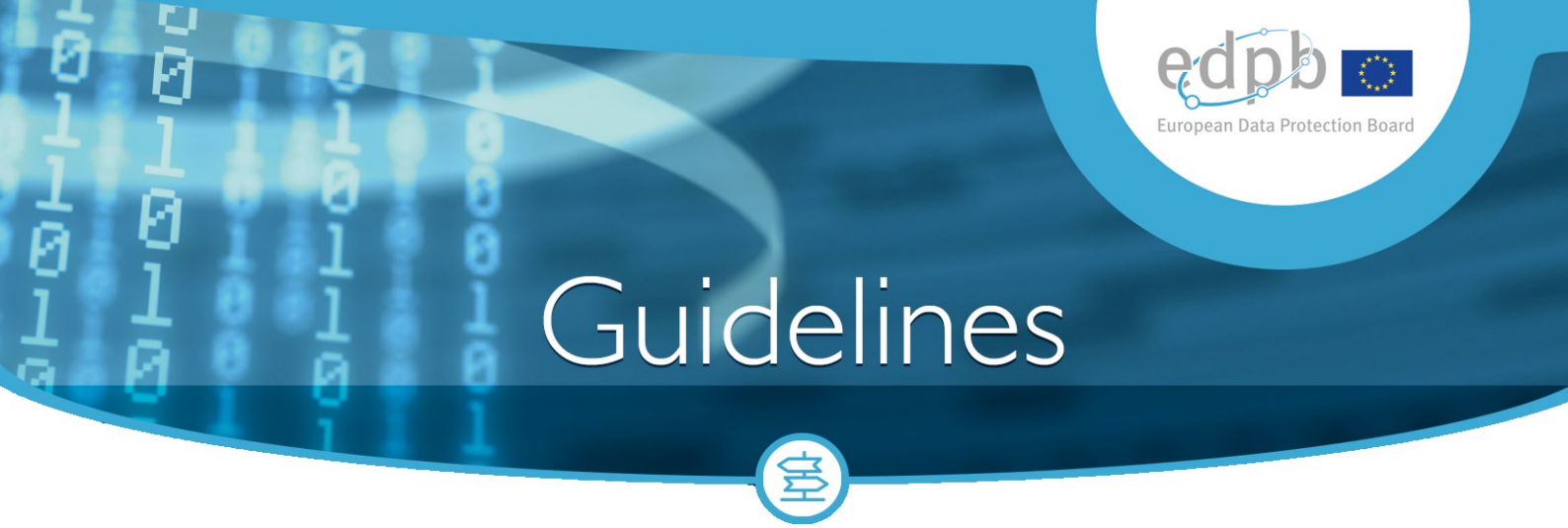

Usmernenia 1/2021

k príkladom týkajúcim sa oznámenia porušenia ochrany osobných údajov

Prijaté 14. decembra 2021

Verzia 2.0

História verzií

Verzia 2.0	14. 12. 2021	Prijatie usmernení po verejnej konzultácii
Verzia 1.0	14. 1. 2021	Prijatie usmernení na účely verejnej konzultácie

Obsah

EURÓPSKY VÝBOR PRE OCHRANU ÚDAJOV

so zreteľom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o EHP, a najmä na prílohu XI a protokol 37 k tejto dohode, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018[1],

so zreteľom na články 12 a 22 svojho rokovacieho poriadku,

so zreteľom na oznámenie Komisie Európskemu parlamentu a Rade s názvom Ochrana údajov ako pilier posilnenia postavenia občanov a prístupu EÚ k digitálnej transformácii – dva roky uplatňovania všeobecného nariadenia o ochrane údajov[2],

PRIJAL TIETO USMERNENIA

1. ÚVOD

1. Všeobecným nariadením o ochrane údajov sa v určitých prípadoch zavádza požiadavka oznámiť porušenie ochrany osobných údajov príslušnému vnútroštátnemu dozornému orgánu a oznámiť toto porušenie jednotlivcom, ktorých osobných údajov sa porušenie týka (články 33 a 34).

2. Pracovná skupina zriadená podľa článku 29 už v októbri 2017 vydala *všeobecné* usmernenia o oznámení porušenia ochrany osobných údajov, v ktorých sa analyzujú príslušné oddiely všeobecného nariadenia o ochrane údajov (Usmernenia o oznámení porušenia ochrany osobných údajov podľa nariadenia 2016/679, WP250) (ďalej len „usmernenia WP250“)[3]. Vzhľadom na povahu a načasovanie týchto usmernení sa v nich však neriešili všetky praktické otázky dostatočne podrobne. Preto bolo potrebné vypracovať usmernenie *na základe konkrétnych prípadov orientovaných na prax*, v ktorom sa využívajú skúsenosti, ktoré dozorné orgány získali od nadobudnutia účinnosti všeobecného nariadenia o ochrane údajov.

3. Tento dokument má slúžiť ako doplnok k usmerneniam WP250 a odráža spoločné skúsenosti dozorných orgánov z EHP od nadobudnutia účinnosti všeobecného nariadenia o ochrane údajov. Jeho cieľom je pomôcť prevádzkovateľom pri rozhodovaní o tom, ako riešiť porušenia ochrany údajov a ktoré faktory zohľadniť pri posudzovaní rizika.

4. Ako prvý krok v úsilí o riešenie porušenia by mali prevádzkovateľ a sprostredkovateľ najskôr porušenie rozpoznať. V článku 4 bode 12 všeobecného nariadenia o ochrane údajov sa „porušenie ochrany osobných

[1] Odkazy na „členské štáty“ v tomto dokumente by sa mali chápať ako odkazy na „členské štáty EHP“.

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

[3] G29 WP250 rev. 1, 6. február 2018, Usmernenia o oznámení porušenia ochrany osobných údajov podľa nariadenia 2016/679 – schválené EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

údajov“ vymedzuje ako „porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim“.

5. Pracovná skupina zriadená podľa článku 29 vo svojom stanovisku č. 03/2014 k oznámeniu o porušení ochrany osobných údajov[4] a vo svojich usmerneniach WP250 vysvetlila, že porušenia možno kategorizovať podľa týchto troch všeobecne známych zásad informačnej bezpečnosti:

   - „porušenie dôvernosti“ – keď dôjde k neoprávnenému alebo náhodnému poskytnutiu osobných údajov alebo prístupu k osobným údajom,
   - „porušenie integrity“ – keď dôjde k neoprávnenej alebo náhodnej zmene osobných údajov,
   - „porušenie dostupnosti“ – keď dôjde k náhodnej alebo neoprávnenej strate prístupu alebo k zničeniu osobných údajov.[5]

6. Porušenie môže mať pre jednotlivcov širokú škálu závažných nepriaznivých dôsledkov, ktoré môžu spôsobiť ujmu na zdraví, majetkovú alebo nemajetkovú ujmu. Vo všeobecnom nariadení o ochrane údajov sa vysvetľuje, že ňou môže byť napríklad strata kontroly nad svojimi osobnými údajmi, obmedzenie práv týchto osôb, diskriminácia, krádež totožnosti alebo podvod, finančná strata, neoprávnená reverzná pseudonymizácia, poškodenie dobrého mena a strata dôvernosti osobných údajov chránených profesijným tajomstvom. Ujma môže takisto zahŕňať akékoľvek iné závažné hospodárske či sociálne znevýhodnenie týchto jednotlivcov. Jednou z najdôležitejších povinností prevádzkovateľa je posúdiť tieto riziká pre práva a slobody dotknutých osôb a prijať primerané technické a organizačné opatrenia na ich riešenie.

7. Vo všeobecnom nariadení o ochrane údajov sa preto od prevádzkovateľa vyžaduje, aby:

   - zdokumentoval každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu[6],
   - toto porušenie oznámil dozornému orgánu s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb[7],
   - oznámil dotknutej osobe porušenie ochrany osobných údajov, ak toto porušenie ochrany osobných údajov pravdepodobne povedie k vysokému riziku pre práva a slobody fyzickej osoby[8].

8. Porušenia ochrany údajov sú nielenže problémom samy o sebe, ale môžu byť takisto známkami zraniteľného a možno zastaraného režimu ochrany údajov či poukazovať na systémové slabé miesta, ktoré treba riešiť. Vo všeobecnosti platí, že je vždy lepšie predchádzať porušeniam ochrany údajov včasnou prípravou, keďže ich závažné dôsledky sú spravidla nezvratné. Predtým než prevádzkovateľ môže v *plnej miere* posúdiť riziko vyplývajúce z porušenia spôsobené určitou formou útoku, mala by sa identifikovať

---

[4] G29 WP213, 25. marec 2014, stanovisko č. 03/2014 k oznámeniu o porušení ochrany osobných údajov, s. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Pozri usmernenia WP250, s. 7. Treba zohľadniť, že porušenie ochrany údajov sa môže týkať buď jednej, alebo viacerých kategórií súbežne alebo ich kombinácie.

[6] Článok 33 ods. 5 všeobecného nariadenia o ochrane údajov.

[7] Článok 33 ods. 1 všeobecného nariadenia o ochrane údajov.

[8] Článok 34 ods. 1 všeobecného nariadenia o ochrane údajov.

hlavná príčina, aby sa zistilo, či sú ešte prítomné zraniteľnosti, ktoré incident spôsobili a ktoré tak ešte možno zneužiť. V mnohých prípadoch je prevádzkovateľ schopný stanoviť, že incident pravdepodobne povedie k riziku, a preto ho treba oznámiť. V iných prípadoch oznámenie netreba odkladať až do úplného posúdenia rizika a následkov porušenia, keďže úplné posúdenie rizika sa môže uskutočňovať súbežne s oznámením a informácie z neho získané možno poskytovať dozornému orgánu vo viacerých etapách bez ďalšieho zbytočného odkladu[9].

9. Porušenie by sa malo oznámiť vtedy, keď sa prevádzkovateľ domnieva, že pravdepodobne povedie k riziku pre práva a slobody dotknutej osoby. Prevádzkovatelia by mali toto posúdenie vykonať, hneď ako sa o porušení dozvedia. Prevádzkovateľ by nemal čakať na podrobné forenzné preskúmanie a (prvé) zmierňujúce kroky, kým posúdi, či je pravdepodobné, že porušenie ochrany údajov povedie k riziku, a či ho preto treba oznámiť.

10. Ak prevádzkovateľ sám posúdi, že riziko je nepravdepodobné, no riziko nakoniec vznikne, príslušný dozorný orgán môže využiť svoje nápravné právomoci a môže uložiť sankcie.

11. Každý prevádzkovateľ a sprostredkovateľ by mal mať zavedené plány a postupy na riešenie prípadných porušení ochrany údajov. Organizácie by mali mať jasnú hierarchickú štruktúru a osoby zodpovedné za určité aspekty postupu nápravy.

12. Pre prevádzkovateľov a sprostredkovateľov je takisto kľúčová odborná príprava a informovanosť zamestnancov o otázkach ochrany údajov so zameraním sa na postupy pri porušení ochrany osobných údajov (identifikácia porušenia ochrany osobných údajov a ďalšie opatrenia, ktoré sa majú prijať, atď.). Táto odborná príprava by sa mala pravidelne opakovať v závislosti od druhu spracovateľskej činnosti a veľkosti prevádzkovateľa a zároveň by sa mala zaoberať najnovším vývojom a výstrahami vyplývajúcimi z kybernetických útokov alebo iných bezpečnostných incidentov.

13. Zásada zodpovednosti a koncepcia špecificky navrhnutej ochrany údajov by mohli zahŕňať analýzu, z ktorej bude vychádzať prevádzkovateľova a sprostredkovateľova vlastná „príručka k riešeniu porušení ochrany osobných údajov“, ktorej cieľom je stanoviť okolnosti pre každú stránku spracúvania v každej hlavnej fáze operácie. Takáto vopred vypracovaná príručka by predstavovala oveľa rýchlejší zdroj informácií, ktorý by prevádzkovateľom a sprostredkovateľom umožnil zmieniť riziká a plniť si povinnosti bez zbytočného odkladu. Zaručilo by sa tým, že ak dôjde k porušeniu ochrany osobných údajov, členovia organizácie by vedeli, čo robiť, a incident by sa pravdepodobne vyriešil rýchlejšie, než keby neboli zavedené žiadne zmierňujúce opatrenia alebo plán.

14. Hoci sú príklady predstavené ďalej v texte fiktívne, vychádzajú z bežných prípadov z kolektívnych skúseností dozorných orgánov s oznámeniami porušení ochrany údajov. Predkladané analýzy sa týkajú výslovne skúmaných príkladov, no s cieľom pomôcť prevádzkovateľom posúdiť ich vlastné porušenia ochrany údajov. Každá zmena okolností prípadov opísaných ďalej v texte môže viesť k odlišnej alebo závažnejšej úrovni rizika, a preto si vyžadujú iné alebo dodatočné opatrenia. V týchto usmerneniach sa prípady zaraďujú do určitých kategórií porušení (napr. ransomvérové útoky). Každý prípad, v ktorom sa rieši určitá kategória porušení, si vyžaduje určité zmierňujúce opatrenia. Tieto opatrenia sa nemusia nevyhnutne opakovať v každej analýze prípadu patriaceho do tej istej kategórie porušení. Pri prípadoch patriacich do tej istej

[9] Článok 33 ods. 4 všeobecného nariadenia o ochrane údajov.

kategórie sa uvádzajú len rozdiely. Čitateľ by si mal preto prečítať všetky prípady relevantné pre príslušnú kategóriu porušenia, aby mohol identifikovať a rozlišovať všetky správne opatrenia, ktoré sa majú prijať.

15. Interné zdokumentovanie porušenia je povinnosťou bez ohľadu na riziká súvisiace s týmto porušením a musí sa uskutočniť v každom jednom prípade. Cieľom prípadov uvedených ďalej v texte je objasniť, či porušenie treba oznámiť dozornému orgánu a dotknutým osobám, ktorých sa týka.

