Gairės

Gairės 01/2021

dėl pranešimo apie asmens duomenų saugumo pažeidimą pavyzdžių

Priimta 2021 m. gruodžio 14 d.

2.0 versija

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versijų rengimo etapai

2.0 versija	2021 12 14	Gairių priėmimas po viešų konsultacijų
1.0 versija	2021 01 14	Gairių priėmimas viešoms konsultacijoms

Turinys

EUROPOS DUOMENŲ APSAUGOS VALDYBA,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – BDAR), 70 straipsnio 1 dalies e punktą,

atsižvelgdama į EEE susitarimą, ypač į jo XI priedą ir 37 protokolą, su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018[1],

atsižvelgdama į savo Darbo tvarkos taisyklių 12 ir 22 straipsnius,

atsižvelgdama į Komisijos komunikatą Europos Parlamentui ir Tarybai *Duomenų apsauga kaip daugiau galių suteikimo piliečiams ir ES požiūrio į perėjimą prie skaitmeninių technologijų pagrindas – dveji metai taikant Bendrąjį duomenų apsaugos reglamentą*[2],

PRIĖMĖ ŠIAS GAIRES

1 ĮVADAS

1. BDAR nustatytas reikalavimas tam tikrais atvejais pranešti apie asmens duomenų saugumo pažeidimą kompetentingai nacionalinei priežiūros institucijai (toliau – PI) ir asmenims, kurių asmens duomenims pažeidimas padarė poveikį (33 ir 34 straipsniai).

2. 2017 m. spalio mėn. 29 straipsnio darbo grupė jau parengė *bendrąsias* gaires dėl pranešimo apie duomenų saugumo pažeidimą, kuriose analizuojami atitinkami BDAR skirsniai (Gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679, WP250) (toliau – Gairės WP250)[3]. Vis dėlto, atsižvelgiant į šių gairių pobūdį ir rengimo laiką, jose nebuvo pakankamai išsamiai išnagrinėti visi praktiniai klausimai. Todėl atsirado poreikis parengti *į praktiką orientuotas, konkrečiais atvejais grindžiamas* gaires, kuriose būtų atsižvelgiama į priežiūros institucijų nuo BDAR taikymo pradžios įgytą patirtį.

3. Šis dokumentas parengtas siekiant papildyti gaires WP250. Jame atsižvelgiama į bendrąją EEE priežiūros institucijų patirtį nuo BDAR taikymo pradžios. Juo siekiama padėti duomenų valdytojams nuspręsti, kaip elgtis duomenų saugumo pažeidimo atveju ir į kokius veiksnius atsižvelgti vertinant pavojus.

[1] Šiame dokumente daromos nuorodos į valstybes nares turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.

[2] COM(2020) 264 *final*, 2020 m. birželio 24 d.

[3] G29 WP250 1 red., 2018 m. vasario 6 d., Gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679, patvirtino EDAV, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

4. Kad galėtų pasistengti pašalinti pažeidimą, duomenų valdytojas ir duomenų tvarkytojas pirmiausia turi gebėti jį atpažinti. BDAR 4 straipsnio 12 punkte asmens duomenų saugumo pažeidimas apibrėžiamas kaip *saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga*.

5. Nuomonėje 03/2014 dėl pranešimo apie pažeidimą[4] ir Gairėse WP250 29 straipsnio darbo grupė yra paaiškinusi, kad pažeidimai gali būti skirstomi į kategorijas pagal šiuos gerai žinomus informacijos saugumo principus:

   - konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie asmens duomenų suteikimas;
   - vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas;
   - prieinamumo pažeidimas – netyčinis arba neleistinas prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas[5].

6. Pažeidimas gali padaryti įvairų didelį neigiamą poveikį asmenims, dėl kurio gali būti padarytas kūno sužalojimas, materialinė arba nematerialinė žala. Bendrajame duomenų apsaugos reglamente paaiškinta, kad dėl tokio pažeidimo gali būti prarasta savo asmens duomenų kontrolė, apribotos asmens teisės, kilti diskriminacija, būti pavogta ar suklastota tapatybė, būti padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas. Be to, tiems asmenims gali būti padaryta kitokia didelė ekonominė ar socialinė žala. Viena iš svarbiausių duomenų valdytojo prievolių yra įvertinti šiuos duomenų subjektų teisėms ir laisvėms kylančius pavojus ir įgyvendinti tinkamas technines ir organizacines jų šalinimo priemones.

