Pokyny 01/2021

Příklady ohlašování případů porušení zabezpečení osobních údajů

Přijaté dne 14. prosince 2021

Verze 2.0

Historie verzí

Verze 2.0	14 12 2021	Přijetí pokynů po veřejné konzultaci
Verze 1.0	14 01 2021	Přijetí pokynů pro veřejnou konzultaci

Obsah

EVROPSKÝ SBOR PRO OCHRANU OSOBNÍCH ÚDAJŮ

s ohledem na čl. 70 odst. 1 písm. e) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“),

s ohledem na Dohodu o EHP, a zejména na její přílohu XI a protokol 37, ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018[1],

s ohledem na články 12 a 22 svého jednacího řádu,

s ohledem na sdělení Komise Evropskému parlamentu a Radě s názvem Ochrana osobních údajů jakožto pilíř posílení postavení občanů a přístup EU k digitální transformaci – dva roky uplatňování obecného nařízení o ochraně údajů[2],

PŘIJAL TYTO POKYNY:

1 ÚVOD

1. GDPR zavádí v určitých případech povinnost oznámit porušení zabezpečení osobních údajů příslušnému vnitrostátnímu dozorovému úřadu a informovat o něm fyzické osoby, jejichž osobních údajů se porušení týká (články 33 a 34).

2. Pracovní skupina zřízená podle článku 29 již v říjnu 2017 vypracovala *obecné* pokyny k ohlašování případů porušení zabezpečení osobních údajů, v nichž analyzovala příslušné oddíly GDPR (Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení 2016/679, WP 250, dále jen „pokyny WP250“)[3]. Vzhledem ke své povaze a době vzniku se však tyto pokyny nezabývaly všemi praktickými otázkami dostatečně podrobně. Proto vyvstala potřeba vypracovat *praktické* pokyny *vycházející z konkrétních případů*, které by využívaly zkušenosti, jež dozorové úřady získaly od doby, kdy GDPR vstoupilo v platnost.

3. Tento dokument, který odráží společné zkušenosti dozorových úřadů v EHP od doby, kdy začalo platit GDPR, má pokyny WP 250 doplnit. Jeho cílem je pomoci správcům údajů při rozhodování o tom, jak postupovat při porušení zabezpečení údajů a jaké faktory je třeba zohlednit při posuzování rizik.

[1] Odkazy na „členské státy“ v celém tomto dokumentu je třeba chápat jako odkazy na „členské státy EHP“.

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

[3] G29 WP250 rev.1, 6. února 2018, Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení 2016/679 – schválené Evropským sborem pro ochranu osobních údajů, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

4. V rámci jakéhokoli pokusu řešit porušení zabezpečení by měli být správce a zpracovatel nejprve schopni porušení zabezpečení rozpoznat. GDPR definuje „porušení zabezpečení osobních údajů“ v čl. 4 odst. 12 jako „porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů“.

5. Ve svém stanovisku 03/2014 k ohlašování případů porušení zabezpečení[4] a v pokynech WP 250 pracovní skupina zřízená podle článku 29 objasnila, že porušení lze kategorizovat podle následujících tří dobře známých zásad zabezpečení informací:

   - „porušení důvěrnosti“ – pokud dojde k neoprávněnému nebo náhodnému zveřejnění nebo zpřístupnění osobních údajů,
   - „porušení integrity“ – pokud dojde k neoprávněnému nebo náhodnému pozměnění osobních údajů,
   - „porušení dostupnosti“ – pokud dojde k náhodné nebo neoprávněné ztrátě přístupu k osobním údajům nebo k jejich zničení.[5]

6. Porušení může mít řadu významných nepříznivých dopadů na fyzické osoby, což může vést k fyzické, hmotné nebo nehmotné újmě. GDPR objasňuje, že to může zahrnovat ztrátu kontroly fyzických osob nad jejich osobními údaji, omezení jejich práv, diskriminaci, krádež či zneužití totožnosti, finanční ztrátu, neoprávněné zrušení pseudonymizace, poškození dobrého jména a ztrátu důvěrnosti osobních údajů chráněných služebním tajemstvím. Může to rovněž zahrnovat jakékoli jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob. Jednou z nejdůležitějších povinností správce údajů je vyhodnotit tato rizika pro práva a svobody subjektů údajů a zavést vhodná technická a organizační opatření k jejich odstranění.

7. V souladu s tím GDPR vyžaduje, aby správce:

   - dokumentoval veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření[6],
   - ohlásil případ porušení zabezpečení osobních údajů dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob[7],
   - oznámil případ porušení zabezpečení osobních údajů subjektu údajů, pokud je pravděpodobné, že toto porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob[8].

8. Porušení zabezpečení údajů je samo o sobě problémem, ale může být také příznakem zranitelného, případně zastaralého režimu zabezpečení údajů a může také naznačovat nedostatky systému, které je třeba

---

[4] G29 WP213, 25. března 2014, Stanovisko 03/2014 k oznamování případů porušení zabezpečení osobních údajů, s. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Viz pokyny WP 250, s. 7. – Je třeba vzít v úvahu, že porušení zabezpečení údajů se může týkat buď jedné kategorie, nebo více kategorií současně, případně může jít o kombinované porušení zabezpečení.

[6] Ustanovení čl. 33 odst. 5 GDPR.

[7] Ustanovení čl. 33 odst. 1 GDPR.

[8] Ustanovení čl. 34 odst. 1 GDPR.

řešit. Obecně platí, že je vždy lepší předcházet porušení zabezpečení údajů přípravou předem, protože některé jeho důsledky jsou ze své podstaty nevratné. Než může správce *plně* posoudit riziko vyplývající z porušení zabezpečení způsobeného nějakou formou útoku, je třeba identifikovat hlavní příčinu problému, aby bylo možné určit, zda stále existují zranitelnosti, které vedly k incidentu, a tudíž mohou být zneužity. V mnoha případech je správce schopen určit, že incident pravděpodobně povede k riziku, a proto má být ohlášen. V ostatních případech není nutné ohlášení odkládat až do úplného posouzení rizik a dopadů spojených s porušením zabezpečení, protože úplné posouzení rizik může probíhat souběžně s ohlášením a takto získané informace mohou být dozorovému úřadu poskytovány postupně bez zbytečného dalšího prodlení[9].

9. Porušení zabezpečení by mělo být ohlášeno, pokud se správce domnívá, že pravděpodobně povede k ohrožení práv a svobod subjektu údajů. Správci by měli toto posouzení provést v okamžiku, kdy se o porušení zabezpečení dozvědí. Správce by neměl čekat na podrobné forenzní zkoumání a (včasné) kroky ke zmírnění rizika, než posoudí, zda je pravděpodobné, že porušení zabezpečení údajů povede k riziku, a mělo by tedy být ohlášeno.

10. Pokud správce sám vyhodnotí riziko jako nepravděpodobné, ale ukáže se, že riziko existuje, může příslušný dozorový úřad využít svých nápravných pravomocí a může rozhodnout o sankcích.

11. Každý správce a zpracovatel by měl mít plány a postupy pro řešení případného porušení zabezpečení údajů. Organizace by měly mít jasně stanovené hierarchické linie a osoby odpovědné za určité aspekty procesu obnovy.

12. Rovněž je nezbytné, aby správci a zpracovatelé zajistili školení a informovanost o problematice ochrany osobních údajů pro své zaměstnance se zaměřením na řízení případů porušení zabezpečení osobních údajů (identifikace incidentu spojeného s porušením zabezpečení osobních údajů a další opatření, která je třeba přijmout, atd.). Toto školení by se mělo pravidelně opakovat v závislosti na typu činnosti zpracování a velikosti správce a mělo by se zabývat nejnovějšími trendy a upozorněními na kybernetické útoky nebo jiné bezpečnostní incidenty.

13. Zásada odpovědnosti a koncepce záměrné ochrany osobních údajů by mohly zahrnovat analýzu, která se promítne do vlastní „Příručky pro řešení případů porušení zabezpečení osobních údajů“ správce a zpracovatele údajů, jejímž cílem je stanovit fakta pro každý aspekt zpracování v každé hlavní fázi operace. Taková předem připravená příručka by byla mnohem rychlejším zdrojem informací, které by správcům a zpracovatelům údajů umožnily zmírnit rizika a splnit povinnosti bez zbytečného odkladu. Zajistilo by to, aby v případě porušení zabezpečení osobních údajů lidé v organizaci věděli, co mají dělat, takže by incident byl s velkou pravděpodobností vyřešen rychleji, než kdyby žádná zmírňující opatření nebo plán neexistovaly.

14. Ačkoli jsou níže uvedené případy fiktivní, vycházejí z typických případů ze společných zkušeností dozorových úřadů s ohlašováním porušení zabezpečení údajů. Nabízené analýzy se výslovně týkají zkoumaných případů, ale jejich cílem je poskytnout správcům údajů pomoc při posuzování jejich vlastních případů porušení ochrany údajů. Jakákoli změna okolností níže popsaných případů může mít za následek jinou nebo významnější úroveň rizika, což vyžaduje odlišná nebo dodatečná opatření. V těchto pokynech jsou případy rozděleny podle určitých kategorií porušení zabezpečení (např. útoky pomocí softwaru s požadavkem na výkupné, tzv. ransomwarové útoky). Při řešení určité kategorie porušení zabezpečení jsou v každém případě požadována určitá zmírňující opatření. Tato opatření nemusí být nutně opakována u každé analýzy případů

[9] Ustanovení čl. 33 odst. 4 GDPR.

patřících do stejné kategorie porušení zabezpečení. U případů spadajících do stejné kategorie jsou uvedeny pouze rozdíly. Čtenář by si proto měl přečíst všechny případy týkající se příslušné kategorie porušení zabezpečení, aby zjistil a rozlišil všechna správná opatření, která je třeba přijmout.

15. Interní dokumentace případu porušení zabezpečení je povinnost nezávislá na rizicích spojených s porušením zabezpečení a musí být provedena v každém případě. Níže uvedené případy se snaží objasnit, zda je třeba případ porušení zabezpečení oznámit dozorovému úřadu a informovat dotčené subjekty údajů.

2 RANSOMWARE

16. Častou příčinou ohlášení porušení zabezpečení údajů je ransomwarový útok na správce údajů. V těchto případech škodlivý kód zašifruje osobní údaje, načež útočník požaduje po správci výkupné výměnou za dešifrovací kód. Tento druh útoku lze obvykle klasifikovat jako porušení dostupnosti, ale často může dojít i k porušení důvěrnosti.

2.1 PŘÍPAD č. 01: Ransomware s řádným zálohováním a bez exfiltrace

Na počítačové systémy malé výrobní společnosti byl proveden ransomwarový útok a data uložená v těchto systémech byla zašifrována. Správce údajů používal šifrování v klidu (encryption at rest), takže všechna data, ke kterým ransomware získal přístup, byla uložena v zašifrované podobě pomocí nejmodernějšího šifrovacího algoritmu. Dešifrovací klíč nebyl při útoku kompromitován, tj. útočník se k němu nemohl dostat ani ho nepřímo použít. Útočník tak měl přístup pouze k zašifrovaným osobním údajům. Zejména nebyl zasažen e-mailový systém společnosti ani klientské systémy, které k němu přistupovaly. Společnost využívá k prošetření incidentu odborné služby externí společnosti zabývající se kybernetickou bezpečností. K dispozici jsou protokoly zaznamenávající všechny datové toky odcházející ze společnosti (včetně odchozích e-mailů). Po analýze protokolů a dat shromážděných detekčními systémy, které společnost používá, interní vyšetřování za podpory externí společnosti zabývající se kybernetickou bezpečností s *jistotou* určilo, že pachatel data pouze zašifroval, aniž by je exfiltroval. Záznamy neukazují žádný odchozí tok dat v době útoku. Osobní údaje, kterých se porušení zabezpečení dotklo, se týkají klientů a zaměstnanců společnosti, celkem několika desítek osob. Záloha byla snadno dostupná a data byla obnovena několik hodin po útoku. Porušení nemělo žádné důsledky pro běžný provoz správce. Nedošlo k žádnému zpoždění při vyplácení zaměstnanců ani při vyřizování žádostí klientů.

