Smernice 01/2021

o primerih v zvezi z uradnim obveščanjem o kršitvah varstva osebnih podatkov

Sprejete 14. decembra 2021

Različica 2.0

Zgodovina različic

Različica 2.0	14. 12. 2021	Sprejetje smernic po javnem posvetovanju
Različica 1.0	14. 1. 2021	Sprejetje smernic za javno posvetovanje

Kazalo

1 UVOD....5

2 IZSILJEVALSKO PROGRAMJE....8

2.1 PRIMER št. 01: izsiljevalsko programje z ustreznim varnostnim kopiranjem in brez eksfiltracije...8

2.1.1 PRIMER št. 01 – predhodni ukrepi in ocena tveganja....8

2.1.2 PRIMER št. 01 – ublažitev in obveznosti....9

2.2 PRIMER št. 02: izsiljevalsko programje brez ustreznega varnostnega kopiranja....10

2.2.1 PRIMER št. 02 – predhodni ukrepi in ocena tveganja....10

2.2.2 PRIMER št. 02 – ublažitev in obveznosti....11

2.3 PRIMER št. 03: izsiljevalsko programje z varnostnim kopiranjem in brez eksfiltracije podatkov v bolnišnici....12

2.3.1 PRIMER št. 03 – predhodni ukrepi in ocena tveganja....12

2.3.2 PRIMER št. 03 – ublažitev in obveznosti....13

2.4 PRIMER št. 04: izsiljevalsko programje brez varnostnega kopiranja in z eksfiltracijo....13

2.4.1 PRIMER št. 04 – predhodni ukrepi in ocena tveganja....14

2.4.2 PRIMER št. 04 – ublažitev in obveznosti....14

2.5 Organizacijski in tehnični ukrepi za preprečevanje/ublažitev posledic napadov z izsiljevalskim programjem....15

3 NAPADI z eksfiltracijo podatkov....16

3.1 PRIMER št. 05: eksfiltracija podatkov o prijavi za delovno mesto s spletnega mesta....16

3.1.1 PRIMER št. 05 – predhodni ukrepi in ocena tveganja....17

3.1.2 PRIMER št. 05 – ublažitev in obveznosti....17

3.2 PRIMER št. 06: eksfiltracija zgoščenega gesla s spletnega mesta....18

3.2.1 PRIMER št. 06 – predhodni ukrepi in ocena tveganja....18

3.2.2 PRIMER št. 06 – ublažitev in obveznosti....18

3.3 PRIMER št. 07: napad s polnjenjem poverilnic na bančnem spletnem mestu....19

3.3.1 PRIMER št. 07 – predhodni ukrepi in ocena tveganja....19

3.3.2 PRIMER št. 07 – ublažitev in obveznosti....20

3.4 Organizacijski in tehnični ukrepi za preprečevanje/ublažitev posledic hekerskih napadov....20

4 NOTRANJI VIR TVEGANJA ZA LJUDI....21

4.1 PRIMER št. 08: eksfiltracija poslovnih podatkov s strani zaposlenega....21

4.1.1 PRIMER št. 08 – predhodni ukrepi in ocena tveganja....22

4.1.2 PRIMER št. 08 – ublažitev in obveznosti....22

4.2 PRIMER št. 09: nenamerni prenos podatkov zaupanja vredni tretji osebi....24

4.2.1 PRIMER št. 09 – predhodni ukrepi in ocena tveganja....24

4.2.2 PRIMER št. 09 – ublažitev in obveznosti....24

4.3 Organizacijski in tehnični ukrepi za preprečevanje/ublažitev vplivov notranjih virov tveganja za ljudi 24
5 IZGUBLJENE ALI UKRADENE NAPRAVE IN PAPIRNI DOKUMENTI....26
5.1 PRIMER št. 10: ukradeno gradivo, v katerem so shranjeni šifrirani osebni podatki....26
5.1.1 PRIMER št. 10 – predhodni ukrepi in ocena tveganja....26
5.1.2 PRIMER št. 10 – ublažitev in obveznosti....26
5.2 PRIMER št. 11: ukradeno gradivo, v katerem so shranjeni nešifrirani osebni podatki....27
5.2.1 PRIMER št. 11 – predhodni ukrepi in ocena tveganja....27
5.2.2 PRIMER št. 11 – ublažitev in obveznosti....28
5.3 PRIMER št. 12: ukradeni dokumenti v papirni obliki z občutljivimi podatki....28
5.3.1 PRIMER št. 12 – predhodni ukrepi in ocena tveganja....28
5.3.2 PRIMER št. 12 – ublažitev in obveznosti....29
5.4 Organizacijski in tehnični ukrepi za preprečevanje/ublažitev posledic izgube ali kraje naprav....29
6 NAPAČNO POSLANA POŠILJKA....30
6.1 PRIMER št. 13: napaka pri poštnem pošiljanju....30
6.1.1 PRIMER št. 13 – predhodni ukrepi in ocena tveganja....30
6.1.2 PRIMER št. 13 – ublažitev in obveznosti....30
6.2 PRIMER št. 14: strogo zaupni osebni podatki, pomotoma poslani po pošti....30
6.2.1 PRIMER št. 14 – predhodni ukrepi in ocena tveganja....31
6.2.2 PRIMER št. 14 – ublažitev in obveznosti....31
6.3 PRIMER št. 15: osebni podatki, pomotoma poslani po pošti....31
6.3.1 PRIMER št. 15 – predhodni ukrepi in ocena tveganja....31
6.3.2 PRIMER št. 15 – ublažitev in obveznosti....32
6.4 PRIMER št. 16: napaka pri poštnem pošiljanju....32
6.4.1 PRIMER št. 16 – predhodni ukrepi in ocena tveganja....33
6.4.2 PRIMER št. 16 – ublažitev in obveznosti....33
6.5 Organizacijski in tehnični ukrepi za preprečevanje/ublažitev posledic napačno poslane pošiljke33
7 Drugi primeri – socialni inženiring....34
7.1 PRIMER št. 17: kraja identitete....34
7.1.1 PRIMER št. 17 – ocena tveganja, ublažitev in obveznosti....34
7.2 PRIMER št. 18: eksfiltracija elektronske pošte....35
7.2.1 PRIMER št. 18 – ocena tveganja, ublažitev in obveznosti....35

EVROPSKI ODBOR ZA VARSTVO PODATKOV JE –

ob upoštevanju člena 70(1)(e) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 12 in 22 svojega poslovnika,

ob upoštevanju sporočila Komisije Evropskemu parlamentu in Svetu z naslovom Varstvo podatkov kot steber krepitve vloge državljanov in pristopa EU k digitalnemu prehodu – dve leti uporabe Splošne uredbe o varstvu podatkov[2] –

SPREJEL NASLEDNJE SMERNICE

1 UVOD

1. Splošna uredba o varstvu podatkov v nekaterih primerih uvaja zahtevo, da se o kršitvi varnosti osebnih podatkov uradno obvesti pristojni nacionalni nadzorni organ (v nadaljevanju: nadzorni organ) in da se posameznikom, katerih osebni podatki so bili predmet kršitve, sporoči, da je prišlo do kršitve (člena 33 in 34).

2. Delovna skupina iz člena 29 je oktobra 2017 že pripravila *splošne* smernice o obveščanju o kršitvah varnosti podatkov, v katerih je analizirala ustrezne oddelke Splošne uredbe o varstvu podatkov (Smernice o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe 2016/679, WP 250) (v nadaljevanju: Smernice WP 250)[3]. Vendar pa te smernice zaradi svoje narave in časovnega okvira niso dovolj podrobno obravnavale vseh praktičnih vprašanj. Zato se je pojavila potreba po *praktično naravnanih* smernicah, *ki temeljijo na primerih* in upoštevajo izkušnje, ki so jih nadzorni organi pridobili od začetka uporabe Splošne uredbe o varstvu podatkov.

3. Ta dokument je namenjen dopolnitvi Smernic WP 250 in izraža skupne izkušnje nadzornih organov EGP od začetka uporabe Splošne uredbe o varstvu podatkov. Njegov cilj je pomagati upravljavcem podatkov pri odločanju, kako obravnavati kršitve varnosti podatkov in katere dejavnike upoštevati pri oceni tveganja.

[1] Sklicevanje na „države članice“ v tem dokumentu bi bilo treba razumeti kot sklicevanje na „države članice EGP“.

[2] COM(2020) 264 final z dne 24. junija 2020.

[3] G29 WP250 rev.1, 6. februar 2018, Smernice o obveščanju o kršitvi varnosti osebnih podatkov na podlagi Uredbe (EU) 2016/679 – potrdil EOVP, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

4. Pri vsakem poskusu obravnave kršitve bi moral biti upravljavec najprej zmožen prepoznati kršitev. V členu 4(12) Splošne uredbe o varstvu podatkov je „kršitev varnosti osebnih podatkov“ opredeljena kot „kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani“.

5. Delovna skupina iz člena 29 je v Mnenju št. 03/2014 o obveščanju o kršitvah[4] in Smernicah WP 250 pojasnila, da je kršitve mogoče razvrstiti na podlagi naslednjih treh dobro znanih načel varnosti informacij:

   - „kršitev zaupnosti“ – kadar gre za nepooblaščeno ali nenamerno razkritje osebnih podatkov ali nepooblaščen ali nenameren dostop do njih;
   - „kršitev celovitosti“ – kadar gre za nepooblaščeno ali nenamerno spremembo osebnih podatkov;
   - „kršitev razpoložljivosti“ – kadar gre za nenamerno ali nepooblaščeno izgubo dostopa do osebnih podatkov ali njihovo uničenje[5].

6. Kršitev ima lahko različne pomembne škodljive učinke na posameznike, kar lahko povzroči fizično, premoženjsko ali nepremoženjsko škodo. V Splošni uredbi o varstvu podatkov je pojasnjeno, da to lahko vključuje izgubo nadzora nad njihovimi osebnimi podatki, omejitev njihovih pravic, diskriminacijo, krajo ali zlorabo identitete, finančno izgubo, neodobreno reverzijo psevdonimizacije, okrnitev ugleda in izgubo zaupnosti osebnih podatkov, zaščitenih s poklicno skrivnostjo. Vključuje lahko tudi katero koli drugo znatno gospodarsko ali socialno škodo za navedene posameznike. Ena od najpomembnejših obveznosti upravljavca podatkov je, da oceni ta tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ter izvede ustrezne tehnične in organizacijske ukrepe za njihovo naslavljanje.

7. V skladu s tem Splošna uredba o varstvu podatkov od upravljavca zahteva, da:

   - dokumentira vsako kršitev varnosti osebnih podatkov, vključno z dejstvi v zvezi s kršitvijo varnosti osebnih podatkov, njene učinke in sprejete popravne ukrepe[6];
   - o kršitvi varnosti osebnih podatkov uradno obvesti nadzorni organ, razen če ni verjetno, da bi kršitev ogrožala pravice in svoboščine posameznikov[7];
   - sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varnosti osebnih podatkov, kadar je verjetno, da bo kršitev varnosti osebnih podatkov povzročila veliko tveganje za pravice in svoboščine posameznikov[8].

8. Kršitve varnosti podatkov so same po sebi težave, vendar so lahko tudi simptomi ranljivega, morda zastarelega sistema varnosti podatkov, lahko pa kažejo tudi pomanjkljivosti sistema, ki jih je treba odpraviti. Na splošno velja, da je kršitve varnosti podatkov vedno bolje preprečiti z vnaprejšnjo pripravo, saj je več

---

[4] G29 WP213, 25. marec 2014, Mnenje št. 03/2014 o obveščanju o kršitvah varstva osebnih podatkov, str. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Glej Smernice WP 250, str. 7. – Upoštevati je treba, da lahko kršitev varstva podatkov zadeva eno ali več kategorij hkrati ali skupaj.

[6] Člen 33(5) Splošne uredbe o varstvu podatkov.

[7] Člen 33(1) Splošne uredbe o varstvu podatkov.

[8] Člen 34(1) Splošne uredbe o varstvu podatkov.

njihovih posledic trajnih. Preden lahko upravljavec *v celoti* oceni tveganje, ki izhaja iz kršitve, povzročene z neko obliko napada, bi bilo treba ugotoviti temeljni vzrok težave, da se ugotovi, ali so morebitne ranljivosti, zaradi katerih je prišlo do incidenta, še vedno prisotne in jih je zato še vedno mogoče izrabiti. V številnih primerih lahko upravljavec ugotovi, da bo incident verjetno povzročil tveganje, zato ga je treba uradno sporočiti. V drugih primerih uradnega obveščanja ni treba odložiti, dokler se v celoti ne ocenita tveganje in učinek kršitve, saj lahko celotna ocena tveganja poteka vzporedno z uradnim obveščanjem, tako pridobljene informacije pa se lahko nadzornemu organu posredujejo po fazah brez nepotrebnega nadaljnjega odlašanja[9].

9. Kršitev bi bilo treba sporočiti, kadar upravljavec meni, da bo verjetno povzročila tveganje za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki. Upravljavci bi morali to oceno izvesti, ko se seznanijo s kršitvijo. Upravljavec ne bi smel čakati na podrobno forenzično preiskavo in (zgodnje) ukrepe za ublažitev, preden oceni, ali je verjetno, da bo kršitev varnosti podatkov povzročila tveganje in bi jo bilo treba zato sporočiti.

10. Če upravljavec sam oceni, da tveganje ni verjetno, vendar se izkaže, da se tveganje uresniči, lahko pristojni nadzorni organ uporabi svoja popravljalna pooblastila in se lahko odloči za sankcije.

11. Vsak upravljavec in obdelovalec bi moral imeti vzpostavljene načrte in postopke za ravnanje ob morebitnih kršitvah varnosti podatkov. Organizacije bi morale imeti jasne načine poročanja in osebe, odgovorne za določene vidike postopka obnove.

12. Za upravljavce in obdelovalce sta bistvena tudi usposabljanje in ozaveščanje zaposlenih o vprašanjih varstva podatkov s poudarkom na obvladovanju kršitev varnosti osebnih podatkov (prepoznavanje incidenta kršitve varnosti osebnih podatkov in nadaljnji ukrepi, ki jih je treba sprejeti, itd.). To usposabljanje bi bilo treba redno ponavljati, odvisno od vrste dejavnosti obdelave in velikosti upravljavca, pri čemer bi bilo treba obravnavati najnovejše trende in opozorila, ki izhajajo iz kibernetskih napadov ali drugih varnostnih incidentov.

