintettek), mind nem anyagi károkhoz (pl. személyazonosság-lopás vagy csalás, mivel a személyazonosító igazolvány adatai érintettek) is vezethet.

2.4.2 04. sz. ESET – Mérséklés és kötelezettségek

46. Az érintettek tájékoztatása alapvető fontosságú, hogy megtehessék a szükséges lépéseket az anyagi kár elkerülése érdekében (pl. letiltsák hitelkártyájukat).

47. A 33. cikk (5) bekezdése szerinti nyilvántartás mellett ebben az esetben kötelező a felügyeleti hatóság értesítése is (33. cikk (1) bekezdés), és az adatkezelő köteles az incidensről az érintettekkel is tájékoztatni (34. cikk (1) bekezdés). Az érintetteket egyénileg is értesítheti, de azon személyek esetében, akiknek a kapcsolattartási adatai nem állnak rendelkezésre, az adatkezelőnek ezt nyilvánosan, pl. a honlapján közzétett értesítés útján kell megtennie, feltéve, hogy az ilyen tájékoztatás nem jár további negatív következményekkel az érintettekre nézve. Ez utóbbi esetben precíz és egyértelmű kommunikációra van szükség, jól láthatóan az adatkezelő honlapján, az általános adatvédelmi rendelet vonatkozó rendelkezéseire való pontos hivatkozással. Előfordulhat továbbá, hogy a szervezetnek frissítenie és javítania kell a személyes adatok szervezeti és technikai biztonságkezelését és a kockázatcsökkentő intézkedéseket és eljárásokat.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	✓

2.5 Szervezeti és technikai intézkedések a zsarolóvírus-támadások hatásainak megelőzésére/mérséklésére

48. Az, hogy zsarolóvírus-támadásra kerülhetett sor, általában egy vagy több sebezhetőséget jelez az adatkezelő rendszerében. Ugyanez vonatkozik azokra a zsarolóvírussal kapcsolatos esetekre is, amelyek során a személyes adatokat titkosították, de azok nem kerültek kiszivárogtatásra. A támadás kimenetelétől és következményeitől függetlenül nem lehet eléggé hangsúlyozni az adatbiztonsági rendszer átfogó

[17] A „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

értékelésének fontosságát, különös tekintettel az informatikai biztonságra. Az azonosított hiányosságokat és biztonsági réseket dokumentálni, és haladéktalanul kezelni szükséges.

49. Ajánlott intézkedések:

(Az alábbi intézkedések felsorolása semmiképpen sem kizárólagos vagy teljes körű. A cél inkább az, hogy a megelőzéssel kapcsolatban ötleteket és lehetséges megoldásokat biztosítson. Minden adatkezelési tevékenység eltérő, ezért az adatkezelőnek kell eldöntenie, hogy az adott helyzethez mely intézkedések illenek leginkább.)

- A firmware, az operációs rendszer és az alkalmazásszoftver naprakészen tartása a szervereken, az ügyfelek gépein, az aktív hálózati komponenseken és az ugyanazon a LAN-on található bármely más gépen (ideértve a wifi-eszközöket is). A megfelelő informatikai biztonsági intézkedésekről való gondoskodás, azok hatékonyságának biztosítása és rendszeres frissítése, ha az adatkezelés vagy a körülmények változnak vagy fejlődnek. Ez magában foglalja részletes naplók vezetését is arról, hogy mely hibajavító csomagokat milyen időbélyegzővel alkalmaztak.

- Az adatkezelő rendszerek és az infrastruktúra tervezése és szervezése az adatrendszerek és hálózatok szegmentálása vagy elkülönítése érdekében annak érdekében, hogy megelőzzék a rosszindulatú szoftverek szervezeten belüli és külső rendszerekbe történő terjedését.

- Naprakész, biztonságos és kipróbált biztonsági mentési eljárás megléte. A közép- és hosszú távú biztonsági mentéshez használt adathordozókat az operatív adattárolástól elkülönítve kell tartani, és még sikeres támadás esetén sem szabad harmadik fél számára hozzáférhetővé tenni (például napi inkrementális biztonsági mentés és heti teljes biztonsági mentés).

- A rosszindulatú szoftverek elleni megfelelő, naprakész, hatékony és integrált szoftver megléte/beszerzése.

- Megfelelő, naprakész, hatékony és integrált tűzfal és behatolásérzékelő és -megelőző rendszer. A hálózati forgalom átirányítása a tűzfalon/behatolásérzékelőn keresztül, még otthon végzett munka vagy mobil munkavégzés esetén is (pl. a szervezeti biztonsági mechanizmusok esetében VPN-kapcsolatok használatával az internethez való hozzáférés során).

- Az alkalmazottak képzése az informatikai támadások felismerésének és megelőzésének módszereire vonatkozóan. Az adatkezelőnek eszközöket kell biztosítania annak megállapítására, hogy az e-mailek és az egyéb kommunikációs eszközök útján kapott üzenetek hitelesek és megbízhatóak-e. Az alkalmazottak képzésének ki kell terjednie annak felismerésére, hogy mikor történt ilyen támadás, valamint hogy miként lehet a végpontot kivenni a hálózatból, és az incidens biztonsági tisztviselőnek való haladéktalan jelentésének kötelezettségére.

- Annak hangsúlyozása, hogy a rosszindulatú kód típusát azonosítani kell annak érdekében, hogy fel lehessen ismerni a támadás következményeit, és meg lehessen találni a megfelelő intézkedéseket a kockázat mérséklésére. Ha a zsarolóvírus-támadás sikeres volt, és nem áll rendelkezésre biztonsági mentés, olyan rendelkezésre álló eszközök alkalmazhatóak az az adatok visszaszerzéséhez, mint például a „no more ransom” (nomoreransom.org) projekt által kifejlesztettek.. Amennyiben azonban rendelkezésre áll biztonságos biztonsági mentés, az adatok ajánlatos arról helyreállítani.

- Az összes naplófájl továbbítása vagy másolása egy központi naplószerverre (esetleg a naplóbejegyzések aláírásával vagy kriptográfiai időbélyegzésével).

- Erős titkosítás és többtényezős hitelesítés, különösen az informatikai rendszerekhez való adminisztratív hozzáférés, valamint a megfelelő kulcs- és jelszókezelés esetében.
- Rendszeres sebezhetőségi és behatolási tesztelés.
- Számítógép-biztonsági eseményekre reagáló csoport (CSIRT) vagy hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT) felállítása a szervezeten belül, vagy egy csoportos CSIRT/CERT-hez való csatlakozás. Incidenskezelési terv, katasztrófa utáni helyreállítási terv és üzletmenet-folytonossági terv készítése, és ezek alapos tesztelésének biztosítása.
- Az ellenintézkedések értékelése során szükség van a kockázatelemzés felülvizsgálatára, tesztelésére és aktualizálására.

3 ADATKISZIVÁRGÁSOS TÁMADÁSOK

50. Az adatkezelő által harmadik felek számára az interneten keresztül nyújtott szolgáltatások sebezhetőségét kihasználó támadások, például az injection támadások (pl. SQL- injection, útkeresztezés), a honlapok feltörése és hasonló módszerek révén elkövetett támadások hasonlíthatnak a zsarolóvírus-támadásokhoz abban az értelemben, hogy a kockázat egy jogosulatlan harmadik fél tevékenységéből ered, de e támadások célja jellemzően a személyes adatok rosszindulatú célból történő másolása, kiszivárogtatása, illetve az azokkal való visszaélés. Ezért ezek főként titoksértést és esetlegesen még sértetlenségi adatsértést képeznek. Ugyanakkor, ha az adatkezelő tisztában van az ilyen típusú incidensek jellemzőivel, számos olyan intézkedés áll rendelkezésére, amely jelentősen csökkentheti a támadás sikeres végrehajtásának kockázatát.

3.1 05. sz. ESET: Az álláspályázati adatok honlapról való kiszivárgása

Egy munkaközvetítő ügynökség kibertámadás áldozata lett, amelynek során rosszindulatú kódot helyeztek el honlapján. Ez a rosszindulatú kód jogosulatlan személy(ek) számára hozzáférhetővé tette az online álláspályázati űrlapokon keresztül benyújtott és a webszervereken tárolt személyes adatokat. A támadás 213 ilyen űrlapot érinthetett, az érintett adatok elemzése után megállapították, hogy az incidens nem érintett különleges adatkategóriákat. Az ebben az esetben telepített rosszindulatú szoftver eszközkészlete olyan funkciókkal rendelkezett, amelyek lehetővé tették a támadó számára, hogy eltávolítsa a kiszivárgás előzményeit, valamint lehetővé tette a szerveren történő adatkezelés nyomon követését és a személyes adatok rögzítését. Az eszközkészletet csak egy hónappal a telepítése után fedezték fel.