17. V tomto případě byly z definice „porušení zabezpečení osobních údajů“ realizovány následující prvky: porušení zabezpečení vedlo k protiprávním změnám a neoprávněnému přístupu k uloženým osobním údajům.

2.1.1 PŘÍPAD č. 01 – Předběžná opatření a posouzení rizik

18. Stejně jako u všech rizik představovaných externími subjekty lze pravděpodobnost úspěšného ransomwarového útoku výrazně snížit zpřísněním zabezpečení prostředí pro správu dat. Většině těchto porušení zabezpečení lze zabránit zajištěním vhodných organizačních, fyzických a technologických bezpečnostních opatření. Příkladem takových opatření je řádné změnové řízení (patch management) a používání vhodného systému detekce malwaru. Správné a oddělené zálohování pomůže zmírnit důsledky úspěšného útoku, pokud k němu dojde. Navíc program vzdělávání, školení a zvyšování informovanosti zaměstnanců (SETA) v oblasti zabezpečení pomůže tomuto druhu útoku předcházet a rozpoznat jej. (Seznam doporučených opatření je uveden v oddíle 2.5.) Mezi těmito opatřeními je nejdůležitější řádné změnové řízení, které zajišťuje aktuálnost systémů a opravu všech známých zranitelností nasazených systémů, protože většina ransomwarových útoků využívá známé zranitelnosti.

19. Při posuzování rizik by měl správce prošetřit porušení zabezpečení a určit typ škodlivého kódu, aby pochopil možné důsledky útoku. Mezi tato rizika, která je třeba zvážit, patří riziko, že data byla exfiltrována, aniž by byla zanechána stopa v protokolech systémů.

20. V tomto příkladu měl útočník přístup k osobním údajům a byla ohrožena důvěrnost šifrovaného textu obsahujícího osobní údaje v zašifrované podobě. Žádná data, která mohla být exfiltrována, však pachatel nemůže přečíst ani použít, alespoň prozatím. Technika šifrování používaná správcem údajů je v souladu s nejnovějšími poznatky. Dešifrovací klíč nebyl prozrazen a pravděpodobně jej nebylo možné zjistit ani jinými prostředky. V důsledku toho jsou rizika v oblasti důvěrnosti u práv a svobod fyzických osob snížena na minimum, pokud nedojde ke kryptoanalytickému pokroku, který v budoucnu umožní přečíst zašifrované údaje.

21. Správce údajů by měl zvážit riziko pro fyzické osoby v důsledku porušení zabezpečení[10]. V tomto případě se zdá, že rizika pro práva a svobody subjektů údajů vyplývají z nedostupnosti osobních údajů a důvěrnost osobních údajů není ohrožena[11]. V tomto příkladu byly nepříznivé účinky porušení zabezpečení zmírněny poměrně brzy poté, co k narušení došlo. Vhodný režim zálohování[12] zmírňuje následky porušení zabezpečení a v tomto případě jej správce dokázal účinně využít.

22. Pokud jde o závažnost důsledků pro subjekty údajů, bylo možné identifikovat pouze mírné důsledky, protože dotčené údaje byly obnoveny během několika hodin, porušení zabezpečení nemělo žádné důsledky pro běžný provoz správce a nemělo žádný významný dopad na subjekty údajů (např. platby zaměstnancům nebo vyřizování žádostí klientů).

2.1.2 PŘÍPAD č. 01 – Zmírnění a povinnosti

23. Bez zálohy může správce provést jen málo opatření k nápravě ztráty osobních údajů a údaje musí být shromážděny znovu. V tomto konkrétním případě však bylo možné dopady útoku účinně omezit obnovením všech napadených systémů do čistého stavu, o němž bylo známo, že neobsahuje škodlivý kód, opravou zranitelností a obnovením dotčených dat brzy po útoku. Bez zálohování dochází ke ztrátě dat a může se zvýšit závažnost, protože může dojít i k rizikům nebo dopadům na jednotlivce.

24. Klíčovou proměnnou při analýze porušení zabezpečení je včasnost efektivní obnovy dat ze snadno dostupné zálohy. Stanovení vhodného časového rámce pro obnovu ohrožených dat závisí na jedinečných okolnostech

---

[10] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz pracovní skupina zřízená podle článku 29 „Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely 2016/679“, WP248 rev. 01, – schváleno Evropským sborem pro ochranu osobních údajů, https://ec.europa.eu/newsroom/article29/items/611236, s. 9.

[11] Technicky vzato, šifrování dat zahrnuje „přístup“ k původním datům a v případě ransomwaru i odstranění původních dat – k zašifrování a odstranění původních dat potřebuje ransomwarový kód získat přístup k datům. Útočník může před smazáním pořídit kopii originálu, ale ne vždy získá osobní údaje. V průběhu vyšetřování správce údajů se mohou objevit nové informace, které toto posouzení změní. Přístup, který vede k protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí osobních údajů nebo k riziku v oblasti zabezpečení pro subjekt údajů, a to i bez interpretace údajů, může být stejně závažný jako přístup s interpretací osobních údajů.

[12] Zálohovací postupy by měly být strukturované, konzistentní a opakovatelné. Příkladem zálohovacích postupů je metoda 3-2-1 a metoda dědeček-otec-syn. Každá metoda by měla být vždy testována z hlediska účinnosti při pokrytí a při obnově dat. Testování by se také mělo opakovat v určitých intervalech a zejména při změnách v operaci zpracování nebo jejích okolnostech, aby byla zajištěna integrita systému.

konkrétního případu porušení zabezpečení. GDPR stanoví, že porušení zabezpečení osobních údajů musí být ohlášeno bez zbytečného odkladu a pokud možno do 72 hodin. Lze tedy konstatovat, že překročení 72hodinové lhůty není vhodné v žádném případě, ale při řešení případů s vysokou mírou rizika lze i dodržení této lhůty považovat za neuspokojivé.

25. V tomto případě správce po podrobném posouzení dopadů a procesu reakce na incident rozhodl, že je nepravděpodobné, že by porušení zabezpečení vedlo k ohrožení práv a svobod fyzických osob, a proto není nutné informovat subjekty údajů, a porušení zabezpečení ani nevyžaduje ohlášení dozorovému úřadu. Stejně jako všechna porušení zabezpečení údajů by však mělo být zdokumentováno v souladu s čl. 33 odst. 5. Rovněž může být potřebné (nebo to později bude dozorový úřad vyžadovat), aby organizace aktualizovala a napravila svá organizační a technická opatření a postupy pro zabezpečení osobních údajů a zmírnění rizik. V rámci této aktualizace a nápravy by organizace měla porušení zabezpečení důkladně prošetřit a zjistit příčiny a metody, které pachatel použil, aby se v budoucnu podobným událostem zabránilo.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	X	X

2.2 PŘÍPAD č. 02: Ransomware bez řádného zálohování

Na jeden z počítačů používaných zemědělskou společností byl proveden ransomwarový útok a data v počítači byla útočníkem zašifrována. Společnost využívá k monitorování své sítě odborné služby externí společnosti zabývající se kybernetickou bezpečností. K dispozici jsou protokoly zaznamenávající všechny datové toky odcházející ze společnosti (včetně odchozích e-mailů). Po analýze protokolů a dat, které shromáždily ostatní detekční systémy, interní vyšetřování za pomoci společnosti zabývající se kybernetickou bezpečností zjistilo, že pachatel data pouze zašifroval, ale neexfiltroval je. Záznamy neukazují žádný odchozí tok dat v době útoku. Osobní údaje, kterých se porušení zabezpečení dotklo, se týkají zaměstnanců a klientů společnosti, celkem několika desítek osob. Nebyly zasaženy žádné zvláštní kategorie údajů. K dispozici nebyla žádná záloha v elektronické podobě. Většina dat byla obnovena z papírových záloh. Obnova dat trvala pět pracovních dnů a vedla k drobným zpožděním v doručování objednávek zákazníkům.

2.2.1 PŘÍPAD č. 02 – Předběžná opatření a posouzení rizik

26. Správce údajů by měl přijmout stejná předběžná opatření, která jsou uvedena v části 2.1 a v oddíle 2.9. Hlavním rozdílem oproti předchozímu případu je absence elektronické zálohy a absence šifrování v klidu. To vede k zásadním rozdílům v následujících krocích.

27. Při posuzování rizik by měl správce prošetřit metodu infiltrace a určit typ škodlivého kódu, aby pochopil možné důsledky útoku. V tomto příkladu ransomware zašifroval osobní údaje, aniž by je exfiltroval. Zdá se tedy, že rizika pro práva a svobody subjektů údajů vyplývají z nedostupnosti osobních údajů a důvěrnost osobních údajů není ohrožena. Při určování rizika je nezbytné důkladně prozkoumat protokoly brány firewall a zvážit, co z jejich obsahu vyplývá. Správce údajů by měl na požádání předložit faktická zjištění těchto šetření.

28. Správce údajů musí mít na paměti, že pokud je útok sofistikovanější, má škodlivý software funkci pro úpravu souborů protokolu a odstranění stop. Vzhledem k tomu, že protokoly nejsou předávány ani replikovány na centrální server protokolů, nemůže správce údajů ani po důkladném šetření, při němž bylo zjištěno, že útočník osobní údaje neexfiltroval, tvrdit, že neexistence záznamu v protokolu dokazuje neexistenci exfiltrace, a proto nelze pravděpodobnost porušení důvěrnosti zcela vyloučit.

29. Správce údajů by měl posoudit rizika tohoto porušení zabezpečení[13], pokud útočník získal přístup k údajům. Při posuzování rizik by správce údajů měl rovněž zohlednit povahu, citlivost, objem a kontext osobních údajů, kterých se porušení zabezpečení týká. V tomto případě nejsou dotčeny žádné zvláštní kategorie osobních údajů a množství údajů, u nichž došlo k porušení zabezpečení, a počet dotčených subjektů údajů je nízký.

30. Shromáždění přesných informací o neoprávněném přístupu je klíčové pro určení úrovně rizika a zabránění novému nebo pokračujícímu útoku. Pokud by data byla zkopírována z databáze, zjevně by to představovalo faktor zvyšující riziko. Když si nejste jisti konkrétními okolnostmi neoprávněného přístupu, je třeba zvážit horší variantu a podle toho vyhodnotit riziko.

31. Absenci záložní databáze lze považovat za faktor zvyšující riziko v závislosti na závažnosti důsledků pro subjekty údajů, které vyplývají z nedostupnosti údajů.

2.2.2 PŘÍPAD č. 02 – Zmírnění a povinnosti

32. Bez zálohy může správce provést jen málo opatření k nápravě ztráty osobních údajů a údaje musí být shromážděny znovu, pokud není k dispozici jiný zdroj (např. e-maily s potvrzením objednávky). Bez zálohování může dojít ke ztrátě dat, jejíž závažnost závisí na dopadu na jednotlivce.

33. Obnovení údajů by nemělo být příliš problematické[14], pokud jsou údaje stále k dispozici v tištěné podobě, ale vzhledem k neexistenci elektronické záložní databáze je ohlášení dozorovému úřadu považováno za nezbytné, protože obnovení údajů trvalo určitou dobu a mohlo způsobit určité zpoždění v doručování objednávek zákazníkům, přičemž se mohlo stát, že nebylo možné obnovit značné množství metadat (např. protokoly, časová razítka).

34. Informování subjektů údajů o porušení zabezpečení může záviset také na délce doby, po kterou nejsou osobní údaje k dispozici, a na obtížích, které by to mohlo způsobit v provozu správce (např. zpoždění při převodu výplat zaměstnanců). Vzhledem k tomu, že tato zpoždění v platbách a dodávkách mohou vést k finančním ztrátám pro osoby, jejichž údaje byly ohroženy, lze také tvrdit, že porušení zabezpečení pravděpodobně vede k vysokému riziku. Neinformovat subjekty údajů nemusí být rovněž možné, pokud je k obnovení zašifrovaných údajů potřebný jejich příspěvek.