13. Načelo odgovornosti in koncept vgrajenega varstva podatkov bi lahko vključevala analizo, ki bi se vnesla v lasten „priročnik za obravnavo kršitev varnosti osebnih podatkov“ upravljavca in obdelovalca podatkov, katerega cilj bi bil ugotoviti dejstva za vsak vidik obdelave v vsaki pomembnejši fazi postopka. Tak vnaprej pripravljen priročnik bi zagotovil veliko hitrejši vir informacij, ki bi upravljavcem in obdelovalcem podatkov omogočil ublažitev tveganj in izpolnjevanje obveznosti brez nepotrebnega odlašanja. To bi zagotovilo, da bi v primeru kršitve varnosti osebnih podatkov ljudje v organizaciji vedeli, kaj storiti, in da bi se incident najverjetneje obravnaval hitreje, kot če ne bi bilo vzpostavljenih ukrepov za ublažitev ali načrta.

14. Čeprav so v nadaljevanju predstavljeni primeri izmišljeni, temeljijo na značilnih primerih iz skupnih izkušenj nadzornih organov z uradnim obveščanjem o kršitvah varnosti podatkov. Ponujene analize se izrecno nanašajo na obravnavane primere, vendar z namenom, da se upravljavcem podatkov zagotovi pomoč pri ocenjevanju lastnih kršitev varnosti podatkov. Vsaka sprememba okoliščin v nadaljevanju opisanih primerih lahko povzroči drugačne ali pomembnejše stopnje tveganja, kar zahteva drugačne ali dodatne ukrepe. V teh smernicah so primeri strukturirani glede na posamezne kategorije kršitev (na primer napadi z izsiljevalskim programjem). Pri obravnavi posameznih kategorij kršitev so v vsakem primeru potrebni določeni blažitveni ukrepi. Ni nujno, da se ti ukrepi ponovijo pri vsaki analizi primera, ki spada v isto kategorijo kršitev. Za primere, ki spadajo v isto kategorijo, so navedene samo razlike. Zato bi moral bralec

[9] Člen 33(4) Splošne uredbe o varstvu podatkov.

prebrati vse primere, ki se nanašajo na ustrezno kategorijo kršitve, da bi opredelil in razločil vse ustrezne ukrepe, ki jih je treba sprejeti.

15. Priprava notranje dokumentacije o kršitvi je obveznost, ki je neodvisna od tveganj, povezanih s kršitvijo, in jo je treba izvesti v vsakem primeru. Primeri, predstavljeni v nadaljevanju, so namenjeni pojasnitvi, ali je treba o kršitvi uradno obvestiti nadzorni organ ter jo sporočiti posameznikom, na katere se nanašajo osebni podatki, in na katere kršitev vpliva, ali ne.

2 IZSILJEVALSKO PROGRAMJE

16. Pogost razlog za uradno obvestilo o kršitvi varnosti podatkov je napad z izsiljevalskim programjem, ki ga je doživel upravljavec podatkov. V teh primerih zlonamerna koda šifrira osebne podatke, nato pa napadalec od upravljavca zahteva odkupnino v zameno za dešifrirno kodo. Take napade je običajno mogoče uvrstiti med kršitve razpoložljivosti, pogosto pa lahko pride tudi do kršitve zaupnosti.

> Računalniški sistemi majhnega proizvodnega podjetja so bili izpostavljeni napadu z izsiljevalskim programjem, podatki, shranjeni v teh sistemih, pa so bili šifrirani. Upravljavec podatkov je uporabljal šifriranje v mirovanju, zato so bili vsi podatki, do katerih je dostopalo izsiljevalsko programje, shranjeni v šifrirani obliki z uporabo najsodobnejšega šifrirnega algoritma. Dešifrirni ključ v napadu ni bil ogrožen, tj. napadalec do njega ni mogel niti dostopati niti ga posredno uporabiti. Posledično je imel napadalec dostop le do šifriranih osebnih podatkov. Zlasti kršitev ni vplivala na sistem elektronske pošte podjetja niti na sisteme strank, ki so bili uporabljeni za dostop do njega. Podjetje za preiskavo incidenta uporablja strokovno znanje zunanjega podjetja za kibernetsko varnost. Na voljo so dnevniki, ki sledijo vsem podatkovnim tokovom, ki zapustijo podjetje (vključno z odhodno e-pošto). Po analizi dnevnikov in podatkov, zbranih s sistemi za odkrivanje, ki jih je podjetje namestilo, je bilo z notranjo preiskavo, ki jo je podprlo zunanje podjetje za kibernetsko varnost, *z gotovostjo* ugotovljeno, da je storilec podatke samo šifriral, ne da bi jih eksfiltriral. Iz dnevnikov ni razviden noben izhodni podatkovni tok v časovnem okviru napada. Osebni podatki, na katere je kršitev vplivala, se nanašajo na stranke in zaposlene v podjetju, skupaj na nekaj ducat posameznikov. Varnostna kopija je bila takoj na voljo in podatki so bili obnovljeni nekaj ur po napadu. Kršitev ni imela nobenih posledic za vsakodnevno delovanje upravljavca. Pri plačilih zaposlenim ali obravnavi zahtevkov strank ni prišlo do zamud.

2.1 PRIMER št. 01: izsiljevalsko programje z ustreznim varnostnim kopiranjem in brez eksfiltracije

17. V tem primeru sta bila uresničena naslednja elementa iz opredelitve „kršitve varnosti osebnih podatkov“: kršitev varnosti je povzročila nezakonito spremembo in nepooblaščen dostop do shranjenih osebnih podatkov.

2.1.1 PRIMER št. 01 – predhodni ukrepi in ocena tveganja

18. Verjetnost, da bo napad z izsiljevalskim programjem uspešen, je mogoče tako kot pri vseh tveganjih, ki jih predstavljajo zunanji akterji, močno zmanjšati z izboljšanjem varnosti okolja za nadzor podatkov. Večino teh kršitev je mogoče preprečiti z zagotavljanjem ustreznih organizacijskih, fizičnih in tehnoloških varnostnih ukrepov. Primera takih ukrepov sta ustrezno upravljanje popravkov in uporaba ustreznega sistema za odkrivanje zlonamerne programske opreme. Ustrezno in ločeno varnostno kopiranje bo pomagalo ublažiti posledice uspešnega napada, če do njega pride. Poleg tega bo program varnostnega izobraževanja, usposabljanja in ozaveščanja zaposlenih pomagal preprečiti in prepoznati take napade. (Seznam priporočljivih ukrepov je v oddelku 2.5.) Med takimi ukrepi je eden najpomembnejših ustrezno

upravljanje popravkov, ki zagotavlja, da so sistemi posodobljeni in da so odpravljene vse znane ranljivosti nameščenih sistemov, saj večina napadov z izsiljevalskim programjem izkorišča dobro znane ranljivosti.

19. Upravljavec bi moral pri ocenjevanju tveganj raziskati kršitev in opredeliti vrsto zlonamerne kode, da bi razumel možne posledice napada. Med takimi tveganji, ki jih je treba upoštevati, je tveganje, da so se podatki eksfiltrirali brez sledi v dnevnikih sistemov.

20. V tem primeru je imel napadalec dostop do osebnih podatkov in zaupnost šifriranega besedila, ki vsebuje osebne podatke v šifrirani obliki, je bila ogrožena. Vendar pa storilec, vsaj za zdaj, ne more prebrati ali uporabiti vseh podatkov, ki bi lahko bili eksfiltrirani. Tehnika šifriranja, ki jo uporablja upravljavec podatkov, je skladna z najnovejšo tehnologijo. Dešifrirni ključ ni bil ogrožen in ga domnevno tudi ni bilo mogoče določiti na drug način. Zato so tveganja za pravice in svoboščine fizičnih oseb, povezana z zaupnostjo, zmanjšana na najmanjšo možno mero, če ne bo prišlo do kriptoanalitskega napredka, zaradi katerega bodo šifrirani podatki v prihodnosti razumljivi.

21. Upravljavec podatkov bi moral upoštevati tveganje za posameznike zaradi kršitve[10]. V tem primeru se zdi, da so tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, posledica nerazpoložljivosti osebnih podatkov, zaupnost osebnih podatkov pa ni ogrožena[11]. V tem primeru so bili škodljivi učinki kršitve ublaženi dokaj kmalu po tem, ko je prišlo do kršitve. Zaradi ustreznega sistema varnostnega kopiranja[12] so učinki kršitve manj resni in v tem primeru ga je upravljavec lahko učinkovito uporabil.

22. Glede resnosti posledic za posameznike, na katere se nanašajo osebni podatki, bi bilo mogoče ugotoviti le manjše posledice, saj so bili zadevni podatki obnovljeni v nekaj urah, kršitev pa ni imela posledic za vsakodnevno delovanje upravljavca in ni bistveno vplivala na posameznike, na katere se nanašajo osebni podatki (na primer plačila zaposlenim ali obravnava zahtevkov strank).

2.1.2 PRIMER št. 01 – ublažitev in obveznosti

23. Brez varnostne kopije lahko upravljavec sprejme le malo ukrepov za odpravo izgube osebnih podatkov in podatke je treba vnovič zbrati. V tem konkretnem primeru pa je bilo mogoče učinke napada učinkovito omejiti s ponastavitvijo vseh ogroženih sistemov na čisto stanje, za katerega je znano, da ne vsebuje

---

[10] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej „Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679 Delovne skupine za varstvo podatkov iz člena 29, DS 248 rev.01 – potrdil EOVP, https://ec.europa.eu/newsroom/article29/items/611236, str. 9.

[11] Tehnično gledano šifriranje podatkov vključuje „dostop“ do izvornih podatkov, v primeru izsiljevalskega programja pa tudi izbris izvirnika – do podatkov mora dostopati izsiljevalska koda, da jih šifrira in odstrani izvorne podatke. Napadalec lahko pred izbrisom naredi kopijo izvirnika, vendar osebnih podatkov ne bo vedno mogoče pridobiti. Med potekom preiskave upravljavca podatkov se lahko pojavijo nove informacije, zaradi katerih se ta ocena spremeni. Dostop, katerega posledica je nezakonito uničenje, izguba, sprememba, nepooblaščeno razkritje osebnih podatkov ali varnostno tveganje za posameznika, na katerega se nanašajo osebni podatki, tudi brez razlage podatkov, je lahko enako resen kot dostop z razlago osebnih podatkov.

[12] Postopki varnostnega kopiranja morajo biti strukturirani, dosledni in ponovljivi. Primera postopkov varnostnega kopiranja sta metoda 3-2-1 in metoda dedek–oče–sin. Vsako metodo bi bilo treba vedno preskusiti glede učinkovitosti pri pokritosti in kadar je treba podatke obnoviti. Preskušanje bi bilo treba tudi ponavljati v določenih časovnih presledkih in zlasti ob spremembah dejanja obdelave ali njegovih okoliščin, da se zagotovi celovitost sistema.

zlonamerne kode, odpravo ranljivosti in obnovitvijo podatkov, ki so bili predmet kršitve, kmalu po napadu. Brez varnostne kopije so podatki izgubljeni, resnost pa se lahko poveča, ker se lahko povečajo tudi tveganja ali vplivi na posameznike.

24. Pri analizi kršitve je ključna spremenljivka pravočasnost učinkovite obnovitve podatkov iz takoj dostopne varnostne kopije. Določitev ustreznega časovnega okvira za obnovitev ogroženih podatkov je odvisna od edinstvenih okoliščin obravnavane kršitve. V Splošni uredbi o varstvu osebnih podatkov je navedeno, da se o kršitvi varnosti osebnih podatkov uradno obvesti brez nepotrebnega odlašanja in po možnosti najpozneje v 72 urah. Zato je mogoče ugotoviti, da prekoračitev 72-urnega roka v nobenem primeru ni priporočljiva, vendar se lahko pri obravnavi primerov z visoko stopnjo tveganja tudi upoštevanje tega roka obravnava kot nezadovoljivo.

25. V tem primeru je upravljavec na podlagi podrobne ocene učinka in postopka odzivanja na incidente ugotovil, da ni verjetno, da bi kršitev povzročila tveganje za pravice in svoboščine posameznikov, zato sporočilo posameznikom, na katere se nanašajo osebni podatki, ni potrebno, niti o kršitvi ni treba uradno obvestiti nadzornega organa. Vendar pa bi bilo treba kršitev, tako kot vse kršitve varnosti podatkov, dokumentirati v skladu s členom 33(5). Organizacija bo morda morala tudi posodobiti in popraviti svoje organizacijske in tehnične ukrepe ter postopke za varnostno ravnanje z osebnimi podatki in ublažitev tveganja (ali pa bo to od nje pozneje zahteval nadzorni organ). V okviru te posodobitve in popravka bi morala organizacija temeljito raziskati kršitev ter opredeliti vzroke in metode, ki jih je uporabil storilec, da bi preprečila podobne dogodke v prihodnosti.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	X	X

2.2 PRIMER št. 02: izsiljevalsko programje brez ustreznega varnostnega kopiranja

Eden od računalnikov, ki jih uporablja kmetijsko podjetje, je bil izpostavljen napadu z izsiljevalskim programjem, pri čemer je napadalec šifriral njegove podatke. Podjetje za spremljanje svojega omrežja uporablja strokovno znanje zunanjega podjetja za kibernetsko varnost. Na voljo so dnevniki, ki sledijo vsem podatkovnim tokovom, ki zapustijo podjetje (vključno z odhodno e-pošto). Po analizi dnevnikov in podatkov, ki so jih zbrali drugi sistemi za odkrivanje, je bilo z notranjo preiskavo, ki jo je podprlo zunanje podjetje za kibernetsko varnost, ugotovljeno, da je storilec podatke samo šifriral, ne da bi jih eksfiltriral. Iz dnevnikov ni razviden noben izhodni podatkovni tok v časovnem okviru napada. Osebni podatki, na katere je kršitev vplivala, se nanašajo na zaposlene in stranke podjetja, skupaj na nekaj ducat posameznikov. Kršitev ni vplivala na nobeno posebno vrsto podatkov. Varnostna kopija v elektronski obliki ni bila na voljo. Večina podatkov je bila obnovljena iz varnostnih kopij v papirni obliki. Obnavljanje podatkov je trajalo pet delovnih dni in je povzročilo manjše zamude pri dobavi naročil strankam.