2. RANSOMVÉR

16. Častým prípadom oznámenia porušenia ochrany údajov je ransomvérový útok, ktorý zasiahol prevádzkovateľa. V týchto prípadoch sa pomocou škodlivého kódu zašifrujú osobné údaje a útočník následne žiada od prevádzkovateľa výkupné výmenou za dešifrovací kód. Tento druh útoku zvyčajne možno zaradiť medzi porušenie dostupnosti, no často môže dôjsť aj k porušeniu dôvernosti.

2.1. PRÍPAD č. 01: Ransomvér s vhodnou zálohou [proper backup] a bez exfiltrácie

Počítačové systémy malej výrobnej spoločnosti boli vystavené ransomvérovému útoku a údaje uložené v týchto systémoch boli zašifrované. Prevádzkovateľ používal šifrovanie v pokoji [encryption at rest], takže všetky údaje, ku ktorým sa ransomvér dostal, boli uložené v zašifrovanej podobe pomocou najmodernejšieho [state-of-the-art] šifrovacieho algoritmu. Počas útoku nedošlo k odhaleniu dešifrovacieho kľúča, t. j. útočník ho nemohol získať ani ho nepriamo použiť. Útočník tak mal prístup len k zašifrovaným osobným údajom. Predovšetkým nebol zasiahnutý ani systém elektronickej pošty spoločnosti, ani žiadne klientské systémy používané na prístup k nemu. Spoločnosť na vyšetrovanie incidentu využíva odborné znalosti externej spoločnosti z oblasti kybernetickej bezpečnosti. Sú k dispozícii logy o všetkých tokoch údajov odchádzajúcich zo spoločnosti (vrátane odoslanej pošty). Po analýze logov a údajov získaných pomocou systémov detekcie, ktoré má spoločnosť zavedené, sa na základe interného vyšetrovania s asistenciou externej spoločnosti z oblasti kybernetickej bezpečnosti s *istotou* zistilo, že páchateľ len zašifroval údaje bez toho, aby ich exfiltroval. Logy neukazujú žiadne toky údajov smerujúce von počas obdobia útoku. Osobné údaje, ktorých sa porušenie týka, sa týkajú klientov a zamestnancov spoločnosti, pričom celkovo ide o niekoľko desiatok jednotlivcov. Okamžite bola k dispozícii záloha a údaje sa obnovili už niekoľko hodín po útoku. Porušenie nemalo žiadne dôsledky pre každodennú činnosť prevádzkovateľa. Nedošlo k omeškaniu platieb zamestnancov ani vybavovania žiadostí klientov.

17. V tomto prípade boli splnené tieto prvky vymedzenia pojmu „porušenie ochrany osobných údajov“: porušenie bezpečnosti viedlo k nezákonnej zmene uložených údajov alebo neoprávnenému prístupu k nim.

2.1.1. PRÍPAD č. 01 – Predchádzajúce opatrenia a posúdenie rizika

18. Rovnako ako pri všetkých rizikách, ktoré predstavujú externí aktéri, pravdepodobnosť úspešného ransomvérového útoku možno výrazne znížiť sprísnením bezpečnosti prostredia, v ktorom sa manipuluje s údajmi. Väčšine týchto porušení možno predísť, ak sa zabezpečí, že sú zavedené vhodné organizačné, fyzické a technologické opatrenia. Príkladmi takýchto opatrení sú náležité riadenie opráv [patch management] a používanie vhodného systému na odhalenie malvéru. Ak je k dispozícii vhodné a samostatné zálohovanie, pomôže to zmierniť dôsledky v prípade úspešného útoku. Okrem toho program vzdelávania, odbornej prípravy a informovanosti zamestnancov (SETA) pomôže predchádzať tomuto druhu útokov a rozpoznávať ho. (V oddiele 2.5 sa nachádza zoznam odporúčaných opatrení.) Spomedzi nich je jedným z najdôležitejších opatrení náležité riadenie opráv, ktorým sa zabezpečí, že systémy sú aktuálne a že všetky známe zraniteľnosti zavedených systémov sú vyriešené, keďže pri väčšine ransomvérových útokov sa využívajú známe zraniteľnosti.

19. Pri posudzovaní rizík by prevádzkovateľ mal vyšetriť porušenie a identifikovať druh škodlivého kódu, aby porozumel možným dôsledkom útoku. Medzi riziká, ktoré treba zvážiť, patrí riziko, že údaje boli exfiltrované bez toho, aby po tom zostala stopa v systémových logoch.

20. V tomto prípade mal útočník prístup k osobným údajom a dôvernosť šifrovaného textu obsahujúceho osobné údaje v zašifrovanej podobe bola narušená. Žiadne údaje, ktoré mohli byť exfiltrované, však páchateľ nemôže prečítať ani použiť, a to aspoň zatiaľ. Technika šifrovania údajov, ktorú používa prevádzkovateľ, zodpovedá najnovšiemu [state-of-the-art] vývoju. Dešifrovací kľúč nebol odhalený a pravdepodobne ho ani nemožno zistiť iným spôsobom. V dôsledku toho sa riziká pre práva a slobody fyzických osôb v súvislosti s dôvernosťou znižujú na minimum, ak sa v kryptoanalýze nedosiahne pokrok, vďaka ktorému budú šifrované údaje v budúcnosti čitateľné.

21. Prevádzkovateľ by mal zohľadniť riziko hroziace jednotlivcom v dôsledku porušenia[10]. V tomto prípade sa zdá, že riziká pre práva a slobody dotknutých osôb vyplývajú z nedostatočnej dostupnosti osobných údajov a dôvernosť osobných údajov nie je narušená[11]. Pri tomto príklade boli nepriaznivé účinky porušenia zmiernené relatívne rýchlo po tom, ako došlo k porušeniu. Vhodný režim zálohovania [12] znižuje závažnosť účinkov porušenia a v tomto prípade bol prevádzkovateľ schopný účinne ho využiť.

22. Pokiaľ ide o závažnosť dôsledkov pre dotknuté osoby, zistili sa len menej závažné dôsledky, keďže údaje, ktorých sa porušenie týkalo, boli obnovené o niekoľko hodín, porušenie nemalo žiadne dôsledky pre každodennú činnosť prevádzkovateľa a významne neovplyvnilo dotknuté osoby (napr. platby zamestnancov alebo vybavovanie žiadostí klientov).

2.1.2. PRÍPAD č. 01 – Zmiernenie a povinnosti

23. Bez zálohy by prevádzkovateľ mohol prijať len málo opatrení na nápravu straty osobných údajov a údaje by bolo treba znova získať. V tomto konkrétnom prípade však bolo možné účinne eliminovať následky útoku tak, že všetky napadnuté systémy sa vrátili do známeho čistého stavu [known clean state], opravili sa zraniteľnosti a údaje, ktorých sa porušenie týka, sa obnovili hneď po útoku. Bez zálohy dochádza k strate údajov a závažnosť sa môže zvýšiť, pretože by mohli hroziť väčšie riziká alebo následky pre jednotlivcov.

---

[10] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri dokument pracovnej skupiny zriadenej podľa článku 29 s názvom Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“, WP248 rev. 01 – schválené EDPB, https://ec.europa.eu/newsroom/article29/items/611236, s. 9.

[11] Po technickej stránke zašifrovanie údajov znamená „prístup“ k pôvodným údajom a v prípade ransomvéru vymazanie pôvodných údajov – na prístup k týmto údajom treba ransomvérový kód, pomocou ktorého sa zašifrujú a odstránia sa pôvodné údaje. Útočník si pred vymazaním môže pôvodné údaje skopírovať, ale nie vždy dochádza k extrakcii osobných údajov. V priebehu prevádzkovateľovho vyšetrovania sa môžu objaviť nové informácie, ktoré zmenia toto posúdenie. Prístup, ktorý vedie k nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov alebo bezpečnostnému riziku pre dotknutú osobu môže byť aj bez interpretácie týchto údajov rovnako závažný ako prístup s interpretáciou osobných údajov.

[12] Postupy zálohovania by mali byť štruktúrované, jednotné a opakovateľné. Príkladmi postupov zálohovania sú metóda 3-2-1 a metóda „Grandfather-Father-Son“. Každá metóda by sa mala otestovať v súvislosti s účinnosťou pokrytia a času obnovy údajov. Testovanie by sa ďalej malo pravidelne opakovať, a to najmä ak dôjde k zmenám spracovateľskej operácie alebo jej podmienok, aby sa zaručila integrita systému.

24. Kľúčovou premennou pri analýze porušenia je včasnosť účinnej obnovy údajov z rýchlo dostupnej zálohy. Stanovenie vhodného časového rámca obnovy napadnutých údajov závisí od jedinečných okolností daného porušenia. Vo všeobecnom nariadení o ochrane údajov sa uvádza, že porušenie ochrany osobných údajov sa oznámi bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín. Preto sa stanovilo, že prekročenie 72-hodinovej lehoty sa v žiadnom prípade neodporúča, no pri riešení prípadov s vysokou úrovňou rizika sa môže aj dodržanie tejto lehoty považovať za neuspokojivé.

25. V tomto prípade prevádzkovateľ po podrobnom posúdení vplyvu a postupe reakcie na incident zistil, že nie je pravdepodobné, že porušenie povedie k riziku pre práva a slobody fyzických osôb, preto nie je potrebné informovať dotknuté osoby, ani sa nevyžaduje oznámenie porušenia dozornému orgánu. Rovnako ako všetky porušenia ochrany údajov sa však musí zdokumentovať v súlade s článkom 33 ods. 5. Organizácia možno takisto bude musieť aktualizovať alebo zlepšiť svoje organizačné a technické opatrenia a postupy v oblasti prístupu k bezpečnosti osobných údajov a zmierňovania rizika (alebo ju o to neskôr môže požiadať dozorný orgán). V rámci tejto aktualizácie a nápravy by organizácia mala dôkladne vyšetriť porušenie a zistiť príčiny a metódy, ktoré páchateľ použil, aby v budúcnosti predišla podobným udalostiam.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	X	X

2.2. PRÍPAD č. 02: Ransomvér bez vhodnej zálohy

Jeden z počítačov, ktoré používa poľnohospodárska spoločnosť, bol vystavený ransomvérovému útoku a údaje uložené v ňom útočník zašifroval. Spoločnosť na monitorovanie svojej siete využíva odborné znalosti externej spoločnosti z oblasti kybernetickej bezpečnosti. Sú k dispozícii logy o všetkých tokoch údajov odchádzajúcich zo spoločnosti (vrátane odoslanej pošty). Po analýze logov a údajov získaných pomocou iných systémov detekcie sa na základe interného vyšetrovania s asistenciou spoločnosti z oblasti kybernetickej bezpečnosti zistilo, že páchateľ len zašifroval údaje bez toho, aby ich exfiltroval. Logy neukazujú žiadne toky údajov smerujúce von počas obdobia útoku. Osobné údaje, ktorých sa porušenie týka, sa týkajú zamestnancov a klientov spoločnosti, pričom celkovo ide o niekoľko desiatok jednotlivcov. Porušenie sa netýkalo žiadnej osobitnej kategórie údajov. Nebola k dispozícii žiadna záloha v elektronickej podobe. Väčšina údajov sa obnovila pomocou záloh v papierovej podobe. Obnova údajov trvala päť dní a spôsobila malé oneskorenie dodania objednávok zákazníkom.

2.2.1. PRÍPAD č. 02 – Predchádzajúce opatrenia a posúdenie rizika

26. Prevádzkovateľ mal prijať rovnaké predchádzajúce opatrenia ako sa uvádzajú v časti 2.1 a oddiele 2.9. Hlavným rozdielom v porovnaní s predchádzajúcim prípadom je chýbajúca elektronická záloha a chýbajúce šifrovanie v pokoji]. Z toho vyplývajú kľúčové rozdiely v nasledujúcich krokoch.

27. Pri posudzovaní rizík by prevádzkovateľ mal vyšetriť metódu preniknutia a identifikovať druh škodlivého kódu, aby porozumel možným dôsledkom útoku. V tomto prípade ransomvér zašifroval osobné údaje bez toho, aby ich exfiltroval. V dôsledku toho sa zdá, že riziká pre práva a slobody dotknutých osôb vyplývajú z nedostatočnej dostupnosti osobných údajov a dôvernosť osobných údajov nie je narušená. Pri stanovení rizika je kľúčové dôkladné posúdenie logov z firewallu a ich dôsledkov. Prevádzkovateľ by mal na požiadanie predložiť skutkové zistenia z týchto vyšetrovaní.

28. Prevádzkovateľ musí pamätať na to, že ak je útok rafinovanejší, malvér je schopný zmeniť logy a vymazať stopy. Vzhľadom na to, že logy sa nepreposielajú ani nekopírujú na centrálny server logov, prevádzkovateľ ani po dôkladnom vyšetrení, počas ktorého sa zistilo, že útočník neexfiltroval osobné údaje, nemôže vyhlásiť,

že chýbajúci logový záznam je dôkazom toho, že nedošlo k exfiltrácii, preto nemožno jednoznačne vylúčiť pravdepodobnosť porušenia dôvernosti.

29. Ak útočník získal prístup k údajom, prevádzkovateľ by mal posúdiť riziká vyplývajúce z toho porušenia[13]. Počas posudzovania rizika by prevádzkovateľ takisto mal zohľadniť povahu, citlivosť, objem a súvislosti osobných údajov, ktorých sa porušenie týka. V tomto prípade sa porušenie netýka žiadnych osobitných kategórií osobných údajov a ide o malé množstvo údajov, ktorých ochrana bola porušená, a nízky počet dotknutých osôb, ktorých sa porušenie týka.