35. Tento případ slouží jako příklad ransomwarového útoku, který představuje riziko pro práva a svobody subjektů údajů, ale nedosahuje vysokého rizika. Měl by být zdokumentován v souladu s čl. 33 odst. 5 a oznámen dozorovému úřadu v souladu s čl. 33 odst. 1. Rovněž může být potřebné (nebo to bude dozorový úřad vyžadovat), aby organizace aktualizovala a napravila svá organizační a technická opatření a postupy pro zabezpečení osobních údajů a zmírnění rizik.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	X

[13] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz poznámka pod čarou 10 výše.

[14] Toto bude záviset na složitosti a struktuře osobních údajů. V nejsložitějších scénářích může obnovení integrity dat, konzistence s metadaty, zajištění správných vztahů v rámci datových struktur a kontrola přesnosti dat vyžadovat značné zdroje a úsilí.

2.3 PŘÍPAD č. 03: Ransomware se zálohováním a bez exfiltrace v nemocnici

Informační systém nemocnice / zdravotnického střediska byl vystaven ransomwarovému útoku a útočník zašifroval značnou část dat. Společnost využívá k monitorování své sítě odborné služby externí společnosti zabývající se kybernetickou bezpečností. K dispozici jsou protokoly zaznamenávající všechny datové toky odcházející ze společnosti (včetně odchozích e-mailů). Po analýze protokolů a dat, které shromáždily ostatní detekční systémy, interní vyšetřování za pomoci společnosti zabývající se kybernetickou bezpečností zjistilo, že pachatel data pouze zašifroval, ale neexfiltroval je. Záznamy neukazují žádný odchozí tok dat v době útoku. Osobní údaje, kterých se porušení zabezpečení dotklo, se týkají zaměstnanců a pacientů, což představuje tisíce osob. K dispozici byly zálohy v elektronické podobě. Většinu dat se podařilo obnovit, ale tato operace trvala dva pracovní dny a vedla k velkým zpožděním v léčbě pacientů, přičemž byly zrušeny/odloženy operace, a ke snížení úrovně služeb z důvodu nedostupnosti systémů.

2.3.1 PŘÍPAD č. 03 – Předběžná opatření a posouzení rizik

36. Správce údajů by měl přijmout stejná předběžná opatření, která jsou uvedena v části 2.1 a v oddíle 2.5. Hlavním rozdílem oproti předchozímu případu je vysoká závažnost důsledků pro podstatnou část subjektů údajů[15].

37. Množství údajů, u nichž došlo k porušení zabezpečení, a počet dotčených subjektů údajů jsou vysoké, protože nemocnice obvykle zpracovávají velké množství údajů. Nedostupnost údajů má velký dopad na podstatnou část subjektů údajů. Kromě toho existuje zbytkové riziko vysoké závažnosti pro důvěrnost údajů o pacientech.

38. Důležitý je typ porušení zabezpečení, povaha, citlivost a objem osobních údajů, kterých se porušení týká. Přestože existovala záloha údajů a bylo možné je obnovit během několika dní, stále existuje vysoké riziko vzhledem k závažnosti následků pro subjekty údajů, které vyplývají z nedostupnosti údajů v okamžiku útoku a v následujících dnech.

2.3.2 PŘÍPAD č. 03 – Zmírnění a povinnosti

39. Ohlášení dozorovému úřadu se považuje za nezbytné, protože se jedná o zvláštní kategorie osobních údajů a obnova údajů by mohla trvat dlouhou dobu, což by mohlo vést k významným zpožděním v péči o pacienty. Informování subjektů údajů o narušení bezpečnosti je nezbytné vzhledem k dopadu na pacienty, a to i po obnovení zašifrovaných údajů. Údaje o všech pacientech ošetřených v nemocnici v posledních letech byly zašifrovány a ovlivněny byly pouze údaje o těch pacientech, kteří měli být v nemocnici ošetřeni v době, kdy

[15] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz poznámka pod čarou 10 výše.

byl počítačový systém nedostupný. Správce by měl porušení zabezpečení údajů oznámit přímo těmto pacientům. Přímé informování ostatních pacientů, z nichž někteří nebyli v nemocnici déle než dvacet let, nemusí být nutné vzhledem k výjimce v čl. 34 odst. 3 písm. c). V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení[16] nebo podobného opatření. V tomto případě by nemocnice měla ransomwarový útok a jeho následky zveřejnit.

40. Tento případ slouží jako příklad ransomwarového útoku s vysokým rizikem pro práva a svobody subjektů údajů. Měl by být zdokumentován v souladu s čl. 33 odst. 5, oznámen dozorovému úřadu v souladu s čl. 33 odst. 1 a sdělen subjektům údajů v souladu s čl. 34 odst. 1. Organizace musí rovněž aktualizovat a napravit svá organizační a technická opatření a postupy pro zabezpečení osobních údajů a zmírnění rizik.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	✓

2.4 PŘÍPAD č. 04: Ransomware bez zálohování a s exfiltrací

Server dopravního podniku byl vystaven ransomwarovému útoku a útočník zašifroval jeho data. Podle zjištění interního vyšetřování pachatel data nejen zašifroval, ale také exfiltroval. Narušeny byly osobní údaje klientů a zaměstnanců a několika tisíc osob, které využívaly služeb společnosti (např. nákup jízdenek online). Kromě základních údajů o totožnosti se porušení zabezpečení týká i čísel průkazů totožnosti a finančních údajů, jako jsou údaje o kreditních kartách. Záložní databáze existovala, ale útočník ji rovněž zašifroval.

2.4.1 PŘÍPAD č. 04 – Předběžná opatření a posouzení rizik

41. Správce údajů by měl přijmout stejná předběžná opatření, která jsou uvedena v části 2.1 a v oddíle 2.5. Ačkoli byla k dispozici záloha, byla útokem také zasažena. Již toto uspořádání vyvolává pochybnosti o kvalitě předchozích bezpečnostních opatření správce IT a mělo by být během vyšetřování dále prověřeno, protože v dobře navrženém režimu zálohování musí být více záloh bezpečně uloženo bez přístupu z hlavního systému, jinak by mohly být ohroženy při stejném útoku. Ransomwarové útoky navíc mohou zůstat neodhaleny několik dní a pomalu zašifrovávat data používaná jen zřídka. Může se tak stát, že vícenásobné zálohování nebude mít žádný význam, a proto by se zálohy měly provádět pravidelně a měly by být izolované. Tím by se zvýšila pravděpodobnost obnovy, i když s větší ztrátou dat.

[16] V 86. bodě odůvodnění GDPR se vysvětluje, že *„tato oznámení by měla být subjektům údajů učiněna, jakmile je to proveditelné, v úzké spolupráci s dozorovým úřadem a v souladu s pokyny tohoto úřadu nebo jiných příslušných orgánů (například donucovacích orgánů). Například v případě potřeby zmírnit bezprostřední riziko způsobení újmy je nutné tuto skutečnost subjektům údajů neprodleně oznámit, zatímco v situaci, kdy je zapotřebí zavést vhodná opatření s cílem zabránit tomu, aby porušení zabezpečení osobních údajů pokračovalo nebo aby docházelo k podobným případům porušení, může být opodstatněna delší lhůta“*.

42. Toto porušení zabezpečení se týká nejen dostupnosti dat, ale také jejich důvěrnosti, protože útočník mohl data ze serveru změnit a/nebo zkopírovat. Z toho vyplývá, že tento typ porušení zabezpečení má za následek vysoké riziko[17].

43. Povaha, citlivost a objem osobních údajů tato rizika dále zvyšují, protože počet dotčených osob je vysoký, stejně jako celkové množství dotčených osobních údajů. Kromě základních údajů o totožnosti se jedná také o doklady totožnosti a finanční údaje, jako jsou údaje o kreditních kartách. Porušení zabezpečení těchto typů údajů představuje vysoké riziko samo o sobě, a pokud jsou údaje zpracovávány společně, mohou být mimo jiné zneužity ke krádeži či zneužití totožnosti.

44. Kvůli chybné logice serveru nebo chybnému organizačnímu řízení byly ransomwarem ovlivněny záložní soubory, což znemožnilo obnovení dat a zvýšilo riziko.

45. Toto porušení zabezpečení údajů představuje vysoké riziko pro práva a svobody jednotlivců, protože by pravděpodobně mohlo vést jak k hmotné (např. finanční ztrátě, protože byly zasaženy údaje o kreditních kartách), tak k nehmotné újmě (např. krádeži či zneužití totožnosti, protože byly zasaženy údaje o průkazech totožnosti).

2.4.2 PŘÍPAD č. 04 – Zmírnění a povinnosti

46. Zásadní je komunikace se subjekty údajů, aby mohly podniknout nezbytné kroky k zamezení hmotné újmy (např. zablokovat své kreditní karty).

47. Kromě zdokumentování porušení podle čl. 33 odst. 5 je v tomto případě povinné také ohlášení dozorovému úřadu (čl. 33 odst. 1) a správce je rovněž povinen oznámit porušení zabezpečení subjektům údajů (čl. 34 odst. 1). Oznámení by mohlo být provedeno individuálně, ale v případě fyzických osob, u nichž nejsou kontaktní údaje k dispozici, by tak měl správce učinit veřejně, přičemž by takové sdělení nemělo mít pro subjekty údajů další negativní důsledky, např. prostřednictvím oznámení na webových stránkách podniku. V druhém případě je nutné přesné a jasné sdělení na viditelném místě na domovské stránce správce s přesnými odkazy na příslušná ustanovení GDPR. Rovněž může být potřebné, aby organizace aktualizovala a napravila svá organizační a technická opatření a postupy pro zabezpečení osobních údajů a zmírnění rizik.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	✓

2.5 Organizační a technická opatření pro prevenci / zmírnění dopadů ransomwarových útoků

48. Skutečnost, že mohlo dojít k ransomwarovému útoku, je obvykle známkou jedné nebo několika zranitelností v systému správce. Platí to i pro případy ransomwaru, kdy byly osobní údaje zašifrovány, ale nebyly exfiltrovány. Bez ohledu na výsledek a důsledky útoku nelze dostatečně zdůraznit význam komplexního hodnocení systému zabezpečení dat – se zvláštním důrazem na bezpečnost IT. Zjištěné nedostatky a bezpečnostní slabiny je třeba zdokumentovat a neprodleně řešit.

49. Doporučená opatření:

[17] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz poznámka pod čarou 10 výše.

(Výčet následujících opatření není v žádném případě výlučný ani úplný. Cílem je spíše poskytnout náměty na prevenci a možná řešení. Každá činnost zpracování je jiná, a proto by měl správce rozhodnout, která opatření se pro danou situaci hodí nejlépe.)