3.1.1 05. sz. ESET – Előzetes intézkedések és kockázatértékelés

51. Az adatkezelő környezetének biztonsága rendkívül fontos, mivel az ilyen incidensek többsége megelőzhető azáltal, hogy valamennyi rendszert folyamatosan frissítenek, a különleges adatokat titkosítják, és az alkalmazásokat magas szintű biztonsági előírásoknak megfelelően fejlesztik ki, például erős hitelesítéssel, a próbálgatásos támadásokkal szembeni intézkedésekkel, a felhasználói bemenetek „kikerülésével” vagy „szanálásával”[18] stb. Időszakos informatikai biztonsági ellenőrzésekre, sebezhetőségi értékelésekre és behatolási tesztekre is szükség van az ilyen jellegű sebezhetőségek előzetes észleléséhez és kijavításához.

[18] A felhasználói bemenetek kikerülése vagy szanálása a bemeneti érvényesítés egy formája, amely biztosítja, hogy csak megfelelően formázott adatokat vigyenek be egy információs rendszerbe.

Ebben a konkrét esetben a fájlintegritást a működési környezetben ellenőrző eszközök segíthettek volna a kóddal történő fertőzés észlelésében. (A javasolt intézkedések listája a 3.7. szakaszban található.)

52. Az adatkezelőnek mindig a támadás típusának és módszereinek meghatározásával kell kezdenie az incidens kivizsgálását annak érdekében, hogy felmérje, milyen intézkedéseket kell tenni. A gyors és hatékony megoldás érdekében az adatkezelőnek rendelkeznie kell egy incidenskezelési tervvel, amely meghatározza az incidens feletti ellenőrzés átvételéhez szükséges gyors lépéseket. Ebben a konkrét esetben az incidens típusa kockázatnövelő tényező volt, mivel nemcsak az adatok bizalmas jellege sérült, hanem a behatolónak lehetősége volt változtatásokat is eszközölni a rendszerben, így az adatok sértetlensége is kérdésessé vált.

53. Az incidens által érintett személyes adatok jellegét, érzékenységét és mennyiségét kell értékelni annak megállapítása érdekében, hogy az incidens milyen mértékben érintette az érintetteket. Bár a személyes adatok különleges kategóriái nem érintettek, a hozzáfért adatok jelentős mennyiségű, az online űrlapokból származó információt tartalmaznak az egyénekről, és az ilyen adatokkal számos módon vissza lehet élni (kéretlen marketingüzenetekkel, személyazonosság-lopással stb.), így a következmények súlyossága növeli az érintettek jogaira és szabadságaira jelentett kockázatot[19].

3.1.2 05. sz. ESET – Mérséklés és kötelezettségek

54. Amennyiben lehetséges, a probléma megoldása után az adatbázist össze kell hasonlítani a biztonsági mentésben tárolt adatbázissal. Az incidensből származó tapasztalatokat fel kell használni az informatikai infrastruktúra frissítése során. Az adatkezelőnek valamennyi érintett informatikai rendszert vissza kell állítania az ismert tiszta állapotba, orvosolnia kell a sebezhetőséget, és a fájlintegritás-ellenőrzésekhez és biztonsági ellenőrzésekhez hasonló új biztonsági intézkedéseket kell bevezetnie a hasonló incidensek jövőbeni elkerülése érdekében. Ha a személyes adatokat nemcsak kiszivárogtatták, hanem törölték is, az adatkezelőnek szisztematikus intézkedéseket kell hoznia a személyes adatok incidens előtti állapotba való helyreállítása érdekében. Szükség lehet teljes biztonsági mentések vagy inkrementális módosítások alkalmazására, majd esetlegesen az utolsó inkrementális biztonsági mentés óta végzett adatkezelés újrafuttatására, ami megköveteli, hogy az adatkezelő képes legyen megismételni az utolsó biztonsági mentés óta végrehajtott módosításokat. Ehhez szükség lehet arra, hogy az adatkezelő úgy tervezze meg a rendszert, hogy a napi bemeneti fájlokat megőrizze arra az esetre, ha azokat újra fel kell dolgozni, és ehhez megbízható tárolási módszerre és megfelelő adatmegőrzési politikára van szükség.

55. A fentiek fényében, mivel az incidens valószínűleg magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az érintetteket mindenképpen tájékoztatni kell a történtekről (34. cikk (1) bekezdés), ami természetesen azt jelenti, hogy az érintett felügyeleti hatóságo(ka)t is be kell vonni az adatvédelmi incidensről szóló értesítés formájában. Az incidens nyilvántartása az általános adatvédelmi rendelet 33. cikk (5) bekezdésének megfelelően kötelező, ami megkönnyíti a helyzet értékelését.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	✓

[19] A *„valószínűsíthetően magas kockázattal járó”* adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

3.2 06. sz. ESET: Hasított jelszavak kiszivárgása egy honlapról

SQL Injection sebezhetőséget használtak ki egy főzéssel foglalkozó honlap szerverén lévő adatbázishoz való hozzáféréshez. A felhasználók csak tetszőleges álneveket választhattak felhasználónévként. Az e-mail-címek ilyen célú felhasználását nem támogatták. Az adatbázisban tárolt jelszavakat erős algoritmussal hasították, és a Salt nem sérült. Érintett adatok: 1 200 felhasználó hasított jelszava. A biztonság kedvéért az adatkezelő e-mailben tájékoztatta az érintetteket az incidensről, és arra kérte őket, hogy változtassák meg jelszavaikat, különösen, ha ugyanazt a jelszót használták más szolgáltatásokhoz is.

3.2.1 06. sz. ESET – Előzetes intézkedések és kockázatértékelés

56. Ebben a konkrét esetben az adatok bizalmas jellege sérül, de az adatbázisban lévő jelszavakat korszerű módszerrel hasították, ami a személyes adatok jellegét, érzékenységét és mennyiségét tekintve csökkenti a kockázatot. Ez az eset nem jelent kockázatot az érintettek jogaira és szabadságaira nézve.

57. Továbbá az érintettek kapcsolattartási adatai (pl. e-mail-címek vagy telefonszámok) nem kerültek veszélybe, ami azt jelenti, hogy nem áll fenn jelentős kockázata annak, hogy az érintettek csalási kísérletek célpontjává válnak (pl. adathalász e-mailek vagy csalárd szöveges üzenetek és telefonhívások). Az incidens a személyes adatok különleges kategóriáit nem érintette.

58. Egyes felhasználónevek személyes adatnak tekinthetők, de a honlap témája nem teszi lehetővé a negatív társításokat. Bár meg kell jegyezni, hogy a kockázatértékelés változhat[20], amennyiben a honlap típusa és a hozzáfért adatok a személyes adatok különleges kategóriáit tárhatják fel (pl. egy politikai párt vagy szakszervezet honlapja). A legkorszerűbb titkosítás alkalmazása enyhítheti az incidens hátrányos hatásait. A korlátozott számú bejelentkezési kísérlet engedélyezése megakadályozza a próbálgatásos bejelentkezési támadások sikerét, így nagymértékben csökkenti a felhasználóneveket már ismerő támadók által jelentett kockázatokat.

3.2.2 06. sz. ESET – Mérséklés és kötelezettségek

59. Az érintettek tájékoztatása bizonyos esetekben enyhítő tényezőnek tekinthető, mivel az érintettek is képesek arra, hogy megtegyék a szükséges lépéseket az incidensből származó további károk megakadályozása érdekében, például jelszavuk megváltoztatásával. Ebben az esetben az értesítés nem volt kötelező, de sok esetben bevált gyakorlatnak tekinthető.

60. Az adatkezelőnek ki kell javítania a sebezhetőséget, és új biztonsági intézkedéseket kell alkalmaznia a hasonló incidensek jövőbeni elkerülése érdekében, például a honlap szisztematikus biztonsági ellenőrzésére lehet szükség.

61. Az incidenst a 33. cikk (5) bekezdésével összhangban nyilván kell tartani, de nincs szükség bejelentésre vagy tájékoztatásra.

62. Erősen ajánlott továbbá, hogy a jelszavakat érintő incidensről minden esetben tájékoztassák az érintetteket, még akkor is, ha a jelszavakat a legkorszerűbb technológiát alkalmazó algoritmussal rendelkező salt-olt hash segítségével tárolták. A jelszavak szerveroldali kezelését elkerülő hitelesítési módszerek alkalmazását kell

[20] A „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

előnyben részesíteni. Az érintettek számára lehetővé kell tenni, hogy megtegyék a megfelelő intézkedéseket saját jelszavaik tekintetében.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	X	X

3.3 07. sz. ESET: A hitelesítő adatok kitöltésével végrehajtott támadás egy banki honlapon

Egy bank egyik online banki honlapja ellen kibertámadást intéztek. A támadás célja az volt, hogy egy rögzített triviális jelszó segítségével az összes lehetséges bejelentkezési felhasználói azonosítót felsorolják. A jelszavak 8 számjegyből állnak. A honlap egy sebezhető pontja miatt egyes esetekben az érintettekre vonatkozó információk (név, vezetéknév, nem, születési idő és hely, adóazonosító szám, felhasználói azonosító kódok) kiszivárogtak a támadóhoz, még akkor is, ha a használt jelszó nem volt helyes vagy a bankszámla már nem volt aktív. A támadásban mintegy 100 000 érintett volt. Ezek közül a támadó körülbelül 2 000 olyan fiókba jelentkezett be sikeresen, amelyek esetében a támadó által kipróbált triviális jelszót használták. Ennek megállapítását követően az adatkezelő képes volt az összes bejelentkezési kísérletet beazonosítani. Az adatkezelő meg tudta erősíteni, hogy a csalás elleni ellenőrzések alapján a támadás során nem hajtottak végre tranzakciókat ezekben a fiókokban. A bank azért volt tisztában az adatvédelmi incidenssel, mert biztonsági műveleti központja a honlapon intézett nagyszámú bejelentkezési kérelmet észlelt. Válaszul az adatkezelő kikapcsolta a honlapra való bejelentkezés lehetőségét, és a veszélyeztetett fiókok jelszavait visszaállította. Az adatkezelő az incidensről csak a veszélyeztetett fiókokkal rendelkező felhasználókat tájékoztatta, azaz azokat a felhasználókat, akiknek a jelszavát felfedték, vagy akiknek az adatait nyilvánosságra hozták.