30. Získanie presných informácií o neoprávnenom prístupe je kľúčové pre stanovenie úrovne rizika a predchádzanie novým alebo pokračujúcim útokom. Ak by sa údaje skopírovali z databázy, tento faktor by jednoznačne zvýšil riziko. V prípade pochybností o špecifikách neoprávneného prístupu by sa malo vychádzať z najhoršieho scenára a podľa toho by sa malo posúdiť riziko.

31. Chýbajúcu zálohu databázy [backup database] možno považovať za faktor zvyšujúci riziko v závislosti od závažnosti dôsledkov pre dotknuté osoby vyplývajúcich z nedostupnosti údajov.

2.2.2. PRÍPAD č. 02 – Zmiernenie a povinnosti

32. Bez zálohy by prevádzkovateľ mohol prijať len málo opatrení na nápravu straty osobných údajov, a ak nie je k dispozícii žiadny iný zdroj (napr. e-maily s potvrdením objednávok), údaje by bolo treba znova získať. Bez zálohy môže dôjsť k strate údajov a závažnosť bude závisieť od následkov pre jednotlivcov.

33. Obnova údajov by sa nemala ukázať ako príliš problematická[14], ak sú údaje ešte dostupné v papierovej podobe, no vzhľadom na chýbajúcu elektronickú zálohu databázy sa oznámenie dozornému orgánu považuje za nevyhnutné, keďže obnova údajov trvala určitú dobu a mohla spôsobiť mierne oneskorenie dodania objednávok zákazníkom a značná časť metaúdajov (napr. logy, časové pečiatky) môže byť neobnoviteľná.

34. Informovanie dotknutých osôb o porušení môže takisto závisieť od dĺžky obdobia, počas ktorého sú osobné údaje nedostupné, a od ťažkostí, ktoré z toho môžu vyplývať pre činnosť prevádzkovateľa (napr. oneskorenie platieb zamestnancov). Keďže toto oneskorenie platieb a dodávok môže jednotlivcom, ktorých osobné údaje boli napadnuté, spôsobiť finančnú stratu, možno takisto tvrdiť, že porušenie pravdepodobne povedie k vysokému riziku. Takisto je možné, že bude nevyhnutné informovať dotknuté osoby, ak je ich pomoc nutná na obnovu šifrovaných údajov.

35. Tento prípad je príkladom ransomvérového útoku s rizikom pre práva a slobody dotknutých osôb, ktoré však nie je vysokým rizikom. Mal by sa zdokumentovať v súlade s článkom 33 ods. 5 a oznámiť dozornému orgánu v súlade s článkom 33 ods. 1. Organizácia možno takisto bude musieť (alebo ju o to môže požiadať dozorný orgán) aktualizovať alebo zlepšiť svoje organizačné a technické opatrenia a postupy v oblasti prístupu k bezpečnosti osobných údajov a zmierňovania rizika.

---

[13] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

[14] Bude to závisieť od zložitosti a štruktúry osobných údajov. V najzložitejších scenároch si môže obnova integrity údajov, konzistentnosti s metaúdajmi, zaistenie správnych vzťahov v rámci štruktúr údajov a kontrola presnosti údajov vyžadovať značné zdroje a úsilie.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	X

2.3. PRÍPAD č. 03: Ransomvér so zálohou a bez exfiltrácie v nemocnici

Informačný systém nemocnice/zdravotného strediska bol vystavený ransomvérovému útoku a útočník zašifroval značnú časť jeho údajov. Spoločnosť na monitorovanie svojej siete využíva odborné znalosti externej spoločnosti z oblasti kybernetickej bezpečnosti. K dispozícii sú logy o všetkých tokoch údajov odchádzajúcich zo spoločnosti (vrátane odoslanej pošty). Po analýze logov a údajov získaných pomocou iných systémov detekcie sa na základe interného vyšetrovania s asistenciou spoločnosti z oblasti kybernetickej bezpečnosti zistilo, že páchateľ len zašifroval údaje bez toho, aby ich exfiltroval. Logy neukazujú žiadne toky údajov smerujúce von počas obdobia útoku. Osobné údaje, ktorých sa porušenie týka, sa týkajú zamestnancov a pacientov, pričom ide o tisíce jednotlivcov. K dispozícii boli zálohy v elektronickej podobe. Väčšina údajov bola obnovená, no táto činnosť trvala dva pracovné dni, čo viedlo k veľkému omeškaniu liečby pacientov spojenému s rušením a odkladom operácií a k zníženiu úrovne služieb v dôsledku nedostupnosti systémov.

2.3.1. PRÍPAD č. 03 – Predchádzajúce opatrenia a posúdenie rizika

36. Prevádzkovateľ mal prijať rovnaké predchádzajúce opatrenia, ako sa uvádzajú v časti 2.1 a oddiele 2.5. Hlavným rozdielom v porovnaní s predchádzajúcim prípadom je vysoká závažnosť dôsledkov pre veľkú časť dotknutých osôb[15].

37. Keďže nemocnice zvyčajne spracúvajú veľké množstvá údajov, ide o veľké množstvo osobných údajov, ktorých ochrana bola porušená, a vysoký počet dotknutých osôb, ktorých sa porušenie týka. Nedostupnosť údajov má závažné následky pre veľkú časť dotknutých osôb. Okrem toho hrozí vysoko závažné zvyškové riziko v súvislosti s dôvernosťou údajov o pacientoch.

38. Dôležitými prvkami sú druh porušenia, povaha, citlivosť a objem osobných údajov, ktorých sa porušenie týka. Hoci existovali zálohy údajov a údaje sa podarilo obnoviť o niekoľko dní, stále hrozí vysoké riziko v dôsledku závažnosti dôsledkov pre dotknuté osoby vyplývajúcich z nedostupnosti údajov v čase útoku a v nasledujúcich dňoch.

2.3.2. PRÍPAD č. 03 – Zmiernenie a povinnosti

39. Oznámenie dozornému orgánu sa považuje za nevyhnutné, keďže ide o osobitné kategórie osobných údajov a obnova údajov by mohla dlho trvať, čo by spôsobilo veľké oneskorenie starostlivosti o pacientov. Informovanie dotknutých osôb o porušení je nevyhnutné v dôsledku následkov pre pacientov, a to aj po obnove šifrovaných údajov. Hoci boli zašifrované údaje o všetkých pacientoch, ktorí sa v nemocnici v posledných rokoch liečili, zasiahnutí boli len tí pacienti, ktorí mali v nemocnici naplánovanú liečbu v čase, keď bol počítačový systém nedostupný. Prevádzkovateľ by mal týchto pacientov priamo informovať o porušení ochrany údajov. Vzhľadom na výnimku v článku 34 ods. 3 písm. c) nemusí byť potrebná priama komunikácia s ostatnými pacientmi, z ktorých mnohí v nemocnici možno už neboli viac než dvadsať rokov.

[15] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

V takom prípade dôjde namiesto toho k informovaniu verejnosti[16] alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom. V tomto prípade by nemocnica mala verejne informovať o ransomvérovom útoku a jeho dôsledkoch.

40. Tento prípad je príkladom ransomvérového útoku s vysokým rizikom pre práva a slobody dotknutých osôb. Mal by sa zdokumentovať v súlade s článkom 33 ods. 5 a oznámiť dozornému orgánu v súlade s článkom 33 ods. 1 a dotknutým osobám v súlade s článkom 34 ods. 1. Organizácia takisto musí aktualizovať alebo zlepšiť svoje organizačné a technické opatrenia a postupy v oblasti prístupu k bezpečnosti osobných údajov a zmierňovania rizika.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	✓

2.4. PRÍPAD č. 04: Ransomvér bez zálohy a s exfiltráciou

Server dopravného podniku bol vystavený ransomvérovému útoku a údaje uložené v ňom útočník zašifroval. Podľa zistení z interného vyšetrovania páchateľ údaje nielen zašifroval, ale aj exfiltroval. Údaje, ktorých ochrana bola porušená, predstavovali osobné údaje klientov a zamestnancov a niekoľko tisíc ľudí využívajúcich služby podniku (napr. nákup lístkov online). Okrem základných údajov o totožnosti sa porušenie týkalo aj čísiel dokladov totožnosti a finančných údajov, ako sú údaje o kreditných kartách. Existovala záloha databázy, no aj tú útočník zašifroval.

2.4.1. PRÍPAD č. 04 – Predchádzajúce opatrenia a posúdenie rizika

41. Prevádzkovateľ mal prijať rovnaké predchádzajúce opatrenia, ako sa uvádzajú v časti 2.1 a oddiele 2.5. Hoci bola k dispozícii záloha, takisto bola predmetom útoku. Už tento postup vzbudzuje pochybnosti o kvalite dovtedajších opatrení prevádzkovateľa v oblasti IT bezpečnosti a počas vyšetrovania by sa mal podrobnejšie prešetriť, keďže v rámci náležite navrhnutého režimu zálohovania musia byť viaceré zálohy bezpečne uložené bez prístupu z hlavného systému, inak by mohli byť ohrozené tým istým útokom. Okrem toho ransomvérové útoky môžu zostať neodhalené niekoľko dní, počas ktorých sa pomaly šifrujú zriedka používané údaje. Viaceré zálohy sa tak môžu stať zbytočnými, takže zálohy by sa mali takisto vytvárať pravidelne a mali by byť samostatné. Zvýšila by sa tak pravdepodobnosť obnovy, hoci s väčšou stratou údajov.

42. Toto porušenie sa netýka len dostupnosti údajov, ale aj dôvernosti, keďže útočník mohol zmeniť a/alebo skopírovať údaje zo serveru. Tento druh porušenia preto vedie k vysokému riziku[17].

[16] V odôvodnení 86 všeobecného nariadenia o ochrane údajov sa vysvetľuje, že *„[t]akéto informovanie dotknutých osôb by sa malo vykonať čo najskôr je to možné, a v úzkej spolupráci s dozorným orgánom v súlade s usmerneniami tohto alebo iného relevantného orgánu, napríklad orgánov presadzovania práva. Napríklad potreba zmierniť bezprostredné riziko škody by si vyžadovala promptné informovanie dotknutých osôb, avšak potreba vykonať primerané opatrenia na zabránenie trvaniu alebo výskytu podobných porušení ochrany osobných údajov môže opodstatniť aj dlhšiu lehotu na informovanie“.*

[17] Pre usmernenia k spracovateľským operáciám, ktoré *„pravdepodobne povedú k vysokému riziku“*, pozri poznámku pod čiarou č. 10.

43. V dôsledku povahy, citlivosti a objemu osobných údajov sa ešte viac zvyšujú riziká, pretože ide o vysoký počet jednotlivcov, ako aj veľké množstvo osobných údajov, ktorých sa porušenie týka. Okrem základných údajov o totožnosti sa porušenie týkalo aj dokladov totožnosti a finančných údajov, ako sú údaje o kreditných kartách. Porušenie ochrany údajov v prípade týchto druhov údajov predstavuje vysoké riziko samo o sebe, a ak sa spracujú spoločne, mohli by sa použiť okrem iného na krádež totožnosti alebo podvod.

44. V dôsledku buď chybnej serverovej logiky, alebo chybných organizačných kontrol, ransomvérový útok zasiahol záložné súbory [backup files], čím sa zabránilo obnoveniu údajov a zvýšilo sa riziko.

45. Toto porušenie ochrany údajov predstavuje vysoké riziko pre práva a slobody jednotlivcov, pretože pravdepodobne povedie k majetkovej (napr. finančná strata, keďže porušenie sa týkalo kreditných kariet) aj nemajetkovej ujme (napr. krádež totožnosti alebo podvod, keďže porušenie sa týkalo údajov z dokladov totožnosti).

2.4.2. PRÍPAD č. 04 – Zmiernenie a povinnosti

46. Informovanie dotknutých osôb je kľúčové, aby mohli podniknúť kroky potrebné na predídenie majetkovej ujme (napr. zablokovať si kreditné karty).

47. Okrem zdokumentovania porušenia v súlade s článkom 33 ods. 5 je v tomto prípade povinné oznámenie dozornému orgánu (článok 33 ods. 1) a prevádzkovateľ je takisto povinný oznámiť porušenie dotknutým osobám (článok 34 ods. 1). Porušenie by sa dotknutým osobám mohlo oznámiť jednotlivo, no v prípade jednotlivcov, ktorých kontaktné údaje nie sú k dispozícii, by tak prevádzkovateľ mal urobiť verejne za predpokladu, že takéto oznámenie by nemalo ďalšie negatívne dôsledky pre dotknuté osoby, napr. prostredníctvom oznámenia na svojom webovom sídle. Tento prípad si vyžaduje presné a jasné oznámenie, ľahko viditeľné na domovskej stránke prevádzkovateľa, s presnými odkazmi na príslušné ustanovenia všeobecného nariadenia o ochrane údajov. Organizácia takisto možno bude musieť aktualizovať alebo zlepšiť svoje organizačné a technické opatrenia a postupy v oblasti prístupu k bezpečnosti osobných údajov a zmierňovania rizika.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	✓

2.5. Organizačné a technické opatrenia na predchádzanie následkom ransomvérových útokov alebo na ich zmiernenie

48. Skutočnosť, že bolo možné, aby k ransomvérovému útoku došlo, je zvyčajne znakom jednej alebo viacerých zraniteľností v systéme prevádzkovateľa. Platí to aj v prípadoch ransomvéru, v ktorých boli osobné údaje zašifrované, no neboli exfiltrované. Bez ohľadu na výsledok a dôsledky útoku je nevyhnutné dostatočne zdôrazniť dôležitosť komplexného hodnotenia systému bezpečnosti údajov – s osobitným zameraním na IT bezpečnosť. Zistené zraniteľné miesta a medzery v bezpečnosti treba bezodkladne zdokumentovať a riešiť.

49. Odporúčané opatrenia:

(Zoznam nasledujúcich opatrení nie je v žiadnom prípade výlučný ani úplný. Jeho cieľom je predstaviť návrhy v oblasti prevencie a možné riešenia. Každá spracovateľská činnosť je iná, a preto by sa mal prevádzkovateľ rozhodnúť, ktoré opatrenia sa v danej situácii najviac hodia.)