2.2.1 PRIMER št. 02 – predhodni ukrepi in ocena tveganja

26. Upravljavec podatkov bi moral sprejeti enake predhodne ukrepe, kot so navedeni v delu 2.1 in oddelku 2.9. Glavna razlika v primerjavi s prejšnjim primerom je v tem, da ni elektronske varnostne kopije in šifriranja v mirovanju. To vodi do bistvenih razlik v naslednjih korakih.

27. Upravljavec bi moral pri ocenjevanju tveganj raziskati način vdora in opredeliti vrsto zlonamerne kode, da bi razumel možne posledice napada. V tem primeru je izsiljevalsko programje šifriralo osebne podatke, ne da bi jih eksfiltriralo. Zato se zdi, da so tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, posledica nerazpoložljivosti osebnih podatkov, zaupnost osebnih podatkov pa ni

ogrožena. Pri določanju tveganja je bistvenega pomena temeljit pregled dnevnikov požarnega zidu in njegovih posledic. Upravljavec podatkov bi moral na zahtevo predložiti dejanske ugotovitve teh preiskav.

28. Upoštevati mora, da ima zlonamerno programje v primeru bolj prefinjenega napada funkcijo urejanja dnevniških datotek in brisanja sledi. Tako – glede na to, da se dnevniki ne pošiljajo ali replicirajo v osrednji dnevniški strežnik – upravljavec podatkov tudi po temeljiti preiskavi, v kateri je bilo ugotovljeno, da napadalec osebnih podatkov ni eksfiltriral, ne more trditi, da neobstoj dnevniškega vnosa dokazuje neobstoj eksfiltracije, zato verjetnosti kršitve zaupnosti ni mogoče v celoti zavrniti.

29. Upravljavec podatkov bi moral oceniti tveganja te kršitve[13], če je napadalec dostopal do podatkov. Med ocenjevanjem tveganja bi moral upravljavec podatkov upoštevati tudi značilnosti, občutljivost, obseg in kontekst osebnih podatkov, na katere je kršitev vplivala. V tem primeru kršitev ni vplivala na nobeno posebno vrsto osebnih podatkov, količina podatkov, ki so bili predmet kršitve, in število posameznikov, na katere se nanašajo osebni podatki in na katere je kršitev vplivala, pa sta majhna.

30. Zbiranje natančnih informacij o nepooblaščenem dostopu je ključno za določitev stopnje tveganja in preprečevanje novega ali nadaljnjega napada. Če bi se podatki kopirali iz podatkovne zbirke, bi bil to očitno dejavnik, ki bi povečal tveganje. V primeru negotovosti glede podrobnosti nezakonitega dostopa bi bilo treba upoštevati slabši scenarij in ustrezno oceniti tveganje.

31. Neobstoj varnostne kopije podatkovne zbirke se lahko šteje za dejavnik povečanja tveganja, odvisno od resnosti posledic za posameznike, na katere se nanašajo osebni podatki, ki izhajajo iz nerazpoložljivosti podatkov.

2.2.2 PRIMER št. 02 – ublažitev in obveznosti

32. Brez varnostne kopije lahko upravljavec izvede le malo ukrepov za odpravo izgube osebnih podatkov in podatke je treba vnovič zbrati, razen če je na voljo kakšen drug vir (na primer elektronska sporočila s potrditvijo naročila). Brez varnostne kopije se lahko podatki izgubijo, resnost pa je odvisna od posledic za posameznike.

33. Obnovitev podatkov ne bi smela biti preveč problematična[14], če so podatki še vedno na voljo v papirni obliki, vendar se glede na to, da ni elektronske varnostne kopije podatkovne zbirke, šteje, da je treba uradno obvestiti nadzorni organ, saj je obnavljanje podatkov trajalo nekaj časa in bi lahko povzročilo nekaj zamud pri dobavi naročil strankam, precejšnje količine metapodatkov (na primer dnevnikov, časovnih žigov) pa morda ne bo mogoče obnoviti.

34. Obveščanje posameznikov, na katere se nanašajo osebni podatki, o kršitvi je lahko odvisno tudi od tega, koliko časa osebni podatki niso na voljo, in od težav, ki bi jih zaradi tega lahko imelo delovanje upravljavca (na primer zamude pri prenosu plačil zaposlenim). Ker lahko te zamude pri plačilih in dobavah povzročijo finančno izgubo posameznikom, katerih podatki so bili ogroženi, je mogoče tudi trditi, da je kršitev verjetno

[13] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

[14] To je odvisno od zapletenosti in strukture osebnih podatkov. V najbolj zapletenih scenarijih lahko vnovična vzpostavitev celovitosti podatkov, skladnost z metapodatki, zagotavljanje pravilnih razmerij v podatkovnih strukturah in preverjanje točnosti podatkov zahtevajo veliko sredstev in truda.

povzročila visoko tveganje. Prav tako se morda ne bo mogoče izogniti obveščanju posameznikov, na katere se nanašajo osebni podatki, če bo za obnovitev šifriranih podatkov potreben njihov prispevek.

35. Ta primer se uporablja kot primer napada z izsiljevalskim programjem s tveganjem za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, vendar ne dosega visokega tveganja. Treba bi ga bilo dokumentirati v skladu s členom 33(5) in o njem uradno obvestiti nadzorni organ v skladu s členom 33(1). Organizacija bo morda morala tudi posodobiti in popraviti svoje organizacijske in tehnične ukrepe ter postopke za varnostno ravnanje z osebnimi podatki in ublažitev tveganja (ali pa bo to od nje zahteval nadzorni organ).

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	X

2.3 PRIMER št. 03: izsiljevalsko programje z varnostnim kopiranjem in brez eksfiltracije podatkov v bolnišnici

Informacijski sistem bolnišnice oziroma zdravstvenega centra je bil izpostavljen napadu z izsiljevalskim programjem, napadalec pa je šifriral velik del njenih podatkov. Podjetje za spremljanje svojega omrežja uporablja strokovno znanje zunanjega podjetja za kibernetsko varnost. Na voljo so dnevniki, ki sledijo vsem podatkovnim tokovom, ki zapustijo podjetje (vključno z odhodno e-pošto). Po analizi dnevnikov in podatkov, ki so jih zbrali drugi sistemi za odkrivanje, je bilo z notranjo preiskavo, ki jo je podprlo zunanje podjetje za kibernetsko varnost, ugotovljeno, da je storilec podatke samo šifriral, ne da bi jih eksfiltriral. Iz dnevnikov ni razviden noben izhodni podatkovni tok v časovnem okviru napada. Osebni podatki, na katere je kršitev vplivala, se nanašajo na zaposlene in paciente, kar je skupaj več tisoč posameznikov. Na voljo so bile varnostne kopije v elektronski obliki. Večina podatkov je bila obnovljena, vendar je ta postopek trajal dva delovna dneva in je povzročil precejšnje zamude pri zdravljenju pacientov, saj so bile operacije odpovedane oziroma odložene, raven storitev pa se je zaradi nerazpoložljivosti sistemov znižala.

2.3.1 PRIMER št. 03 – predhodni ukrepi in ocena tveganja

36. Upravljavec podatkov bi moral sprejeti enake predhodne ukrepe, kot so navedeni v delu 2.1 in oddelku 2.5. Glavna razlika v primerjavi s prejšnjim primerom so zelo resne posledice za velik del posameznikov, na katere se nanašajo osebni podatki[15].

[15] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

37. Količina podatkov, ki so bili predmet kršitve, ter število posameznikov, na katere se nanašajo osebni podatki in na katere je kršitev vplivala, sta velika, saj bolnišnice navadno obdelujejo velike količine podatkov. Nerazpoložljivost podatkov močno vpliva na velik del posameznikov, na katere se nanašajo osebni podatki. Poleg tega obstaja preostalo zelo resno tveganje za zaupnost podatkov o pacientih.

38. Pomembni so vrsta kršitve ter značilnosti, občutljivost in obseg osebnih podatkov, na katere je kršitev vplivala. Čeprav je obstajala varnostna kopija podatkov in bi bilo podatke mogoče obnoviti v nekaj dneh, še vedno obstaja visoko tveganje zaradi resnosti posledic za posameznike, na katere se nanašajo osebni podatki, ki izhajajo iz nerazpoložljivosti podatkov v trenutku napada in v naslednjih dneh.

2.3.2 PRIMER št. 03 – ublažitev in obveznosti

39. Uradno obvestilo nadzornemu organu se šteje za potrebno, ker gre za posebne vrste osebnih podatkov in ker bi obnovitev podatkov lahko trajala dolgo, kar bi povzročilo velike zamude pri oskrbi pacientov. Obveščanje posameznikov, na katere se nanašajo osebni podatki, o kršitvi, je potrebno zaradi vpliva na paciente tudi po obnovitvi šifriranih podatkov. Ker so bili podatki o vseh pacientih, ki so bili v zadnjih letih zdravljeni v bolnišnici, šifrirani, je kršitev vplivala samo na tiste paciente, ki so bili predvideni za zdravljenje v bolnišnici v času, ko računalniški sistem ni bil na voljo. Upravljavec bi moral kršitev varstva podatkov zadevnim pacientom sporočiti neposredno. Neposredno sporočanje drugim pacientom, od katerih nekateri morda niso bili v bolnišnici več kot dvajset let, zaradi izjeme iz člena 34(3)(c) morda ni potrebno. V takem primeru se namesto tega objavi javno sporočilo[16] ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni. V tem primeru bi morala bolnišnica o napadu z izsiljevalskim programjem in njegovih učinkih obvestiti javnost.

40. Ta primer se uporablja kot primer napada z izsiljevalskim programjem z visokim tveganjem za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Treba bi ga bilo dokumentirati v skladu s členom 33(5), o njem uradno obvestiti nadzorni organ v skladu s členom 33(1) in ga sporočiti posameznikom, na katere se nanašajo osebni podatki, v skladu s členom 34(1). Organizacija mora tudi posodobiti in popraviti svoje organizacijske in tehnične ukrepe ter postopke za varnostno ravnanje z osebnimi podatki in ublažitev tveganja.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	✓

2.4 PRIMER št. 04: izsiljevalsko programje brez varnostnega kopiranja in z eksfiltracijo

[16] V uvodni izjavi 86 Splošne uredbe o varstvu podatkov je pojasnjeno, da „[bi morali] [p]osamezniki, na katere se nanašajo osebni podatki, [...] prejeti tako sporočilo, kakor hitro je to razumno mogoče in v tesnem sodelovanju z nadzornim organom ter ob upoštevanju smernic, ki jih je podal nadzorni organ ali drugi ustrezni organi, kot so organi za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj. Potreba po ublažitvi neposrednega tveganja nastanka škode bi na primer terjala takojšnjo sporočilo posameznikom, na katere se nanašajo osebni podatki, potreba po izvajanju ustreznih ukrepov zoper nadaljnje ali podobne kršitve varnosti osebnih podatkov pa bi lahko upravičila daljši rok za sporočilo.“

Strežnik podjetja za javni prevoz je bil izpostavljen napadu z izsiljevalskim programjem, napadalec pa je šifriral njegove podatke. Glede na ugotovitve notranje preiskave storilec podatkov ni le šifriral, ampak jih je tudi eksfiltriral. Vrsta podatkov, ki so bili predmet kršitve, so bili osebni podatki strank in zaposlenih ter več tisoč ljudi, ki so uporabljali storitve podjetja (na primer nakup vozovnic prek spleta). Poleg osnovnih osebnih podatkov so bile v kršitev vključene tudi številke osebnih izkaznic in finančni podatki, kot so podatki o kreditnih karticah. Obstajala je varnostna kopija podatkovne zbirke, vendar jo je napadalec prav tako šifriral.

2.4.1 PRIMER št. 04 – predhodni ukrepi in ocena tveganja

41. Upravljavec podatkov bi moral sprejeti enake predhodne ukrepe, kot so navedeni v delu 2.1 in oddelku 2.5. Čeprav je bilo vzpostavljeno varnostno kopiranje, je napad vplival tudi nanj. Ta ureditev sama sproža vprašanja o kakovosti predhodnih varnostnih ukrepov upravljavca na področju informacijske tehnologije in bi jo bilo treba med preiskavo dodatno preučiti, saj mora biti v dobro zasnovanem sistemu varnostnega kopiranja več varnostnih kopij varno shranjenih brez dostopa iz glavnega sistema, sicer bi lahko bile ogrožene z istim napadom. Poleg tega lahko napadi z izsiljevalskim programjem ostanejo neodkriti več dni in počasi šifrirajo redko uporabljene podatke. To lahko povzroči neuporabnost več varnostnih kopij, zato bi bilo treba tudi varnostne kopije pripravljati periodično in jih izolirati. S tem bi se povečala verjetnost obnovitve, čeprav z večjo izgubo podatkov.

42. Ta kršitev se ne nanaša le na razpoložljivosti podatkov, temveč tudi na zaupnost, saj je napadalec morda spremenil in/ali kopiral podatke iz strežnika. Zato taka kršitev povzroča visoko tveganje[17].

43. Značilnosti, občutljivost in obseg osebnih podatkov še povečujejo tveganja, saj je število posameznikov, na katere kršitev vpliva, veliko, prav tako pa tudi skupna količina osebnih podatkov, na katere kršitev vpliva. Poleg osnovnih osebnih podatkov so vključeni tudi osebni dokumenti in finančni podatki, kot so podatki o kreditnih karticah. Kršitev varstva podatkov v zvezi s takimi podatki že sama po sebi pomeni veliko tveganje, če pa se obdelujejo skupaj, se lahko med drugim uporabijo za krajo identitete ali goljufijo.

44. Zaradi napačne strežniške logike ali organizacijskih kontrol je izsiljevalsko programje vplivalo na varnostne kopije datotek, kar je preprečilo obnovitev podatkov in povečalo tveganje.

45. Ta kršitev varstva podatkov pomeni veliko tveganje za pravice in svoboščine posameznikov, saj bi lahko povzročila tako premoženjsko (na primer finančno izgubo, saj je kršitev vplivala na podatke o kreditnih karticah) kot tudi nepremoženjsko škodo (na primer krajo identitete ali goljufijo, saj je kršitev vplivala na podatke o osebnih izkaznicah).