3.3.1 07. sz. ESET – Előzetes intézkedések és kockázatértékelés

63. Fontos megemlíteni, hogy a rendkívül személyes jellegű adatokat[21] kezelő adatkezelők nagyobb felelősséget viselnek a megfelelő adatbiztonság biztosítása tekintetében, pl. biztonsági műveleti központ és egyéb incidensmegelőzési, -felderítési és -reagálási intézkedések megléte. E szigorúbb előírások be nem tartása minden bizonnyal súlyosabb intézkedéseket von maga után a felügyeleti hatóság vizsgálata során.

64. Az incidens a személyazonossági és felhasználói azonosító adatokon túl pénzügyi adatokat is érint, ami különösen súlyossá teszi az incidenst. Az érintett személyek száma magas.

65. Az, hogy ilyen érzékeny környezetben adatvédelmi incidens történhetett, az adatkezelő rendszerének jelentős adatbiztonsági hiányosságaira enged következtetni, és jelezheti azt az időpontot, amikor az általános adatvédelmi rendelet 24. cikkének (1) bekezdésével, 25. cikkének (1) bekezdésével és 32. cikkének (1) bekezdéséve összhangban „szükségessé” vált az érintett intézkedések felülvizsgálata és aktualizálása. A sérült adatok lehetővé teszik az érintettek egyedi azonosítását, és egyéb információkat is tartalmaznak róluk

[21] Például az érintettek által használt fizetési módokra vonatkozó információk, például kártyaszámok, bankszámlák, online fizetés, bérszámfejtések, bankszámlakivonatok, gazdasági tanulmányok vagy bármely más olyan információ, amely az érintettekre vonatkozó gazdasági információkat fedhet fel.

(ideértve a nemet, születési időt és helyet), továbbá a támadó felhasználhatja azokat az ügyfelek jelszavainak kitalálására vagy a bank ügyfelei ellen irányuló adathalász kampány lebonyolítására.

66. Ezen okok miatt úgy ítélték meg, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve[22]. Ezért az anyagi kár (pl. pénzügyi veszteség) és nem anyagi kár (pl. személyazonosság-lopás vagy csalás) bekövetkezése is elképzelhető.

3.3.2 07. sz. ESET – Mérséklés és kötelezettségek

67. Az adatkezelőnek az esetleírásban említett intézkedései megfelelőek. Az adatkezelő az incidenst követően kijavította a weboldal sebezhetőségét, és egyéb lépéseket is tett a hasonló jövőbeli adatvédelmi incidensek megelőzése érdekében, például kétfaktoros hitelesítéssel egészítette ki az érintett honlapot, és áttért az erős ügyfél-hitelesítésre.

68. Az incidensnek az általános adatvédelmi rendelet 33. cikkének (5) bekezdése szerinti nyilvántartása és a felügyeleti hatóság incidensről való értesítése ebben a forgatókönyvben nem opcionális. Az adatkezelőnek emellett az általános adatvédelmi rendelet 34. cikkének megfelelően értesítenie kell mind a 100 000 érintettet (ideértve azokat az érintetteket is, akiknek a fiókjai nem kerültek veszélybe).

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	✓

3.4 Szervezeti és technikai intézkedések a hackertámadások hatásainak megelőzésére/mérséklésére

69. Akárcsak a zsarolóvírus-támadások esetében, az informatikai biztonság újraértékelése a támadás kimenetelétől és következményeitől függetlenül kötelező az adatkezelők számára hasonló esetekben.

70. Ajánlott intézkedések[23]:

(Az alábbi intézkedések felsorolása semmiképpen sem kizárólagos vagy teljes körű. A cél inkább az, hogy a megelőzéssel kapcsolatban ötleteket és lehetséges megoldásokat biztosítson. Minden adatkezelési tevékenység eltérő, ezért az adatkezelőnek kell eldöntenie, hogy az adott helyzethez mely intézkedések illenek leginkább.)

- Korszerű titkosítás és kulcskezelés, különösen jelszavak, különleges vagy pénzügyi adatok feldolgozása esetén. A titkos információk (jelszavak) kriptográfiai hasítása és salting minden esetben előnyben részesül a jelszavak titkosításával szemben. A jelszavak szerveroldali feldolgozásának szükségességét elkerülő hitelesítési módszerek használatát előnyben részesítik.

- A rendszer naprakészen tartása (szoftver és firmware). Valamennyi informatikai biztonsági intézkedésről való gondoskodás, azok hatékonyságának biztosítása és rendszeres frissítése, ha az adatkezelés vagy a körülmények változnak vagy fejlődnek. Annak érdekében, hogy az általános adatvédelmi rendelet 5. cikk (2) bekezdésével összhangban igazolni lehessen az 5. cikk (1) bekezdése f) pontjának való megfelelést, az

[22] A „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

[23] A biztonságos webalkalmazás fejlesztése tekintetében lásd továbbá: https://www.owasp.org/index.php/Main_Page

adatkezelőnek nyilvántartást kell vezetnie valamennyi elvégzett frissítésről, ideértve azok alkalmazási időpontjait is.

- Erős hitelesítési módszerek, például kétfaktoros hitelesítés és hitelesítési szerverek használata, kiegészítve a jelszavakra vonatkozó naprakész politikával.
- A biztonságos fejlesztési előírások magukban foglalják a felhasználói bevitel szűrését (a lehetőségekhez mérten engedélyezőlistázással), a felhasználói bevitelek kikerülését és a próbálgatásos támadással való visszaélést megakadályozó intézkedéseket (például az újbóli próbálkozások maximális számának korlátozását). A „webalkalmazási tűzfalak" segíthetnek e technika hatékony alkalmazásában.
- Erős felhasználói jogosultságok és hozzáférés-szabályozási politika.
- Megfelelő, naprakész, hatékony és integrált tűzfal, behatolásérzékelő és egyéb behatolásvédelmi rendszerek használata.
- Rendszeres informatikai biztonsági ellenőrzések és sebezhetőségi értékelések (behatolási tesztelés).
- Rendszeres felülvizsgálat és tesztelés annak biztosítására, hogy a biztonsági mentések segítségével helyre lehessen állítani minden olyan adatot, amelynek integritását vagy rendelkezésre állását az incidens érintette.
- Nincs munkamenet-azonosító az URL-ben egyszerű szövegben.

4 EMBER OKOZTA BELSŐ KOCKÁZATI FORRÁS

71. Az emberi hiba adatvédelmi incidensekben betöltött szerepét ki kell emelni, mivel az gyakran előfordul. Mivel az ilyen típusú incidensek lehetnek szándékosak és nem szándékosak, az adatkezelőknek nagyon nehéz azonosítaniuk a sebezhetőségeket és intézkedéseket hozniuk azok elkerülésére. Az adatvédelmi és a magánélet védelmével foglalkozó biztosok nemzetközi konferenciája felismerte az ilyen emberi tényezők kezelésének fontosságát, és 2019 októberében állásfoglalást fogadott el az emberi hiba adatvédelmi incidensekben játszott szerepének kezeléséről[24]. Ezen állásfoglalás hangsúlyozza, hogy az emberi hibák megelőzése érdekében megfelelő védelmi intézkedéseket kell hozni, és nem kimerítő felsorolást nyújt az ilyen óvintézkedésekről és megközelítésekről.

4.1 08. sz. ESET: Üzleti adatok munkavállaló általi kiszivárogtatása

Egy vállalat munkavállalója felmondási ideje alatt üzleti adatokat másol ki a vállalati adatbázisból. A munkavállaló csak a munkaköri feladatai ellátása céljából jogosult hozzáférni az adatokhoz. Hónapokkal a felmondása után a munkavállaló az így szerzett adatokat (alapvető kapcsolattartási adatok) egy általa kezelt új adatkezelési rendszerbe viszi be annak érdekében, hogy felvegye a kapcsolatot a vállalat ügyfeleivel és új vállalkozásához csábítsa őket.