7. Todėl BDAR iš duomenų valdytojo reikalaujama:

   - dokumentuoti visus asmens duomenų saugumo pažeidimus, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį ir taisomuosius veiksmus, kurių buvo imtasi[6];
   - pranešti apie asmens duomenų saugumo pažeidimą priežiūros institucijai, nebent dėl asmens duomenų saugumo pažeidimo neturėtų kilti pavojus fizinių asmenų teisėms ir laisvėms[7];
   - pranešti apie asmens duomenų saugumo pažeidimą duomenų subjektui, jei dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms[8];

8. Duomenų saugumo pažeidimas yra problema savaime, bet taip pat gali būti pažeidžiamos, galbūt pasenusios duomenų saugumo sistemos požymis ir rodyti šalintinus sistemos trūkumus. Paprastai visada

---

[4] G29 WP213, 2014 m. kovo 25 d., Nuomonė 03/2014 dėl pranešimo apie asmens duomenų saugumo pažeidimą, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Žr. Gaires WP 250, p. 7. – būtina atkreipti dėmesį į tai, kad duomenų saugumo pažeidimas gali būti susijęs su viena kategorija, keliomis kategorijomis vienu metu arba gali apimti kelias kategorijas.

[6] BDAR 33 straipsnio 5 dalis.

[7] BDAR 33 straipsnio 1 dalis.

[8] BDAR 34 straipsnio 1 dalis.

geriau užkirsti kelią duomenų saugumo pažeidimams, pasirengiant iš anksto, nes kai kurie rimti jų padariniai dėl jų pobūdžio yra neištaisomi. Kad galėtų *visapusiškai* įvertinti kokio nors pobūdžio išpuoliu padaryto pažeidimo pavojų, duomenų valdytojas pirmiausia turėtų nustatyti pagrindinę problemos priežastį, siekdamas išsiaiškinti, ar tebėra spragų, dėl kurių kilo incidentas, ir ar jas vis dar galima išnaudoti. Dažniausiai duomenų valdytojas gali nustatyti, kad dėl incidento gali kilti pavojus, ir todėl apie šį incidentą reikia pranešti. Kitais atvejais pranešimo nereikia atidėti tol, kol bus visiškai įvertintas su pažeidimu susijęs pavojus ir poveikis, nes išsamus pavojų vertinimas gali būti atliekamas tuo pačiu metu, kai teikiamas pranešimas, todėl gaunamą informaciją priežiūros institucijai galima teikti etapais, ilgiau nepagrįstai nedelsiant[9].

9. Jei duomenų valdytojas mano, kad dėl pažeidimo gali kilti pavojus duomenų subjekto teisėms ir laisvėms, apie pažeidimą reikėtų pranešti. Šį vertinimą duomenų valdytojai turėtų atlikti tuo metu, kai sužino apie pažeidimą. Prieš vertindamas, ar dėl duomenų saugumo pažeidimo gali kilti pavojus ir ar todėl apie šį pažeidimą reikėtų pranešti, duomenų valdytojas neturėtų laukti, kol bus atliktas išsamus ekspertinis tyrimas ir imtasi (ankstyvųjų) poveikio mažinimo veiksmų.

10. Jei duomenų valdytojas atlikęs savo vertinimą nustato, kad pavojus kilti neturėtų, bet paaiškėja, kad pavojus atsiranda, kompetentinga PI gali naudotis savo įgaliojimais imtis taisomųjų veiksmų ir gali nuspręsti taikyti sankcijas.

11. Kiekvienas duomenų valdytojas ir duomenų tvarkytojas turėtų būti parengęs galimų duomenų saugumo pažeidimų atvejų nagrinėjimo planus ir procedūras. Organizacijos turėtų būti nustačiusios aiškius atskaitomybės ryšius ir už tam tikrus atkūrimo proceso aspektus atsakingus asmenis.