- Udržování firmwaru, operačního systému a aplikačního softwaru na serverech, klientských počítačích, aktivních síťových komponentách a všech ostatních počítačích ve stejné síti LAN (včetně zařízení Wi-Fi) v aktuálním stavu. Zajištění vhodných bezpečnostních opatření IT, jejich účinnosti a jejich pravidelné aktualizace v případě změny či vývoje zpracování nebo okolností. Zahrnuje to vedení podrobných protokolů o tom, které opravy a v jakém časovém okamžiku byly použity.
- Navrhování a organizace systémů zpracování a infrastruktury pro segmentaci nebo izolaci datových systémů a sítí, aby se zabránilo šíření malwaru v rámci organizace a do externích systémů.
- Existence aktuálního, bezpečného a testovaného postupu zálohování. Média pro střednědobé a dlouhodobé zálohování by měla být uložena odděleně od provozních datových úložišť a mimo dosah třetích stran, a to i v případě úspěšného útoku (např. denní přírůstkové zálohování a týdenní plné zálohování).
- Mít / pořídit vhodný, aktuální, účinný a integrovaný software proti škodlivému softwaru.
- Mít vhodný, aktuální, účinný a integrovaný firewall a systém detekce a prevence narušení. Směrování síťového provozu přes firewall/detekci narušení, a to i v případě domácí kanceláře nebo mobilní práce (např. pomocí připojení VPN k organizačním bezpečnostním mechanismům při přístupu na internet).
- Školení zaměstnanců o metodách rozpoznávání a prevence IT útoků. Správce by měl poskytnout prostředky pro zjištění, zda jsou e-maily a zprávy získané jinými komunikačními prostředky autentické a důvěryhodné. Zaměstnanci by měli být proškoleni, aby rozpoznali, že k takovému útoku došlo, aby věděli jak vyřadit koncový bod ze sítě, a že jsou povinni okamžitě útok nahlásit bezpečnostnímu pracovníkovi.
- Zdůrazněte potřebu identifikace typu škodlivého kódu, abyste viděli důsledky útoku a mohli najít správná opatření ke zmírnění rizika. V případě, že se ransomwarový útok podařil a není k dispozici žádná záloha, lze k získání dat použít dostupné nástroje, například nástroje projektu „no more ransom“ (nomoreransom.org). Pokud však máte k dispozici bezpečnou zálohu, doporučujeme obnovit data z ní.
- Předávání nebo replikace všech protokolů na centrální server protokolů (případně včetně podepisování nebo kryptografického časového razítkování záznamů protokolů).
- Silné šifrování a vícefaktorové ověřování, zejména pro administrativní přístup k IT systémům, vhodná správa klíčů a hesel.
- Pravidelné testování zranitelnosti a penetrace.
- Založte v rámci organizace skupinu pro reakce na počítačové bezpečnostní incidenty (CSIRT) nebo skupinu pro reakce na počítačové hrozby (CERT), případně společnou skupinu CSIRT/CERT. Vytvořte plán reakce na incidenty, plán obnovy po havárii a záložní postup a zajistěte, aby byly důkladně otestovány.
- Při posuzování protiopatření je třeba přezkoumat, otestovat a aktualizovat analýzu rizik.

3 ÚTOKY S EXFILTRACÍ DAT

50. Útoky, které zneužívají zranitelnosti služeb nabízených správcem třetím stranám prostřednictvím internetu, např. útoky typu injection (např. SQL injection, path traversal), kompromitace webových stránek a podobné metody, se mohou podobat ransomwarovým útokům, protože riziko plyne z činnosti neoprávněné třetí strany, ale tyto útoky obvykle směřují ke kopírování, exfiltraci a zneužití osobních údajů k určitému škodlivému účelu. Jedná se tedy především o porušení důvěrnosti a případně také integrity dat. Zároveň platí, že pokud si je správce vědom charakteristik tohoto druhu porušení zabezpečení, má k dispozici řadu opatření, která mohou riziko úspěšného provedení útoku podstatně snížit.

3.1 PŘÍPAD č. 05: Exfiltrace dat z webových stránek pro uchazeče o zaměstnání

Agentura práce se stala obětí kybernetického útoku, při kterém byl na její webové stránky umístěn škodlivý kód. Tento škodlivý kód zpřístupnil neoprávněným osobám osobní údaje zadané prostřednictvím online formulářů poptávky po zaměstnání a uložené na webovém serveru. Postiženo mohlo být 213 takových formulářů, po analýze dotčených údajů bylo zjištěno, že porušením zabezpečení nebyly dotčeny žádné zvláštní kategorie údajů. Konkrétní nainstalovaná sada nástrojů malwaru měla funkce, které útočníkovi umožnily odstranit veškerou historii exfiltrace a také umožnily sledovat zpracování na serveru a zachytit osobní údaje. Tato sada nástrojů byla odhalena až měsíc po

3.1.1 PŘÍPAD č. 05 – Předběžná opatření a posouzení rizik

51. Bezpečnost prostředí správce údajů je nesmírně důležitá, protože většině těchto porušení zabezpečení lze zabránit tím, že se zajistí průběžná aktualizace všech systémů, šifrování citlivých údajů a vývoj aplikací podle vysokých bezpečnostních standardů, jako je silné ověřování, opatření proti útokům hrubou silou, „únik“ nebo „sanitace“[18] uživatelských vstupů atd. Pravidelné audity bezpečnosti IT, hodnocení zranitelností a penetrační testy jsou rovněž nutné k tomu, aby bylo možné tyto druhy zranitelností včas odhalit a opravit. V tomto konkrétním případě mohly nástroje pro sledování integrity souborů v produkčním prostředí pomoci odhalit injektáž kódu. (Seznam doporučených opatření je uveden v oddíle 3.7).

52. Správce by měl vždy začít vyšetřovat porušení zabezpečení tak, že určí typ útoku a jeho metody, aby mohl posoudit, jaká opatření je třeba přijmout. Aby byl postup rychlý a účinný, měl by mít správce údajů k dispozici plán reakce na incident, který stanoví rychlé a nezbytné kroky k převzetí kontroly nad incidentem. V tomto konkrétním případě byl typ porušení zabezpečení faktorem zvyšujícím riziko, protože byla nejen narušena důvěrnost údajů, ale infiltrátor měl také prostředky k tomu, aby provedl změny v systému, což zpochybňuje i integritu údajů.

53. Měla by být posouzena povaha, citlivost a objem osobních údajů, kterých se porušení zabezpečení týká, aby bylo možné určit, do jaké míry se porušení dotklo subjektů údajů. Ačkoli nebyly dotčeny žádné zvláštní kategorie osobních údajů, zpřístupněné údaje obsahují značné množství informací o fyzických osobách z

[18] Únik nebo sanitace uživatelských vstupů je forma validace vstupů, která zajišťuje, aby byla do informačního systému zadávána pouze správně formátovaná data.

online formulářů a tyto údaje by mohly být zneužity různými způsoby (jako cíl nevyžádané reklamy, krádež totožnosti atd.), takže závažnost důsledků by měla zvyšovat riziko pro práva a svobody subjektů údajů[19].

3.1.2 PŘÍPAD č. 05 – Zmírnění a povinnosti

54. Pokud je to možné, je třeba po vyřešení problému porovnat databázi s databází uloženou v zabezpečené záloze. Zkušenosti získané z porušení zabezpečení by měly být využity při aktualizaci infrastruktury IT. Správce údajů by měl uvést všechny dotčené IT systémy do známého čistého stavu, odstranit zranitelnost a zavést nová bezpečnostní opatření, aby v budoucnu nedocházelo k podobným porušením zabezpečení údajů, např. kontroly integrity souborů a bezpečnostní audity. Pokud došlo nejen k exfiltraci osobních údajů, ale také k jejich vymazání, musí správce přijmout systematická opatření k obnovení osobních údajů do stavu, v jakém byly před porušením zabezpečení. Může být nutné použít úplné zálohy, přírůstkové změny a poté případně znovu spustit zpracování od poslední přírůstkové zálohy – což vyžaduje, aby správce dokázal replikovat změny provedené od poslední zálohy. Správce by musel mít systém navržený tak, aby uchovával denní vstupní soubory pro případ, že je bude třeba znovu zpracovat, a je nutný robustní způsob ukládání a vhodná politika uchovávání.

55. Jelikož je pravděpodobné, že porušení povede k vysokému riziku pro práva a svobody fyzických osob, vzhledem k výše uvedenému by o něm měly být v každém případě informovány subjekty údajů (čl. 34 odst. 1), což samozřejmě znamená, že informován by měl být i příslušný dozorový úřad (dozorové úřady) formou ohlášení porušení zabezpečení údajů. Zdokumentování porušení je povinné podle čl. 33 odst. 5 GDPR a usnadňuje posouzení situace.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	✓

3.2 PŘÍPAD č. 06: Exfiltrace zašifrovaného hesla z webové stránky

K získání přístupu do databáze serveru webové stránky věnované vaření byla zneužita zranitelnost pomocí injektáže SQL. Uživatelé si mohli jako uživatelská jména zvolit pouze libovolné pseudonymy. Bylo doporučeno, aby se pro tento účel nepoužívaly e-mailové adresy. Hesla uložená v databázi byla zašifrována silným algoritmem a nebyla narušena kryptografická „sůl“. Dotčené údaje: zašifrovaná hesla 1 200 uživatelů. Správce z bezpečnostních důvodů informoval subjekty údajů o porušení zabezpečení e-mailem a požádal je, aby si změnili hesla, zejména pokud stejné heslo používali i pro

3.2.1 PŘÍPAD č. 06 – Předběžná opatření a posouzení rizik

56. V tomto konkrétním případě je důvěrnost údajů ohrožena, ale hesla v databázi byla zašifrována aktuální metodou, což snižuje riziko s ohledem na povahu, citlivost a objem osobních údajů. Tento případ nepředstavuje žádné riziko pro práva a svobody subjektů údajů.

[19] Pokyny k operacím zpracování, které *„pravděpodobně budou mít za následek vysoké riziko“*, viz poznámka pod čarou 10 výše.

57. Kromě toho nebyly ohroženy žádné kontaktní údaje (např. e-mailové adresy nebo telefonní čísla) subjektů údajů, což znamená, že neexistuje žádné významné riziko, že by se subjekty údajů staly terčem pokusů o podvod (např. obdržení podvodných e-mailů nebo podvodných textových zpráv a telefonátů). Nejednalo se o žádné zvláštní kategorie osobních údajů.

58. Některá uživatelská jména by mohla být považována za osobní údaje, ale předmět webu neumožňuje negativní konotace. Je však třeba poznamenat, že posouzení rizik se může změnit[20], pokud by typ webových stránek a zpřístupněná data mohly odhalit zvláštní kategorie osobních údajů (např. webové stránky politické strany nebo odborové organizace). Použití nejmodernějšího šifrování by mohlo zmírnit nepříznivé účinky narušení. Zajištění, aby byl počet pokusů o přihlášení omezen, zabrání úspěšným útokům hrubou silou, čímž se do značné míry sníží rizika způsobená útočníky, kteří již znají uživatelská jména.

3.2.2 PŘÍPAD č. 06 – Zmírnění a povinnosti

59. Informování subjektů údajů by v některých případech mohlo být považováno za zmírňující faktor, protože i subjekty údajů mohou učinit nezbytná opatření, aby zabránily další újmě způsobené porušením zabezpečení, například změnou hesla. V tomto případě nebylo informování povinné, ale v mnoha případech jej lze považovat za správnou praxi.

60. Správce údajů by měl zranitelnost odstranit a zavést nová bezpečnostní opatření, aby se předešlo podobným porušením zabezpečení údajů v budoucnu, například systematické bezpečnostní audity webových stránek.

61. Porušení zabezpečení by mělo být zdokumentováno v souladu s čl. 33 odst. 5, ale není třeba žádné ohlašování ani informování.

62. Rovněž se důrazně doporučuje v každém případě informovat o narušení hesla subjekty údajů, a to i v případě, že hesla byla uložena pomocí „osoleného hashe“ (salted hash) s algoritmem odpovídajícím nejnovějším poznatkům. Je vhodnější používat metody ověřování, které nevyžadují nutnost zpracovávat hesla na straně serveru. Subjekty údajů by měly mít možnost zvolit si vhodná opatření týkající se jejich vlastních hesel.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	X	X

3.3 PŘÍPAD č. 07: Útok na bankovní webové stránky pomocí přihlašovacích údajů (credential stuffing)

[20] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz poznámka pod čarou 10 výše.

Na banku byl proveden kybernetický útok na jedné z jejích stránek internetového bankovnictví. Cílem útoku byl výčet všech možných přihlašovacích uživatelských ID pomocí stanoveného triviálního hesla. Hesla se skládají z osmi číslic. V důsledku zranitelnosti webové stránky došlo v některých případech k úniku informací o subjektech údajů (jméno, příjmení, pohlaví, datum a místo narození, daňové identifikační číslo, identifikační kódy uživatelů) k útočníkovi, a to i v případě, že použité heslo nebylo správné nebo bankovní účet již nebyl aktivní. Týkalo se to přibližně 100 000 subjektů údajů. Pomocí uniklých informací se útočník úspěšně přihlásil ke zhruba 2 000 účtům, které používaly triviální heslo, které útočník zkusil. Správce dokázal následně identifikovat všechny neoprávněné pokusy o přihlášení. Správce údajů mohl potvrdit, že podle kontrol proti podvodům nebyly během útoku na těchto účtech provedeny žádné transakce. Banka o porušení zabezpečení dat věděla, protože její bezpečnostní středisko zjistilo vysoký počet žádostí o přihlášení směřujících na webovou stránku. V reakci na to správce zrušil možnost přihlášení na webovou stránku jejím vypnutím a vynutil si obnovení hesel napadených účtů. Správce o narušení informoval pouze uživatele s ohroženými účty, tj. uživatele, jejichž hesla byla ohrožena nebo jejichž údaje unikly.