4.1.1 08. sz. ESET – Előzetes intézkedések és kockázatértékelés

72. Ebben a konkrét esetben nem hoztak előzetes intézkedéseket annak megakadályozására, hogy a munkavállaló lemásolja a vállalat ügyfeleinek kapcsolattartási adatait, mivel a munkavállaló munkaköri feladatainak elvégzéséhez jogszerűen hozzáférhetett – és hozzá is fért – ezekhez az információkhoz. Mivel a

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

legtöbb ügyfélkapcsolati munkakör betöltése megköveteli, hogy az alkalmazottak valamilyen módon hozzáférjenek a személyes adatokhoz, ezeket az adatvédelmi incidenseket a legnehezebb megelőzni. A hozzáférés körének limitálása korlátozhatja az adott munkavállaló által végezhető munkát. A jól átgondolt hozzáférési irányelvek és a folyamatos ellenőrzés ugyanakkor segíthet az ilyen incidensek megelőzésében.

73. A kockázatértékelés során szokás szerint figyelembe kell venni az incidens típusát és az érintett személyes adatok jellegét, érzékenységét és mennyiségét. Az ilyen típusú incidensek jellemzően titoksértések, mivel az adatbázis általában érintetlenül marad, tartalmát „csupán" lemásolják további felhasználás céljából. Az érintett adatok mennyisége általában szintén alacsony vagy közepes. Ebben a konkrét esetben a személyes adatok különleges kategóriái nem érintettek, a munkavállalónak kizárólag az ügyfelek elérhetőségi adataira volt szüksége, hogy a vállalattól való távozása után felvehesse velük a kapcsolatot. Ezért az érintett adatok nem minősülnek különleges adatoknak.

74. Bár előfordulhat, hogy az adatokat rosszhiszeműen lemásoló volt munkavállaló egyetlen célja az, hogy saját kereskedelmi céljai érdekében megszerezze a vállalat ügyfélkörének kapcsolattartási adatait, az adatkezelő nincs abban a helyzetben, hogy az érintettekre vonatkozó kockázatot alacsonynak tekintse, mivel az adatkezelő semmilyen megerősítéssel nem rendelkezik a munkavállaló szándékairól. Így, bár lehetséges, hogy az incidens következtében az érintettek csak a volt munkavállaló kéretlen önmarketingjének lesznek kitéve, nem zárható ki az ellopott adatokkal való további és súlyosabb visszaélés sem, attól függően, hogy a volt munkavállaló milyen céllal kezeli az adatokat[25].

4.1.2 08. sz. ESET – Mérséklés és kötelezettségek

75. Az incidens hátrányos hatásainak enyhítése a fenti esetben nehézségekbe ütközik. Lehetséges, hogy azonnali jogi lépéseket kell tenni annak érdekében, hogy a volt munkavállaló ne élhessen vissza az adatokkal és ne terjessze azokat tovább. Következő lépésként a hasonló jövőbeli helyzetek elkerülését kell célul kitűzni. Az adatkezelő megpróbálhatja felszólítani a volt munkavállalót, hogy hagyjon fel az adatok felhasználásával, de ezen intézkedés sikere a legjobb esetben is kétséges. Megfelelő technikai intézkedések, például az adatok másolásának vagy cserélhető eszközökre történő letöltésének lehetetlenné tétele segíthet.

76. Az ilyen típusú esetekre nincs „univerzális" megoldás, ugyanakkor a szisztematikus megközelítés segíthet megelőzésükben. A vállalat például mérlegelheti, hogy – amennyiben lehetséges – bizonyos hozzáférési módokat megvon a felmondási szándékukat jelző munkavállalóktól, vagy hozzáférési naplókat alkalmaz, hogy a nem kívánt hozzáférések naplózhatók és megjelölhetők legyenek. A munkavállalókkal aláírt szerződésnek tartalmaznia kell az ilyen intézkedéseket tiltó záradékokat.

77. Mindent egybevetve, mivel az adott incidens nem jár magas kockázattal a természetes személyek jogaira és szabadságaira nézve, elegendő a felügyeleti hatóság értesítése. Az érintettek tájékoztatása azonban az adatkezelő számára is előnyös lehet, hiszen jobb lehet, ha az érintettek nem a velük kapcsolatba lépni próbáló volt munkavállalótól, hanem a vállalattól értesülnek az adatszivárgásról. Az adatvédelmi incidenst a 33. cikk (5) bekezdésével összhangban nyilván kell tartani.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	X

[25] A „*valószínűsíthetően magas kockázattal járó*" adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

4.2 09. sz. ESET: Az adatok megbízható harmadik fél részére történő véletlen továbbítása

Egy biztosítási ügynök észrevette, hogy – egy e-mailben kapott Excel-fájl hibás beállításai következtében – két tucat olyan ügyféllel kapcsolatos információhoz férhetett hozzá, akik nem tartoztak a hatáskörébe. Az ügynököt szakmai titoktartási kötelezettség terheli, és ő volt az e-mail kizárólagos címzettje. Az adatkezelő és a biztosítási ügynök közötti megállapodás arra kötelezi az ügynököt, hogy indokolatlan késedelem nélkül jelezze az adatkezelőnek az adatvédelmi incidenst. Ezért az ügynök azonnal jelezte a hibát az adatkezelőnek, aki kijavította a fájlt, majd újra kiküldte azt, arra kérve az ügynököt, hogy törölje a korábbi üzenetet. A fent említett megállapodás értelmében az ügynöknek a törlést írásbeli nyilatkozatban kell megerősítenie, amit meg is tett. A megszerzett információk nem tartalmaznak különleges kategóriájú személyes adatokat, kizárólag kapcsolattartási adatokat és magára a biztosításra vonatkozó adatokat (biztosítási típus, összeg). Az incidens által érintett személyes adatok elemzését követően az adatkezelő nem állapított meg olyan különleges jellemzőket sem az egyének, sem az adatkezelő vonatkozásában, amelyek befolyásolhatnák az incidens hatásának mértékét.

4.2.1 09. sz. ESET – Előzetes intézkedések és kockázatértékelés

78. Ebben az esetben az incidens nem egy munkavállaló szándékos cselekedetéből, hanem egy figyelmetlenségből eredő, nem szándékos emberi hibából ered. Az ilyen jellegű incidensek elkerülhetők lehetnek, illetve gyakoriságuk csökkenthető a) olyan képzési, oktatási és tudatosságnövelő programok alkalmazásával, amelyek során a munkavállalók jobban megértik a személyes adatok védelmének fontosságát, b) az e-mailben történő fájlcsere csökkentésével, ami helyett például külön rendszereket lehet alkalmazni az ügyféladatok kezelésére, c) a fájlok küldés előtti kettős ellenőrzésével, d) a fájlok létrehozásának és elküldésének elkülönítésével.

79. Ez az adatvédelmi incidens kizárólag az adatok bizalmas jellegét érinti, azok integritása és hozzáférhetősége érintetlen marad. Az adatvédelmi incidens kizárólag mintegy két tucat ügyfelet érintett, ezért az érintett adatok mennyisége alacsonynak tekinthető. Továbbá az érintett személyes adatok nem tartalmaznak különleges adatokat. Kockázatcsökkentő tényezőnek tekinthető az is, hogy az adatfeldolgozó az adatvédelmi incidensről való tudomásszerzését követően azonnal felvette a kapcsolatot az adatkezelővel. (Annak lehetőségét is értékelni kell, hogy az adatokat más biztosítási ügynököknek is továbbíthatták, és amennyiben ez beigazolódik, megfelelő intézkedéseket kell tenni.) Az adatvédelmi incidens után tett megfelelő lépéseknek köszönhetően az adatvédelmi incidens valószínűleg nem lesz hatással az érintettek jogaira és szabadságaira nézve.

80. Az érintett személyek alacsony száma, az incidens azonnali észlelése és az incidens hatásainak minimalizálása érdekében hozott intézkedések együttesen biztosítják, hogy ez az eset nem jelent kockázatot.

4.2.2 09. sz. ESET – Mérséklés és kötelezettségek

81. Ezenkívül más kockázatcsökkentő körülmények is szerepet játszanak: az ügynököt szakmai titoktartási kötelezettség terheli; az ügynök maga jelentette a problémát az adatkezelőnek; és kérésre maga törölte a fájlt. A tudatosság növelése és a személyes adatokat tartalmazó dokumentumok ellenőrzésének esetleges további lépésekkel történő kiegészítése valószínűleg segíthet a hasonló esetek jövőbeni elkerülésében.

82. Az incidens 33. cikk (5) bekezdése szerinti nyilvántartásán kívül nincs szükség egyéb intézkedésre.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	X	X

4.3 Szervezeti és technikai intézkedések az ember okozta belső kockázati források hatásainak megelőzésére/mérséklésére

83. Az alábbiakban említett intézkedések kombinációja – az eset egyedi jellemzőitől függően alkalmazva – segíthet csökkenteni a hasonló incidens megismétlődésének esélyét.

84. Ajánlott intézkedések:

(Az alábbi intézkedések felsorolása semmiképpen sem kizárólagos vagy teljes körű. A cél inkább az, hogy a megelőzéssel kapcsolatban ötleteket és lehetséges megoldásokat biztosítson. Minden adatkezelési tevékenység eltérő, ezért az adatkezelőnek kell eldöntenie, hogy az adott helyzethez mely intézkedések illenek leginkább.)