- Priebežná aktualizácia firmvéru [firmware], operačného systému a aplikačného softvéru na serveroch, klientskych zariadeniach, aktívnych prvkov siete a na všetkých ostatných zariadeniach v tej istej miestnej sieti [LAN] (vrátane zariadení s bezdrôtovým pripojením [Wi-Fi]). Zabezpečenie vhodných opatrení

v oblasti IT bezpečnosti, uistenie sa o ich účinnosti a ich pravidelná aktualizácia pri zmene alebo vývoji spracúvania alebo okolností. Zahŕňa to vedenie podrobných logov o tom, ktoré opravy sa uskutočnili, na ktorej časovej známke.

- Navrhovanie a organizácia systémov a infraštruktúry spracúvania na segmentáciu alebo izoláciu systémov a sietí s údajmi s cieľom zabrániť šíreniu malvéru v rámci organizácie a do externých systémov.
- Existencia aktuálneho, bezpečného a odskúšaného postupu zálohovania. Médiá na strednodobé a dlhodobé zálohy by sa mali uchovávať oddelene od operačného úložiska údajov a tretích strán, ktoré by k nim nemali mať prístup ani v prípade úspešného útoku (ako napríklad každodenné prírastkové zálohovanie [incremental backup] alebo týždenné úplné zálohovanie [full backup]).
- Používanie/získanie vhodného, aktuálneho, účinného a integrovaného softvéru proti malvéru.
- Používanie vhodného, aktuálneho, účinného a integrovaného firewallu a systému detekcie a prevencie prienikov. Usmerňovanie sieťovej prevádzky cez firewall/detekciu prienikov, a to aj v prípade práce z domu alebo mobilnej práce (napr. pomocou pripojení VPN k organizačným bezpečnostným mechanizmom pri prístupe na internet).
- Odborná príprava zamestnancov v oblasti rozpoznávania IT útokov a ich prevencie. Prevádzkovateľ by mal zabezpečiť prostriedky na stanovenie toho, či e-maily a správy získané inými komunikačnými prostriedkami sú pravé a dôveryhodné. Zamestnanci by mali absolvovať odbornú prípravu s cieľom rozpoznávať, kedy došlo k takémuto útoku a ako odpojiť koncový bod od siete, a o svojej povinnosti okamžite to oznámiť osobe zodpovednej za bezpečnosť.
- Zdôraznenie potreby identifikovať druh škodlivého kódu s cieľom zistiť dôsledky útoku a vedieť nájsť správne opatrenia na zmiernenie rizika. V prípade, že ransomvérový útok bol úspešný a nie je k dispozícii žiadna záloha, možno pri opätovnom získaní údajov použiť nástroje, ako sú nástroje projektu „no more ransom“ (nomoreransom.org). V prípade, že je k dispozícii bezpečná záloha, odporúča sa obnova údajov zo zálohy.
- Preposielanie alebo kopírovanie všetkých logov na centrálny server logov (prípadne vrátane podpisovania alebo kryptografických časových známok záznamov logov [log entries]).
- Silné šifrovanie a viacstupňová autentifikácia, najmä pre administratívny prístup k systémom IT, náležité riadenie kľúčov a hesiel.
- Pravidelné testovanie zraniteľností a penetračné testovanie.
- Zriadenie jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT) alebo tímu reakcie na núdzové počítačové situácie (CERT) v rámci organizácie alebo zapojenie sa do kolektívnej jednotky CSIRT/kolektívneho tímu CERT. Vypracovanie plánu reakcie na incidenty, plánu obnovy systému po zlyhaní a plánu na zabezpečenie kontinuity činností a zabezpečenie ich dôkladného testovania.
- Pri posudzovaní protiopatrení by sa mala preskúmať, otestovať a aktualizovať analýza rizika.

3. ÚTOKY S EXFILTRÁCIOU ÚDAJOV

50. Útoky využívajúce zraniteľnosti v službách, ktoré prevádzkovateľ ponúka tretím stranám cez internet, napr. spáchané prostredníctvom injekčných útokov [injection attacks] (napr. útok typu „SQL injection“, „path traversal“), kompromitovanie webového sídla a podobné metódy sa môžu podobať na ransomvérové útoky v tom zmysle, že riziko vyplýva z konania neoprávnenej tretej strany, no cieľom týchto útokov je zvyčajne kopírovať, exfiltrovať a zneužiť osobné údaje na nekalé účely. Preto ide predovšetkým o porušenie dôvernosti a prípadne aj integrity údajov. Zároveň platí, že ak prevádzkovateľ pozná charakteristiky tohto druhu porušení k dispozícii má mnohé opatrenia, ktorými môže značne znížiť riziko úspešného vykonania útoku.

3.1. PRÍPAD č. 05: Exfiltrácia údajov zo žiadostí o zamestnanie z webového sídla

Personálna agentúra sa stala obeťou kybernetického útoku, počas ktorého útočníci umiestnili na jej webové sídlo škodlivý kód. Prostredníctvom tohto škodlivého kódu získala neoprávnená osoba (neoprávnené osoby) prístup k osobným informáciám poskytnutým prostredníctvom online formulárov na uchádzanie sa o zamestnanie uloženým na webovom serveri. Útok sa pravdepodobne týkal 213 takýchto formulárov, po analýze údajov, ktorých sa porušenie týkalo, sa zistilo, že porušenie sa netýkalo žiadnej osobitnej kategórie údajov. Tento nainštalovaný súbor malvérových nástrojov [malware toolkit] mal funkcie, ktoré útočníkovi umožnili vymazať všetky záznamy o exfiltrácii a takisto mu umožnili monitorovanie spracúvania na serveri a zachytávanie osobných údajov. Tento súbor nástrojov bol odhalený až mesiac po jeho inštalácii.

3.1.1. PRÍPAD č. 05 – Predchádzajúce opatrenia a posúdenie rizika

51. Nesmierne dôležitá je bezpečnosť prostredia prevádzkovateľa, keďže väčšine týchto porušení možno predísť, ak sa zabezpečí, že všetky systémy sa neustále aktualizujú, citlivé údaje sa šifrujú a aplikácie sa vyvíjajú v súlade s vysokými bezpečnostnými normami, ako je silná autentifikácia, opatrenia na zaistenie proti útokom hrubou silou [brute force attacks], „escaping“ alebo „sanitácia“[18] používateľských vstupov atď. Na včasné odhalenie týchto druhov zraniteľností a ich nápravu sú takisto potrebné pravidelné bezpečnostné IT audity, posúdenia zraniteľností a penetračné testy. V tomto konkrétnom prípade mohli nástroje na monitorovanie integrity súborov vo vývojárskom prostredí [production environment] pomôcť odhaliť injekciu kódu [code injection]. (V oddiele 3.7 sa nachádza zoznam odporúčaných opatrení.)

52. Prevádzkovateľ by mal vždy začať vyšetrovanie porušenia tým, že identifikuje druh útoku a jeho metódy, aby posúdil, aké opatrenia sa majú prijať. V záujme rýchlosti a účinnosti by prevádzkovateľ mal mať zavedený plán reakcie na incidenty, v ktorom sa uvádzajú rýchle kroky potrebné na zvládnutie incidentu. V tomto konkrétnom prípade bol daný druh porušenia faktorom zvyšujúcim riziko, keďže nielenže bola narušená dôvernosť údajov, ale páchateľ mal takisto prostriedky na vykonanie zmien v systéme, čím sa spochybnila aj integrita údajov.

53. S cieľom stanoviť, aký je rozsah dôsledkov porušenia na dotknuté osoby, by sa mala posúdiť povaha, citlivosť a objem osobných údajov, ktorých sa porušenie týka. Hoci sa porušenie netýkalo žiadnych osobitných kategórií údajov, údaje, ku ktorým útočník získal prístup, obsahovali významné množstvo informácií o jednotlivcoch z online formulárov a tieto údaje by mohli byť zneužité viacerými spôsobmi (oslovovanie s nevyžiadaným marketingom, krádež totožnosti atď.), takže závažnosť dôsledkov by mohla zvýšiť riziko pre práva a slobody dotknutých osôb[19].

3.1.2. PRÍPAD č. 05 – Zmiernenie a povinnosti

54. Ak je to možné, po vyriešení problému by sa databáza mala porovnať s databázou uloženou na zabezpečenej zálohe. Poznatky získané z porušenia by sa mali využiť na aktualizáciu IT infraštruktúry. Prevádzkovateľ by mal vrátiť všetky zasiahnuté IT systémy do známeho čistého stavu [known clean state], napraviť zraniteľnosti a prijať nové bezpečnostné opatrenia s cieľom predchádzať podobným porušeniam ochrany údajov v budúcnosti, napr. kontroly integrity súborov a bezpečnostné audity. Ak

[18] Escaping alebo sanitácia používateľských vstupov je forma validácie vstupov, ktorou sa zabezpečí, že do informačného systému sa zapíšu len riadne formátované údaje.

[19] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

dôjde nielen k exfiltrácii, ale aj k vymazaniu osobných údajov, prevádzkovateľ musí prijať systematické opatrenia na obnovu osobných údajov v stave, v akom boli pred porušením. Možno bude nevyhnutné použiť úplné zálohy, vykonať postupné zmeny [incremental changes] a prípadne zopakovať spracúvanie od posledného prírastkového zálohovania, na čo musí byť prevádzkovateľ schopný replikovať zmeny vykonané od posledného zálohovania. Na to môže byť potrebné, aby mal prevádzkovateľ systém navrhnutý tak, aby uchovával každodenné vstupné súbory pre prípad, že sa budú musieť znova spracúvať a to si vyžaduje spoľahlivú metódu ukladania a vhodnú politiku uchovávania.

55. Vzhľadom na uvedené skutočnosti o porušení treba rozhodne informovať dotknuté osoby (článok 34 ods. 1), keďže porušenie pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, čo samozrejme znamená, že príslušné dozorné orgány by takisto mali byť zapojené prostredníctvom oznámenia porušenia osobných údajov. Zdokumentovanie porušenia je povinné podľa článku 33 ods. 5 všeobecného nariadenia o ochrane údajov a uľahčuje vyhodnotenie situácie.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	✓

3.2. PRÍPAD č. 06: Exfiltrácia hašovaného hesla z webového sídla

Pri útoku typu „SQL injection“ sa využila zraniteľnosť s cieľom získať prístup k databáze servera webového sídla venovaného vareniu. Používatelia mali povolené zvoliť si ako používateľské mená len ľubovoľné pseudonymy. Boli nabádaní k tomu, aby na tento účel nepoužívali e-mailové adresy. Heslá uložené v databáze boli hašované pomocou silného algoritmu a kryptografická soľ (salt) nebola narušená. Údaje, ktorých sa porušenie týkalo: hašované heslá 1 200 používateľov. Prevádzkovateľ v záujme bezpečnosti informoval dotknuté osoby o porušení e-mailom a požiadal ich, aby si zmenili heslá, a to najmä ak používali tie isté heslá aj pre ďalšie služby.

3.2.1. PRÍPAD č. 06 – Predchádzajúce opatrenia a posúdenie rizika

56. V tomto konkrétnom prípade bola narušená dôvernosť údajov, no heslá v databáze boli hašované aktuálnou metódou, ktorá znižuje riziko v súvislosti s povahou, citlivosťou a objemom osobných údajov. Tento prípad nepredstavuje žiadne riziko pre práva a slobody dotknutých osôb.

57. Okrem toho neboli odhalené žiadne kontaktné údaje (napr. e-mailové adresy alebo telefónne čísla) dotknutých osôb, čo znamená, že nehrozí významné riziko, že dotknuté osoby sa stanú cieľom pokusov o podvod (napr. prijímanie phishingových e-mailov alebo podvodných textových správ a telefonátov). Porušenie sa netýkalo žiadnej osobitnej kategórie osobných údajov.

58. Niektoré používateľské mená možno považovať za osobné údaje, no predmet webového sídla ich neumožňuje zneužiť na nekalé účely. Treba však poznamenať, že posúdenie vplyvu sa môže zmeniť[20], ak by druh webového sídla a údaje, ku ktorým útočník získal prístup, mohli odhaliť osobitné kategórie osobných údajov (napr. webové sídlo politickej strany alebo odborovej organizácie). Používanie najmodernejšieho [state of the art] šifrovania by mohlo zmierniť nepriaznivé následky porušenia. Za predpokladu, že je povolený

[20] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

obmedzený počet pokusov o prihlásenie, predíde sa tým úspešným útokom hrubou silou na účely prihlásenia [brute force login attacks], čím sa značne znížia riziká, ktoré predstavujú útočníci, ktorí už poznajú používateľské mena.

3.2.2. PRÍPAD č. 06 – Zmiernenie a povinnosti

59. Oznámenie dotknutým osobám by sa v niektorých prípadoch mohlo považovať za zmierňujúci faktor, keďže dotknuté osoby sú takisto schopné prijať kroky potrebné na predídenie ďalšej ujme spôsobenej porušením, napríklad tým, že si zmenia heslo. V tomto prípade oznámenie nebolo povinné, no v mnohých prípadoch sa môže považovať za osvedčený postup.

60. Prevádzkovateľ by mal napraviť zraniteľnosť a prijať nové bezpečnostné opatrenia na predídenie podobným porušeniam ochrany údajov v budúcnosti, ako napríklad systematické bezpečnostné audity webového sídla.

61. Porušenie by sa malo zdokumentovať v súlade s článkom 33 ods. 5, no nie je potrebné žiadne oznámenie alebo informovanie.