3.3.1 PŘÍPAD č. 07 – Předběžná opatření a posouzení rizik

63. Je důležité uvést, že správci, kteří nakládají s údaji vysoce osobní povahy[21], mají větší odpovědnost, pokud jde o zajištění odpovídajícího zabezpečení údajů, např. mají mít bezpečnostní středisko a další opatření pro prevenci, odhalování a reakci na incidenty. Nedodržení těchto vyšších standardů bude mít nepochybně za následek závažnější opatření při vyšetřování vedeném dozorovým úřadem.

64. Porušení zabezpečení se týká nejen finančních údajů, ale i informací o totožnosti a identifikačních údajů uživatele, což je obzvláště závažné. Počet postižených osob je vysoký.

65. Skutečnost, že k porušení zabezpečení mohlo dojít v takto citlivém prostředí, poukazuje na významné mezery v zabezpečení údajů v systému správce a může ukazovat, že nastal čas, kdy je „nezbytné“ přezkoumat a aktualizovat dotčená opatření v souladu s čl. 24 odst. 1, čl. 25 odst. 1 a čl. 32 odst. 1 GDPR. Uniklé údaje umožňují jedinečnou identifikaci subjektů údajů a obsahují další informace o nich (včetně pohlaví, data a místa narození), navíc je útočník může využít k uhodnutí hesla zákazníků nebo k provedení spear phishingové kampaně zaměřené na zákazníky banky.

66. Z uvedených důvodů bylo toto porušení zabezpečení údajů považováno za porušení, které pravděpodobně povede k vysokému riziku pro práva a svobody všech dotčených subjektů údajů[22]. Proto lze předpokládat vznik hmotné (např. finanční ztráty) i nehmotné újmy (např. krádeže či zneužití totožnosti).

3.3.2 PŘÍPAD č. 07 – Zmírnění a povinnosti

67. Opatření správce uvedená v popisu případu jsou přiměřená. V návaznosti na toto porušení zabezpečení banka také opravila zranitelnost webových stránek a přijala další opatření, která mají podobným porušením

[21] Například informace subjektů údajů týkající se platebních metod, jako jsou čísla karet, bankovní účty, online platby, výplatní pásky, bankovní výpisy, ekonomické studie nebo jakékoli jiné informace, které mohou odhalit ekonomické údaje týkající se subjektů údajů.

[22] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz poznámka pod čarou 10 výše.

zabezpečení dat v budoucnu zabránit, například přidala na dotčené webové stránky dvoufaktorové ověřování a přešla na silné ověřování zákazníků.

68. Zdokumentování porušení podle čl. 33 odst. 5 GDPR a jeho ohlášení dozorovému úřadu není v tomto případě dobrovolné. Dále by měl správce v souladu s článkem 34 GDPR informovat všech 100 000 subjektů údajů (včetně subjektů údajů, jejichž účty nebyly ohroženy).

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	✓

3.4 Organizační a technická opatření pro prevenci / zmírnění dopadů hackerských útoků

69. Stejně jako v případě ransomwarových útoků, bez ohledu na výsledek a následky útoku, je v podobných případech pro správce povinné přehodnotit zabezpečení IT.

70. Doporučená opatření:[23]

(Výčet následujících opatření není v žádném případě výlučný ani úplný. Cílem je spíše poskytnout náměty na prevenci a možná řešení. Každá činnost zpracování je jiná, a proto by měl správce rozhodnout, která opatření se pro danou situaci hodí nejlépe.)

- Nejmodernější šifrování a správa klíčů, zejména při zpracování hesel, citlivých nebo finančních údajů. Před šifrováním hesel se vždy upřednostňuje kryptografické hashování a „solení“ tajných informací (hesel). Výhodnější je používat metody ověřování, které odstraňují nutnost zpracovávat hesla na straně serveru.
- Udržování systému v aktuálním stavu (software a firmware). Zajištění všech bezpečnostních opatření IT, jejich účinnosti a jejich pravidelné aktualizace v případě změny nebo vývoje zpracování nebo okolností. Aby bylo možné prokázat dodržení ustanovení čl. 5 odst. 1 písm. f) v souladu s čl. 5 odst. 2 nařízení GDPR, měl by správce vést záznamy o všech provedených aktualizacích, včetně doby jejich provedení.
- Používání silných metod ověřování, jako je dvoufaktorové ověřování a ověřovací servery, doplněné o aktualizovanou politiku hesel.
- Standardy bezpečného vývoje zahrnují filtrování uživatelských vstupů (v maximální možné míře pomocí bílého seznamu), vyloučení uživatelských vstupů a opatření proti hrubé síle (například omezení maximálního počtu opakovaných pokusů). Efektivnímu využití této techniky mohou napomoci „firewally webových aplikací“.
- Zavedení přísných zásad správy uživatelských oprávnění a řízení přístupu.
- Používání vhodných, aktuálních, účinných a integrovaných systémů firewallů, detekce narušení a dalších systémů obrany perimetru.
- Systematické audity zabezpečení IT a hodnocení zranitelnosti (penetrační testy).
- Pravidelné revize a testování, aby bylo zajištěno, že k obnově všech dat, jejichž integrita nebo dostupnost byla narušena, bude možné použít zálohy.

[23] O vývoji bezpečných webových aplikací viz také: https://www.owasp.org/index.php/Main_Page.

- Žádné ID relace v adrese URL v prostém textu.

4 INTERNÍ ZDROJ RIZIK ZPŮSOBENÝ LIDSKÝM FAKTOREM

71. Je třeba zdůraznit roli lidského faktoru při porušení zabezpečení osobních údajů, protože jde o častou příčinu. Vzhledem k tomu, že tyto typy porušení zabezpečení mohou být úmyslné i neúmyslné, je pro správce údajů velmi obtížné identifikovat zranitelná místa a přijmout opatření, která je vyloučí. Mezinárodní konference inspektorů ochrany údajů a soukromí uznala důležitost řešení těchto lidských faktorů a v říjnu 2019 přijala usnesení, které se zabývá úlohou lidské chyby při porušení zabezpečení osobních údajů[24]. Toto usnesení zdůrazňuje, že by měla být přijata vhodná ochranná opatření, aby se zabránilo lidským chybám, a uvádí neúplný seznam takových ochranných opatření a přístupů.

4.1 PŘÍPAD č. 08: Exfiltrace obchodních dat zaměstnancem

Zaměstnanec společnosti si během výpovědní lhůty zkopíruje obchodní údaje z databáze společnosti. Zaměstnanec je oprávněn přistupovat k údajům pouze za účelem plnění svých pracovních úkolů. O několik měsíců později, po ukončení pracovního poměru, použije takto získané údaje (základní kontaktní údaje) pro nové zpracování údajů, jehož je správcem, aby kontaktoval klienty společnosti a přilákal je do svého nového podnikání.

4.1.1 PŘÍPAD č. 08 – Předběžná opatření a posouzení rizik

72. V tomto konkrétním případě nebyla přijata žádná předběžná opatření, která by zaměstnanci zabránila kopírovat kontaktní údaje klientů společnosti, protože zaměstnanec potřeboval mít – a měl – oprávněný přístup k těmto informacím pro účely plnění svých pracovních úkolů. Vzhledem k tomu, že většina pracovních pozic v oblasti vztahů se zákazníky vyžaduje určitý druh přístupu zaměstnanců k osobním údajům, zabránit takovým případům porušení zabezpečení osobních údajů bývá nejobtížnější. Omezení rozsahu přístupu může omezit práci, kterou daný zaměstnanec vykonává. Dobře promyšlené zásady přístupu a neustálá kontrola však mohou takovým porušením zabezpečení zabránit.

73. Jako obvykle je třeba při posuzování rizik zohlednit typ porušení zabezpečení a povahu, citlivost a objem dotčených osobních údajů. Tyto typy porušení zabezpečení jsou typické porušením důvěrnosti, protože databáze obvykle zůstane nedotčená, „pouze“ je zkopírován její obsah pro další použití. Množství dotčených dat je obvykle také nízké nebo střední. V tomto konkrétním případě nebyly dotčeny žádné zvláštní kategorie osobních údajů, zaměstnanec potřeboval pouze kontaktní údaje klientů, aby se s nimi mohl po odchodu ze společnosti spojit. Dotčené údaje tedy nejsou citlivé.

74. Přestože jediný cíl bývalého zaměstnance, který údaje svévolně zkopíroval, může být omezen na získání kontaktních údajů klientely společnosti pro vlastní obchodní účely, správce nemůže považovat riziko pro dotčené subjekty údajů za nízké, protože nemá žádnou jistotu ohledně úmyslů zaměstnance. Ačkoli se tedy důsledky porušení zabezpečení mohou omezit na neoprávněný vlastní marketing bývalého zaměstnance,

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

není vyloučeno další a závažnější zneužití odcizených údajů v závislosti na účelu zpracování, které bývalý zaměstnanec prováděl[25].

4.1.2 PŘÍPAD č. 08 – Zmírnění a povinnosti

75. Zmírnění nepříznivých účinků porušení zabezpečení je ve výše uvedeném případě obtížné. Zřejmě bude nutné okamžitě podniknout právní kroky, aby se bývalému zaměstnanci zabránilo v dalším zneužívání a šíření údajů. Dalším krokem by mělo být předcházení podobným situacím v budoucnu. Správce se může pokusit bývalému zaměstnanci nařídit, aby údaje přestal používat, ale úspěšnost tohoto postupu je přinejmenším nepravděpodobná. Pomoci mohou vhodná technická opatření, jako je nemožnost kopírování nebo stahování dat na přenosná zařízení.

76. Pro tyto případy neexistuje univerzální řešení, ale systematický přístup jim může pomoci předcházet. Společnost může například zvážit – pokud je to možné – odebrání určitých forem přístupu zaměstnancům, kteří vykazují úmysl odejít, nebo zavedení záznamů o přístupu, aby bylo možné nežádoucí přístup zaznamenat a označit. Smlouva podepsaná se zaměstnanci by měla obsahovat ustanovení, která takové jednání zakazují.

77. Vzhledem k tomu, že dané porušení nepovede k vysokému riziku pro práva a svobody fyzických osob, lze obecně uvést, že postačí oznámení dozorovému úřadu. Informování subjektů údajů však může být prospěšné i pro správce údajů, protože může být lepší, když se o úniku údajů dozví od společnosti než od bývalého zaměstnance, který se je snaží kontaktovat. Dokumentace o porušení zabezpečení údajů podle čl. 33 odst. 5 je právní povinností.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	X

[25] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz poznámka pod čarou 10 výše.

4.2 PŘÍPAD č. 09: Náhodný přenos dat důvěryhodné třetí straně

Pojišťovací agent si všiml, že kvůli chybnému nastavení souboru Excel, který obdržel e-mailem, získal přístup k informacím o dvou desítkách zákazníků, kteří nespadají do jeho působnosti. Je vázán služebním tajemstvím a byl jediným příjemcem e-mailu. Ujednání mezi správcem údajů a pojišťovacím agentem zavazuje agenta, aby správci údajů bez zbytečného odkladu oznámil porušení zabezpečení osobních údajů. Proto agent okamžitě signalizoval chybu správci, který soubor opravil, znovu odeslal a požádal agenta, aby předchozí zprávu smazal. Podle výše uvedeného ujednání musí agent výmaz potvrdit písemným prohlášením, což učinil. Získané informace neobsahují žádné zvláštní kategorie osobních údajů, pouze kontaktní údaje a údaje o samotném pojištění (druh pojištění, pojistná částka). Po analýze osobních údajů dotčených porušením zabezpečení správce údajů nezjistil žádné zvláštní charakteristiky na straně fyzických osob nebo správce údajů, které by mohly ovlivnit míru dopadu porušení zabezpečení.