- A munkavállalók számára a magánélet védelmére és biztonságára vonatkozó kötelezettségeikről, valamint a személyes adatok biztonságát fenyegető veszélyek észleléséről és bejelentéséről szóló képzés, oktatás és tudatosságnövelő programok rendszeres végrehajtása[26]. Tudatosságnövelő program kidolgozása, amely emlékezteti a munkavállalókat az adatvédelmi incidensekhez vezető leggyakoribb hibákra és azok elkerülésére.
- Erős és hatékony adatvédelmi és magánélet-védelmi gyakorlatok, eljárások és rendszerek kialakítása[27].
- Az adatvédelmi gyakorlatok, eljárások és rendszerek értékelése a folyamatos hatékonyság biztosítása érdekében[28].
- Megfelelő hozzáférés-szabályozási irányelvek kidolgozása és a felhasználók szabályok betartására való kötelezése.
- A felhasználók hitelesítését kikényszerítő technikák alkalmazása a különleges személyes adatokhoz való hozzáférés során.
- A felhasználó vállalati fiókjának letiltása, amint az adott személy elhagyja a vállalatot.
- A szokatlan adatáramlások ellenőrzése a fájlszerver és a dolgozói munkaállomások között.
- Az I/O-interfészek biztonságának beállítása a BIOS-ban vagy a számítógépes interfészek használatát ellenőrző szoftver használatával (pl. USB/CD/DVD stb. lezárása vagy feloldása).
- A munkavállalók hozzáférési politikájának felülvizsgálata (pl. A különleges adatokhoz való hozzáférés naplózása és a felhasználó kötelezése üzleti indok megadására, hogy ez az ellenőrzések során rendelkezésre álljon).
- A nyílt felhőszolgáltatások letiltása.

[26] Az állásfoglalás 2. szakaszának i. alszakasza az adatvédelmi incidensek során elkövetett emberi hiba szerepének kezelésére irányul.

[27] Az állásfoglalás 2. szakaszának ii. alszakasza az adatvédelmi incidensek során elkövetett emberi hiba szerepének kezelésére irányul.

[28] Az állásfoglalás 2. szakaszának iii. alszakasza az adatvédelmi incidensek során elkövetett emberi hiba szerepének kezelésére irányul.

- Az ismert nyílt levelezési szolgáltatásokhoz való hozzáférés megtiltása és megakadályozása.
- A képernyőnyomtatási funkció letiltása az operációs rendszerben.
- A tiszta asztal politika érvényesítése.
- Az összes számítógép automatizált zárolása bizonyos ideig tartó inaktivitás után.
- Különböző mechanizmusok (pl. [vezeték nélküli] token a bejelentkezéshez/zárolt fiókok megnyitásához) alkalmazása a felhasználók megosztott környezetben való gyors váltása érdekében.
- A személyes adatok kezeléséhez olyan külön rendszerek használata, amelyek megfelelő hozzáférés-ellenőrzési mechanizmusokat alkalmaznak, és amelyek megakadályozzák az emberi hibákat, például a nem a megfelelő személynek küldött üzenetek elküldését. A táblázatok és egyéb irodai dokumentumok használata nem megfelelő eszköz az ügyféladatok kezelésére.

5 ELVESZETT VAGY ELLOPOTT ESZKÖZÖK ÉS PAPÍRALAPÚ DOKUMENTUMOK

85. Gyakori eset a hordozható eszközök elvesztése vagy ellopása. Ezekben az esetekben az adatkezelőnek figyelembe kell vennie az adatkezelési művelet körülményeit, például az eszközön tárolt adatok típusát, valamint a támogató eszközöket és az incidenst megelőzően a megfelelő biztonsági szint biztosítása érdekében hozott intézkedéseket. Mindezek az elemek befolyásolják az adatvédelmi incidens lehetséges hatásait. A kockázatértékelés nehézségekbe ütközhet, mivel az eszköz már nem áll rendelkezésre.

86. Az ilyen jellegű incidensek mindig titoksértésnek minősíthetők. Ha azonban az ellopott adatbázisról nem történt biztonsági mentés, akkor az incidens típusa lehet hozzáférhetőségi adatsértés és sértetlenségi adatsértés is.

87. Az alábbi forgatókönyvek azt mutatják, hogy a fent említett körülmények hogyan befolyásolják az adatvédelmi incidens valószínűségét és súlyosságát.

5.1 10. sz. ESET: Titkosított személyes adatokat tároló ellopott anyagok

A gyermekek napközi otthonába való betörés során elloptak két táblagépet. A táblagépeken egy olyan alkalmazás volt, amely személyes adatokat tartalmazott a napközi otthonba járó gyermekekről. Név, születési dátum, a gyermekek oktatására vonatkozó személyes adatok voltak érintettek. A betörés idején kikapcsolt, kóddal védett táblagépeket és az alkalmazást is erős jelszó védte. A biztonsági mentés adatai hatékonyan és könnyen hozzáférhetők voltak az adatkezelő számára. Miután tudomást szerzett a betörésről, a napközi otthon távoli parancsot adott ki a táblagépek törlésére vonatkozóan nem sokkal a betörés felfedezése után.

5.1.1 10. sz. ESET – Előzetes intézkedések és kockázatértékelés

88. Ebben a konkrét esetben az adatkezelő megfelelő intézkedéseket tett az esetleges adatvédelmi incidens megelőzésére és hatásainak enyhítésére az eszköz titkosítása, a megfelelő jelszavas védelem alkalmazása és a táblagépeken tárolt adatok biztonsági mentésének biztosítása révén. (A javasolt intézkedések listája az 5.7. szakaszban található.)

89. Miután tudomást szerzett az adatvédelmi incidensről, az adatkezelőnek értékelnie kell a kockázatforrást, az adatkezelést támogató rendszereket, az érintett személyes adatok típusát és az adatvédelmi incidensnek az érintett személyekre gyakorolt esetleges hatásait. A fent leírt adatvédelmi incidens érinthette volna az

érintett adatok bizalmas jellegét, hozzáférhetőségét és integritását, azonban az adatkezelő által az adatvédelmi incidens előtt és után elvégzett megfelelő eljárásoknak köszönhetően ezek egyike sem következett be.

5.1.2 10. sz. ESET – Mérséklés és kötelezettségek

90. Az eszközökön lévő személyes adatok bizalmas jellege nem sérült, mivel mind a táblagépek, mind az alkalmazások erős jelszavas védelemmel voltak ellátva. A táblagépeket úgy állították be, hogy a jelszó beállítása egyben az eszközön lévő adatok titkosítását is jelenti. Ezt tovább fokozta az adatkezelő azon intézkedése, hogy az ellopott készülékekről távolról mindent megkísérelt letörölni.

91. A megtett intézkedéseknek köszönhetően az adatok bizalmas jellege is fennmaradt. Emellett a biztonsági mentés biztosította a személyes adatok folyamatos hozzáférhetőségét, így nem következhetett be semmilyen esetleges negatív hatás.

92. Mindezek miatt valószínűtlen, hogy a fent leírt adatvédelmi incidens kockázatot jelentett volna az érintettek jogaira és szabadságaira nézve, ezért nem volt szükség a felügyeleti hatóság vagy az érintettek értesítésére. Ugyanakkor ezt az adatvédelmi incidenst is nyilván kell tartani a 33. cikk (5) bekezdésével összhangban.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	X	X

5.2 11. sz. ESET: Nem titkosított személyes adatokat tároló ellopott anyagok

Egy szolgáltató vállalat alkalmazottjának elektronikus notebook-ját ellopták. Az ellopott noteszgép több mint 100 000 ügyfél keresztnevét, vezetéknevét, nemét, címét és születési dátumát tartalmazta. Az ellopott eszköz hozzáférhetetlensége miatt nem lehetett megállapítani, hogy a személyes adatok más kategóriái is érintettek-e. A noteszgép merevlemezéhez való hozzáférés nem volt jelszóval védve. A személyes adatokat a rendelkezésre álló napi biztonsági mentésekből helyre lehetett állítani.

5.2.1 11. sz. ESET – Előzetes intézkedések és kockázatértékelés

93. Az adatkezelő nem tett előzetes biztonsági intézkedéseket, így az ellopott noteszgépen tárolt személyes adatok könnyen hozzáférhetőek voltak a tolvaj vagy bármely más személy számára, aki a lopást követően a készülék birtokába került.

94. Az adatvédelmi incidens az ellopott eszközön tárolt adatok bizalmas jellegét érinti.

95. A személyes adatokat tartalmazó notebook ebben az esetben sebezhető volt, mivel nem rendelkezett jelszóvédelemmel vagy titkosítással. Az alapvető biztonsági intézkedések hiánya növeli az érintettek kockázati szintjét. Emellett az érintettek azonosítása is problémás, ami szintén növeli az adatvédelmi incidens súlyosságát. Az érintett személyek jelentős száma növeli a kockázatot, mindazonáltal az adatvédelmi incidens nem érintette a személyes adatok különleges kategóriáit.

96. A kockázatértékelés[29] során az adatkezelőnek figyelembe kell vennie a titoksértés lehetséges következményeit és hátrányos hatásait. Az incidens következtében az ellopott eszközön rendelkezésre álló adatokra támaszkodva személyazonossági csalást követhetnek el az érintettek ellen, így a kockázat magasnak tekinthető.