2.4.2 PRIMER št. 04 – ublažitev in obveznosti

46. Sporočanje posameznikom, na katere se nanašajo osebni podatki, je bistveno, da lahko sprejmejo potrebne ukrepe za preprečitev materialne škode (na primer blokirajo svoje kreditne kartice).

47. Poleg dokumentiranja kršitve v skladu s členom 33(5) je v tem primeru obvezno tudi uradno obvestilo nadzornemu organu (člen 33(1)), upravljavec pa mora kršitev sporočiti tudi posameznikom, na katere se nanašajo osebni podatki (člen 34(1)). To bi se lahko izvedlo za vsako posamezno osebo posebej, za posameznike, pri katerih kontaktni podatki niso na voljo, pa bi moral upravljavec to storiti javno, če tako

[17] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

sporočanje ne bi moglo povzročiti dodatnih negativnih posledic za posameznike, na katere se nanašajo osebni podatki, na primer z uradnim obvestilom na spletnem mestu. V slednjem primeru je potrebno natančno in jasno sporočilo na vidnem mestu na domači strani upravljavca z natančnim sklicevanjem na ustrezne določbe Splošne uredbe o varstvu podatkov. Organizacija bo morala tudi posodobiti in popraviti svoje organizacijske in tehnične ukrepe ter postopke za varnostno ravnanje z osebnimi podatki in ublažitev tveganja.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	✓

2.5 Organizacijski in tehnični ukrepi za preprečevanje oziroma ublažitev posledic napadov z izsiljevalskim programjem

48. Dejstvo, da bi lahko prišlo do napada z izsiljevalskim programjem, je običajno znak ene ali več ranljivosti v upravljavčevem sistemu. To velja tudi v primerih izsiljevalskega programja, v katerem so bili osebni podatki šifrirani, ne pa tudi eksfiltrirani. Ne glede na rezultat in posledice napada ni mogoče dovolj poudariti pomena celovite ocene sistema za varnost podatkov, s posebnim poudarkom na varnosti na področju informacijske tehnologije. Ugotovljene pomanjkljivosti in varnostne luknje je treba dokumentirati ter jih nemudoma odpraviti.

49. Priporočljivi ukrepi:

(Seznam naslednjih ukrepov nikakor ni izključujoč ali izčrpen. Njegov cilj je zagotoviti ideje za preprečevanje in možne rešitve. Vsaka dejavnost obdelave je drugačna, zato se mora upravljavec sam odločiti, kateri ukrepi so v dani situaciji najprimernejši.)

- *Posodabljanje strojne programske opreme, operacijskega sistema in aplikacijskega programja v strežnikih, napravah odjemalcev, aktivnih omrežnih komponentah in vseh drugih napravah v istem lokalnem omrežju (vključno z napravami Wi-Fi). Zagotavljanje ustreznih varnostnih ukrepov na področju informacijske tehnologije, skrb za njihovo učinkovitost in redno posodabljanje, ko se obdelava ali okoliščine spremenijo ali razvijejo. To vključuje vodenje podrobnih dnevnikov o tem, kateri popravki so bili uporabljeni pri katerem časovnem žigu.*
- *Načrtovanje in organiziranje sistemov obdelave in infrastrukture za segmentacijo ali izolacijo podatkovnih sistemov in omrežij, da se prepreči širjenje zlonamerne programske opreme znotraj organizacije in v zunanje sisteme.*
- *Obstoj posodobljenega, varnega in preizkušenega postopka varnostnega kopiranja. Mediji za srednje- in dolgoročno varnostno kopiranje bi morali biti ločeni od operativnega shranjevanja podatkov in nedosegljivi tretjim osebam tudi v primeru uspešnega napada (na primer dnevno prirastno varnostno kopiranje in tedensko popolno varnostno kopiranje).*
- *Imeti oziroma pridobiti bi bilo treba ustrezno, posodobljeno, učinkovito in integrirano programsko opremo za odkrivanje zlonamerne programske opreme.*
- *Imeti bi bilo treba ustrezen, posodobljen, učinkovit in integriran požarni zid ter sistem za odkrivanje in preprečevanje vdorov. Usmerjanje omrežnega prometa skozi požarni zid oziroma sistem za odkrivanje vdorov, tudi v primeru domače pisarne ali mobilnega dela (na primer z uporabo povezav VPN z organizacijskimi varnostnimi mehanizmi pri dostopanju do interneta).*

- *Usposabljanje zaposlenih o metodah prepoznavanja in preprečevanja napadov na informacijsko tehnologijo. Upravljavec bi moral zagotoviti sredstva za ugotavljanje, ali so elektronska sporočila in sporočila, pridobljena z drugimi komunikacijskimi sredstvi, verodostojna in zaupanja vredna. Zaposlene bi bilo treba usposobiti, da bi prepoznali, kdaj se je tak napad zgodil, da bi vedeli, kako odstraniti končno točko iz omrežja, in da bi se seznanili s svojo obveznostjo, da nemudoma obvestijo uradno osebo za varnost.*

- *Poudarjanje potrebe po opredelitvi vrste zlonamerne kode, da se ugotovi, kakšne so posledice napada, in poiščejo ustrezni ukrepi za ublažitev tveganja. Če je napad z izsiljevalskim programjem uspel in ni na voljo nobene varnostne kopije, se lahko za pridobitev podatkov uporabijo razpoložljiva orodja, kot so orodja v okviru projekta „No More Ransom“ (nič več odkupnine) (nomoreransom.org). Če je na voljo varna varnostna kopija, je priporočljivo obnoviti podatke iz nje.*

- *Pošiljanje ali repliciranje vseh dnevnikov v osrednji dnevniški strežnik (po možnosti vključno s podpisovanjem ali kriptografskim časovnim žigosanjem dnevniških vnosov).*

- *Močno šifriranje in večfaktorska avtentikacija, zlasti za upravni dostop do informacijskih sistemov, ter ustrezno upravljanje ključev in gesel.*

- *Redno preskušanje ranljivosti in penetracijsko testiranje.*

- *Ustanovitev skupine za odzivanje na incidente na področju računalniške varnosti ali skupine za odzivanje na računalniške grožnje znotraj organizacije ali pridružitev skupni skupini za odzivanje na incidente na področju računalniške varnosti oziroma skupini za odzivanje na računalniške grožnje. Priprava načrta za odzivanje na incidente, sanacijskega načrta po nesreči in načrta neprekinjenega poslovanja ter zagotovitev, da so ti načrti temeljito preskušeni.*

- *Pri ocenjevanju protiukrepov bi bilo treba analizo tveganja pregledati, preizkusiti in posodobiti.*

3 NAPADI Z EKSFILTRACIJO PODATKOV

50. Napadi, pri katerih se izkoriščajo ranljivosti storitev, ki jih upravljavec ponuja tretjim osebam prek interneta, na primer z napadi z vrinjenjem (na primer SQL-vrinjenje, prečkanje poti), ogrožanjem spletnih strani in podobnimi metodami, so lahko podobni napadom z izsiljevalskim programjem, saj tveganje izhaja iz dejanja nepooblaščene tretje osebe, cilji teh napadov pa so običajno kopiranje, eksfiltracija in zloraba osebnih podatkov v zlonamerne namene. Zato gre večinoma za kršitve zaupnosti in po možnosti tudi celovitosti podatkov. Če se upravljavec zaveda značilnosti takih kršitev, so mu hkrati na voljo številni ukrepi, s katerimi lahko bistveno zmanjša tveganje uspešne izvedbe napada.

3.1 PRIMER št. 05: eksfiltracija podatkov o prijavi za delovno mesto s spletnega mesta

Zavod za zaposlovanje je bil žrtev kibernetskega napada, s katerim je bila na njegovo spletno mesto nameščena zlonamerna koda. Zaradi te zlonamerne kode so bili osebni podatki, ki so bili poslani prek spletnih obrazcev za prijavo za delovno mesto in shranjeni na spletnem strežniku, dostopni nepooblaščenim osebam. Kršitev bi lahko vplivala na 213 takih obrazcev, vendar je bilo po analizi podatkov, ki so bili predmet kršitve, ugotovljeno, da kršitev ni vplivala na nobeno posebno vrsto podatkov. Poseben nameščen paket zlonamerne programske opreme je vključeval funkcije, ki so napadalcu omogočale, da je odstranil vso zgodovino eksfiltracije podatkov, ter spremljanje obdelave v strežniku in zajemanje osebnih podatkov. Paket je bil odkrit šele mesec po njegovi namestitvi.

3.1.1 PRIMER št. 05 – predhodni ukrepi in ocena tveganja

51. Varnost okolja upravljavca podatkov je izjemno pomembna, saj je večino teh kršitev mogoče preprečiti z zagotavljanjem stalnega posodabljanja vseh sistemov, šifriranja občutljivih podatkov in razvoja aplikacij v skladu z visokimi varnostnimi standardi, kot so močna avtentikacija, ukrepi proti napadom z grobo silo, onemogočanje določenih znakov pri vnosih uporabnika ali „čiščenje“ vnosov uporabnika[18] itd. Potrebne so tudi redne revizije varnosti na področju informacijske tehnologije, ocene ranljivosti in penetracijski testi, da se take ranljivosti odkrijejo vnaprej in odpravijo. V tem konkretnem primeru bi lahko orodja za spremljanje celovitosti datotek v produkcijskem okolju pomagala odkriti vrinjenje kode. (Seznam priporočljivih ukrepov je v oddelku 3.7.)

52. Upravljavec bi moral kršitev vedno začeti preiskovati z opredelitvijo vrste napada in njegovih metod, da oceni, katere ukrepe je treba sprejeti. Da bi bilo to hitro in učinkovito, bi moral imeti upravljavec podatkov pripravljen načrt odzivanja na incidente, v katerem bi bili določeni hitri in potrebni ukrepi za prevzem nadzora nad incidentom. V tem konkretnem primeru je bila vrsta kršitve dejavnik, ki je povečal tveganje, saj ni bila omejena le zaupnost podatkov, temveč je imel vdiralec tudi sredstva za ugotavljanje sprememb v sistemu, zato je postala vprašljiva tudi celovitost podatkov.

53. Za ugotovitev, koliko je kršitev vplivala na posameznike, na katere se nanašajo osebni podatki, bi bilo treba oceniti značilnosti, občutljivost in obseg osebnih podatkov, na katere je kršitev vplivala. Čeprav kršitev ni vplivala na nobeno posebno vrsto osebnih podatkov, so podatki, do katerih se je dostopalo, vsebovali precej informacij o posameznikih iz spletnih obrazcev in bi jih bilo mogoče zlorabiti na več načinov (ciljno usmerjanje z neželenim trženjem, kraja identitete itd.), zato bi morala resnost posledic povečati tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki[19].

3.1.2 PRIMER št. 05 – ublažitev in obveznosti

54. Če je mogoče, bi bilo treba po rešitvi težave primerjati podatkovno zbirko s tisto, ki je shranjena v varni varnostni kopiji. Izkušnje, pridobljene pri kršitvi, bi bilo treba uporabiti pri posodabljanju informacijske infrastrukture. Upravljavec podatkov bi moral vse informacijske sisteme, na katere je kršitev vplivala, vrniti v znano čisto stanje, odpraviti ranljivost in izvesti nove varnostne ukrepe, da bi preprečil podobne kršitve varstva podatkov v prihodnosti, na primer preverjanja celovitosti datotek in varnostne revizije. Če se osebni podatki niso samo eksfiltrirali, ampak so bili tudi izbrisani, mora upravljavec sistematično ukrepati za povrnitev osebnih podatkov v stanje, v katerem so bili pred kršitvijo. Morda bo treba uporabiti popolne varnostne kopije, prirastne spremembe in nato morda vnovič zagnati obdelavo od zadnje prirastne varnostne kopije, kar zahteva, da je upravljavec sposoben ponoviti spremembe, opravljene od zadnje varnostne kopije. To bi lahko zahtevalo, da ima upravljavec sistem, ki je zasnovan tako, da hrani dnevne vhodne datoteke, če jih je treba vnovič obdelati, ter zahteva zanesljivo metodo shranjevanja in ustrezno politiko hrambe.

55. Ob upoštevanju zgoraj navedenega je treba glede na to, da bo kršitev verjetno povzročila veliko tveganje za pravice in svoboščine posameznikov, o njej vsekakor obvestiti posameznike, na katere se nanašajo osebni podatki (člen 34(1)), kar seveda pomeni, da bi bilo treba v obrazec uradnega obvestila o kršitvi varstva

[18] Onemogočanje določenih znakov pri vnosih uporabnika ali čiščenje vnosov uporabnika je oblika potrjevanja vnosov, ki zagotavlja, da se v informacijski sistem vnesejo le pravilno oblikovani podatki.

[19] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

podatkov vključiti tudi ustrezne nadzorne organe. Dokumentiranje kršitve je v skladu s členom 33(5) Splošne uredbe o varstvu podatkov obvezno in olajša oceno stanja.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	✓

3.2 PRIMER št. 06: eksfiltracija zgoščenega gesla s spletnega mesta

Ranljivost za SQL-vrinjenje je bila izrabljena za dostop do podatkovne zbirke strežnika spletnega mesta s kuharskimi recepti. Uporabniki so lahko kot uporabniška imena izbrali le poljubne psevdonime. Uporaba elektronskih naslovov v ta namen je bila odsvetovana. Gesla, shranjena v podatkovni zbirki, so bila zgoščena z močnim algoritmom, sol pa ni bila ogrožena. Podatki, ki so bili predmet kršitve: zgoščena gesla 1.200 uporabnikov. Upravljavec je posameznike, na katere se nanašajo osebni podatki, zaradi varnosti o kršitvi obvestil po elektronski pošti in jih pozval, naj spremenijo svoja gesla, zlasti če so isto geslo uporabljali za druge storitve.

3.2.1 PRIMER št. 06 – predhodni ukrepi in ocena tveganja

56. V tem konkretnem primeru je zaupnost podatkov ogrožena, vendar so bila gesla v podatkovni zbirki zgoščena z najsodobnejšo metodo, kar naj bi zmanjšalo tveganje glede na značilnosti občutljivost in obseg osebnih podatkov. Ta primer ne pomeni tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.