62. Takisto sa dôrazne odporúča v každom prípade informovať dotknuté osoby o porušení týkajúcom sa hesiel, a to aj keď boli heslá uložené pomocou osoleného hašu [salted hash] s algoritmom zodpovedajúcim najnovšiemu vývoju [state-of-the art]. Vhodnejšie je používať autentifikačné metódy bez potreby spracúvania hesiel na strane servera. Dotknuté osoby by sa mali môcť rozhodnúť, či prijmú vhodné opatrenia v súvislosti so svojimi vlastnými heslami.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	X	X

3.3. PRÍPAD č. 07: Útok typu „credential stuffing“ na webovú stránku banky

Banka sa stala terčom kybernetického útoku na jedno z jej webových sídiel online bankovníctva. Cieľom útoku bolo vyskúšať všetky možné identifikátory na prihlásenie používateľa pomocou pevne stanoveného triviálneho hesla. Heslá sa skladajú z ôsmich číslic. V dôsledku zraniteľnosti webovej stránky v niektorých prípadoch informácie týkajúce sa dotknutých osôb (meno, priezvisko, rod, dátum a miesto narodenia, daňové číslo, kódy na overenie totožnosti používateľa) unikli a dostali sa k útočníkovi, hoci použité heslo nebolo správne alebo bankový účet už nebol aktívny. Porušenie sa týkalo približne 100 000 dotknutých osôb. Z nich sa útočník úspešne prihlásil približne do 2 000 účtov, ktoré používali triviálne heslo, ktoré útočník skúšal. Prevádzkovateľ bol po tomto čine schopný identifikovať všetky neoprávnené pokusy o prihlásenie. Prevádzkovateľ mohol potvrdiť, že podľa kontrol zameraných proti podvodom sa na týchto účtoch počas útoku nevykonali žiadne transakcie. Banka sa dozvedela o porušení ochrany údajov, pretože jej stredisko pre bezpečnostné operácie zaznamenalo veľký počet žiadostí o prihlásenie adresovaných tejto webovej stránke. Prevádzkovateľ následne zrušil možnosť prihlásiť sa na webovú stránku tým, že ju vypol a vykonal vynútené obnovenie hesiel napadnutých účtov. Prevádzkovateľ oznámil porušenie len používateľom s napadnutými účtami, t. j. používateľom, ktorých heslá boli odhalené alebo ktorých údaje unikli.

3.3.1. PRÍPAD č. 07 – Predchádzajúce opatrenia a posúdenie rizika

63. Treba uviesť, že prevádzkovatelia nakladajúci s údajmi veľmi citlivého charakteru[21] majú väčšiu zodpovednosť za zabezpečenie náležitej bezpečnosti údajov, napr. prevádzkovaním strediska pre bezpečnostné operácie a ďalšími opatreniami na predchádzanie incidentom, ich odhaľovanie a reakciu na ne. Nedodržiavanie týchto vyšších noriem s istotou povedie k závažnejším opatreniam počas vyšetrovania dozorného orgánu.

64. Porušenie sa týka finančných údajov iných ako totožnosť a informácie o identifikátoroch používateľov, a preto je mimoriadne závažné. Porušenie sa týka vysokého počtu jednotlivcov.

65. Skutočnosť, že v takomto citlivom prostredí mohlo dôjsť k porušeniu, poukazuje na veľké medzery v bezpečnosti systému prevádzkovateľa a môže byť znakom toho, že je potrebné preskúmať a aktualizovať opatrenia, ktorých sa porušenie týka v súlade s článkom 24 ods. 1, článkom 25 ods. 1 a článkom 32 ods. 1 všeobecného nariadenia o ochrane údajov. Údaje, ktorých ochrana bola porušená, umožňujú jedinečnú identifikáciu dotknutých osôb a obsahujú ďalšie informácie o nich (vrátane rodu, dátumu a miesta narodenia). Útočník ich môže použiť aj na to, aby uhádol heslá zákazníkov alebo uskutočnil kampaň cieleného phishingu [a spear phishing campaign] zameranú na zákazníkov banky.

66. Z týchto dôvodov sa možno domnievať, že porušenie ochrany údajov pravdepodobne povedie k vysokému riziku pre práva a slobody všetkých dotknutých osôb[22], ktorých sa týka. Možným výsledkom je preto spôsobenie majetkovej (napr. finančná strata) a nemajetkovej ujmy (napr. krádež totožnosti alebo podvod).

[21] Napríklad informácie dotknutých osôb, ktoré sa týkajú metód platby, ako sú čísla kariet, bankové účty, platba online, výplatné pásky, výpisy z bankového účtu, ekonomické štúdie alebo akékoľvek iné informácie, ktoré môžu odhaliť ekonomické informácie týkajúce sa dotknutých osôb.

[22] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

3.3.2. PRÍPAD č. 07 – Zmiernenie a povinnosti

67. Opatrenia prevádzkovateľa uvedené v opise prípadu sú primerané. Po porušení takisto napravil zraniteľnosti webovej stránky a podnikol ďalšie kroky na predídenie podobným porušeniam ochrany údajov v budúcnosti, napríklad pridaním dvojstupňovej autentifikácie na predmetnú webovú stránku a prechodom na silnú autentifikáciu zákazníka.

68. Zdokumentovanie porušenia podľa článku 33 ods. 5 všeobecného nariadenia o ochrane údajov a oznámenie porušenia dozornému orgánu v tomto scenári nie sú dobrovoľné. Prevádzkovateľ by ho mal oznámiť aj všetkým 100 000 dotknutým osobám (vrátane dotknutých osôb, ktorých účty neboli odhalené) v súlade s článkom 34 všeobecného nariadenia o ochrane údajov.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	✓

3.4. Organizačné a technické opatrenia na predchádzanie následkom hackerských útokov alebo na ich zmiernenie

69. Rovnako ako v prípade ransomvérových útokov, bez ohľadu na výsledok a dôsledky útoku, sú prevádzkovatelia v podobných prípadoch povinní prehodnotiť IT bezpečnosť.

70. Odporúčané opatrenia:[23]

(Zoznam nasledujúcich opatrení nie je v žiadnom prípade výlučný ani úplný. Jeho cieľom je predstaviť návrhy v oblasti prevencie a možné riešenia. Každá spracovateľská činnosť je iná, a preto by sa mal prevádzkovateľ rozhodnúť, ktoré opatrenia sa v danej situácii najviac hodia.)

- Najnovšie [state-of-the-art] šifrovanie a riadenie kľúčov, najmä v prípadoch, v ktorých sa spracúvajú heslá, citlivé alebo finančné údaje. Kryptografické hašovanie alebo solenie (salting) v prípade tajných informácií (hesiel) je vždy vhodnejšie ako šifrovanie hesiel. Vhodnejšie je používanie autentifikačných metód, ktoré eliminujú potrebu spracúvať heslá na strane servera.
- Priebežná aktualizácia systému (softvéru aj firmvéru). Zabezpečenie zavedenia všetkých IT bezpečnostných opatrení, uistenie sa o ich účinnosti a ich pravidelná aktualizácia pri zmene alebo vývoji spracúvania alebo okolností. Aby mohol prevádzkovateľ preukázať dodržiavanie ustanovení článku 5 ods. 1 písm. f) v súlade s článkom 5 ods. 2 všeobecného nariadenia o ochrane údajov, mal by viesť záznamy o všetkých vykonaných aktualizáciách vrátane času, keď sa vykonali.
- Používanie silných autentifikačných metód, ako je dvojstupňová autentifikácia a autentifikačné servery, doplnené o aktuálnu politiku hesiel.
- Normy bezpečného vývoja zahŕňajú filtrovanie používateľských vstupov (ak je to možné, s použitím bieleho zoznamu [white listing]), „escaping“ používateľských vstupov a opatrenia na predchádzanie útokom hrubou silou (napríklad obmedzenie maximálneho počtu pokusov). K účinnému používaniu tejto metódy môžu prispieť „firewall pre webové aplikácie“ [Web Application Firewalls].
- Zavedená politika silných používateľských oprávnení a riadenia kontrol prístupu.
- Používanie vhodného, aktuálneho, účinného a integrovaného firewallu a systému detekcie prienikov a iných systémov na ochranu perimetra.
- Systematické IT bezpečnostné audity a posúdenia zraniteľnosti (penetračné testovanie).

[23] Viac informácií o vývoji bezpečných webových aplikácií sa nachádza na tomto odkaze: https://www.owasp.org/index.php/Main_Page.

- Pravidelné preskúmanie a testovanie s cieľom uistiť sa, že na obnovu akýchkoľvek údajov, ktorých integrita alebo dostupnosť bola porušená, možno použiť zálohy.
- Žiadna identifikácia relácie v URL v textovej forme.

4. INTERNÝ ZDROJ RIZIKA SPÔSOBENÝ ĽUDSKÝM FAKTROM

71. Úlohu ľudských pochybení pri porušeniach ochrany osobných údajov je potrebné zdôrazniť pre jej častý výskyt. Keďže tieto druhy porušení môžu byť úmyselné aj neúmyselné, pre prevádzkovateľov je veľmi ťažké identifikovať zraniteľnosti a prijať opatrenia na to, aby im zabránili. Na Medzinárodnej konferencii splnomocnencov pre ochranu údajov a súkromia v októbri 2019 sa uznala dôležitosť riešenia takýchto ľudských faktorov a prijalo sa uznesenie o riešení úlohy chyby ľudského faktora v porušeniach ochrany osobných údajov[24]. V tomto uznesení sa zdôrazňuje, že na predchádzanie chybám ľudského faktora by sa mali prijať vhodné ochranné opatrenia a uvádza sa orientačný zoznam takýchto záruk a prístupov.

4.1. PRÍPAD č. 08: Exfiltrácia obchodných údajov zo strany zamestnanca

Zamestnanec spoločnosti vo výpovednej lehote skopíruje obchodné údaje z databázy spoločnosti. Tento zamestnanec je oprávnený na prístup k údajom len na účely plnenia svojich pracovných úloh. O niekoľko mesiacov po tom, ako odišiel z práce, použije takto získané údaje (základné kontaktné údaje) ako východisko pre nové spracúvanie údajov, ktorých je prevádzkovateľom, na to, aby kontaktoval klientov spoločnosti a prilákal ich do svojho nového podnikania.

4.1.1. PRÍPAD č. 08 – Predchádzajúce opatrenia a posúdenie rizika

72. V tomto konkrétnom prípade sa neprijali žiadne predchádzajúce opatrenia, ktoré by zamestnancovi zabránili skopírovať kontaktné údaje klientely spoločnosti, keďže tieto informácie potreboval a mal k nim oprávnený prístup na plnenie svojich pracovných úloh. Keďže výkon práce v oblasti vzťahov so zákazníkmi si väčšinou vyžaduje, aby mal zamestnanec určitým spôsobom prístup k osobným údajom, týmto porušeniam ochrany údajov možno predchádzať najťažšie. Obmedzenia rozsahu prístupu môžu obmedziť prácu, ktorú je daný zamestnanec schopný vykonávať. Dobre premyslené politiky prístupu a neustála kontrola však môžu pomôcť predísť takýmto porušeniam.

73. Ako zvyčajne pri posúdení rizika treba zohľadniť druh porušenia a povahu, citlivosť a objem osobných údajov, ktorých sa porušenie týka. Tieto druhy porušenia sú zvyčajne porušeniami dôvernosti, keďže databáza zvyčajne zostane neporušená a jej obsah sa „len“ skopíruje na použitie v budúcnosti. Zvyčajne ide o malé alebo priemerné množstvo údajov, ktorých sa porušenie týka. V tomto konkrétnom prípade sa porušenie netýkalo žiadnych osobitných kategórií osobných údajov a zamestnanec potreboval len kontaktné údaje klientov, aby po opustení spoločnosti s nimi mohol nadviazať kontakt. Dotknuté údaje preto nie sú citlivé.

74. Hoci jediný cieľ bývalého zamestnanca, ktorý s nekalým úmyslom skopíroval údaje, možno obmedziť na získanie kontaktných údajov klientely spoločnosti na svoje vlastné obchodné účely, prevádzkovateľ nemôže považovať riziko pre dotknuté osoby, ktorých sa porušenie týka, za nízke, keďže nemá žiadne záruky v súvislosti s úmyslami tohto zamestnanca. A tak hoci dôsledky porušenia možno obmedziť na vystavenie

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

neželanému vlastnému marketingu bývalého zamestnanca, nevylučuje sa ďalšie a závažnejšie zneužitie ukradnutých údajov v závislosti od účelu spracúvania, ktorý si bývalý zamestnanec zvolí[25].

4.1.2. PRÍPAD č. 08 – Zmiernenie a povinnosti

75. Zmiernenie nepriaznivých následkov porušenia je v uvedenom prípade ťažké. Môže si vyžadovať okamžité právne kroky s cieľom zabrániť bývalému zamestnancovi údaje ďalej zneužívať a šíriť. V ďalšom kroku by malo byť cieľom predídenie podobným situáciám v budúcnosti. Prevádzkovateľ sa môže pokúsiť nariadiť bývalému zamestnancovi, aby údaje prestal používať, no úspešnosť takéhoto kroku je prinajmenšom pochybná. Pomôcť môžu vhodné technické opatrenia, ako napríklad znemožnenie kopírovania alebo stiahnutia údajov na prenosné zariadenie.

76. V týchto prípadoch neexistuje žiadne univerzálne riešenie, no systematický prístup môže pomôcť predísť im. Ak to je možné, spoločnosť môže napríklad zvážiť zrušenie určitých foriem prístupu u zamestnancov, ktorí prejavili úmysel odísť zo zamestnania, alebo zaviesť prístupové logy, aby sa neželaný prístup mohol zaznamenať a označiť. Zmluvy podpisované so zamestnancami by mali obsahovať doložky, ktoré zakazujú takéto konanie.