5.2.2 11. sz. ESET – Mérséklés és kötelezettségek

97. Az eszköz titkosításának bekapcsolása és a tárolt adatbázis erős jelszavas védelme megakadályozhatta volna, hogy az adatvédelmi incidens az érintettek jogait és szabadságait veszélyeztesse.

98. E körülmények miatt a felügyeleti hatóság értesítése szükséges, és az érintetteket is értesíteni kell.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	✓

5.3 12. sz. ESET: Különleges adatokat tartalmazó ellopott papíralapú dokumentumok

Egy kábítószer-függőséggel foglalkozó rehabilitációs intézményből elloptak egy papíralapú naplót. A napló a rehabilitációs intézménybe felvett betegek alapvető személyazonossági és egészségügyi adatait tartalmazta. Az adatokat kizárólag papíron tárolták, és a betegeket kezelő orvosok számára nem állt rendelkezésre biztonsági másolat. A könyvet nem zárt fiókban vagy szobában tárolták, az adatkezelő nem rendelkezett sem hozzáférés-ellenőrzési rendszerrel, sem más biztonsági intézkedéssel a papíralapú dokumentáció tekintetében.

5.3.1 12. sz. ESET – Előzetes intézkedések és kockázatértékelés

99. Az adatkezelő nem tett előzetes biztonsági intézkedéseket, így a naplóban tárolt személyes adatok könnyen hozzáférhetőek voltak a megtaláló számára. Ráadásul a naplóban tárolt személyes adatok jellege miatt a biztonsági mentés hiánya nagyon komoly kockázati tényező.

100. Ez az eset példaként szolgál a magas kockázatú adatvédelmi incidensre. A megfelelő biztonsági óvintézkedések elmulasztása miatt az általános adatvédelmi rendelet 9. cikkének (1) bekezdése szerinti különleges egészségügyi adatok vesztek el. Mivel ebben az esetben a személyes adatok különleges kategóriájáról volt szó, az érintettek potenciális kockázata megnövekedett, amit a kockázatot értékelő adatkezelőnek is figyelembe kell vennie[30].

101. Ez az incidens az érintett személyes adatok bizalmas jellegét, hozzáférhetőségét és integritását érinti. Az incidens következtében az orvosi titoktartás sérül, és jogosulatlan harmadik felek hozzáférést szerezhetnek a betegek személyes egészségügyi adataihoz, ami súlyos hatással lehet a betegek magánéletére. A hozzáférhetőségi adatsértés a betegek folyamatos kezelését is megzavarhatja. Mivel a napló egyes részeinek módosítása/törlése nem zárható ki, a személyes adatok integritása is sérül.

5.3.2 12. sz. ESET – Mérséklés és kötelezettségek

102. A védelmi intézkedések értékelése során figyelembe kell venni a támogató eszköz típusát is. Mivel a betegnapló fizikai dokumentum volt, védelmét az elektronikus eszközökhöz képest másképp kellett volna

[29] A „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

[30] A „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

megszervezni. A betegek nevének álnevesítésével, a könyv biztonságos helyiségben és zárt fiókban vagy szobában történő tárolásával, valamint a hozzáférés megfelelő, hitelesítéssel történő ellenőrzésével megelőzhető lett volna az adatvédelmi incidens.

103. A fent leírt adatvédelmi incidens súlyos következményekkel járhat az érintett érintettekre nézve; ezért a felügyeleti hatóság értesítése és az érintettek tájékoztatása kötelező.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	✓

5.4 Szervezeti és technikai intézkedések az eszközök elvesztése vagy ellopása által okozott hatások megelőzésére/mérséklésére

104. Az alábbiakban említett intézkedések kombinációja – az eset egyedi jellemzőitől függően alkalmazva – segíthet csökkenteni a hasonló incidens megismétlődésének esélyét.

105. Ajánlott intézkedések:

(Az alábbi intézkedések felsorolása semmiképpen sem kizárólagos vagy teljes körű. A cél inkább az, hogy a megelőzéssel kapcsolatban ötleteket és lehetséges megoldásokat biztosítson. Minden adatkezelési tevékenység eltérő, ezért az adatkezelőnek kell eldöntenie, hogy az adott helyzethez mely intézkedések illenek leginkább.)

- Kapcsolja be az eszköz titkosítását (például Bitlocker, Veracrypt vagy DM-Crypt).
- Használjon jelkódot/jelszót valamennyi eszközön. Titkosítson minden mobil elektronikus eszközt olyan módon, hogy a visszafejtéshez összetett jelszó megadása legyen szükséges.
- Alkalmazzon többfaktoros hitelesítést.
- Kapcsolja be a nagymértékben mobil eszközök olyan funkcióit, amelyek lehetővé teszik azok helyének meghatározását elvesztés vagy elkeveredés esetén.
- Használjon MDM (Mobile Devices Management – mobileszköz-kezelő) szoftvert/alkalmazást és lokalizációt. Használjon tükröződésgátló szűrőket. Zárjon le minden felügyelet nélkül hagyott eszközt.
- Amennyiben lehetséges és a szóban forgó adatkezelés szempontjából megfelelő, a személyes adatokat ne mobileszközön, hanem egy központi háttértár-kiszolgálón tárolja.
- Ha a munkaállomás a vállalati helyi hálózathoz csatlakozik, készítsen automatikus biztonsági mentést a munkamappákról, feltéve, hogy elkerülhetetlen, hogy személyes adatokat tároljanak ezekben
- Használjon biztonságos VPN-t (pl. amely a biztonságos kapcsolat létrehozásához külön második tényezős hitelesítési kulcsot kér) a mobileszközök és a háttértár-kiszolgálók összekapcsolásához.
- Biztosítson fizikai zárakat a munkavállalók számára, hogy lehetővé tegye számukra az általuk használt mobileszközök fizikai védelmét, amíg azok felügyelet nélkül maradnak.
- Szabályozza megfelelően az eszközök vállalaton kívüli használatát.
- Szabályozza megfelelően az eszközök vállalaton belüli használatát.
- Használjon MDM (Mobile Devices Management – mobileszköz-kezelő) szoftvert/alkalmazást és engedélyezze a távoli törlés funkciót.

- Alkalmazzon központosított eszközkezelőt, amelynek keretében a végfelhasználók minimális jogokkal bírnak a szoftverek telepítése tekintetében.
- Telepítsen fizikai hozzáférés-ellenőrzéseket.
- Kerülje a különleges információk mobileszközökön vagy merevlemezeken történő tárolását. Ha szükség van a vállalat belső rendszeréhez való hozzáférésre, a korábbiakban említettekhez hasonló biztonságos csatornákat kell használni.

6 TÉVES POSTÁZÁS

106. A kockázat forrása ebben az esetben is belső emberi hiba, de itt nem rosszindulatú cselekmény vezetett az incidenshez. Az incidenst figyelmetlenség okozta. A történtek után az adatkezelő keveset tud tenni, ezért a megelőzés ezekben az esetekben nagyobb jelentőséggel bír, mint más típusú incidensek esetében.

6.1 13. sz. ESET: Postai levelezésben elkövetett hiba

Egy kiskereskedelmi vállalat a rendelést követően elkészített két cipőcsomagot. Emberi hiba következtében összekeverték a számlákat a két csomagban, így mindkét terméket és a vonatkozó számlákat is rossz személynek küldték. Ez azt jelenti, hogy a vevők egymás megrendeléseit kapták meg, ideértve a személyes adatokat tartalmazó csomagolási számlákat is. Miután az adatkezelő tudomást szerzett az incidensről, visszahívta a megrendeléseket, és elküldte azokat a megfelelő címzetteknek.

6.1.1 13. sz. ESET – Előzetes intézkedések és kockázatértékelés

107. A számlák a sikeres szállításhoz szükséges személyes adatokat (név, cím, valamint a megvásárolt termék és annak ára) tartalmazták. Fontos megállapítani, hogyan történhetett az emberi hiba, és hogy miként lehetett volna azt valamilyen módon megelőzni. A leírt konkrét esetben a kockázat alacsony, mivel a személyes adatok olyan különleges kategóriái vagy olyan egyéb adatok nem érintettek, amelyekkel jelentős negatív következményekkel járó visszaélést lehetne elkövetni; az incidens nem az adatkezelő rendszerszintű hibájából ered, és csak két személy érintett. Nem állapítható meg egyénekre gyakorolt negatív hatás.

6.1.2 13. sz. ESET – Mérséklés és kötelezettségek

108. Az adatkezelőnek gondoskodnia kell az áruk és a kísérő számlák ingyenes visszaküldéséről, és fel kell kérnie a téves címzetteket, hogy a másik személy személyes adatait tartalmazó számlák valamennyi lehetséges példányát semmisítsék meg/töröljék.