57. Poleg tega niso bili ogroženi kontaktni podatki (na primer elektronski naslovi ali telefonske številke) posameznikov, na katere se nanašajo osebni podatki, kar pomeni, da za posameznike, na katere se nanašajo osebni podatki, ni večjega tveganja, da bi postali tarča poskusov goljufije (na primer prejemanje elektronskih sporočil za zvabljanje ali goljufivih besedilnih sporočil in telefonskih klicev). Nobene posebne vrste podatkov ni bilo vključene.

58. Nekatera uporabniška imena bi se lahko štela za osebne podatke, vendar tema spletnega mesta ne dopušča negativnih konotacij. Čeprav je treba opozoriti, da se lahko ocena tveganja spremeni[20], če bi vrsta spletnega mesta in podatki, do katerih se dostopa, lahko razkrili posebne vrste osebnih podatkov (na primer spletno mesto politične stranke ali sindikata). Z uporabo najsodobnejšega šifriranja bi se lahko ublažili škodljivi učinki kršitve. Z zagotovitvijo, da je dovoljeno omejeno število poskusov prijave, se bo preprečila uspešnost napadov z grobo silo ob prijavi, s čimer se bo močno zmanjšalo tveganje, ki ga pomenijo napadalci, ki že poznajo uporabniška imena.

3.2.2 PRIMER št. 06 – ublažitev in obveznosti

59. Sporočilo posameznikom, na katere se nanašajo osebni podatki, bi se lahko v nekaterih primerih štelo za blažilni dejavnik, saj lahko ti sprejmejo potrebne ukrepe za preprečitev nadaljnje škode zaradi kršitve, na

[20] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

primer tako, da spremenijo svoje geslo. V tem primeru uradno obveščanje ni bilo obvezno, vendar se lahko v številnih primerih šteje za dobro prakso.

60. Upravljavec podatkov bi moral odpraviti ranljivost in izvajati nove varnostne ukrepe, da bi se izognil podobnim kršitvam varstva podatkov v prihodnosti, kot so na primer sistematične varnostne revizije spletnega mesta.

61. Kršitev bi bilo treba dokumentirati v skladu s členom 33(5), vendar uradno obveščanje ali sporočanje ni potrebno.

62. Prav tako je zelo priporočljivo, da se posameznike, na katere se nanašajo osebni podatki, v vsakem primeru obvesti o kršitvi, ki vključuje gesla, tudi če so bila gesla shranjena z uporabo soljenega zgoščenega gesla z algoritmom, ki je skladen z najsodobnejšo tehnologijo. Zaželena je uporaba metod avtentikacije, ki preprečujejo potrebo po obdelavi gesel na strani strežnika. Posamezniki, na katere se nanašajo osebni podatki, bi morali imeti možnost izbire, da sprejmejo ustrezne ukrepe v zvezi s svojimi gesli.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	X	X

3.3 PRIMER št. 07: napad s polnjenjem poverilnic na bančnem spletnem mestu

Banka je bila žrtev kibernetskega napada na eno od svojih spletnih mest za spletno bančništvo. Cilj napada je bil našteti vsa možna uporabniška imena za prijavo z uporabo določenega trivialnega gesla. Gesla so bila sestavljena iz osmih številk. Zaradi ranljivosti spletnega mesta so k napadalcu v nekaterih primerih ušle informacije o posameznikih, na katere se nanašajo osebni podatki (ime, priimek, spol, datum in kraj rojstva, davčna številka, identifikacijske kode uporabnikov), tudi če uporabljeno geslo ni bilo pravilno ali če bančni račun ni bil več aktiven. To je vplivalo na približno 100.000 posameznikov, na katere se nanašajo osebni podatki. Od tega se je napadalec uspešno prijavil v približno 2.000 računov, za katere se je uporabljalo trivialno geslo, ki ga je napadalec poskusil uporabiti. Upravljavec je lahko naknadno prepoznal vse nezakonite poskuse prijave. Upravljavec podatkov je lahko potrdil, da na podlagi preverjanj za preprečevanje goljufij med napadom ni bila izvedena nobena transakcija s temi računi. Banka je bila seznanjena s kršitvijo varstva podatkov, ker je njen center za varnostne operacije zaznal veliko število zahtevkov za prijavo, usmerjenih na spletno mesto. Upravljavec je v odziv na to onemogočil možnost prijave na spletno mesto tako, da ga je izklopil, in izsilil ponastavitev gesla ogroženih računov. O kršitvi je obvestil samo uporabnike z ogroženimi računi, tj. uporabnike, katerih gesla so bila ogrožena ali katerih podatki so bili razkriti.

3.3.1 PRIMER št. 07 – predhodni ukrepi in ocena tveganja

63. Omeniti je treba, da imajo upravljavci, ki obdelujejo podatke zelo osebne narave[21], večjo odgovornost glede zagotavljanja ustrezne varnosti podatkov, na primer z varnostnim operativnim centrom in drugimi ukrepi

[21] Kot so informacije o posameznikih, na katere se nanašajo osebni podatki, ki se nanašajo na metode plačevanja, kot so številke kartic, bančni računi, spletna plačila, plačilne liste, bančni izpiski, ekonomske študije ali katere koli druge informacije, ki lahko razkrijejo ekonomske informacije v zvezi s posamezniki, na katere se nanašajo osebni podatki.

za preprečevanje in odkrivanje incidentov ter odzivanje nanje. Neizpolnjevanje teh višjih standardov bo zagotovo povzročilo strožje ukrepe med preiskavo nadzornega organa.

64. Kršitev se poleg podatkov o identiteti in uporabniškem imenu nanaša tudi na finančne podatke, zato je še posebej resna. Število posameznikov, na katere kršitev vpliva, je veliko.

65. Dejstvo, da se kršitev lahko zgodi v tako občutljivem okolju, kaže na velike pomanjkljivosti v sistemu upravljavca ter lahko kaže, da je „treba“ v skladu s členi 24(1), 25(1) in 32(1) Splošne uredbe o varstvu podatkov pregledati in posodobiti zadevne ukrepe. Podatki, ki so predmet kršitve, omogočajo enolično identifikacijo posameznikov, na katere se nanašajo osebni podatki, in vsebujejo druge informacije o njih (vključno s spolom, datumom in krajem rojstva), poleg tega jih lahko napadalec uporabi za ugibanje gesel strank ali za izvedbo kampanje usmerjenega lažnega predstavljanja, namenjene strankam banke.

66. Iz teh razlogov se je štelo, da bi kršitev varstva podatkov verjetno povzročila veliko tveganje za pravice in svoboščine vseh zadevnih posameznikov, na katere se nanašajo osebni podatki[22]. Zato je mogoče pričakovati nastanek materialne (na primer finančna izguba) in nematerialne škode (na primer kraja identitete ali goljufija).

3.3.2 PRIMER št. 07 – ublažitev in obveznosti

67. Ukrepi upravljavca, navedeni v opisu primera, so ustrezni. Po kršitvi je odpravil tudi ranljivost spletnega mesta in sprejel druge ukrepe za preprečevanje podobnih kršitev varstva podatkov v prihodnosti, kot sta dodajanje dvofaktorske avtentikacije zadevnemu spletnemu mestu in prehod na močno avtentikacijo strank.

68. Dokumentiranje kršitve v skladu s členom 33(5) Splošne uredbe o varstvu podatkov in uradno obvestilo nadzornemu organu o njej v tem scenariju nista izbirna. Poleg tega bi moral upravljavec v skladu s členom 34 Splošne uredbe o varstvu podatkov obvestiti vseh 100.000 posameznikov, na katere se nanašajo osebni podatki (vključno s tistimi, katerih računi niso bili ogroženi).

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	✓

3.4 Organizacijski in tehnični ukrepi za preprečevanje oziroma ublažitev posledic hekerskih napadov

69. Tako kot v primeru napadov z izsiljevalskim programjem je ne glede na rezultat in posledice napada za upravljavce v podobnih primerih obvezna vnovična ocena varnosti na področju informacijske tehnologije.

70. Priporočljivi ukrepi[23]:

(Seznam naslednjih ukrepov nikakor ni izključujoč ali izčrpen. Njegov cilj je zagotoviti ideje za preprečevanje in možne rešitve. Vsaka dejavnost obdelave je drugačna, zato se mora upravljavec sam odločiti, kateri ukrepi so v dani situaciji najprimernejši.)

[22] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

[23] Za varen razvoj spletnih aplikacij glej tudi: https://www.owasp.org/index.php/Main_Page.

- *Najsodobnejše šifriranje in upravljanje ključev, zlasti pri obdelavi gesel, občutljivih ali finančnih podatkov. Kriptografsko zgoščevanje in soljenje za tajne podatke (gesla) imata vedno prednost pred šifriranjem gesel. Zaželena je uporaba metod avtentikacije, s katerimi se odpravi potreba po obdelavi gesel na strani strežnika.*
- *Posodabljanje sistema (programska in strojna oprema). Zagotavljanje, da se izvajajo vsi varnostni ukrepi na področju informacijske tehnologije, skrb za njihovo učinkovitost in redno posodabljanje, ko se obdelava ali okoliščine spremenijo ali razvijejo. Za zagotovitev skladnosti s členom 5(1)(f) v skladu s členom 5(2) Splošne uredbe o varstvu podatkov bi moral upravljavec voditi evidenco vseh izvedenih posodobitev, vključno s časom njihove uporabe.*
- *Uporaba močnih metod avtentikacije, kot so dvofaktorska avtentikacija in avtentikacijski strežniki, ki jih dopolnjuje posodobljena politika gesel.*
- *Standardi varnega razvoja vključujejo filtriranje uporabniških vnosov (z uporabo belih seznamov, če je to izvedljivo), onemogočanje določenih znakov pri vnosih uporabnika in ukrepe za preprečevanje grobe sile (kot je omejitev največjega števila vnovičnih poskusov). „Požarni zidovi spletnih aplikacij“ lahko pripomorejo k učinkoviti uporabi te tehnike.*
- *Vzpostavljena stroga politika upravljanja uporabniških pravic in nadzora dostopa.*
- *Uporaba ustreznih, posodobljenih, učinkovitih in integriranih požarnih zidov, sistemov za odkrivanje vdorov in drugih sistemov za obrambo zunanjih točk.*
- *Sistematične revizije varnosti na področju informacijske tehnologije in ocene ranljivosti (penetracijsko testiranje).*
- Redni pregledi in preskušanje za zagotovitev, da je mogoče varnostne kopije uporabiti za obnovitev vseh podatkov, katerih celovitost ali razpoložljivost je bila ogrožena.
- *V naslovu URL v golem besedilu ni identifikacijske številke seje.*

4 NOTRANJI VIR TVEGANJA ZA LJUDI

71. Zaradi njenega pogostega pojavljanja je treba opozoriti na vlogo človeške napake pri kršitvah varnosti osebnih podatkov. Ker so take kršitve lahko namerne in nenamerne, upravljavci podatkov zelo težko opredelijo ranljivosti in sprejmejo ukrepe za njihovo preprečevanje. Mednarodna konferenca pooblaščencev za varstvo podatkov in zasebnost je priznala pomen obravnave takih človeških dejavnikov in oktobra 2019 sprejela resolucijo o obravnavi vloge človeških napak pri kršitvah varnosti osebnih podatkov[24]. V tej resoluciji je poudarjeno, da bi bilo treba sprejeti ustrezne zaščitne ukrepe za preprečevanje človeških napak, vključuje pa tudi neizčrpen seznam takih zaščitnih ukrepov in pristopov.

4.1 PRIMER št. 08: eksfiltracija poslovnih podatkov s strani zaposlenega

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

Zaposleni v podjetju med odpovednim rokom kopira poslovne podatke iz podatkovne zbirke podjetja. Pooblaščen je za dostop do podatkov samo za opravljanje svojih delovnih nalog. Več mesecev pozneje, po prenehanju delovnega razmerja, tako pridobljene podatke (osnovne kontaktne podatke) uporabi za obdelavo novih podatkov, ki jih upravlja, da bi navezal stik s strankami podjetja in jih privabil k svojemu novemu poslu.

4.1.1 PRIMER št. 08 – predhodni ukrepi in ocena tveganja

72. V tem konkretnem primeru niso bili sprejeti predhodni ukrepi, ki bi zaposlenemu preprečili kopiranje kontaktnih podatkov strank podjetja, saj je potreboval – in imel – zakonit dostop do teh podatkov za opravljanje delovnih nalog. Ker izpolnjevanje večine delovnih nalog v zvezi s strankami zahteva neke vrste dostop zaposlenih do osebnih podatkov, je te kršitve varstva podatkov morda najtežje preprečiti. Z omejitvami obsega dostopa se lahko omeji delo, ki ga lahko opravi posamezen zaposleni. Vendar pa lahko dobro premišljene politike dostopa in stalen nadzor pomagajo preprečiti take kršitve.

73. Kot običajno je treba med ocenjevanjem tveganja upoštevati vrsto kršitve ter značilnosti, občutljivost in obseg osebnih podatkov, ki so predmet kršitve. Take kršitve so po navadi kršitve zaupnosti, saj podatkovna zbirka običajno ostane nedotaknjena, njena vsebina pa se „zgolj“ kopira za nadaljnjo uporabo. Tudi količina podatkov, ki so predmet kršitve, je običajno majhna ali srednja. V tem konkretnem primeru kršitev ni vplivala na nobeno posebno vrsto osebnih podatkov, saj je zaposleni potreboval le kontaktne podatke strank, da bi lahko navezal stik z njimi po odhodu iz podjetja. Zato zadevni podatki niso občutljivi.

74. Čeprav je edini cilj nekdanjega zaposlenega, ki je zlonamerno kopiral podatke, morda omejen na pridobitev kontaktnih podatkov strank podjetja za lastne komercialne namene, upravljavec tveganja za posameznike, na katere se nanašajo osebni podatki in na katere je kršitev vplivala, ne more obravnavati kot majhno, saj nima nobenega zagotovila o namenih zaposlenega. Čeprav so lahko posledice kršitve omejene na izpostavljenost nezaslišanemu lastnemu trženju nekdanjega zaposlenega, ni izključena nadaljnja in hujša zloraba ukradenih podatkov, odvisno od namena obdelave, ki jo je vzpostavil nekdanji zaposleni[25].