4.2.1 PŘÍPAD č. 09 – Předběžná opatření a posouzení rizik

78. Porušení zabezpečení zde nevyplývá z úmyslného jednání zaměstnance, ale z neúmyslné lidské chyby způsobené nepozorností. Těmto druhům porušení zabezpečení lze předejít nebo snížit jejich četnost a) povinným školením, vzdělávacími a osvětovými programy, v rámci kterých zaměstnanci lépe pochopí význam ochrany osobních údajů; b) omezením výměny souborů prostřednictvím e-mailu, namísto toho lze například pro zpracování údajů o zákaznících používat specializované systémy; c) dvojí kontrolou souborů před odesláním; d) oddělením vytváření a odesílání souborů.

79. Toto porušení zabezpečení se týká pouze důvěrnosti údajů, není dotčena integrita a přístupnost. Porušení zabezpečení údajů se týkalo pouze asi dvou desítek zákazníků, proto lze množství dotčených dat považovat za nízké. Dotčené osobní údaje navíc neobsahují žádné citlivé údaje. Skutečnost, že zpracovatel údajů ihned poté, co se dozvěděl o porušení zabezpečení údajů, kontaktoval správce údajů, lze považovat za faktor zmírňující riziko. (Měla by se také posoudit možnost, že údaje byly zaslány i jiným pojišťovacím agentům, a pokud se potvrdí, měla by být přijata vhodná opatření.) Vzhledem k tomu, že po porušení zabezpečení osobních údajů byla přijata vhodná opatření, nebude to mít pravděpodobně žádný dopad na práva a svobody subjektů údajů.

80. Vzhledem ke kombinaci nízkého počtu dotčených osob, okamžitého zjištění porušení zabezpečení a opatření přijatých k minimalizaci jeho dopadů není tento konkrétní případ rizikový.

4.2.2 PŘÍPAD č. 09 – Zmírnění a povinnosti

81. Kromě toho jsou ve hře i další okolnosti zmírňující riziko: agent je vázán služebním tajemstvím; sám nahlásil problém správci a na požádání soubor smazal. Zvýšení informovanosti a případné zahrnutí dalších kroků při kontrole dokumentů s osobními údaji pravděpodobně pomůže předejít podobným případům v budoucnu.

82. Kromě zdokumentování porušení zabezpečení v souladu s čl. 33 odst. 5 není třeba podnikat žádné další kroky.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	X	X

4.3 Organizační a technická opatření pro prevenci / zmírnění dopadů interních zdrojů rizik způsobených lidským faktorem

83. Pravděpodobnost opakování podobného porušení zabezpečení by měla pomoci snížit kombinace níže uvedených opatření, aplikovaných v závislosti na jedinečných rysech případu.

84. Doporučená opatření:

(Výčet následujících opatření není v žádném případě výlučný ani úplný. Cílem je spíše poskytnout náměty na prevenci a možná řešení. Každá činnost zpracování je jiná, a proto by měl správce rozhodnout, která opatření se pro danou situaci hodí nejlépe.)

- Pravidelné provádění školení, vzdělávacích a osvětových programů pro zaměstnance o jejich povinnostech v oblasti ochrany soukromí a bezpečnosti a o odhalování a oznamování hrozeb pro bezpečnost osobních údajů[26]. Vypracujte program zvyšování informovanosti, který zaměstnancům připomene nejčastější chyby vedoucí k porušení zabezpečení osobních údajů a způsoby, jak se jim vyhnout.
- Zavedení spolehlivých a účinných praktik, postupů a systémů ochrany údajů a soukromí[27].
- Hodnocení praktik, postupů a systémů ochrany soukromí s cílem zajistit jejich trvalou účinnost[28].
- Vytvoření správných zásad řízení přístupu a zajištění, aby uživatelé museli dodržovat pravidla.
- Zavedení technik vynucujících ověření uživatele při přístupu k citlivým osobním údajům.
- Deaktivace podnikového účtu uživatele, jakmile tato osoba podnik opustí.
- Kontrola neobvyklého toku dat mezi souborovým serverem a pracovními stanicemi zaměstnanců.
- Nastavení zabezpečení rozhraní I/O v systému BIOS nebo pomocí softwaru, který řídí používání rozhraní počítače (uzamčení nebo odemčení, např. USB/CD/DVD atd.).
- Přezkoumání zásad přístupu zaměstnanců (např. protokolování přístupu k citlivým údajům a požadavek, aby uživatel zadal obchodní důvod, aby byl k dispozici pro audity).
- Deaktivace otevřených cloudových služeb.
- Zákaz a zamezení přístupu ke známým otevřeným poštovním službám.
- Deaktivace funkce tisku obrazovky v OS.
- Prosazování zásad čistého pracovního stolu.
- Automatické uzamčení všech počítačů po určité době nečinnosti.
- Použití mechanismů (např. (bezdrátový) token pro přihlášení / otevření uzamčených účtů) pro rychlé přepínání uživatelů ve sdíleném prostředí.
- Používání specializovaných systémů pro správu osobních údajů, které používají vhodné mechanismy kontroly přístupu a které zabraňují lidské chybě, například zaslání sdělení nesprávnému subjektu. Používání tabulek a jiných kancelářských dokumentů není vhodným prostředkem pro správu údajů o klientech.

---

[26] Oddíl 2) bod i) usnesení k řešení úlohy lidského faktoru u případů porušení zabezpečení osobních údajů.

[27] Oddíl 2) bod ii) usnesení k řešení úlohy lidského faktoru u případů porušení zabezpečení osobních údajů.

[28] Oddíl 2) bod iii) usnesení k řešení úlohy lidského faktoru u případů porušení zabezpečení osobních údajů.

5 ZTRACENÁ NEBO ODCIZENÁ ZAŘÍZENÍ A PAPÍROVÉ DOKUMENTY

85. Častým případem je ztráta nebo krádež přenosných zařízení. V těchto případech musí správce vzít v úvahu okolnosti operace zpracování, jako je typ údajů uložených v zařízení, jakož i podpůrné prostředky, a opatření přijatá před porušením zabezpečení, aby byla zajištěna odpovídající úroveň bezpečnosti. Všechny tyto prvky ovlivňují potenciální dopady porušení zabezpečení údajů. Posouzení rizik může být obtížné, protože zařízení již není k dispozici.

86. Tyto druhy porušení zabezpečení lze vždy klasifikovat jako porušení důvěrnosti. Pokud však neexistuje žádná záloha ukradené databáze, může se jednat také o porušení dostupnosti a integrity.

87. Níže uvedené scénáře ukazují, jak výše uvedené okolnosti ovlivňují pravděpodobnost a závažnost porušení zabezpečení údajů.

5.1 PŘÍPAD č. 10: Odcizený materiál uchovávající zašifrované osobní údaje

Při vloupání do dětské školky byly odcizeny dva tablety. Tablety obsahovaly aplikaci, v níž byly uchovávány osobní údaje o dětech navštěvujících školku. Jednalo se o jméno, datum narození, osobní údaje o vzdělání dětí. Jak zašifrované tablety, které byly v době vloupání vypnuté, tak aplikace byly chráněny silným heslem. Správce měl efektivně a snadno k dispozici záložní data. Poté, co se školka o vloupání dozvěděla, vydala krátce po zjištění vloupání na dálku příkaz k vymazání tabletů.

5.1.1 PŘÍPAD č. 10 – Předběžná opatření a posouzení rizik

88. V tomto konkrétním případě přijal správce údajů odpovídající opatření k prevenci a zmírnění dopadů možného porušení zabezpečení údajů tím, že použil šifrování zařízení, zavedl odpovídající ochranu heslem a zajistil zálohování údajů uložených v tabletech. (Seznam doporučených opatření je uveden v oddíle 5.7.)

89. Jakmile se správce údajů o porušení zabezpečení dozví, měl by posoudit zdroj rizika, systémy podporující zpracování údajů, typ dotčených osobních údajů a možné dopady porušení zabezpečení údajů na dotčené osoby. Výše popsané porušení zabezpečení údajů by se týkalo důvěrnosti, dostupnosti a integrity dotčených údajů, nicméně díky vhodnému postupu správce údajů před porušením zabezpečení údajů i po něm k žádnému z nich nedošlo.

5.1.2 PŘÍPAD č. 10 – Zmírnění a povinnosti

90. Důvěrnost osobních údajů v zařízeních nebyla ohrožena díky silné ochraně heslem na tabletech i v aplikacích. Tablety byly nastaveny tak, že nastavení hesla znamená také zašifrování dat v zařízení. Toto bylo dále posíleno tím, že se správce pokusil z ukradených zařízení vše na dálku vymazat.

91. Díky přijatým opatřením byla zachována i důvěrnost údajů. Zálohování navíc zajistilo nepřetržitou dostupnost osobních údajů, takže nemohlo dojít k žádnému potenciálnímu negativnímu dopadu.

92. Vzhledem k těmto skutečnostem je nepravděpodobné, že by výše popsané porušení zabezpečení údajů mělo za následek riziko pro práva a svobody subjektů údajů, a proto nebylo zapotřebí ohlášení dozorovému úřadu ani dotčeným subjektům údajů. Toto porušení zabezpečení údajů však musí být rovněž zdokumentováno v souladu s čl. 33 odst. 5.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	X	X

5.2 PŘÍPAD č. 11: Odcizený materiál uchovávající nešifrované osobní údaje

Zaměstnanci společnosti poskytující služby byl odcizen elektronický notebook. Ukradený notebook obsahoval jména, příjmení, pohlaví, adresy a data narození více než 100 000 zákazníků. Vzhledem k nedostupnosti odcizeného zařízení nebylo možné zjistit, zda byly zasaženy i další kategorie osobních údajů. Přístup na pevný disk notebooku nebyl chráněn žádným heslem. Osobní údaje lze obnovit z dostupných denních záloh.

5.2.1 PŘÍPAD č. 11 – Předběžná opatření a posouzení rizik

93. Správce údajů nepřijal žádná předběžná bezpečnostní opatření, a proto byly osobní údaje uložené v odcizeném notebooku snadno přístupné zloději nebo jakékoli jiné osobě, která se k zařízení dostala později.

94. Toto porušení zabezpečení se týká důvěrnosti údajů uložených v odcizeném zařízení.

95. Notebook s osobními údaji byl v tomto případě zranitelný, protože nebyl chráněn heslem ani šifrováním. Nedostatek základních bezpečnostních opatření zvyšuje míru rizika pro dotčené subjekty údajů. Kromě toho je problematická i identifikace dotčených subjektů údajů, což rovněž zvyšuje závažnost porušení zabezpečení. Značný počet dotčených osob zvyšuje riziko, nicméně porušením zabezpečení osobních údajů nebyly dotčeny žádné zvláštní kategorie osobních údajů.

96. Při posuzování rizik[29] by měl správce zohlednit možné důsledky a nepříznivé dopady porušení důvěrnosti. V důsledku porušení zabezpečení může dojít k zneužití totožnosti dotčených subjektů údajů na základě údajů dostupných v odcizeném zařízení, takže riziko je považováno za vysoké.

5.2.2 PŘÍPAD č. 11 – Zmírnění a povinnosti

97. Zapnutí šifrování zařízení a použití silné ochrany uložené databáze heslem mohlo zabránit tomu, aby porušení ochrany údajů vedlo k ohrožení práv a svobod subjektů údajů.

98. Vzhledem k těmto okolnostem je nutné ohlášení dozorovému úřadu, přičemž je nutné informovat také dotčené subjekty údajů.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	✓

5.3 PŘÍPAD č. 12: Odcizení tištěných dokumentů s citlivými údaji

[29] Pokyny k operacím zpracování, které *„pravděpodobně budou mít za následek vysoké riziko“*, viz poznámka pod čarou 10 výše.