109. Még ha maga az incidens nem is jelent magas kockázatot az érintett személyek jogaira és szabadságaira nézve, és így az általános adatvédelmi rendelet 34. cikke nem írja elő az érintettek tájékoztatását, az incidensről való tájékoztatásuk nem kerülhető el, mivel a kockázat mérsékléséhez szükség van az együttműködésükre.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	X	X

6.2 14. sz. ESET: Tévedésből postai úton elküldött, szigorúan bizalmas személyes adatok

Egy közigazgatási hivatal foglalkoztatási osztálya e-mail-üzenetet küldött a közelgő képzésekről a rendszerében álláskeresőként regisztrált személyeknek. Az e-mailhez tévedésből csatoltak egy dokumentumot, amely az álláskeresők személyes adatait (név, e-mail-cím, postacím, társadalombiztosítási szám) tartalmazta. Az érintett személyek száma több mint 60 000. Ezt követően a hivatal felvette a kapcsolatot az összes címzettel, és arra kérte őket, hogy töröljék az előző üzenetet, és ne használják fel az abban foglalt információkat.

6.2.1 14. sz. ESET – Előzetes intézkedések és kockázatértékelés

110. Szigorúbb szabályokat kellett volna bevezetni az ilyen üzenetek küldése tekintetében. További ellenőrzési mechanizmusok bevezetését kell mérlegelni.

111. Az érintett személyek száma jelentős, és a társadalombiztosítási számuk, valamint egyéb, alapvető személyes adataik érintettsége tovább növeli a kockázatot, amely magasnak tekinthető[31]. Az adatkezelő nem tudja megakadályozni az adatok címzettek általi esetleges terjesztését.

6.2.2 14. sz. ESET – Mérséklés és kötelezettségek

112. Mint korábban említettük, a hasonló incidensek kockázatainak hatékony csökkentésére szolgáló eszközök korlátozottak. Bár az adatkezelő kérte az üzenet törlését, nem kényszerítheti erre a címzetteket, és ennek következtében nem lehet biztos abban sem, hogy azok eleget tesznek a kérésnek.

113. Az alábbi három intézkedés végrehajtásának magától értetődőnek kell lennie egy ilyen esetben.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	✓

6.3 15. sz. ESET: Tévedésből levélben elküldött személyes adatok

Egy szállodában 5 napig tartó jogi angol tanfolyam résztvevőinek listáját tévedésből a szálloda helyett a tanfolyam 15 korábbi résztvevőjének küldték el. A lista a 15 résztvevő nevét, e-mail-címét és étkezési preferenciáit tartalmazza. Csak két résztvevő töltötte ki étkezési preferenciáit, és jelezte, hogy laktózérzékeny. Egyik résztvevő sem rendelkezik védett személyazonossággal. Az adatkezelő a lista elküldése után azonnal felfedezi a hibát, és tájékoztatja a címzetteket a hibáról, és felkéri őket a lista törlésére.

6.3.1 15. sz. ESET – Előzetes intézkedések és kockázatértékelés

114. Szigorú szabályokat kellett volna bevezetni a személyes adatokat tartalmazó üzenetek küldése tekintetében. További ellenőrzési mechanizmusok bevezetését kell mérlegelni.

115. A személyes adatok jellegéből, érzékenységéből, mennyiségéből és kontextusából eredő kockázatok alacsonyak. A személyes adatok két résztvevő étkezési preferenciáira vonatkozó különleges adatokat tartalmaznak. Bár a laktózérzékenység egészségügyi adatnak minősül, annak kockázata, hogy ezeket az

[31] A *„valószínűsíthetően magas kockázattal járó”* adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

adatokat káros módon használják fel, viszonylag alacsonynak tekinthető. Bár az egészségügyi adatok esetében általában feltételezhető, hogy az incidens valószínűleg magas kockázatot jelent az érintettre nézve[32], ebben a konkrét esetben nem azonosítható olyan kockázat, hogy az incidens a laktózérzékenységre vonatkozó információk jogosulatlan nyilvánosságra hozatala miatt az érintettnek fizikai, anyagi vagy nem anyagi kárt okozna. Néhány más étkezési preferenciával ellentétben a laktózérzékenység általában nem köthető vallási vagy világnézeti meggyőződéshez. A sérült adatok mennyisége és az érintettek száma is nagyon alacsony.

6.3.2 15. sz. ESET – Mérséklés és kötelezettségek

116. Összefoglalva megállapítható, hogy az incidensnek nem volt jelentős hatása az érintettekre. Kockázatcsökkentő tényezőnek tekinthető az is, hogy az adatkezelő a hibáról való tudomásszerzését követően azonnal felvette a kapcsolatot a címzettekkel.

117. Ha egy e-mailt téves/jogosulatlan címzettnek küldenek, ajánlott, hogy az adatkezelő titkos másolatban (Bcc) is küldjön egy utánkövető e-mailt a nem szándékos címzetteknek, amelyben elnézést kér, utasítja őket a hibás e-mail törlésére, továbbá tájékoztatja a címzetteket, hogy nem jogosultak a nem részükre megküldeni szánt e-mail-címek további használatára.

118. E tények miatt valószínűtlen, hogy a fent leírt adatvédelmi incidens kockázatot jelentett volna az érintettek jogaira és szabadságaira nézve, ezért nem volt szükség a felügyeleti hatóság vagy az érintettek értesítésére. Ugyanakkor ezt az adatvédelmi incidenst is nyilván kell tartani a 33. cikk (5) bekezdésével összhangban.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	X	X

6.4 16. sz. ESET: Postai levelezésben elkövetett hiba

Egy biztosítási csoport gépjármű-biztosításokat kínál. Ennek érdekében postai úton rendszeresen kiigazított biztosítási kötvényeket küld ügyfeleinek. A levél a kötvénytulajdonos neve és címe mellett tartalmazza a gépjármű kitakart számjegyek nélküli rendszámát, a folyó és a következő biztosítási év biztosítási díjait, a hozzávetőleges éves futásteljesítményt és a biztosított születési dátumát. Az általános adatvédelmi rendelet 9. cikke szerinti egészségügyi adatok, fizetési adatok (banki adatok), gazdasági és pénzügyi adatok nem szerepelnek a levélben.

A leveleket automatizált borítékoló gépek csomagolják. Műszaki hiba következtében két különböző kötvénytulajdonosnak szóló levelet helyeznek egy borítékba, amelyet egy kötvénytulajdonosnak küldenek el levélpostai úton. A kötvénytulajdonos otthon kinyitja a levelet, és megnézi a megfelelően kézbesített levelét, valamint a másik kötvénytulajdonos helytelenül kézbesített levelét.

6.4.1 16. sz. ESET – Előzetes intézkedések és kockázatértékelés

119. A helytelenül kézbesített levél tartalmazza a nevet, a címet, a születési dátumot, a gépjármű takaratlan rendszámát és a folyó és a következő évi biztosítási díj besorolását. Az érintett személyre gyakorolt hatások közepesnek tekintendők, mivel nyilvánosan nem hozzáférhető információk, mint a születési dátum vagy a gépjármű takaratlan rendszáma, illetve a biztosítási díjemelésre vonatkozó részletek jutnak a jogosulatlan címzett tudomására. Az adatokkal való visszaélés valószínűsége az értékelés alapján alacsony és közepes közötti. Bár számos címzett valószínűleg a szemétbe dobja a tévesen kapott levelet, egyedi esetekben nem

[32] Lásd: WP 250. számú iránymutatás, 23. o.

zárható ki teljes mértékben, hogy a levelet közösségi oldalakon teszik közzé, vagy felveszik a kapcsolatot a kötvénytulajdonossal.

6.4.2 16. sz. ESET – Mérséklés és kötelezettségek

120. Az adatkezelőnek saját költségén kell visszaküldenie az eredeti dokumentumot. A téves címzettet arról is tájékoztatni kell, hogy nem élhet vissza a kapott információval.

121. Valószínűleg soha nem lehet teljes mértékben megelőzni a postai kézbesítési hibát a teljesen automatizált gépekkel történő tömeges levelezés során. Megnövekedett gyakoriság esetén azonban ellenőrizni kell, hogy a borítékoló gépek kellően helyes mértékben vannak-e beállítva és karbantartva, vagy valamilyen más rendszerszintű probléma vezet-e ilyen incidenshez.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	X

6.5 Szervezeti és technikai intézkedések a téves postázás hatásainak megelőzésére/mérséklésére

122. Az alábbiakban említett intézkedések kombinációja – az eset egyedi jellemzőitől függően alkalmazva – segíthet csökkenteni a hasonló incidens megismétlődésének esélyét.