77. Keďže dané porušenie nepovedie k vysokému riziku pre práva a slobody fyzických osôb, postačí teda oznámenie dozornému orgánu. Pre prevádzkovateľa však môže byť užitočné informovať aj dotknuté osoby, pretože môže byť vhodnejšie, ak sa dozvedia o úniku údajov od danej spoločnosti, a nie od bývalého zamestnanca, ktorý sa ich snaží kontaktovať. Zdokumentovanie porušenia ochrany údajov v súlade s článkom 33 ods. 5 je zákonnou povinnosťou.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	X

4.2. PRÍPAD č. 09: Náhodné poskytnutie údajov dôveryhodnej tretej strane

Poisťovací agent si všimol, že v dôsledku chybných nastavení súboru programu Excel, ktorý dostal e-mailom, bol schopný získať prístup k informáciám týkajúcim sa približne dvadsiatich zákazníkov, ktorí nepatria do jeho oblasti pôsobnosti. Je viazaný profesijným tajomstvom a bol jediným príjemcom tohto e-mailu. Podľa dojednania medzi prevádzkovateľom a poisťovacím agentom je agent povinný bez zbytočného odkladu nahlásiť prevádzkovateľovi porušenie ochrany osobných údajov. Agent preto okamžite nahlásil chybu prevádzkovateľovi, ktorý súbor opravil a znova ho odoslal, pričom požiadal agenta, aby predchádzajúcu správu vymazal. Podľa uvedeného dojednania musí agent potvrdiť vymazanie písomným vyhlásením, čo aj urobil. Získané informácie neobsahujú žiadne osobitné kategórie osobných údajov, len kontaktné údaje a údaje o samotnom poistení (druh poistenia, suma). Po analýze osobných údajov, ktorých sa porušenie týka, prevádzkovateľ nezistil žiadne osobitné charakteristiky na strane jednotlivcov ani prevádzkovateľa, ktoré by mohli ovplyvniť úroveň následkov porušenia.

[25] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

4.2.1. PRÍPAD č. 09 – Predchádzajúce opatrenia a posúdenie rizika

78. V tomto prípade porušenie nevychádza z úmyselného konania zamestnanca, ale z neúmyselnej chyby ľudského faktora spôsobenej nepozornosťou. Týmto druhom porušení možno predchádzať alebo možno znížiť ich výskyt a) vykonávaním programov odbornej prípravy, vzdelávacích programov a programov na zvyšovanie informovanosti, v rámci ktorých zamestnanci lepšie porozumejú významu ochrany osobných údajov; b) redukovaním výmeny súborov prostredníctvom e-mailu, namiesto ktorého možno použiť napríklad špeciálne systémy na spracúvanie údajov o zákazníkoch; c) dvojitou kontrolou súborov pred odoslaním; d) oddelením vytvárania súborov a ich odosielania.

79. Toto porušenie ochrany údajov sa týka len dôvernosti údajov, pričom integrita a dostupnosť zostali nedotknuté. Porušenie ochrany údajov sa týkalo približne len dvadsiatich zákazníkov, preto množstvo údajov, ktorých sa porušenie týka, možno považovať za malé. Okrem toho osobné údaje, ktorých sa porušenie týka, neobsahujú žiadne citlivé údaje. Skutočnosť, že sprostredkovateľ kontaktoval prevádzkovateľa hneď po tom, ako sa dozvedel o porušení ochrany osobných údajov, možno považovať za faktor zmierňujúci riziko. (Takisto by sa mala posúdiť možnosť, že údaje boli odoslané iným poisťovacím agentom, a ak sa potvrdí, mali by sa prijať náležité opatrenia.) Vďaka tomu, že po porušení ochrany osobných údajov sa prijali vhodné kroky, pravdepodobne nebude mať toto porušenie žiadne následky na práva a slobody dotknutých osôb.

80. Kombinácia malého počtu jednotlivcov, ktorých sa porušenie týka, okamžitého odhalenia porušenia a opatrení prijatých na minimalizáciu jeho následkov znamenajú, že tento konkrétny prípad so sebou neprináša žiadne riziko.

4.2.2. PRÍPAD č. 09 – Zmiernenie a povinnosti

81. Okrem toho sú prítomné aj ďalšie okolnosti zmierňujúce riziko: agent je viazaný profesijným tajomstvom, sám nahlásil problém prevádzkovateľovi a súbor na požiadanie vymazal. Zvyšovanie informovanosti a prípadné rozšírenie kontroly dokumentov s osobnými údajmi o ďalšie kroky pravdepodobne pomôže predchádzať podobným prípadom v budúcnosti.

82. Okrem zdokumentovania porušenia v súlade s článkom 33 ods. 5 v tomto prípade nie sú potrebné žiadne ďalšie kroky.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	X	X

4.3. Organizačné a technické opatrenia na predchádzanie následkov interných zdrojov rizika spôsobených ľudským faktorom alebo na ich zmiernenie

83. Kombinácia opatrení uvedených ďalej v texte (uplatňuje sa v závislosti od jedinečných prvkov prípadu) by mala pomôcť znížiť šancu opakovaného výskytu podobného porušenia.

84. Odporúčané opatrenia:

(Zoznam nasledujúcich opatrení nie je v žiadnom prípade výlučný ani úplný. Jeho cieľom je predstaviť návrhy v oblasti prevencie a možné riešenia. Každá spracovateľská činnosť je iná, a preto by sa mal prevádzkovateľ rozhodnúť, ktoré opatrenia sa v danej situácii najviac hodia.)

- Pravidelná realizácia programov odbornej prípravy, vzdelávacích programov a programov na zvyšovanie informovanosti pre zamestnancov o ich povinnostiach v oblasti ochrany súkromia a bezpečnosti

a odhaľovania a nahlasovania hrozieb pre bezpečnosť osobných údajov[26]. Vypracovanie programu na zvyšovanie informovanosti, v rámci ktorého si zamestnanci zopakujú najbežnejšie chyby vedúce k porušeniam ochrany osobných údajov a to, ako im predchádzať.

- Zavedenie spoľahlivých a účinných metód, postupov a systémov v oblasti ochrany osobných údajov a súkromia[27].
- Hodnotenie metód, postupov a systémov v oblasti ochrany súkromia s cieľom zaistiť nepretržitú účinnosť[28].
- Zavedenie náležitých politík prístupu a vyžadovanie, aby používatelia dodržiavali pravidlá.
- Zavedenie metód na vyžiadanie autentifikácie používateľa pri prístupe k citlivým osobným údajom.
- Zrušenie podnikového účtu používateľa, hneď ako daná osoba odíde z podniku.
- Kontrola nezvyčajného toku údajov medzi súborovým serverom [file server] a pracovnými stanicami zamestnancov.
- Zriadenie bezpečnosti vstupno-výstupného rozhrania [I/O interface security] v systéme BIOS alebo použitím softvéru kontrolujúceho používanie počítačových rozhraní (zamknúť alebo odomknúť napr. USB/CD/DVD atď.).
- Preskúmanie politiky prístupu zamestnancov (napr. zaznamenávanie prístupu k citlivým údajom a vyžadovanie od používateľa, aby uviedol pracovný dôvod, ktorý bude k dispozícii na účely auditu).
- Zrušenie služieb otvoreného cloudu [open cloud services].
- Zakázanie a zabránenie prístupu k známym otvoreným e-mailovým službám [open mail services].
- Zrušenie funkcie snímky obrazovky v operačnom systéme.
- Presadzovanie politiky čistého stola.
- Automatické zamykanie všetkých počítačov po určitom čase nečinnosti.
- Používanie mechanizmov [napr. (bezdrôtový) token na prihlásenie sa do zamknutých účtov/otvorenie týchto účtov] na rýchle prepínanie používateľov v spoločných prostrediach.
- Používanie špeciálnych systémov na riadenie osobných údajov, ktoré používajú vhodné mechanizmy kontroly prístupu a ktoré predchádzajú chybám ľudského faktora, ako je odoslanie správy nesprávnemu adresátovi. Používanie tabuľkových hárkov a iných kancelárskych dokumentov nie je vhodným spôsobom riadenia údajov o klientoch.

5. STRATENÉ ALEBO UKRADNUTÉ ZARIADENIA A DOKUMENTY V PAPIEROVEJ FORME

85. Častým druhom prípadov je strata alebo krádež prenosných zariadení. V týchto prípadoch musí prevádzkovateľ zohľadniť okolnosti spracovateľskej operácie, ako napríklad druh údajov uložených na zariadení, ako aj podporné aktíva a opatrenia na zabezpečenie náležitej úrovne bezpečnosti prijaté pred porušením. Všetky tieto prvky majú vplyv na potenciálne následky porušenia ochrany údajov. Keďže predmetné zariadenie už nie je k dispozícii, posúdenie rizika môže byť zložité.

[26] Oddiel 2 pododdiel i) uznesenia o riešení úlohy chyby ľudského faktora v porušeniach ochrany osobných údajov.

[27] Oddiel 2 pododdiel ii) uznesenia o riešení úlohy chyby ľudského faktora v porušeniach ochrany osobných údajov.

[28] Oddiel 2 pododdiel iii) uznesenia o riešení úlohy chyby ľudského faktora v porušeniach ochrany osobných údajov.

86. Tieto druhy porušenia možno vždy klasifikovať ako porušenia dôvernosti. Ak však neexistovala záloha ukradnutej databázy, tento druh porušenia môže byť aj porušením dostupnosti a porušením integrity.

87. Nasledujúce scenáre ilustrujú, aký vplyv majú uvedené okolnosti na pravdepodobnosť a závažnosť porušenia ochrany údajov.

5.1. PRÍPAD č. 10: Ukradnutý materiál s uloženými zašifrovanými osobnými údajmi

Počas vlámania do zariadenia starostlivosti o deti boli ukradnuté dva tablety. Tablety obsahovali aplikáciu s uloženými osobnými údajmi detí navštevujúcich zariadenie starostlivosti o deti. Išlo o meno, dátum narodenia a osobné údaje o vzdelávaní detí. Zašifrované tablety, ktoré boli v čase vlámania vypnuté a aj aplikácia boli chránené silným heslom. Prevádzkovateľ mal prakticky hneď k dispozícii zálohované údaje. Po tom, ako sa zariadenie starostlivosti o deti dozvedelo o vlámaní, vydalo na diaľku príkaz vymazať tablety krátko po odhalení vlámania.

5.1.1. PRÍPAD č. 10 – Predchádzajúce opatrenia a posúdenie rizika

88. V tomto konkrétnom prípade prevádzkovateľ prijal náležité opatrenia na predídenie následkom potenciálneho porušenia ochrany údajov a ich zmiernenie používaním zašifrovaných zariadení, zavedením riadnej ochrany heslami a zabezpečením zálohy údajov uložených na tabletoch. (V oddiele 5.7 sa nachádza zoznam odporúčaných opatrení.)

89. Po tom ako sa prevádzkovateľ dozvedel o porušení by mal posúdiť zdroj rizika, systémy podporujúce spracúvanie údajov, druh osobných údajov, ktorých sa porušenie týka a potenciálne následky porušenia ochrany údajov pre dotknutých jednotlivcov. Opísané porušenie ochrany údajov by sa týkalo dôvernosti, dostupnosti a integrity predmetných údajov, no vďaka náležitému postupu prevádzkovateľa pred porušením ochrany osobných údajov a po ňom k ničomu z toho nedošlo.

5.1.2. PRÍPAD č. 10 – Zmiernenie a povinnosti

90. Dôvernosť osobných údajov v zariadeniach nebola narušená vďaka ochrane silným heslom na tabletoch a aj v aplikácii. Tablety boli nastavené tak, že po nastavení hesla sú údaje na zariadení aj zašifrované. Prevádzkovateľ sa navyše pokúsil na diaľku z ukradnutých zariadení všetko vymazať.

91. Vďaka prijatým opatreniam zostala aj dôvernosť údajov neporušená. Okrem toho sa zálohovaním zaistila nepretržitá dostupnosť osobných údajov, a preto porušenie nemohlo mať žiadne negatívne následky.

92. Z týchto dôvodov je nepravdepodobné, že uvedené porušenie ochrany údajov povedie k vysokému riziku pre práva a slobody dotknutých osôb, preto nebolo potrebné oznámiť ho dozornému orgánu ani dotknutým osobám. Toto porušenie ochrany údajov sa však takisto musí zdokumentovať v súlade s článkom 33 ods. 5.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	X	**X**

5.2. PRÍPAD č. 11: Ukradnutý materiál s uloženými nezašifrovanými osobnými údajmi

Došlo ku krádeži elektronického prenosného počítača zamestnanca spoločnosti poskytujúcej služby. Ukradnutý prenosný počítač obsahuje mená, priezviská, pohlavie, adresy a dátumy narodenia viac než 100 000 zákazníkov. V dôsledku nedostupnosti ukradnutého zariadenia nebolo možné zistiť, či boli predmetom porušenia aj iné kategórie osobných údajov. Prístup k pevnému disku prenosného počítača nebol chránený žiadnym heslom. Osobné údaje sa podarilo obnoviť z dostupných každodenných záloh.

5.2.1. PRÍPAD č. 11 – Predchádzajúce opatrenia a posúdenie rizika

93. Prevádzkovateľ neprijal žiadne predchádzajúce bezpečnostné opatrenia, a preto mal zlodej alebo každá ďalšia osoba, ktorá sa po ňom stala držiteľom zariadenia, jednoduchý prístup k osobným údajom uloženým na ukradnutom prenosnom počítači.

94. Toto porušenie ochrany údajov sa týka dôvernosti údajov uložených na ukradnutom zariadení.

95. Prenosný počítač obsahujúci osobné údaje bol v tomto prípade zraniteľný, lebo na ňom chýbala akákoľvek ochrana heslom alebo šifrovanie. Chýbajúce základné bezpečnostné opatrenia zvyšujú úroveň rizika pre dotknuté osoby, ktorých sa porušenie týka. Okrem toho je problematická aj identifikácia dotknutých osôb, ktorých sa porušenie týka, čo takisto zvyšuje závažnosť porušenia. Riziko sa zvyšuje aj pre veľký počet dotknutých jednotlivcov, no napriek tomu sa porušenie netýkalo žiadnych osobitných kategórií osobných údajov.