4.1.2 PRIMER št. 08 – ublažitev in obveznosti

75. V zgornjem primeru je škodljive učinke kršitve težko ublažiti. Morda bo potrebno takojšnje pravno ukrepanje, da se nekdanjemu zaposlenemu preprečita nadaljnja zloraba in razširjanje podatkov. V naslednjem koraku bi moral biti cilj preprečevati podobne primere v prihodnosti. Upravljavec lahko poskuša nekdanjemu zaposlenemu odrediti, naj preneha uporabljati podatke, vendar je uspeh tega ukrepa v najboljšem primeru vprašljiv. Pomagajo lahko ustrezni tehnični ukrepi, kot je onemogočanje kopiranja ali prenosa podatkov na prenosne naprave.

76. Za take primere ni univerzalne rešitve, vendar lahko sistematičen pristop pripomore k njihovemu preprečevanju. Podjetje lahko na primer premisli, če je to mogoče, o umiku nekaterih oblik dostopa zaposlenim, ki so sporočili, da nameravajo zapustiti podjetje, ali o uvedbi dnevnikov dostopa, da se lahko neželeni dostop zabeleži in označi. Pogodba, podpisana z zaposlenimi, bi morala vsebovati klavzule, ki prepovedujejo taka dejanja.

77. Ker zadevna kršitev ne bo povzročila velikega tveganja za pravice in svoboščine fizičnih oseb, bo zadostovalo uradno obvestilo nadzornemu organu. Vendar bi bilo obveščanje posameznikov, na katere se nanašajo

[25] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

osebni podatki, lahko koristno tudi za upravljavca podatkov, saj bi bilo morda bolje, da bi o uhajanju podatkov izvedeli od podjetja in ne od nekdanjega zaposlenega, ki poskuša navezati stik z njimi. Dokumentiranje kršitev varstva podatkov v skladu s členom 33(5) je zakonska obveznost.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	X

4.2 PRIMER št. 09: nenamerni prenos podatkov zaupanja vredni tretji osebi

Zavarovalni zastopnik je opazil, da je lahko – zaradi napačnih nastavitev Excelove datoteke, ki jo je prejel po elektronski pošti – dostopal do informacij, povezanih z dvema ducatoma strank, ki niso spadale v njegovo področje pristojnosti. Zavezan je varovanju poslovnih skrivnosti in je bil edini prejemnik elektronskega sporočila. Dogovor med upravljavcem podatkov in zavarovalnim zastopnikom zavezuje zastopnika, da upravljavcu podatkov brez nepotrebnega odlašanja sporoči kršitev varnosti osebnih podatkov. Zato je zastopnik sporočil napako kontrolorju, ki je datoteko popravil in jo vnovič poslal ter prosil zastopnika, naj prejšnje sporočilo izbriše. V skladu z zgoraj navedenim dogovorom mora zastopnik potrditi izbris v pisni izjavi, kar je tudi storil. Pridobljene informacije ne vključujejo posebnih vrst osebnih podatkov, temveč le kontaktne podatke in podatke o samem zavarovanju (vrsta zavarovanja, znesek). Po analizi osebnih podatkov, na katere je kršitev vplivala, upravljavec podatkov ni ugotovil nobenih posebnih značilnosti na strani posameznikov ali upravljavca podatkov, ki bi lahko vplivale na stopnjo vpliva kršitve.

4.2.1 PRIMER št. 09 – predhodni ukrepi in ocena tveganja

78. V tem primeru kršitev ni posledica namernega dejanja zaposlenega, temveč nenamerne človeške napake zaradi nepozornosti. Take kršitve je mogoče preprečiti ali zmanjšati njihovo pogostost z (a) izvajanjem programov usposabljanja, izobraževanja in ozaveščanja, s katerimi zaposleni pridobijo boljše razumevanje pomena varstva osebnih podatkov; (b) zmanjšanjem izmenjave datotek prek elektronske pošte in uporabo namenskih sistemov, na primer za obdelavo podatkov strank; (c) dvojnim preverjanjem datotek pred pošiljanjem ter (d) ločenim ustvarjanjem in pošiljanjem datotek.

79. Ta kršitev varnosti podatkov se nanaša le na zaupnost podatkov, celovitost in dostopnost podatkov pa nista ogroženi. Kršitev varnosti podatkov je zadevala le približno dva ducata strank, zato se količina podatkov, ki so predmet kršitve, lahko šteje za majhno. Poleg tega osebni podatki, ki so predmet kršitve, ne vsebujejo nobenih občutljivih podatkov. Dejstvo, da je obdelovalec podatkov takoj, ko je izvedel za kršitev varstva podatkov, navezal stik z upravljavcem podatkov, se lahko šteje za dejavnik zmanjšanja tveganja. (Oceniti bi bilo treba tudi možnost, da so bili podatki poslani drugim zavarovalnim zastopnikom, in če se to potrdi, sprejeti ustrezne ukrepe.) Zaradi ustreznih ukrepov, sprejetih po kršitvi varnosti podatkov, kršitev verjetno ne bo vplivala na pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.

80. Zaradi kombinacije majhnega števila posameznikov, na katere je kršitev vplivala, takojšnjega odkritja kršitve in ukrepov, sprejetih za zmanjšanje njenih učinkov, v tem konkretnem primeru ni tveganja.

4.2.2 PRIMER št. 09 – ublažitev in obveznosti

81. Poleg tega so pomembne tudi druge okoliščine, ki zmanjšujejo tveganje: zastopnik je zavezan varovanju poslovnih skrivnosti; težavo je sam prijavil upravljavcu podatkov in na zahtevo je izbrisal datoteko. Ozaveščanje in morebitna vključitev dodatnih ukrepov pri preverjanju dokumentov, ki vključujejo osebne podatke, bosta verjetno pomagala preprečiti podobne primere v prihodnosti.

82. Razen dokumentiranja kršitve v skladu s členom 33(5) ni treba sprejeti nobenih drugih ukrepov.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	X	X

4.3 Organizacijski in tehnični ukrepi za preprečevanje oziroma ublažitev vplivov notranjih virov tveganja za ljudi

83. Kombinacija spodaj navedenih ukrepov, ki se uporabljajo glede na edinstvene značilnosti primera, bi morala pripomoči k zmanjšanju verjetnosti, da bi se podobna kršitev ponovila.

84. Priporočljivi ukrepi:

(Seznam naslednjih ukrepov nikakor ni izključujoč ali izčrpen. Njegov cilj je zagotoviti ideje za preprečevanje in možne rešitve. Vsaka dejavnost obdelave je drugačna, zato se mora upravljavec sam odločiti, kateri ukrepi so v dani situaciji najprimernejši.)

- *Redno izvajanje programov usposabljanja, izobraževanja in ozaveščanja zaposlenih o njihovih obveznostih glede zasebnosti in varnosti ter odkrivanja groženj varnosti osebnih podatkov in poročanja o njih*[26]*. Razvoj programa ozaveščanja za opominjanje zaposlenih na najpogostejše napake, ki vodijo do kršitev varstva osebnih podatkov, in na to, kako jih preprečiti.*
- *Vzpostavitev zanesljivih in učinkovitih praks, postopkov in sistemov za varstvo podatkov in zasebnosti*[27]*.*
- *Vrednotenje praks, postopkov in sistemov varstva zasebnosti za zagotovitev stalne učinkovitosti*[28]*.*
- *Oblikovanje ustreznih politik za nadzor dostopa in siljenje uporabnikov k upoštevanju pravil.*
- *Izvajanje tehnik za obvezno avtentikacijo uporabnikov pri dostopu do občutljivih osebnih podatkov.*
- *Onemogočanje računa uporabnika, povezanega s podjetjem, takoj ko oseba zapusti podjetje.*
- *Preverjanje neobičajnega pretoka podatkov med datotečnim strežnikom in delovnimi postajami zaposlenih.*
- *Nastavitev varnosti vhodno-izhodnih vmesnikov v sistemu BIOS ali nadzorovanje uporabe računalniških vmesnikov z uporabo programske opreme (zaklepanje ali odklepanje, na primer USB/CD/DVD).*
- *Pregled politike dostopa zaposlenih (na primer beleženje dostopa do občutljivih podatkov in zahtevanje, da uporabnik vnese poslovni razlog, tako da je ta na voljo za revizijo).*
- *Onemogočanje odprtih storitev v oblaku.*
- *Prepoved in preprečevanje dostopa do znanih odprtih poštnih storitev.*
- *Onemogočanje funkcije posnetka zaslona v operacijskem sistemu.*
- *Uveljavljanje politike čiste pisalne mize.*
- *Avtomatsko zaklepanje vseh računalnikov po določenem času neaktivnosti.*

[26] Oddelek 2, pododdelek (i), resolucije za obravnavanje vloge človeških napak pri kršitvah varstva osebnih podatkov.

[27] Oddelek 2, pododdelek (ii), resolucije za obravnavanje vloge človeških napak pri kršitvah varstva osebnih podatkov.

[28] Oddelek 2, pododdelek (iii), resolucije za obravnavanje vloge človeških napak pri kršitvah varstva osebnih podatkov.

- *Uporaba mehanizmov (na primer (brezžičnega) žetona za prijavo oziroma odpiranje zaklenjenih računov) za hitre menjave uporabnikov v skupnih okoljih.*
- *Uporaba namenskih sistemov za upravljanje osebnih podatkov, ki uporabljajo ustrezne mehanizme za nadzor dostopa in preprečujejo človeške napake, kot je pošiljanje sporočil napačni osebi. Uporaba preglednic in drugih pisarniških dokumentov ni primerno sredstvo za upravljanje podatkov o strankah.*

5 IZGUBLJENE ALI UKRADENE NAPRAVE IN PAPIRNI DOKUMENTI

85. Pogosta vrsta primerov je izguba ali kraja prenosnih naprav. V teh primerih mora upravljavec upoštevati okoliščine dejanja obdelave, kot je vrsta podatkov, shranjenih v napravi, ter podporna sredstva in ukrepe, sprejete pred kršitvijo, da se zagotovi ustrezna raven varnosti. Vsi ti elementi vplivajo na možne posledice kršitve varstva podatkov. Ocena tveganja je lahko težavna, ker naprava ni več na voljo.

86. Take kršitve je mogoče vedno uvrstiti med kršitve zaupnosti. Če za ukradeno podatkovno zbirko ni varnostne kopije, sta lahko vrsti kršitev tudi kršitev razpoložljivosti in kršitev celovitosti.

87. Scenariji v nadaljevanju prikazujejo, kako zgoraj navedene okoliščine vplivajo na verjetnost in resnost kršitve varstva podatkov.

5.1 PRIMER št. 10: ukradeno gradivo, v katerem so shranjeni šifrirani osebni podatki

Med vlomom v vrtec sta bila ukradena dva tablična računalnika. Tablična računalnika sta vsebovala aplikacijo z osebnimi podatki o otrocih, ki so obiskovali vrtec. Šlo je za ime, datum rojstva in osebne podatke o izobraževanju otrok. Šifrirana tablična računalnika, ki sta bila med vlomom izklopljena, in aplikacija so bili zaščiteni z močnim geslom. Varnostne kopije podatkov so bile upravljavcu učinkovito in takoj na voljo. Ko so v vrtcu izvedeli za vlom, so kmalu po odkritju vloma na daljavo izdali ukaz za izbris podatkov s tabličnih računalnikov.

5.1.1 PRIMER št. 10 – predhodni ukrepi in ocena tveganja

88. V tem konkretnem primeru je upravljavec podatkov sprejel ustrezne ukrepe za preprečevanje in ublažitev učinkov morebitne kršitve varstva podatkov z uporabo šifriranja naprave, uvedbo ustrezne zaščite z geslom in zagotovitvijo varnostnih kopij podatkov, shranjenih v tabličnih računalnikih. (Seznam priporočljivih ukrepov je v oddelku 5.7.)

89. Ko upravljavec podatkov izve za kršitev, bi moral oceniti vir tveganja, sisteme, ki podpirajo obdelavo podatkov, vrsto zadevnih osebnih podatkov in morebitne učinke kršitve na zadevne posameznike. Zgoraj opisana kršitev varstva podatkov bi zadevala zaupnost, razpoložljivost in celovitost zadevnih podatkov, vendar zaradi ustreznih postopkov upravljavca podatkov pred kršitvijo varstva podatkov in po njej kršitev ni vplivala na nič od naštetega.

5.1.2 PRIMER št. 10 – ublažitev in obveznosti

90. Zaupnost osebnih podatkov v napravah ni bila ogrožena zaradi zaščite z močnim geslom na obeh tabličnih računalnikih in aplikacijah. Tablična računalnika sta bila nastavljena tako, da nastavitev gesla pomeni tudi šifriranje podatkov v napravi. To je bilo dodatno okrepljeno z ukrepanjem upravljavca, ki je poskušal na daljavo izbrisati vse podatke iz ukradenih naprav.

91. Zaradi sprejetih ukrepov je bila ohranjena tudi zaupnost podatkov. Poleg tega je bila z varnostnim kopiranjem zagotovljena stalna razpoložljivost osebnih podatkov, zato ni moglo priti do morebitnih negativnih posledic.

92. Zaradi teh dejstev ni bilo verjetno, da bi zgoraj opisana kršitev varstva podatkov povzročila tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, zato uradno obvestilo varnostnemu organu ali zadevnim posameznikom, na katere se nanašajo osebni podatki, ni bilo potrebno. Vendar je treba tudi to kršitev varstva podatkov dokumentirati v skladu s členom 33(5).

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	X	X

5.2 PRIMER št. 11: ukradeno gradivo, v katerem so shranjeni nešifrirani osebni podatki

Uslužbencu podjetja, ki zagotavlja storitve, je bila ukradena elektronska prenosna naprava. Ukradeni prenosni računalnik je vseboval ime, priimek, spol, naslov in rojstni datum več kot 100.000 strank. Zaradi nerazpoložljivosti ukradene naprave ni bilo mogoče ugotoviti, ali so bile predmet kraje tudi druge vrste osebnih podatkov. Dostop do trdega diska prenosnega računalnika ni bil zaščiten z geslom. Osebne podatke je bilo mogoče obnoviti iz dnevnih varnostnih kopij, ki so bile na voljo.