12. Duomenų valdytojams ir duomenų tvarkytojams taip pat labai svarbu mokyti savo darbuotojus ir didinti jų informuotumą duomenų apsaugos klausimais, daug dėmesio skiriant asmens duomenų saugumo pažeidimų valdymui (kaip nustatyti asmens duomenų saugumo pažeidimą, kokių tolesnių veiksmų turėtų būti imamasi ir pan.). Šis mokymas turėtų būti reguliariai kartojamas, atsižvelgiant į duomenų tvarkymo veiklos pobūdį ir duomenų valdytojo organizacijos dydį, per jį turėtų būti aptariamos naujausios tendencijos ir su kibernetiniais išpuoliais arba kitais saugumo incidentais susiję įspėjimai.

13. Atskaitomybės principas ir pritaikytosios duomenų apsaugos koncepcija galėtų apimti analizę, įtrauktiną į duomenų valdytojo ir duomenų tvarkytojo vadovą *Kaip elgtis įvykus asmens duomenų saugumo pažeidimui?*, kurio tikslas – nustatyti faktus dėl kiekvieno duomenų tvarkymo aspekto kiekviename svarbiame operacijos etape. Šis iš anksto parengtas vadovas būtų informacijos šaltinis, kuriuo naudodamiesi duomenų valdytojai ir duomenų tvarkytojai galėtų daug sparčiau mažinti pavojus ir nepagrįstai nedelsdami įvykdyti prievoles. Taip būtų užtikrinama, kad, įvykus asmens duomenų saugumo pažeidimui, organizacijos darbuotojai žinotų, ką daryti, todėl veiksmų dėl incidento būtų imtasi neabejotinai sparčiau, nei neparengus poveikio mažinimo priemonių arba plano.

14. Nors toliau aprašyti atvejai yra išgalvoti, jie pagrįsti tipiniais kolektyvinės su pranešimais apie duomenų saugumo pažeidimus susijusios priežiūros institucijų patirties atvejais. Nors siūloma analizė siejasi tik su nagrinėjamais atvejais, ji pateikiama siekiant padėti duomenų valdytojams įvertinti savo duomenų saugumo pažeidimus. Pasikeitus bet kurioms toliau aprašytų atvejų aplinkybėms, gali kilti kitoks arba didesnis pavojus, todėl gali prireikti imtis kitokių arba papildomų priemonių. Šiose gairėse atvejai suskirstyti pagal tam tikras pažeidimų kategorijas (pvz., išpirkos reikalavimo programinės įrangos išpuoliai). Tam tikrų

[9] BDAR 33 straipsnio 4 dalis.

poveikio mažinimo priemonių raginama imtis kiekvienu tam tikrų kategorijų pažeidimų atveju. Šios priemonės nebūtinai kaskart nurodytos kiekvieno su ta pačia pažeidimų kategorija susijusio atvejo analizėje. Dėl tos pačios kategorijos atvejų nurodoma tik tai, kas skiriasi. Todėl, norint nustatyti ir atskirti visas tinkamas taikytinas priemones, reikėtų perskaityti visus su atitinkama pažeidimo kategorija susijusius atvejus.

15. Dokumentuoti pažeidimą organizacijos viduje privaloma kiekvienu atveju, neatsižvelgiant į su pažeidimu susijusius pavojus. Toliau aprašytais atvejais siekiama paaiškinti, ar apie pažeidimą reikia pranešti priežiūros institucijai ir susijusiems duomenų subjektams.

2 IŠPIRKOS REIKALAVIMO PROGRAMINĖ ĮRANGA

16. Dažna pranešimo apie duomenų saugumo pažeidimą priežastis – duomenų valdytojo patirtas išpirkos reikalavimo programinės įrangos išpuolis. Šiuo atveju kenkėjišku kodu užšifruojami asmens duomenys, o paskui įsilaužėlis reikalauja, kad duomenų valdytojas mainais už iššifravimo kodą sumokėtų išpirką. Toks išpuolis gali būti priskiriamas prie prieinamumo pažeidimų, bet dažnai taip pat gali įvykti konfidencialumo pažeidimas.