96. Počas posudzovania rizika[29] by prevádzkovateľ mal zohľadniť potenciálne dôsledky a nežiaduce následky porušenia dôvernosti. V dôsledku porušenia sa môžu dotknuté osoby, ktorých sa porušenie týka, stať obeťou krádeže totožnosti na základe údajov dostupných na ukradnutom zariadení, a preto sa riziko považuje za vysoké.

5.2.2. PRÍPAD č. 11 – Zmiernenie a povinnosti

97. Zapnutím šifrovania zariadenia a použitím ochrany uloženej databázy pomocou silného hesla sa mohlo predísť tomu, aby porušenie ochrany údajov viedlo k riziku pre práva a slobody dotknutých osôb.

98. Vzhľadom na tieto okolnosti je potrebné oznámenie dozornému orgánu, ako aj oznámenie príslušným dotknutým osobám.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	✓

5.3. PRÍPAD č. 12: Ukradnuté dokumenty s citlivými údajmi v papierovej forme

Zo zariadenia protidrogovej liečebne bola ukradnutá papierová evidenčná kniha. Evidenčná kniha obsahovala základné informácie o totožnosti a zdraví pacientov prijatých do zariadenia protidrogovej liečby. Údaje boli uložené len v papierovej forme a lekári ošetrujúci pacientov nemali k dispozícii žiadnu zálohu. Evidenčná kniha sa neuchovávala v zamknutej zásuvke alebo miestnosti a prevádzkovateľ nemal ani režim kontroly prístupu ani žiadne iné opatrenia na ochranu dokumentácie v papierovej forme.

5.3.1. PRÍPAD č. 12 – Predchádzajúce opatrenia a posúdenie rizika

99. Prevádzkovateľ neprijal žiadne predchádzajúce bezpečnostné opatrenia, a preto mala osoba, ktorá evidenčnú knihu našla, jednoduchý prístup k osobným údajom, ktoré obsahovala. Okrem toho povaha

[29] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

osobných údajov uložených v evidenčnej knihe, ku ktorým neexistuje záloha údajov predstavuje veľmi závažný rizikový faktor.

100. Tento prípad je príkladom porušenia ochrany údajov s vysokým rizikom. Z dôvodu neprijatia náležitých bezpečnostných opatrení došlo k strate citlivých údajov týkajúcich sa zdravia podľa článku 9 ods. 1 všeobecného nariadenia o ochrane údajov. Keďže v tomto prípade išlo o osobitnú kategóriu osobných údajov, zvýšili sa potenciálne riziká pre dotknuté osoby, ktorých sa porušenie týka, a prevádzkovateľ by to mal takisto zohľadniť pri posudzovaní rizika[30].

101. Porušenie sa týka dôvernosti, dostupnosti a integrity predmetných osobných údajov. V dôsledku porušenia došlo k porušeniu lekárskeho tajomstva a neoprávnené tretie strany môžu získať prístup k súkromným lekárskym informáciám o pacientoch, čo môže mať závažné následky pre osobný život pacienta. Porušenie dostupnosti môže ďalej narušiť kontinuálnosť liečby pacienta. Keďže nemožno vylúčiť zmenu alebo vymazanie častí obsahu evidenčnej knihy, je narušená aj integrita osobných údajov.

5.3.2. PRÍPAD č. 12 – Zmiernenie a povinnosti

102. Počas posúdenia bezpečnostných opatrení by sa mal zvážiť aj druh podporného aktíva. Keďže evidenčná kniha bola fyzickým dokumentom, jej ochrana sa mala zabezpečiť inak než pri elektronickom zariadení. Porušeniu ochrany údajov sa mohlo predísť pseudonymizáciou mien pacientov, uchovávaním knihy v chránených priestoroch a v zamknutej zásuvke alebo miestnosti a vhodnou kontrolou prístupu s autentifikáciou pri prístupe.

103. Uvedené porušenie ochrany údajov mohlo mať vážne následky pre dotknuté osoby, ktorých sa týkalo, preto je oznámenie dozornému orgánu a oznámenie porušenia príslušným dotknutým osobám povinné.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	✓

5.4. Organizačné a technické opatrenia na predchádzanie následkom straty alebo krádeže zariadení alebo na ich zmiernenie

104. Kombinácia opatrení uvedených ďalej v texte (uplatňuje sa v závislosti od jedinečných prvkov prípadu) by mala pomôcť znížiť šancu opakovaného výskytu podobného porušenia.

105. Odporúčané opatrenia:

(Zoznam nasledujúcich opatrení nie je v žiadnom prípade výlučný ani úplný. Jeho cieľom je predstaviť návrhy v oblasti prevencie a možné riešenia. Každá spracovateľská činnosť je iná, a preto by sa mal prevádzkovateľ rozhodnúť, ktoré opatrenia sa v danej situácii najviac hodia.)

- Zapnite šifrovanie zariadenia (napríklad Bitlocker, Veracrypt alebo DM-Crypt).
- Používajte prístupový kód/heslo na všetkých zariadeniach. Zašifrujte všetky mobilné elektronické zariadenia tak, aby si ich dešifrovanie vyžadovalo zadanie zložitého hesla.
- Používajte viacstupňovú autentifikáciu.
- Zapnite funkcie vysoko mobilných zariadení [highly mobile devices], ktoré umožňujú zistenie ich polohy v prípade straty alebo založenia.

[30] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

- Používajte softvér/aplikácie na správu mobilných zariadení [Mobile Devices Management] a určenie polohy. Používajte antireflexné filtre [anti-glare filtres]. Vypnite každé zariadenie, ktoré je ponechané bez dozoru.
- Ak je to možné a vhodné pri danom spracúvaní údajov, neukladajte osobné údaje na mobilné zariadenie, ale na centrálny koncový server [back-end server].
- Ak je pracovná stanica pripojená k podnikovej miestnej sieti (LAN), vytvárajte automatické zálohy pracovných priečinkov, ak je ukladanie osobných údajov do nich nevyhnutné.
- Používajte bezpečnú VPN (ktorá si napr. vyžaduje samostatný dvojstupňový autentifikačný kľúč na vytvorenie bezpečného spojenia) na pripojenie mobilných zariadení ku koncovým serverom.
- Poskytnite zamestnancom fyzické zámky, aby mohli fyzicky zabezpečiť svoje mobilné zariadenia, ktoré používajú, keď sú ponechané bez dozoru.
- Vhodné usmernenia ako používať zariadenia mimo spoločnosti.
- Vhodné usmernenia ako používať zariadenia vo vnútri spoločnosti.
- Používajte softvér/aplikácie na správu mobilných zariadení a povoľte funkciu vymazania na diaľku.
- Používajte centralizovanú správu zariadení s minimálnymi právami koncových používateľov na inštaláciu softvéru.
- Nainštalujte fyzické kontroly prístupu.
- Vyhýbajte sa ukladaniu citlivých informácií do mobilných zariadení alebo na pevné disky. Ak je potrebné získať prístup k internému systému spoločnosti, mali by sa používať zabezpečené kanály, ako napríklad tie, ktoré už boli uvedené.

6. CHYBNÉ ODOSLANIE

106. Aj v tomto prípade je zdrojom rizika interná chyba ľudského faktora, porušenie však nevychádzalo zo zlého úmyslu. Porušenie bolo dôsledkom nepozornosti. Prevádzkovateľ nemôže podniknúť takmer žiadne následné kroky, a preto je v týchto prípadoch prevencia dôležitejšia než pri iných druhoch porušenia.

6.1. PRÍPAD č. 13: Chybné odoslanie pošty

Maloobchodná spoločnosť zabalila dve objednávky topánok. Z dôvodu chyby ľudského faktora sa zamenili dve faktúry, v dôsledku čoho oba výrobky a príslušné faktúry boli zaslané nesprávnej osobe. Znamená to, že dvaja zákazníci dostali objednávku toho druhého vrátane faktúr obsahujúcich osobné údaje. Po tom, ako sa prevádzkovateľ dozvedel o porušení, objednávky stiahol a zaslal ich správnym príjemcom.

6.1.1. PRÍPAD č. 13 – Predchádzajúce opatrenia a posúdenie rizika

107. Faktúry obsahovali osobné údaje potrebné na úspešné dodanie (meno, adresu a zakúpený predmet s cenou). Je dôležité zistiť, ako vôbec k tejto chybe ľudského faktora mohlo dôjsť a či a ako sa jej dalo predísť. V konkrétnom opísanom prípade je riziko nízke, keďže sa netýkal žiadnych osobitných kategórií osobných údajov ani iných údajov, ktorých zneužitie môže viesť k značným negatívnym následkom, k porušeniu nedošlo v dôsledku systémovej chyby na strane prevádzkovateľa a týkalo sa len dvoch jednotlivcov. Nezistili sa žiadne negatívne následky na jednotlivcov.

6.1.2. PRÍPAD č. 13 – Zmiernenie a povinnosti

108. Prevádzkovateľ by mal zabezpečiť bezplatné vrátenie predmetov a sprievodných faktúr a takisto by mal požiadať nesprávnych príjemcov o zničenie/vymazanie všetkých prípadných kópií faktúr obsahujúcich osobné údaje toho druhého.

109. Aj keď toto porušenie ako také nepredstavuje vysoké riziko pre práva a slobody jednotlivcov, ktorých sa porušenie týka, a preto nie je povinné oznámenie dotknutým osobám podľa článku 34 všeobecného nariadenia o ochrane údajov, nemožno sa vyhnúť oznámeniu porušenia týmto osobám, keďže ich spolupráca je potrebná na zmiernenie rizika.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	X	X

6.2. PRÍPAD č. 14: Prísne dôverné osobné údaje omylom zaslané e-mailom

Oddelenie zamestnanosti úradu verejnej správy odoslalo e-mailom správu o plánovaných školeniach jednotlivcom evidovaným v systéme ako uchádzači o zamestnanie. K tomuto e-mailu bol omylom pripojený dokument obsahujúci osobné údaje všetkých týchto uchádzačov o zamestnanie (meno, e-mailová adresa, poštová adresa, číslo sociálneho zabezpečenia). Porušenie sa týka viac ako 60 000 jednotlivcov. Úrad následne kontaktoval všetkých príjemcov a požiadal ich, aby vymazali predchádzajúcu správu a nepoužívali informácie, ktoré obsahovala.

6.2.1. PRÍPAD č. 14 – Predchádzajúce opatrenia a posúdenie rizika

110. Pre odosielanie takýchto správ mali platiť prísnejšie pravidlá. Treba zvážiť zavedenie dodatočných kontrolných mechanizmov.

111. Porušenie sa týka vysokého počtu jednotlivcov a to, že predmetom porušenia bolo okrem iných základnejších osobných údajov aj číslo ich sociálneho zabezpečenia, ešte viac zvyšuje riziko, ktoré možno klasifikovať ako vysoké[31]. Prevádzkovateľ nemôže zabrániť prípadnému šíreniu údajov zo strany niektorého z príjemcov.

6.2.2. PRÍPAD č. 14 – Zmiernenie a povinnosti

112. Ako už bolo uvedené, prostriedky na účinné zmiernenie rizík takéhoto porušenia sú obmedzené. Hoci prevádzkovateľ príjemcov požiadal o vymazanie správy, nemôže ich k tomu prinútiť a v dôsledku toho nemôže byť istý, že jeho žiadosti vyhoveli.

113. V takomto prípade by malo byť samozrejmosťou prijatie všetkých troch nasledujúcich opatrení:

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	✓

6.3. PRÍPAD č. 15: Osobné údaje omylom zaslané e-mailom

Zoznam všetkých účastníkov päťdňového kurzu právnej angličtiny, ktorý sa koná v hoteli, je namiesto hotela omylom odoslaný pätnástim bývalým účastníkom kurzu. Tento zoznam obsahuje mená, e-mailové adresy a stravovacie preferencie pätnástich účastníkov. Len dvaja účastníci napísali svoje stravovacie preferencie, pričom uviedli, že trpia neznášanlivosťou laktózy. Totožnosť žiadneho z účastníkov nie je chránená. Prevádzkovateľ chybu odhalí hneď po odoslaní zoznamu, príjemcov informuje o chybe a požiada ich, aby zoznam vymazali.

[31] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

6.3.1. PRÍPAD č. 15 – Predchádzajúce opatrenia a posúdenie rizika

114. Pre odosielanie správ obsahujúcich osobné údaje mali platiť prísne pravidlá. Treba zvážiť zavedenie dodatočných kontrolných mechanizmov.

115. Riziká vyplývajúce z povahy, citlivosti, objemu a súvislostí osobných údajov sú nízke. Osobné údaje zahŕňajú citlivé údaje o stravovacích preferenciách dvoch účastníkov. Aj keď je informácia o tom, že osoba trpí neznášanlivosťou laktózy, údajom o zdraví, riziko, že tento údaj sa použije na nekalý účel, by sa malo považovať za relatívne nízke. Hoci v prípade údajov týkajúcich sa zdravia sa zvyčajne predpokladá, že porušenie pravdepodobne povedie k vysokému riziku pre dotknutú osobu[32], zároveň v tomto konkrétnom prípade nemožno identifikovať žiadne riziko, ktoré by porušenie spôsobilo dotknutej osobe ujmu na zdraví, majetkovú alebo nemajetkovú ujmu v dôsledku neoprávneného prezradenia informácie o neznášanlivosti laktózy. V porovnaní s inými stravovacími preferenciami neznášanlivosť laktózy zvyčajne nemožno spájať so žiadnou náboženskou alebo filozofickou vierou. Ide o malé množstvo osobných údajov, ktorých ochrana bola porušená a nízky počet dotknutých osôb, ktorých sa porušenie týka.