5.2.1 PRIMER št. 11 – predhodni ukrepi in ocena tveganja

93. Upravljavec podatkov ni izvedel nobenih predhodnih varnostnih ukrepov, zato so bili osebni podatki, shranjeni v ukradenem prenosnem računalniku, zlahka dostopni tatu ali kateri koli drugi osebi, ki je napravo pozneje dobila v posest.

94. Ta kršitev varstva podatkov zadeva zaupnost podatkov, shranjenih v ukradeni napravi.

95. Prenosni računalnik z osebnimi podatki je bil v tem primeru ranljiv, ker ni bil zaščiten z geslom ali šifriran. Pomanjkanje osnovnih varnostnih ukrepov povečuje raven tveganja za posameznike, na katere se nanašajo osebni podatki in na katere je kršitev vplivala. Poleg tega je problematična tudi identifikacija zadevnih posameznikov, na katere se nanašajo osebni podatki, kar prav tako povečuje resnost kršitve. Precejšnje število zadevnih posameznikov povečuje tveganje, kljub temu pa kršitev podatkov ni zadevala posebnih vrst osebnih podatkov.

96. Upravljavec bi moral pri oceni tveganja[29] upoštevati morebitne posledice in škodljive učinke kršitve zaupnosti. Zaradi kršitve so lahko zadevni posamezniki, na katere se nanašajo osebni podatki, žrtve identitetne prevare na podlagi podatkov, ki so na voljo v ukradeni napravi, zato se tveganje šteje za visoko.

5.2.2 PRIMER št. 11 – ublažitev in obveznosti

97. Z vključitvijo šifriranja naprave in zaščito shranjene podatkovne zbirke z močnim geslom bi se lahko preprečilo, da bi kršitev varnosti podatkov povzročila tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.

98. Zaradi teh okoliščin je treba uradno obvestiti nadzorni organ, pa tudi zadevne posameznike, na katere se nanašajo osebni podatki.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	✓

5.3 PRIMER št. 12: ukradeni dokumenti v papirni obliki z občutljivimi podatki

Iz ustanove za zdravljenje odvisnosti od drog je bil ukraden dnevnik v papirni obliki. Dnevnik je vseboval osnovne podatke o identiteti in zdravstvenem stanju pacientov, sprejetih v ustanovo za zdravljenje odvisnosti. Podatki so bili shranjeni samo na papirju, zdravniki, ki so zdravili paciente, pa niso imeli na voljo nobene varnostne kopije. Dnevnik ni bil shranjen v zaklenjenem predalu ali zaklenjeni sobi, upravljavec podatkov pa ni imel vzpostavljenega sistema za nadzor dostopa niti nobenega drugega zaščitnega ukrepa za papirno dokumentacijo.

5.3.1 PRIMER št. 12 – predhodni ukrepi in ocena tveganja

99. Upravljavec podatkov ni izvedel nobenih predhodnih varnostnih ukrepov, zato so bili osebni podatki, shranjeni v tem dnevniku, zlahka dostopni osebi, ki ga je našla. Poleg tega je zaradi značilnosti osebnih podatkov, shranjenih v dnevniku, neobstoj varnostnih kopij zelo resen dejavnik tveganja.

100. Ta primer se uporablja kot primer kršitve varnosti podatkov z visokim tveganjem. Zaradi neizvedbe ustreznih varnostnih ukrepov so bili izgubljeni občutljivi zdravstveni podatki v skladu s členom 9(1) Splošne uredbe o varstvu podatkov. Ker je šlo v tem primeru za posebno vrsto osebnih podatkov, so bila možna tveganja za zadevne posameznike, na katere se nanašajo osebni podatki, večja, kar bi moral upoštevati tudi upravljavec, ki ocenjuje tveganje[30].

101. Ta kršitev se nanaša na zaupnost, razpoložljivost in celovitost zadevnih osebnih podatkov. Zaradi kršitve je kršena zdravniška molčečnost in nepooblaščene tretje osebe lahko dostopajo do pacientovih zasebnih zdravstvenih podatkov, kar lahko resno vpliva na pacientovo zasebno življenje. Kršitev dostopnosti lahko tudi ovira neprekinjeno zdravljenje pacientov. Ker ni mogoče izključiti spremembe oziroma izbrisa delov vsebine dnevnika, je ogrožena tudi celovitost osebnih podatkov.

[29] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

[30] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

5.3.2 PRIMER št. 12 – ublažitev in obveznosti

102. Med ocenjevanjem zaščitnih ukrepov bi bilo treba upoštevati tudi vrsto podpornega sredstva. Ker je bil dnevnik pacientov fizični dokument, bi moralo biti njegovo varovanje organizirano drugače kot varovanje elektronske naprave. Psevdonimizacija imen pacientov, hramba dnevnika v varovanih prostorih in v zaklenjenem predalu ali sobi ter ustrezen nadzor dostopa z avtentikacijo pri dostopu do nje bi lahko preprečili kršitev varnosti podatkov.

103. Zgoraj opisana kršitev varnosti podatkov lahko resno vpliva na zadevne posameznike, na katere se nanašajo osebni podatki; zato je obvezno uradno obvestiti nadzorni organ in sporočiti kršitev zadevnim posameznikom, na katere se nanašajo osebni podatki.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	✓

5.4 Organizacijski in tehnični ukrepi za preprečevanje oziroma ublažitev posledic izgube ali kraje naprav

104. Kombinacija spodaj navedenih ukrepov, ki se uporabljajo glede na edinstvene značilnosti primera, bi morala pripomoči k zmanjšanju verjetnosti, da se podobna kršitev ponovi.

105. Priporočljivi ukrepi:

(Seznam naslednjih ukrepov nikakor ni izključujoč ali izčrpen. Njegov cilj je zagotoviti ideje za preprečevanje in možne rešitve. Vsaka dejavnost obdelave je drugačna, zato se mora upravljavec sam odločiti, kateri ukrepi so v dani situaciji najprimernejši.)

- Vklop funkcije šifriranja naprave (na primer Bitlocker, Veracrypt ali DM-Crypt).
- Uporaba vstopne kode oziroma gesla v vseh napravah . Vse mobilne elektronske naprave naj bodo šifrirane na način, ki za dešifriranje zahteva vnos zapletenega gesla.
- Uporaba večfaktorske avtentikacije.
- Vklop funkcije visoko mobilnih elektronskih naprav, ki omogočajo njihovo iskanje, če se naprava izgubi ali založi.
- Uporaba programske opreme oziroma aplikacije za upravljanje mobilnih naprav in lokalizacijo upravljanja mobilnih naprav. Uporaba filtrov proti bleščanju. Zapiranje vseh nenadzorovanih naprav.
- Če je to mogoče in primerno za zadevno obdelavo podatkov, se osebnih podatkov ne shranjuje v mobilno napravo, temveč v osrednji zaledni strežnik.
- Če je delovna postaja povezana s korporativnim lokalnim omrežjem, se naredi samodejno varnostno kopijo iz delovnih map, če je neizogibno, da se v njih hranijo osebni podatki.
- Za povezovanje mobilnih naprav z zalednimi strežniki se uporablja varno omrežje VPN (ki na primer za vzpostavitev varne povezave zahteva ločen ključ za dvofaktorsko avtentikacijo).
- Zaposlenim se zagotovi fizične ključavnice, da bodo lahko fizično zavarovali mobilne naprave, ki jih uporabljajo, ko ostanejo brez nadzora.
- Zagotovi se ustrezna ureditev uporabe naprav zunaj podjetja.

- Zagotovi se ustrezna ureditev uporabe naprav v podjetju.
- Uporaba programske opreme oziroma aplikacije za upravljanje mobilnih naprav in omogočanje funkcije brisanja na daljavo.
- Uporaba centraliziranega upravljanja naprav z minimalnimi pravicami za namestitev programske opreme za končne uporabnike.
- Namestitev a nadzor fizičnega dostopa.
- Izogibanje shranjevanja občutljivih informacij v mobilnih napravah ali na trdih diskih. Če je potreben dostop do notranjega sistema podjetja, bi bilo treba uporabiti varne kanale, kot je navedeno zgoraj.

6 NAPAČNO POSLANA POŠILJKA

106. Tudi v tem primeru je vir tveganja notranja človeška napaka, vendar kršitev ni posledica zlonamernega dejanja. Do nje je prišlo zaradi nepozornosti. Potem ko se je zgodila, upravljavec ne more storiti veliko, zato je preprečevanje v teh primerih še pomembnejše kot pri drugih vrstah kršitev.

6.1 PRIMER št. 13: napaka pri poštnem pošiljanju

Maloprodajno podjetje je zapakiralo čevlje za dve naročili. Zaradi človeške napake je prišlo do zamenjave računov za paketa, tako da sta bila oba izdelka in ustrezna računa za paketa poslana napačni osebi. To pomeni, da sta obe stranki prejeli naročilo druga druge, vključno z računom za paket, ki je vseboval osebne podatke. Ko je upravljavec izvedel za kršitev, je naročili preklical in naročene čevlje poslal pravima prejemnikoma.

6.1.1 PRIMER št. 13 – predhodni ukrepi in ocena tveganja

107. Računa sta vsebovala osebne podatke, potrebne za uspešno dostavo (ime in priimek, naslov ter kupljeni izdelek in njegovo ceno). Pomembno je ugotoviti, kako je do človeške napake sploh lahko prišlo in ali bi jo bilo mogoče kakor koli preprečiti. V opisanem konkretnem primeru je tveganje majhno, saj niso bile vključene posebne vrste osebnih podatkov ali drugi podatki, katerih zloraba bi lahko povzročila znatne negativne učinke, kršitev ni posledica sistemske napake upravljavca in zadeva le dva posameznika. Negativnega učinka na posameznika ni bilo mogoče ugotoviti.

6.1.2 PRIMER št. 13 – ublažitev in obveznosti

108. Upravljavec bi moral zagotoviti brezplačno vračilo izdelkov in priloženih računov, od napačnih prejemnikov pa bi moral tudi zahtevati, naj uničita oziroma izbrišeta vse morebitne kopije računov, ki vsebujejo osebne podatke druge osebe.

109. Čeprav sama kršitev ne pomeni velikega tveganja za pravice in svoboščine posameznikov, na katere je kršitev vplivala, in zato sporočilo posameznikom, na katere se nanašajo osebni podatki, v skladu s členom 34 Splošne uredbe o varstvu podatkov ni obvezno, se takemu obvestilu o kršitvi ni mogoče izogniti, saj je za zmanjšanje tveganja potrebno sodelovanje posameznikov, na katere se nanašajo osebni podatki.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	X	X

6.2 PRIMER št. 14: strogo zaupni osebni podatki, pomotoma poslani po pošti

Oddelek za zaposlovanje urada javne uprave je posameznikom, ki so bili v njegovem sistemu registrirani kot iskalci zaposlitve, poslal elektronsko sporočilo o prihodnjih usposabljanjih. Po pomoti je bil temu elektronskemu sporočilu priložen dokument, ki je vseboval osebne podatke vseh teh iskalcev zaposlitve (ime in priimek, elektronski naslov, poštni naslov, številko socialnega zavarovanja). Kršitev je vplivala na več kot 60.000 posameznikov. Urad je nato navezal stik z vsemi prejemniki in jih prosil, naj izbrišejo prejšnje sporočilo in naj ne uporabljajo podatkov, ki jih je vsebovalo.

6.2.1 PRIMER št. 14 – predhodni ukrepi in ocena tveganja

110. Za pošiljanje takih sporočil bi bilo treba uvesti strožja pravila. Premisliti je treba o uvedbi dodatnih nadzornih mehanizmov.

111. Število posameznikov, na katere je kršitev vplivala, je precejšnje, vključenost njihove številke socialnega zavarovanja skupaj z drugimi, bolj osnovnimi osebnimi podatki pa še dodatno povečuje tveganje, ki ga je mogoče opredeliti kot veliko[31]. Upravljavec ne more preprečiti morebitnega širjenja podatkov s strani katerega koli od prejemnikov.

6.2.2 PRIMER št. 14 – ublažitev in obveznosti

112. Kot je bilo že navedeno, so sredstva za učinkovito zmanjšanje tveganj podobne kršitve omejena. Čeprav je upravljavec zahteval izbris sporočila, prejemnikov k temu ne more prisiliti, posledično pa tudi ne more biti prepričan, da bodo zahtevo izpolnili.

113. Izvedba vseh treh spodaj navedenih ukrepov bi morala biti v takem primeru samoumevna.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	✓

6.3 PRIMER št. 15: osebni podatki, pomotoma poslani po pošti

Seznam udeležencev petdnevnega tečaja pravne angleščine, ki poteka v hotelu, je po pomoti poslan 15 nekdanjim udeležencem tečaja namesto hotelu. Seznam vsebuje imena, elektronske naslove in želje glede prehrane 15 udeležencev. Samo dva udeleženca sta sporočila svoje želje glede prehrane in navedla, da sta preobčutljiva na laktozo. Nobeden od udeležencev nima zaščitene identitete. Upravljavec odkrije napako takoj po pošiljanju seznama in o njej obvesti prejemnike ter jih prosi, naj seznam izbrišejo.

6.3.1 PRIMER št. 15 – predhodni ukrepi in ocena tveganja

114. Za pošiljanje sporočil, ki vsebujejo osebne podatke, bi bilo treba uvesti stroga pravila. Premisliti je treba o uvedbi dodatnih nadzornih mehanizmov.

[31] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

115. Tveganja, ki izhajajo iz značilnosti, občutljivosti, obsega in konteksta osebnih podatkov, so majhna. Osebni podatki vključujejo občutljive podatke o željah glede prehrane dveh udeležencev. Tudi če je informacija, da je nekdo preobčutljiv na laktozo, zdravstveni podatek, je treba tveganje, da bo ta podatek uporabljen na škodljiv način, šteti za razmeroma majhno. Čeprav se v primeru podatkov o zdravju običajno domneva, da bo kršitev verjetno povzročila veliko tveganje za posameznika, na katerega se nanašajo osebni podatki[32], v tem konkretnem primeru ni mogoče ugotoviti tveganja, da bi kršitev zaradi nedovoljenega razkritja informacij o preobčutljivosti na laktozo povzročila fizično, premoženjsko ali nepremoženjsko škodo posamezniku, na katerega se nanašajo osebni podatki. V nasprotju z nekaterimi drugimi željami glede prehrane preobčutljivosti na laktozo običajno ni mogoče povezati z verskimi ali filozofskimi prepričanji. Tudi količina podatkov, ki so bili predmet kršitve, in število posameznikov, na katere se nanašajo osebni podatki in na katere je kršitev vplivala, sta zelo majhna.