Z odvykacího zařízení pro drogově závislé byl odcizen papírový deník návštěv. Deník obsahoval základní identifikační a zdravotní údaje pacientů přijatých do rehabilitačního zařízení. Údaje byly uloženy pouze v papírové podobě a lékaři, kteří pacienty ošetřovali, neměli k dispozici žádnou zálohu. Deník nebyl uložen v uzamčené zásuvce ani v uzamčené místnosti, správce údajů neměl pro papírovou dokumentaci zaveden režim kontroly přístupu ani žádné jiné bezpečnostní opatření.

5.3.1 PŘÍPAD č. 12 – Předběžná opatření a posouzení rizik

99. Správce údajů nepřijal žádná předběžná bezpečnostní opatření, a proto byly osobní údaje uložené v tomto deníku snadno přístupné osobě, která je našla. Navíc je vzhledem k povaze osobních údajů uložených v deníku chybějící zálohování dat velmi závažným rizikovým faktorem.

100. Tento případ slouží jako příklad vysoce rizikového porušení zabezpečení údajů. Z důvodu nezajištění odpovídajících bezpečnostních opatření došlo ke ztrátě citlivých zdravotních údajů podle čl. 9 odst. 1 nařízení GDPR. Vzhledem k tomu, že se v tomto případě jednalo o zvláštní kategorii osobních údajů, zvýšila se potenciální rizika pro dotčené subjekty údajů, což by měl správce při posuzování rizik rovněž zohlednit[30].

101. Toto porušení zabezpečení se týká důvěrnosti, dostupnosti a integrity dotčených osobních údajů. V důsledku porušení zabezpečení je ohroženo lékařské tajemství a přístup k soukromým lékařským informacím pacientů mohou získat neoprávněné třetí strany, což může mít závažný dopad na jejich osobní život. Porušení dostupnosti může také narušit kontinuitu léčby pacientů. Vzhledem k tomu, že nelze vyloučit změnu/vymazání části obsahu deníku, je ohrožena i integrita osobních údajů.

5.3.2 PŘÍPAD č. 12 – Zmírnění a povinnosti

102. Při posuzování ochranných opatření je třeba vzít v úvahu i typ použitého prostředku. Vzhledem k tomu, že deník návštěv pacientů byl fyzickým dokumentem, měla být jeho ochrana provedena jinak než ochrana elektronického zařízení. Pseudonymizace jmen pacientů, uložení deníku v zabezpečených prostorách a v uzamčené zásuvce nebo místnosti a řádná kontrola přístupu s ověřením totožnosti při přístupu k němu mohly porušení zabezpečení údajů zabránit.

103. Výše popsané porušení zabezpečení údajů může mít závažný dopad na dotčené subjekty údajů; proto je ohlášení dozorovému úřadu a informování dotčených subjektů údajů o porušení zabezpečení povinné.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	✓

5.4 Organizační a technická opatření pro prevenci / zmírnění dopadů ztráty nebo krádeže zařízení

104. Pravděpodobnost opakování podobného porušení zabezpečení by měla pomoci snížit kombinace níže uvedených opatření, aplikovaných v závislosti na jedinečných rysech případu.

105. Doporučená opatření:

[30] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz poznámka pod čarou 10 výše.

(Výčet následujících opatření není v žádném případě výlučný ani úplný. Cílem je spíše poskytnout náměty na prevenci a možná řešení. Každá činnost zpracování je jiná, a proto by měl správce rozhodnout, která opatření se pro danou situaci hodí nejlépe.)

- Zapněte šifrování zařízení (například Bitlocker, Veracrypt nebo DM-Crypt).
- Na všech zařízeních používejte přístupový kód/heslo. Šifrujte všechna mobilní elektronická zařízení způsobem, který vyžaduje zadání hesla, které lze dešifrovat jen obtížně.
- Používejte vícefaktorové ověřování.
- Zapněte funkce vysoce mobilních zařízení, které umožňují jejich lokalizaci v případě ztráty nebo nesprávného umístění.
- Použití softwaru/aplikace MDM (Mobile Devices Management) a lokalizace. Používejte antireflexní filtry. Všechna zařízení bez dozoru vypínejte.
- Pokud je to možné a vhodné pro dané zpracování údajů, neukládejte osobní údaje do mobilního zařízení, ale na centrální databázový server.
- Pokud je pracovní stanice připojena k firemní síti LAN, provádějte automatické zálohování z pracovních složek, pokud je nevyhnutelné, aby v pracovní stanici byla uložena osobní data.
- Pro připojení mobilních zařízení k databázovým serverům používejte zabezpečenou síť VPN (např. takovou, která pro vytvoření zabezpečeného připojení vyžaduje samostatný ověřovací klíč pomocí druhého faktoru).
- Poskytněte zaměstnancům fyzické zámky, aby mohli fyzicky zabezpečit mobilní zařízení, která používají, když jsou tato zařízení bez dozoru.
- Správná regulace používání zařízení mimo společnost.
- Správná regulace používání zařízení uvnitř společnosti.
- Použijte software/aplikaci MDM (Mobile Devices Management) a povolte funkci vzdáleného vymazání.
- Používejte centralizovanou správu zařízení s minimálními právy pro koncové uživatele k instalaci softwaru.
- Nainstalujte fyzické kontroly přístupu.
- Neukládejte citlivé informace do mobilních zařízení ani na pevné disky. V případě potřeby přístupu do interního systému společnosti by měly být použity zabezpečené kanály, jak je uvedeno výše.

6 ODESLÁNÍ NA CHYBNOU ADRESU

106. Zdrojem rizika je i v tomto případě interní lidská chyba, ale zde k porušení zabezpečení nedošlo v důsledku úmyslného jednání. Jednalo se o důsledek nepozornosti. Pokud k tomuto dojde, správce nemá moc možností, jak zakročit, takže prevence je v těchto případech ještě důležitější než u jiných typů porušení zabezpečení.

6.1 PŘÍPAD č. 13: Chyba u poštovní zásilky

Maloobchodní společnost zabalila dvě objednávky obuvi. V důsledku lidské chyby došlo k záměně dvou dodacích listů, takže oba výrobky a příslušné dodací listy byly zaslány nesprávným osobám. To znamená, že tito dva zákazníci dostali objednávku toho druhého, včetně dodacích listů obsahujících osobní údaje. Poté, co se správce údajů o porušení zabezpečení dozvěděl, objednávky stáhl a odeslal je správným příjemcům.

6.1.1 PŘÍPAD č. 13 – Předběžná opatření a posouzení rizik

107. Dodací listy obsahovaly osobní údaje potřebné pro úspěšné doručení (jméno, adresu a zakoupené zboží a jeho cenu). Je důležité zjistit, jak k této chybě způsobené lidským faktorem mohlo vůbec dojít a zda jí bylo možné nějakým způsobem zabránit. V daném případě je riziko nízké, protože se nejedná o žádné zvláštní kategorie osobních údajů ani jiné údaje, jejichž zneužití by mohlo mít závažné negativní účinky, porušení zabezpečení není důsledkem systémové chyby na straně správce a týká se pouze dvou osob. Nebyl zjištěn žádný negativní vliv na jedince.

6.1.2 PŘÍPAD č. 13 – Zmírnění a povinnosti

108. Správce by měl zajistit bezplatné vrácení zboží a přiložených dodacích listů a měl by také požádat nesprávné příjemce, aby zničili/vymazali všechny případné kopie dodacích listů, které obsahují osobní údaje druhé osoby.

109. I když samotné porušení zabezpečení nepředstavuje vysoké riziko pro práva a svobody dotčených fyzických osob, a proto článek 34 nařízení GDPR nepředepisuje informování subjektů údajů, nelze se jejich informování o porušení zabezpečení vyhnout, protože ke zmírnění rizika je nutná jejich spolupráce.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	X	X

6.2 PŘÍPAD č. 14: Vysoce důvěrné osobní údaje zaslané omylem

Oddělení úřadu práce rozeslalo e-mailovou zprávu – o nadcházejících školeních – osobám, které jsou v jeho systému registrovány jako uchazeči o zaměstnání. K tomuto e-mailu byl omylem přiložen dokument obsahující osobní údaje všech těchto uchazečů o zaměstnání (jméno, e-mailová adresa, poštovní adresa, číslo sociálního pojištění). Počet postižených osob je více než 60 000. Úřad následně kontaktoval všechny příjemce a požádal je, aby předchozí zprávu smazali a informace v ní obsažené nepoužívali.

6.2.1 PŘÍPAD č. 14 – Předběžná opatření a posouzení rizik

110. Pro zasílání takových zpráv měla být zavedena přísnější pravidla. Je třeba zvážit zavedení dalších kontrolních mechanismů.

111. Počet postižených osob je značný a uvedení jejich čísla sociálního zabezpečení spolu s dalšími osobními údaji obecnějšího charakteru dále zvyšuje riziko, které lze označit za vysoké[31]. Případné šíření údajů některým z příjemců nemůže správce údajů omezit.

[31] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz poznámka pod čarou 10 výše.

6.2.2 PŘÍPAD č. 14 – Zmírnění a povinnosti

112. Jak již bylo zmíněno, prostředky pro účinné zmírnění rizik u podobného porušení zabezpečení jsou omezené. Ačkoli správce požádal o vymazání zprávy, nemůže k tomu příjemce donutit, a proto si ani nemůže být jist, že příjemci žádosti vyhoví.

113. Provedení všech tří níže uvedených opatření by mělo být v takovém případě samozřejmostí.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	✓

6.3 PŘÍPAD č. 15: Osobní údaje zaslané omylem

Seznam účastníků kurzu právnické angličtiny, který se koná v hotelu po dobu pěti dnů, je omylem místo hotelu zaslán patnácti bývalým účastníkům kurzu. Seznam obsahuje jména, e-mailové adresy a stravovací preference těchto patnácti účastníků. Své stravovací preference vyplnili pouze dva účastníci a uvedli, že mají intoleranci laktózy. Žádný z účastníků nemá chráněnou totožnost. Správce zjistí chybu ihned po odeslání seznamu a informuje příjemce o chybě a požádá je o vymazání seznamu.

6.3.1 PŘÍPAD č. 15 – Předběžná opatření a posouzení rizik

114. Pro zasílání zpráv obsahujících osobní údaje měla být zavedena přísná pravidla. Je třeba zvážit zavedení dalších kontrolních mechanismů.

115. Rizika vyplývající z povahy, citlivosti, objemu a kontextu osobních údajů jsou nízká. Osobní údaje zahrnují citlivé údaje o stravovacích preferencích dvou účastníků. I když je informace o tom, že někdo nesnáší laktózu, zdravotním údajem, riziko, že tento údaj bude použit škodlivým způsobem, lze považovat za relativně nízké. Přestože se v případě údajů týkajících se zdraví obvykle předpokládá, že porušení zabezpečení může mít za následek vysoké riziko pro subjekt údajů[32], v tomto konkrétním případě zároveň nelze identifikovat riziko, že by porušení zabezpečení vedlo k fyzické, hmotné nebo nehmotné újmě subjektu údajů v důsledku neoprávněného zveřejnění informací o nesnášenlivosti laktózy. Na rozdíl od některých jiných stravovacích preferencí nemůže být intolerance laktózy obvykle spojena s žádným náboženským nebo filozofickým přesvědčením. Množství údajů, u nichž došlo k porušení zabezpečení, a počet dotčených subjektů údajů je rovněž velmi nízký.

6.3.2 PŘÍPAD č. 15 – Zmírnění a povinnosti

116. Souhrnně lze konstatovat, že porušení zabezpečení nemělo na subjekty údajů žádný významný dopad. Za polehčující okolnost lze považovat skutečnost, že správce ihned poté, co se o chybě dozvěděl, kontaktoval příjemce.

117. Pokud je e-mail zaslán nesprávnému/neoprávněnému příjemci, doporučuje se, aby správce údajů zaslal nezamýšleným příjemcům další e-mail formou skryté kopie s omluvou, pokynem ke smazání dotčeného e-mailu a upozorněním příjemců, že nemají právo dále používat e-mailové adresy, které jim byly zaslány.