6.3.2. PRÍPAD č. 15 – Zmiernenie a povinnosti

116. Možno konštatovať, že porušenie nemalo žiadne závažné následky na dotknuté osoby. Skutočnosť, že prevádzkovateľ kontaktoval príjemcov hneď po tom, ako sa dozvedel o chybe, možno považovať za faktor zmierňujúci riziko.

117. Ak dôjde k odoslaniu e-mailu nesprávnemu/neoprávnenému príjemcovi, odporúča sa, aby prevádzkovateľ použil funkciu skrytej kópie (Bcc) na zaslanie nadväzného e-mailu nechceným príjemcom s ospravedlnením a pokynom, aby problematický e-mail vymazali a informáciou o tom, že nemajú právo ďalej používať e-mailové adresy, ktoré týmto spôsobom zistili.

118. Z týchto dôvodov je nepravdepodobné, že toto porušenie ochrany údajov povedie k vysokému riziku pre práva a slobody dotknutých osôb, preto nebolo potrebné oznámiť ho dozornému orgánu ani dotknutým osobám. Toto porušenie ochrany údajov sa však takisto musí zdokumentovať v súlade s článkom 33 ods. 5.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	X	X

6.4. PRÍPAD č. 16: Chybné odoslanie pošty

Poisťovacia skupina ponúka poistenie automobilov. Na tento účel odosiela pravidelne upravované poistné sumy poštou. Okrem mena a adresy poistníka takýto list obsahuje aj evidenčné číslo vozidla bez skrytých číslic, poistné sadzby v aktuálnom a nasledujúcom poistnom roku, približný počet ročne najazdených kilometrov a dátum narodenia poistníka. Neobsahuje údaje týkajúce sa zdravia podľa článku 9 všeobecného nariadenia o ochrane údajov, platobné údaje (bankové údaje), ekonomické ani finančné údaje.

Listy balia automatizované obálkovacie stroje. V dôsledku mechanickej chyby sa do jednej obálky vložia dva listy rôznych poistníkov a poštou sa odošlú jednému z poistníkov. Tento poistník doma otvorí list a pozrie si svoj správne doručený list, ako aj nesprávne doručený list druhého poistníka.

[32] Pozri usmernenia WP250, s. 23.

6.4.1. PRÍPAD č. 16 – Predchádzajúce opatrenia a posúdenie rizika

119. Nesprávne doručený list obsahuje meno, adresu, dátum narodenia, odmaskované evidenčné číslo vozidla a klasifikáciu poistnej sadzby v aktuálnom a nasledujúcom roku. Následky pre osobu, ktorej sa porušenie týka, sa považujú za priemerné, keďže informácie, ktoré nie sú verejne dostupné, ako je dátum narodenia alebo odmaskované evidenčné čísla vozidiel a podrobnosti o zvýšení poistných sadzieb, sú vyzradené neoprávnenému príjemcovi. Pravdepodobnosť zneužitia týchto údajov sa posudzuje ako nízka až stredná. Hoci mnohí príjemcovia nesprávne doručený list pravdepodobne zahodia, v jednotlivých prípadoch nemožno jednoznačne vylúčiť, že nedôjde k uverejneniu tohto listu na sociálnych sieťach alebo ku kontaktovaniu poistníka.

6.4.2. PRÍPAD č. 16 – Zmiernenie a povinnosti

120. Prevádzkovateľ by mal zabezpečiť vrátenie pôvodného dokumentu na svoje vlastné náklady. Takisto by mal informovať nesprávneho príjemcu o tom, že nesmie zneužiť informácie, ktoré si prečítal.

121. Pri odosielaní hromadnej pošty pomocou plne automatizovaných strojov pravdepodobne nikdy nebude možné úplne predísť chybám v doručovaní pošty. V prípade zvýšeného výskytu je však nevyhnutné skontrolovať, či sú obálkovacie stroje správne nastavené a udržované v dobrom stave alebo či takéto porušenie spôsobuje iný systémový problém.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	X

6.5. Organizačné a technické opatrenia na predchádzanie následkom chybného odoslania alebo na ich zmiernenie

122. Kombinácia opatrení uvedených ďalej v texte (uplatňuje sa v závislosti od jedinečných prvkov prípadu) by mala pomôcť znížiť šancu opakovaného výskytu podobného porušenia.

123. Odporúčané opatrenia:

(Zoznam nasledujúcich opatrení nie je v žiadnom prípade výlučný ani úplný. Jeho cieľom je predstaviť návrhy v oblasti prevencie a možné riešenia. Každá spracovateľská činnosť je iná, a preto by sa mal prevádzkovateľ rozhodnúť, ktoré opatrenia sa v danej situácii najviac hodia.)

- Nastavenie presných noriem pre odosielanie listov/e-mailov bez možnosti voľného výkladu.
- Náležitá odborná príprava personálu ako odosielať listy/e-maily.
- Pri odosielaní e-mailov viacerým príjemcom sa títo príjemcovia automaticky uvádzajú do poľa skrytej správy (Bcc).
- Keď sa e-maily odosielajú viacerým príjemcom a príjemcovia nie sú uvedení v poli skrytej správy (Bcc), vyžaduje sa dodatočné potvrdenie.
- Uplatňovanie zásady kontroly štyroch očí.
- Automatické adresovanie namiesto manuálneho, pri ktorom sa údaje získavajú z dostupnej a aktuálnej databázy; systém automatického adresovania by sa mal pravidelne kontrolovať na odhalenie skrytých chýb a nesprávnych nastavení.
- Používanie funkcie zdržania odoslania správy (napr. správu možno vymazať/zmeniť určitý čas po kliknutí na tlačidlo odoslať).
- Vypnutie automatického dopĺňania pri písaní e-mailových adries.
- Stretnutia na zvyšovanie informovanosti o najbežnejších chybách vedúcich k porušeniu ochrany osobných údajov.

- Odborná príprava a manuály o tom, ako riešiť incidenty vedúce k porušeniu ochrany osobných údajov a koho informovať (zapojiť zodpovednú osobu).

7. ĎALŠIE PRÍPADY – SOCIÁLNE INŽINIERSTVO

7.1. PRÍPAD č. 17: Krádež totožnosti

Kontaktné centrum telekomunikačnej spoločnosti dostane telefonát od osoby, ktorá sa predstaví ako klient. Domnelý klient spoločnosť požiada o zmenu e-mailovej adresy, na ktorú sa v budúcnosti majú zasielať informácie o vyúčtovaní. Pracovník kontaktného centra potvrdí totožnosť klienta položením otázok o určitých osobných údajoch, ako sa stanovuje v postupoch tejto spoločnosti. Volajúci správne uvedie požadované daňové identifikačné číslo klienta a poštovú adresu (pretože mal prístup k týmto informáciám). Po potvrdení operátor vykoná požadovanú zmenu a informácie o vyúčtovaní sa následne budú zasielať na novú e-mailovú adresu. Tento postup nezahŕňa zaslanie žiadneho oznámenia na bývalú kontaktnú e-mailovú adresu. Nasledujúci mesiac kontaktuje spoločnosť legitímny klient a pýta sa, prečo nedostáva faktúry na svoju e-mailovú adresu, pričom popiera, že telefonoval do centra so žiadosťou o zmenu kontaktnej e-mailovej adresy. Spoločnosť si neskôr uvedomí, že informácie sa zasielali neoprávnenému používateľovi a zmenu zruší.

7.1.1. PRÍPAD č. 17 – Posúdenie rizika, zmiernenie a povinnosti

124. Tento prípad je príkladom dôležitosti predchádzajúcich opatrení. Z hľadiska rizika toto porušenie predstavuje vysokú úroveň rizika[33], keďže informácie o vyúčtovaní môžu odhaliť údaje o súkromnom živote dotknutej osoby (napr. zvyky, kontakty) a mohli by spôsobiť majetkovú ujmu (napr. prenasledovanie, ohrozenie telesnej integrity). Osobné údaje získané počas tohto útoku sa môžu takisto použiť na uľahčenie prevzatia účtu v tejto organizácii alebo zneužitie ďalších autentifikačných opatrení v iných organizáciách. Vzhľadom na tieto riziká by malo „vhodné“ autentifikačné opatrenie spĺňať vysoké štandardy v závislosti od toho, ktoré osobné údaje možno po autentifikácii spracúvať.

125. V dôsledku toho prevádzkovateľ musí porušenie oznámiť dozornému orgánu aj dotknutej osobe.

126. Vzhľadom na tento prípad je jednoznačne potrebné vylepšiť proces predchádzajúceho overenia klienta. Metóda používaná na autentifikáciu nebola dostatočná. Strana s nekalým úmyslom dokázala predstierať, že je oprávneným používateľom, použitím verejne dostupných informácií a informácií, ku ktorým mala inak prístup.

127. Používanie tohto druhu statickej autentifikácie na základe poznania [static knowledge-based authentification] (pri ktorej sa odpoveď nemení a informácie nie sú „tajné“ ako v prípade hesla) sa neodporúča.

128. Organizácia by namiesto toho mala použiť formu autentifikácie, ktorá by viedla k vysokému stupňu istoty, že overený používateľ je oprávnenou osobou a nikým iným. Tento problém by vyriešilo zavedenie metódy viacstupňovej autentifikácie out-of-band kanálom [out-of-band multi-factor authentification], napr. overením požiadavky o zmenu odoslaním potvrdenia žiadosti na predchádzajúcu kontaktnú adresu alebo položením dodatočných otázok a vyžiadaním informácií viditeľných len na predchádzajúcich faktúrach.

[33] Pre usmernenia k spracovateľským operáciám, ktoré „*pravdepodobne povedú k vysokému riziku*“, pozri poznámku pod čiarou č. 10.

Prevádzkovateľ má zodpovednosť rozhodnúť sa, ktoré opatrenia zaviesť, keďže najlepšie pozná podrobnosti a požiadavky svojej internej prevádzky.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	✓

7.2. PRÍPAD č. 18: Exfiltrácia e-mailov

Tri mesiace po konfigurácii e-mailov sieť hypermarketov zistila, že niektoré e-mailové účty boli zmenené a boli vytvorené pravidlá, na základe ktorých sa každý e-mail obsahujúci určité výrazy (napr. „faktúra“, „platba“, „bankový prevod“, „overenie kreditnej karty“, „údaje o bankovom účte“) presunul do nepoužívaného priečinka a takisto sa preposlal na externú e-mailovú adresu. Už predtým však došlo k útoku vo forme sociálneho inžinierstva [social engineering attack], t. j. útočník, ktorý sa predstavil ako dodávateľ, dal zmeniť údaje o bankovom účte tohto dodávateľa na svoje vlastné. Dovtedy tak bolo odoslaných niekoľko falošných faktúr, ktoré zahŕňali tieto nové údaje bankového účtu. Monitorovací systém e-mailovej platformy nakoniec vydal upozornenie v súvislosti s týmito priečinkami. Spoločnosť nebola schopná odhaliť, ako útočník vôbec dokázal získať prístup k e-mailovým účtom, no domnievala sa, že na vine bol infikovaný e-mail, ktorý poskytol prístup ku skupine používateľov zodpovedných za výplaty.

Prostredníctvom preposielania e-mailov na základe kľúčových slov útočník získal informácie o 99 zamestnancoch: mená 89 dotknutých osôb a ich mzdu v konkrétnom mesiaci; mená, osobný stav, počet detí, mzdu, pracovný čas a zvyšné informácie o plate desiatich zamestnancov, ktorých zmluvy sa skončili. Prevádzkovateľ porušenie oznámil len desiatim zamestnancom z tejto druhej skupiny.

7.2.1. PRÍPAD č. 18 – Posúdenie rizika, zmiernenie a povinnosti

129. Aj keď získavanie osobných údajov pravdepodobne nie je cieľom útočníka, porušenie ochrany osobných údajov pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, keďže porušenie mohlo viesť k majetkovej (napr. finančná strata) aj nemajetkovej ujme (napr. krádež totožnosti alebo podvod) alebo by sa údaje mohli použiť na umožnenie iných útokov (napr. phishing). Porušenie by sa preto malo oznámiť všetkým 99 zamestnancom, a nie len 10 zamestnancom, ktorých informácie o plate unikli.

130. Po tom, ako sa prevádzkovateľ dozvedel o porušení, vykonal nútenú zmenu hesiel napadnutých účtov, zablokoval odosielanie e-mailov na e-mailový účet útočníka, informoval o konaní útočníka poskytovateľa e-mailovej služby, zrušil pravidlá vytvorené útočníkom a sprísnil upozornenia monitorovacieho systému tak, aby vydal upozornenie hneď po vytvorení automatického pravidla. Alternatívne by prevádzkovateľ takisto mohol zrušiť právo používateľov vytvárať pravidlá preposielania tak, že by sa to robilo len na požiadanie a jedine cez IT oddelenie, alebo by pre oblasti, v ktorých sa manipuluje s finančnými údajmi, mohol zaviesť politiku, v rámci ktorej by používatelia mali kontrolovať a nahlasovať pravidlá nastavené na ich účtoch raz týždenne alebo častejšie.

131. Skutočnosť, že došlo k porušeniu a porušenie zostalo tak dlho neodhalené, ako aj skutočnosť, že v dlhšom časovom horizonte by sa sociálne inžinierstvo mohlo použiť na zmenu väčšieho množstva údajov, zdôraznili závažné problémy v bezpečnosti IT systému prevádzkovateľa. Tieto problémy by sa bezodkladne mali riešiť, napríklad väčším dôrazom na preskúmanie automatizácie [automation reviews] a kontroly zmien, odhaľovanie incidentov a reakčné opatrenia. Prevádzkovatelia manipulujúci s osobnými údajmi, finančnými informáciami atď. majú väčšiu zodpovednosť za zabezpečenie primeranej bezpečnosti údajov.

Opatrenia potrebné na základe identifikovaných rizík		
Interná dokumentácia	Oznámenie dozornému orgánu	Oznámenie dotknutým osobám
✓	✓	✓