6.3.2 PRIMER št. 15 – ublažitev in obveznosti

116. Na kratko, ugotoviti je mogoče, da kršitev ni bistveno vplivala na posameznike, na katere se nanašajo osebni podatki. Dejstvo, da je upravljavec takoj, ko je izvedel za napako, navezal stik s prejemniki, se lahko šteje za olajševalno okoliščino.

117. Če je elektronsko sporočilo poslano napačnemu oziroma nepooblaščenemu prejemniku, je priporočljivo, da upravljavec podatkov nepredvidenim prejemnikom pošlje naknadno elektronsko sporočilo s slepo kopijo, v katerem se opraviči, naroči, da bi bilo treba elektronsko sporočilo, ki pomeni kršitev, izbrisati, in prejemnike obvesti, da nimajo pravice do nadaljnje uporabe elektronskih naslovov, ki so jim bili razkriti.

118. Zaradi teh dejstev ni bilo verjetno, da bi ta kršitev varstva podatkov povzročila tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, zato uradno obvestilo varnostnemu organu ali zadevnim posameznikom, na katere se nanašajo osebni podatki, ni bilo potrebno. Vendar je treba tudi to kršitev varstva podatkov dokumentirati v skladu s členom 33(5).

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	X	X

6.4 PRIMER št. 16: napaka pri poštnem pošiljanju

Zavarovalniška skupina ponuja avtomobilska zavarovanja. V ta namen po pošti pošilja zavarovalne police, ki se redno prilagajajo. Pismo poleg imena in naslova zavarovalca vsebuje registrsko številko vozila brez prikritih številk, stopnje zavarovalnih premij za tekoče in naslednje zavarovalno leto, okvirno letno število prevoženih kilometrov in datum rojstva zavarovanca. Zdravstveni podatki v skladu s členom 9 Splošne uredbe o varstvu podatkov, podatki o plačilih (bančni podatki) ter ekonomski in finančni podatki niso vključeni.

Pisma se vstavljajo v ovojnice z avtomatiziranimi stroji za kuvertiranje. Zaradi mehanske napake sta dve pismi za različna zavarovalca vstavljeni v eno ovojnico in poslani enemu zavarovalcu kot pisemska pošiljka. Zavarovalec doma odpre ovojnico in prebere svoje pravilno dostavljeno pismo ter nepravilno dostavljeno pismo drugega zavarovalca.

[32] Glej Smernice WP 250, str. 23.

6.4.1 PRIMER št. 16 – predhodni ukrepi in ocena tveganja

119. Napačno dostavljeno pismo vsebuje ime, naslov, datum rojstva, nezakrito registrsko številko vozila ter določeno stopnjo zavarovalne premije za tekoče in naslednje leto. Učinke za osebo, na katero kršitev vpliva, je treba šteti za srednje, saj so nepooblaščenemu prejemniku razkrite informacije, ki niso javno dostopne, kot so datum rojstva ali nezakrite registrske številke vozil in podatki o zvišanju stopenj zavarovalnih premij. Verjetnost zlorabe teh podatkov je ocenjena kot majhna do srednja. Čeprav bo veliko prejemnikov napačno prejeto pismo verjetno odvrglo v smeti, v posameznih primerih ni mogoče popolnoma izključiti, da bo pismo objavljeno na družbenih omrežjih ali da bo zavarovanec navezal stik z njim.

6.4.2 PRIMER št. 16 – ublažitev in obveznosti

120. Upravljavec mora na lastne stroške zahtevati vračilo izvirnega dokumenta na lastne stroške. Napačnega prejemnika bi bilo treba tudi obvestiti, da ne sme zlorabiti prebranih informacij.

121. Pri množičnem poštnem pošiljanju, pri katerem se uporabljajo popolnoma avtomatizirani stroji, verjetno nikoli ne bo mogoče v celoti preprečiti napake pri poštni dostavi. Vendar je treba v primeru večje pogostosti preveriti, ali so stroji za kuvertiranje dovolj pravilno nastavljeni in vzdrževani ter ali je taka kršitev posledica kakšne druge sistemske težave.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	X

6.5 Organizacijski in tehnični ukrepi za preprečevanje oziroma ublažitev posledic napačno poslane pošiljke

122. Kombinacija spodaj navedenih ukrepov, ki se uporabljajo glede na edinstvene značilnosti primera, bi morala pripomoči k zmanjšanju verjetnosti, da se podobna kršitev ponovi.

123. Priporočljivi ukrepi:

(*Seznam naslednjih ukrepov nikakor ni izključujoč ali izčrpen. Njegov cilj je zagotoviti ideje za preprečevanje in možne rešitve. Vsaka dejavnost obdelave je drugačna, zato se mora upravljavec sam odločiti, kateri ukrepi so v dani situaciji najprimernejši.*)

- Določitev natančnih standardov za pošiljanje pisem oziroma elektronskih sporočil, ki ne dopuščajo različnih razlag.
- Ustrezno usposabljanje osebja za pošiljanje pisem oziroma elektronskih poročil.
- Pri pošiljanju elektronskih sporočil več prejemnikom so ti privzeto navedeni v polju „Skp“.
- Pri pošiljanju elektronskih sporočil več prejemnikom je potrebna dodatna potrditev in prejemniki niso navedeni v polju „Skp“.
- Uporaba načela štirih oči.
- Samodejno naslavljanje namesto ročnega, s podatki, pridobljenimi iz razpoložljive in posodobljene podatkovne zbirke; sistem samodejnega naslavljanja bi bilo treba redno pregledovati, da se ugotovijo skrite napake in nepravilne nastavitve.
- Uporaba zakasnitve sporočila (na primer sporočilo je mogoče izbrisati oziroma urediti v določenem obdobju po kliku na gumb za pošiljanje).
- Onemogočanje samodejnega dokončanja pri vnašanju elektronskih naslovov.

- Informativna srečanja o najpogostejših napakah, ki vodijo do kršitve varstva osebnih podatkov.
- Usposabljanja in priročniki o tem, kako obravnavati incidente, ki vodijo do kršitve varstva osebnih podatkov, in koga obvestiti (vključitev pooblaščene osebe za varstvo podatkov).

7 DRUGI PRIMERI – SOCIALNI INŽENIRING

7.1 PRIMER št. 17: kraja identitete

Kontaktni center telekomunikacijskega podjetja prejme telefonski klic osebe, ki se predstavi kot stranka. Domnevna stranka od podjetja zahteva, naj spremeni elektronski naslov, na katerega naj se od takrat naprej pošiljajo informacije o obračunu. Delavec kontaktnega centra potrdi identiteto stranke tako, da zahteva določene osebne podatke, kot je določeno v postopkih podjetja. Klicatelj pravilno navede davčno številko in poštni naslov zahtevane stranke (ker je imel dostop do teh elementov). Po potrditvi operater izvede zahtevano spremembo in od takrat naprej se informacije o obračunu pošiljajo na novi elektronski naslov. Postopek ne predvideva pošiljanja uradnega obvestila na prejšnji kontaktni elektronski naslov. Naslednji mesec se zakonita stranka obrne na podjetje z vprašanjem, zakaj ne prejema računov na svoj elektronski naslov, pri čemer zanika klic, s katerim naj bi zahtevala spremembo kontaktnega elektronskega naslova. Pozneje podjetje ugotovi, da so bile informacije poslane nezakonitemu uporabniku, in prekliče spremembo.

7.1.1 PRIMER št. 17 – ocena tveganja, ublažitev in obveznosti

124. Ta primer se uporablja kot primer pomembnosti predhodnih ukrepov. Kršitev z vidika tveganja pomeni visoko stopnjo tveganja[33], saj lahko podatki o obračunu zagotovijo informacije o zasebnem življenju posameznika, na katerega se nanašajo osebni podatki (na primer navade, stiki), in bi lahko povzročili premoženjsko škodo (na primer zasledovanje, tveganje za telesno integriteto). Osebni podatki, pridobljeni med tem napadom, se lahko uporabijo tudi za lažji prevzem stranke v tej organizaciji ali za izrabljanje nadaljnjih ukrepov na področju avtentikacije v drugih organizacijah. Ob upoštevanju teh tveganj bi moral „ustrezen“ ukrep na področju avtentikacije izpolnjevati visoke standarde, odvisno od tega, kateri osebni podatki se lahko obdelujejo kot rezultat avtentikacije.

125. Zato mora upravljavec uradno obvestiti nadzorni organ in poslati sporočilo posamezniku, na katerega se nanašajo osebni podatki.

126. Glede na ta primer je treba očitno izpopolniti postopek predhodnega potrjevanja strank. Metode, uporabljene za avtentikacijo, niso bile zadostne. Zlonamerna oseba se je lahko z uporabo javno dostopnih informacij in informacij, do katerih je sicer imela dostop, pretvarjala, da je predvideni uporabnik.

[33] Za smernice o tem, ali „je verjetno, da [bodo dejanja obdelave] povzročil[a] veliko tveganje“, glej sprotno opombo 10 zgoraj.

127. Uporaba take statične avtentikacije na podlagi znanja (pri kateri se odgovor ne spreminja in pri kateri informacije niso „tajne“, kot bi bilo to v primeru gesla) ni priporočljiva.

128. Namesto tega bi morala organizacija uporabiti obliko avtentikacije, ki bi omogočila visoko stopnjo zaupanja, da je avtentificirani uporabnik predvidena oseba in ne kdo drug. Uvedba metode zunajpasovne večfaktorske avtentikacije bi rešila težavo, na primer za preverjanje zahteve po spremembi s pošiljanjem zahteve za potrditev na prejšnji kontaktni naslov, ali z dodajanjem dodatnih vprašanj in zahtevanjem informacij, vidnih samo na prejšnjih računih. Za odločitev o tem, katere ukrepe je treba uvesti, je odgovoren upravljavec, saj najbolje pozna podrobnosti in zahteve svojega notranjega delovanja.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	✓

7.2 PRIMER št. 18: eksfiltracija elektronske pošte

Veriga hipermarketov je tri mesece po konfiguraciji ugotovila, da so bili nekateri e-poštni računi spremenjeni, pravila pa ustvarjena tako, da je bilo vsako elektronsko sporočilo, ki je vsebovalo določene izraze (na primer „račun“, „plačilo“, „bančno nakazilo“, „avtentikacija kreditne kartice“, „podatki o bančnem računu“), prestavljeno v neuporabljeno mapo in tudi posredovano na zunanji elektronski naslov. Prav tako je bil do takrat že izveden napad s socialnim inženiringom, tj. napadalec, ki se je izdajal za dobavitelja, je podatke o bančnem računu zadevnega dobavitelja spremenil v svoje. Nazadnje, do takrat je bilo poslanih več lažnih računov, ki so vključevali nove podatke o bančnem računu. Sistem za spremljanje e-poštne platforme je na koncu izdal opozorilo o mapah. Podjetje ni moglo ugotoviti, kako je napadalec sploh lahko pridobil dostop do e-poštnih računov, vendar je domnevalo, da je okuženo elektronsko sporočilo omogočilo dostop skupini uporabnikov, odgovornih za plačila.

Zaradi posredovanja elektronskih sporočil na podlagi ključnih besed je napadalec prejel naslednje informacije o 99 zaposlenih: ime in plača v določenem mesecu 89 posameznikov, na katere se nanašajo osebni podatki; ime in priimek, osebno stanje, število otrok, plača, delovne ure in preostale informacije na plačilni listi 10 zaposlenih, katerih pogodbe so bile prekinjene. Upravljavec je obvestil le 10 zaposlenih, ki so spadali v drugo skupino.

7.2.1 PRIMER št. 18 – ocena tveganja, ublažitev in obveznosti

129. Čeprav napadalec verjetno ni želel zbrati osebnih podatkov, saj bi kršitev lahko povzročila premoženjsko (na primer finančno izgubo) in nepremoženjsko škodo (na primer krajo identitete ali goljufijo) ali pa bi se podatki lahko uporabili za olajšanje drugih napadov (na primer zvabljanje podatkov), bi kršitev varstva osebnih podatkov verjetno povzročila veliko tveganje za pravice in svoboščine posameznikov. Zato bi bilo treba kršitev sporočiti vsem 99 zaposlenim in ne le 10 zaposlenim, katerih informacije o plači so bile razkrite.

130. Upravljavec je po seznanitvi s kršitvijo izsilil spremembo gesla za ogrožene račune, blokiral pošiljanje elektronskih sporočil na e-poštni račun napadalca, uradno obvestil ponudnika storitev elektronske pošte, ki jo je uporabil napadalec, o njegovih dejanjih, odstranil pravila, ki jih je nastavil napadalec, in izpopolnil opozorila sistema za spremljanje, da bi se opozorilo pojavilo takoj, ko se ustvari samodejno pravilo. Upravljavec bi lahko uporabnikom tudi odvzel pravico določanja pravil glede posredovanja, tako da bi to skupina za storitve informacijske tehnologije storila le na zahtevo, ali pa bi uvedel politiko, da morajo uporabniki enkrat na teden ali pogosteje na področjih, na katerih se obdelujejo finančni podatki, preveriti pravila, ki so jih določili za svoje račune, in poročati o njih.

131. Dejstvo, da se je kršitev lahko zgodila in ostala tako dolgo neopažena, ter dejstvo, da bi se v daljšem obdobju lahko uporabil socialni inženiring za spreminjanje več podatkov, sta opozorila na pomembne težave v upravljavčevem sistemu zagotavljanja varnosti informacijske tehnologije. Te težave bi bilo treba odpraviti brez odlašanja, na primer s poudarjanjem pregledov avtomatizacije in nadzorom nad spremembami ter ukrepi za odkrivanje incidentov in odzivanje nanje. Upravljavci, ki obdelujejo občutljive podatke, finančne informacije itd., imajo večjo odgovornost v smislu zagotavljanja ustrezne varnosti podatkov.

Potrebni ukrepi na podlagi ugotovljenih tveganj		
Notranja dokumentacija	Uradno obvestilo nadzornemu organu	Sporočilo posameznikom, na katere se nanašajo osebni podatki
✓	✓	✓