118. Vzhledem k těmto skutečnostem je nepravděpodobné, že by porušení zabezpečení údajů mělo za následek riziko pro práva a svobody subjektů údajů, a proto nebylo nutné ohlášení dozorovému úřadu ani dotčeným

[32] Viz pokyny WP 250, s. 23.

subjektům údajů. I toto porušení ochrany údajů však musí rovněž zdokumentováno v souladu s čl. 33 odst. 5.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	X	X

6.4 PŘÍPAD č. 16: Chyba u poštovní zásilky

Pojišťovací skupina nabízí pojištění vozidel. Za tímto účelem pravidelně rozesílá poštou upravené zásady placení pojistného. Kromě jména a adresy pojistníka dopis obsahuje registrační značku vozidla bez maskovaných číslic, sazby pojištění pro aktuální a příští pojistný rok, přibližný roční nájezd kilometrů a datum narození pojistníka. Nejsou uvedeny zdravotní údaje podle článku 9 GDPR, platební údaje (bankovní spojení), ekonomické a finanční údaje.

Dopisy se balí pomocí automatických obálkovacích strojů. Z důvodu mechanické chyby jsou do jedné obálky vloženy dva dopisy pro různé pojistníky a pošta je zašle jednomu pojistníkovi. Pojistník dopis doma otevře a přečte si svůj správně doručený dopis i nesprávně doručený dopis pro jiného pojistníka.

6.4.1 PŘÍPAD č. 16 – Předběžná opatření a posouzení rizik

119. Nesprávně doručený dopis obsahuje jméno, adresu, datum narození, nemaskovanou registrační značku vozidla a klasifikaci pojistné sazby na běžný a příští rok. Dopady na postiženou osobu je třeba považovat za střední, protože neoprávněnému příjemci jsou sděleny informace, které nejsou veřejně dostupné, jako je datum narození nebo nemaskované registrační číslo vozidla a podrobnosti o zvýšení sazeb pojištění. Pravděpodobnost zneužití těchto údajů je hodnocena jako nízká až střední. Přestože mnoho příjemců pravděpodobně dopis, který jim byl doručen omylem, vyhodí do koše, nelze v jednotlivých případech zcela vyloučit, že dopis bude zveřejněn na sociálních sítích nebo že bude kontaktován pojistník.

6.4.2 PŘÍPAD č. 16 – Zmírnění a povinnosti

120. Správce by si měl nechat originál dokumentu vrátit na vlastní náklady. Nesprávný příjemce by měl být rovněž informován o tom, že nesmí přečtené informace zneužít.

121. Pravděpodobně nebude nikdy možné zcela zabránit chybám při doručování hromadných zásilek pomocí plně automatizovaných strojů. V případě zvýšené četnosti je však nutné zkontrolovat, zda jsou obálkovací stroje dostatečně správně nastaveny a udržovány nebo zda k takovému porušení zabezpečení nevede nějaký jiný systémový problém.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	X

6.5 Organizační a technická opatření pro prevenci / zmírnění dopadů chybného zaslání

122. Pravděpodobnost opakování podobného porušení zabezpečení by měla pomoci snížit kombinace níže uvedených opatření, aplikovaných v závislosti na jedinečných rysech případu.

123. Doporučená opatření:

(Výčet následujících opatření není v žádném případě výlučný ani úplný. Cílem je spíše poskytnout náměty na prevenci a možná řešení. Každá činnost zpracování je jiná, a proto by měl správce rozhodnout, která opatření se pro danou situaci hodí nejlépe.)

- Stanovení přesných standardů – bez možnosti volného výkladu – pro zasílání dopisů/e-mailů.
- Dostatečné školení zaměstnanců o tom, jak posílat dopisy/e-maily.
- Při odesílání e-mailů více příjemcům jsou příjemci standardně uvedeni v poli „skrytá kopie“.
- Při odesílání e-mailů více příjemcům, kteří nejsou uvedeni v poli „skrytá kopie“, je vyžadováno zvláštní potvrzení.
- Uplatnění principu čtyř očí.
- Automatické adresování namísto ručního, s daty získanými z dostupné a aktuální databáze; automatický adresní systém by měl být pravidelně kontrolován ohledně toho, zda neobsahuje skryté chyby a nesprávná nastavení.
- Použití zpožděného odesílání zpráv (např. po kliknutí na tlačítko „odeslat“ může být zpráva v určitém časovém období smazána/upravena).
- Vypnutí automatického dokončování při zadávání e-mailových adres.
- Seznámení s nejčastějšími chybami, které vedou k porušení zabezpečení osobních údajů.
- Školení a příručky o tom, jak řešit incidenty vedoucí k porušení zabezpečení osobních údajů a koho informovat (zapojení inspektora ochrany údajů).

7 DALŠÍ PŘÍPADY – SOCIÁLNÍ INŽENÝRSTVÍ

7.1 PŘÍPAD č. 17: Krádež totožnosti

Kontaktní centrum telekomunikační společnosti obdrží telefonát od osoby, která se vydává za klienta. Údajný klient požaduje, aby společnost změnila e-mailovou adresu, na kterou mu mají být od této chvíle zasílány fakturační údaje. Pracovník kontaktního centra ověří totožnost klienta tím, že si vyžádá určité osobní údaje, jak to definují postupy společnosti. Volající správně uvede požadované daňové identifikační číslo a poštovní adresu klienta (protože měl k těmto údajům přístup). Po ověření operátor provede požadovanou změnu a od té doby jsou fakturační údaje zasílány na novou e-mailovou adresu. Tento postup nepředpokládá žádné oznámení na původní e-mailový kontakt. Následující měsíc se právoplatný klient obrátí na společnost s dotazem, proč mu na jeho e-mailovou adresu nepřišlo vyúčtování, a popře, že by volal a požadoval změnu e-mailového kontaktu. Společnost později zjistí, že informace byly odeslány neoprávněnému uživateli, a změnu zruší.

7.1.1 PŘÍPAD č. 17 – Posouzení rizik, jejich zmírnění a povinnosti

124. Tento případ slouží jako příklad důležitosti předběžných opatření. Z hlediska rizika představuje toto porušení zabezpečení vysokou míru rizika33, neboť fakturační údaje mohou poskytnout informace o soukromém životě subjektu údajů (např. zvyky, kontakty) a mohly by vést k hmotné újmě (např. pronásledování, ohrožení fyzické integrity). Osobní údaje získané během tohoto útoku mohou být také použity k usnadnění převzetí klienta v této organizaci nebo ke zneužití dalších ověřovacích opatření v jiných organizacích. Vzhledem k těmto rizikům by „vhodné“ ověřovací opatření mělo splňovat vysoké standardy v závislosti na tom, jaké osobní údaje mohou být při ověřování zpracovávány.

125. Proto je třeba, aby správce údajů zaslal oznámení jak dozorovému úřadu, tak subjektu údajů.

126. Samozřejmě je třeba s ohledem na tento případ zdokonalit původní proces ověření klienta. Metody používané pro ověřování nebyly dostatečné. Neoprávněná strana dokázala předstírat, že je zamýšleným uživatelem, a to s využitím veřejně dostupných informací a informací, ke kterým měla jinak přístup.

127. Použití tohoto typu statického ověřování založeného na znalostech (kdy se odpověď nemění a kdy informace nejsou „tajné“, jako je tomu v případě hesla) se nedoporučuje.

128. Místo toho by organizace měla používat takovou formu ověřování, která by vedla k vysoké míře jistoty, že ověřovaný uživatel je zamýšlená osoba, a nikoli někdo jiný. Problém by vyřešilo zavedení dodatečné metody vícefaktorového ověřování, např. ověření požadavku na změnu zasláním žádosti o potvrzení původnímu kontaktu; nebo přidání dalších otázek a vyžadování informací, které lze nalézt pouze v předchozích vyúčtováních. Rozhodnutí o tom, jaká opatření zavést, je na správci, který nejlépe zná podrobnosti a požadavky svého vnitřního provozu.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	✓

7.2 PŘÍPAD č. 18: Exfiltrace e-mailů

[33] Pokyny k operacím zpracování, které „*pravděpodobně budou mít za následek vysoké riziko*“, viz poznámka pod čarou 10 výše.

Řetězec hypermarketů po třech měsících od konfigurace zjistil, že některé e-mailové účty byly pozměněny a byla vytvořena pravidla, podle nichž byl každý e-mail obsahující určité výrazy (např. „faktura“, „platba“, „bankovní převod“, „ověření platební karty“, „údaje o bankovním účtu“) přesunut do nepoužívané složky a také přeposlán na externí e-mailovou adresu. V té době již byl rovněž proveden útok formou sociálního inženýrství, tj. útočník, který se vydával za dodavatele, nechal změnit údaje o bankovním účtu tohoto dodavatele na své vlastní. Nakonec bylo ve stejné době odesláno několik falešných faktur, které obsahovaly údaje s novým bankovním spojením. Monitorovací systém e-mailové platformy vydal pouze upozornění týkající se složek. Společnost nedokázala zjistit, jakým způsobem se útočníkovi podařilo získat přístup k e-mailovým účtům, ale předpokládala, že na vině byl infikovaný e-mail, který umožnil přístup do skupiny uživatelů odpovědných za platby.

V důsledku přeposílání e-mailů na základě klíčových slov získal útočník informace o 99 zaměstnancích: jméno a mzda za konkrétní měsíc týkající se 89 subjektů údajů; jméno, rodinný stav, počet dětí, mzda, pracovní doba a ostatní informace o vyplacené mzdě deseti zaměstnanců, jejichž pracovní poměr skončil. Správce informoval pouze těchto deset zaměstnanců patřících do druhé skupiny.

7.2.1 PŘÍPAD č. 18 – Posouzení rizik, jejich zmírnění a povinnosti

129. I když cílem útočníka pravděpodobně nebylo shromáždit osobní údaje, porušení zabezpečení osobních údajů bude pravděpodobně mít za následek vysoké riziko pro práva a svobody fyzických osob, protože mohlo vést jak k hmotné (např. finanční ztrátě), tak k nehmotné újmě (např. krádeži či zneužití totožnosti), nebo mohly být údaje použity k usnadnění jiných útoků (např. phishing). Proto by o narušení mělo být informováno všech 99 zaměstnanců, a nikoli pouze deset zaměstnanců, jejichž informace o mzdě unikly.

130. Poté, co se správce dozvěděl o narušení, vynutil změnu hesla u napadených účtů, zablokoval odesílání e-mailů na e-mailový účet útočníka, informoval poskytovatele služeb o e-mailu používaném útočníkem k jeho činnosti, odstranil pravidla nastavená útočníkem a zlepšil výstrahy monitorovacího systému tak, aby vydaly upozornění, jakmile je vytvořeno automatické pravidlo. Správce by také mohl zrušit právo uživatelů nastavovat pravidla pro přeposílání, aby uživatelé museli o nastavení přeposílání požádat tým IT služeb, nebo by mohl zavést zásadu, že uživatelé mají jednou týdně nebo častěji zkontrolovat a nahlásit pravidla nastavená na svých účtech v oblastech, kde se pracuje s finančními údaji.

131. Skutečnost, že k narušení mohlo dojít a že zůstalo tak dlouho neodhaleno, a skutečnost, že dlouhodoběji mohlo být využíváno sociální inženýrství ke změně dalších údajů, poukázaly na významné problémy ve správcově systému zabezpečení IT. Tyto problémy by měly být neprodleně řešeny, například zaměřením se na přezkum automatizačních procesů a kontroly změn, opatření pro detekci incidentů a reakci na ně. Správci, kteří nakládají s citlivými údaji, finančními informacemi apod., mají větší odpovědnost, pokud jde o zajištění odpovídajícího zabezpečení údajů.

Opatření nezbytná na základě zjištěných rizik		
Interní dokumentace	Ohlášení dozorovému úřadu	Komunikace se subjekty údajů
✓	✓	✓