123. Ajánlott intézkedések:

(*Az alábbi intézkedések felsorolása semmiképpen sem kizárólagos vagy teljes körű. A cél inkább az, hogy a megelőzéssel kapcsolatban ötleteket és lehetséges megoldásokat biztosítson. Minden adatkezelési tevékenység eltérő, ezért az adatkezelőnek kell eldöntenie, hogy az adott helyzethez mely intézkedések illenek leginkább.*)

- A levelek/e-mailek küldésére vonatkozó pontos – értelmezésnek teret nem engedő – előírások meghatározása.
- Megfelelő képzés a személyzet számára a levelek/e-mailek küldésének módjáról.
- A több címzettnek küldött e-mailek esetében a címzettek alapértelmezés szerint a „bcc” (titkos másolat) mezőben való felsorolása.
- További megerősítés szükséges, ha az e-maileket több címzettnek küldik, és ezek nem a „bcc” (titkos másolat) mezőben vannak felsorolva.
- A négy szem elvének alkalmazása.
- Automatikus címzés a kézi címzés helyett, a rendelkezésre álló és naprakész adatbázisból nyert adatok alapján; az automatikus címzési rendszert rendszeresen felül kell vizsgálni a rejtett hibák és a helytelen beállítások ellenőrzése érdekében.
- Üzenetkésleltetés alkalmazása (pl. az üzenet a nyomógomb megnyomása után egy bizonyos időn belül törölhető/szerkeszthető).
- Az automatikus kitöltés letiltása az e-mail-címek beírásakor.
- Az adatvédelmi incidensekhez vezető leggyakoribb hibákról szóló tudatosságnövelő foglalkozások.
- Képzések és kézikönyvek a személyes adatok sérüléséhez vezető adatvédelmi incidensek kezeléséről és arról, hogy kinek kell tájékoztatást nyújtani (az adatvédelmi tisztviselő bevonása).

7 EGYÉB ESETEK – PSZICHOLÓGIAI MANIPULÁCIÓ (SOCIAL ENGINEERING)

7.1 17. sz. ESET: Személyazonosság-lopás

Egy távközlési vállalat ügyfélszolgálata telefonhívást fogad egy magát ügyfélnek kiadó személytől. Az állítólagos ügyfél azt kéri a cégtől, hogy változtassa meg azt az e-mail-címet, amelyre a továbbiakban a számlázási információkat küldi. Az ügyfélszolgálat munkatársa a vállalati eljárásokban meghatározottak szerint bizonyos személyes adatok bekérésével igazolja az ügyfél személyazonosságát. A hívó fél helyesen adja meg az ügyfél kért adószámát és postacímét (mivel hozzáférése volt ezekhez az elemekhez). Az érvényesítést követően az operátor elvégzi a kért módosítást, és ettől kezdve a számlázási információkat az új e-mail-címre küldik. Az eljárás nem írja elő a korábbi e-mail-kapcsolat értesítését. A következő hónapban a valódi ügyfél kapcsolatba lép a céggel, és érdeklődik, hogy miért nem kap számlákat az e-mail-címére, és tagadja, hogy bármilyen hívást kezdeményezett volna, amelyben az e-mail-elérhetőség megváltoztatását kérte volna. Később a vállalat felismeri, hogy az információkat egy jogosulatlan felhasználónak küldték el, és visszaállítja a módosítást.

7.1.1 17. sz. ESET – Kockázatértékelés, mérséklés és kötelezettségek

124. Ez az eset példaként szolgál az előzetes intézkedések fontosságára. Az incidens kockázati szempontból magas szintű kockázattal jár[33], mivel a számlázási adatok információval szolgálhatnak az érintett magánéletéről (pl. szokások, kapcsolatok), és anyagi károkat okozhatnak (pl. zaklatás, testi épség veszélyeztetése). Az e támadás során megszerzett személyes adatok felhasználhatók arra is, hogy megkönnyítsék az adott szervezetnél a fiókok átvételét, vagy más szervezeteknél további hitelesítési intézkedéseket foganatosítsanak. Figyelembe véve ezeket a kockázatokat, a „megfelelő” hitelesítési intézkedésnek magas mércének kell megfelelnie, attól függően, hogy a hitelesítés eredményeként milyen személyes adatok kezelhetők.

125. Ennek eredményeképpen az adatkezelőnek a felügyeleti hatóságot is értesítenie kell, és az érintettet is tájékoztatnia kell.

126. Az előzetes ügyfél-hitelesítési eljárást egyértelműen át kell dolgozni a jelen eset tükrében. A hitelesítésre alkalmazott módszerek nem voltak elégségesek. A rosszindulatú fél a nyilvánosan elérhető információk és az egyébként számára hozzáférhető információk segítségével képes volt a célfelhasználónak kiadni magát.

127. Az ilyen típusú statikus, tudásalapú hitelesítés (ahol a válasz nem változik, és az információ nem „titkos”, mint például jelszó esetén) használata nem ajánlott.

128. Ehelyett a szervezetnek olyan hitelesítési formát kellene alkalmaznia, amely nagymértékű biztonsággal képes garantálni, hogy a hitelesített felhasználó a kívánt személy, és nem akárki más. A problémát egy sávon kívüli többfaktoros hitelesítési módszer bevezetése oldaná meg, pl. a módosítási igény hitelesítésére egy megerősítési kérés küldésével a korábbi kapcsolattartónak; vagy kiegészítő kérdések hozzáadásával és

[33] A „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekkel kapcsolatos iránymutatás tekintetében lásd a fenti 10. lábjegyzetet.

kizárólag a korábbi számlákon látható információk megkövetelésével. Az adatkezelő felelőssége eldönteni, hogy milyen intézkedéseket vezet be, mivel ő ismeri legjobban a szervezet belső működésének részleteit és követelményeit.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	✓

7.2 18. sz. ESET: E-mail-kiszivárogtatás

Egy hipermarketlánc 3 hónappal a konfiguráció után észlelte, hogy néhány e-mail-fiókot megváltoztattak, és olyan szabályokat hoztak létre, hogy bizonyos kifejezéseket (pl. „számla”, „fizetés”, „banki átutalás”, „hitelkártya-hitelesítés”, „bankszámla adatai”) tartalmazó e-mailek egy nem használt mappába kerüljenek, továbbá egy külső e-mail-címre kerüljenek továbbításra. Emellett addigra már egy pszichológiai manipulációs támadást is végrehajtottak, azaz a magát szolgáltatónak kiadó támadó a szolgáltató bankszámlaadatait a sajátjára módosította. Végül, addigra már több hamis számlát is elküldtek, amelyek az új bankszámlaadatokat tartalmazták. Az e-mail-platform ellenőrző rendszere végül riasztást adott ki a mappákról. A vállalat nem tudta kideríteni, hogy a támadó hogyan tudott először hozzáférni az e-mail-fiókokhoz, de feltételezte, hogy egy fertőzött e-mail volt a hibás, amely hozzáférést adott a fizetésekért felelős felhasználói csoporthoz.

Az e-mailek kulcsszavas továbbítása miatt a támadó 99 munkavállalóról szerzett információkat: 89 érintettre vonatkozóan az adott hónap nevét és bérét; továbbá 10 olyan munkavállaló nevét, családi állapotát, gyermekeinek számát, bérét, munkaidejét és a bér felvételére vonatkozó többletinformációit, akiknek a szerződése megszűnt. Az adatkezelő kizárólag az utóbbi csoporthoz tartozó 10 munkavállalót értesítette.

7.2.1 18. sz. ESET – Kockázatértékelés, mérséklés és kötelezettségek

129. Még ha a támadó célja valószínűleg nem is a személyes adatok gyűjtése volt, mivel az incidens anyagi (pl. pénzügyi veszteség) és nem anyagi kárhoz (pl. személyazonosság-lopás vagy csalás) egyaránt vezethet, illetve az adatok felhasználhatók más támadások (pl. adathalászat) elősegítésére, az adatvédelmi incidens valószínűleg magas kockázatot jelent a természetes személyek jogaira és szabadságaira nézve. Ezért az incidensről mind a 99 munkavállalót tájékoztatni kell, és nem csak azt a 10 munkavállalót, akiknek a béradatai kiszivárogtak.

130. Miután tudomást szerzett az incidensről, az adatkezelő kikényszerítette a veszélyeztetett fiókok jelszavainak megváltoztatását, blokkolta az e-mailek támadó e-mail-fiókjára való küldését, értesítette a támadó által használt e-mail-szolgáltatóját a támadó tevékenységéről, eltávolította a támadó által létrehozott szabályokat, és finomította az ellenőrző rendszer riasztásait annak érdekében, hogy az automatikus szabályok létrehozatalakor riasztást adjon. Alternatív megoldásként az adatkezelő megszüntetheti a felhasználók jogát a továbbítási szabályok beállítására, amelyet csak kérésre, az informatikai szolgáltató csapat tehet meg, illetve bevezethet egy olyan előírást, amely szerint a felhasználóknak hetente egyszer, vagy a pénzügyi adatokat kezelő területeken gyakrabban ellenőrizniük és jelenteniük kell a fiókjaik vonatkozásában beállított szabályokat.

131. Az, hogy az incidens megtörténhetett és ilyen sokáig észrevétlen maradhatott, valamint az, hogy hosszabb időn keresztül lehetséges lett volna pszichológiai manipulációt alkalmazni további adatok megváltoztatására, jelentős problémákra világított rá az adatkezelő informatikai biztonsági rendszerében. E problémákat haladéktalanul orvosolni kell, például hangsúlyt kell fektetni az automatizálás felülvizsgálataira és a változás-

ellenőrzésekre, az incidensek észlelésére és a válaszintézkedésekre. A különleges adatokat, pénzügyi információkat stb. kezelő adatkezelőknek nagyobb a felelőssége a megfelelő adatbiztonság biztosítása tekintetében.

Az azonosított kockázatok alapján szükséges intézkedések		
Belső nyilvántartás	A felügyeleti hatóság értesítése	Az érintettek tájékoztatása
✓	✓	✓