2.1 1 ATVEJIS. Išpirkos reikalavimo programinė įranga, tinkama atsarginė kopija, duomenys neeksfiltruoti

Nedidelės gamybos bendrovės kompiuterinėse sistemose įvykdytas išpirkos reikalavimo programinės įrangos išpuolis, kurio metu užšifruoti šiose sistemose saugoti duomenys. Duomenų valdytojas taikė šifravimo ramybės būsenoje metodą, todėl visi duomenys, prie kurių buvo įgyta prieiga naudojant išpirkos reikalavimo programinę įrangą, buvo saugomi užšifruoti pagal pažangiausią šifravimo algoritmą. Iššifravimo raktas per išpuolį pažeistas nebuvo, t. y. įsilaužėliui nepavyko nei jo gauti, nei netiesiogiai panaudoti. Todėl įsilaužėlis įgijo prieigą tik prie užšifruotų asmens duomenų. Ypač nenukentėjo nei bendrovės el. pašto sistema, nei klientų sistemos, kurios naudojamos prie jos jungiantis. Incidentą bendrovė tiria naudodamasi ekspertinių žinių turinčios išorės kibernetinio saugumo bendrovės pagalba. Yra žurnalai, kuriuose galima atsekti visus iš bendrovės siunčiamus duomenų srautus (įskaitant išsiunčiamąjį el. paštą). Išanalizavus žurnalus ir duomenis, kurie buvo surinkti bendrovės taikytomis aptikimo sistemomis, su išorės kibernetinio saugumo bendrovės pagalba atlikto vidaus tyrimo metu buvo *patikimai* nustatyta, kad pažeidėjas duomenis tik užšifravo, bet jų neeksfiltravo. Iš žurnalų matyti, kad išpuolio laikotarpiu išsiunčiamųjų duomenų srautų nebuvo. Per pažeidimą nukentėję asmens duomenys susiję su bendrovės klientais ir darbuotojais – iš viso su keliasdešimt asmenų. Kadangi buvo galima iškart naudoti atsarginę kopiją, duomenys buvo atkurti per kelias valandas nuo išpuolio. Pažeidimas nesutrikdė kasdienės duomenų valdytojo veiklos.

17. Šiuo atveju įgyvendinti šie asmens duomenų saugumo pažeidimo apibrėžties elementai: per saugumo pažeidimą buvo neteisėtai pakeisti saugomi asmens duomenys ir buvo įgyta neleistina prieiga prie jų.

2.1.1 1 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

18. Kaip ir dėl visų išorės subjektų keliamų pavojų pažymėtina, kad sėkmingo išpirkos reikalavimo programinės įrangos išpuolio tikimybę galima labai sumažinti padidinant duomenų valdymo aplinkos saugumą. Daugumos šių pažeidimų galima išvengti užtikrinus, kad imtasi tinkamų organizacinių, fizinių ir technologinių saugumo priemonių. Iš šių priemonių būtų galima paminėti, pvz., tinkamą pataisų valdymą ir tinkamą apsaugos nuo kenkimo programinės įrangos ir šios įrangos aptikimo sistemą. Darant tinkamas, atskirai saugomas atsargines kopijas, lengviau sumažinti galimo sėkmingo išpuolio padarinius. Be to, padėti užkirsti kelią tokiems išpuoliams ir juos atpažinti galima įgyvendinant darbuotojų švietimo, mokymo ir

informavimo programą saugumo klausimais. (Rekomenduojamų priemonių sąrašas pateiktas 2.5 skirsnyje.) Pati svarbiausia iš šių priemonių yra tinkamas pataisų valdymas, kuriuo užtikrinama, kad sistemos būtų atnaujinamos, o visos žinomos taikomų sistemų spragos – pašalinamos, nes išpirkos reikalavimo programinės įrangos išpuoliais dažniausiai išnaudojamos gerai žinomos spragos.

19. Kad galėtų išsiaiškinti galimus išpuolio padarinius, vertindamas pavojus duomenų valdytojas turėtų ištirti pažeidimą ir nustatyti taikyto kenkėjiško kodo tipą. Be kita ko, reikėtų atkreipti dėmesį į pavojų, kad duomenys galėjo būti eksfiltruoti nepaliekant pėdsakų sistemų žurnaluose.

20. Šiame pavyzdyje įsilaužėlis turėjo prieigą prie asmens duomenų ir buvo pažeistas skaitinio teksto, kuriame buvo asmens duomenų užšifruotu formatu, konfidencialumas. Vis dėlto pažeidėjas negali perskaityti arba naudoti jokių galimai eksfiltruotų duomenų, bet jau kol kas. Duomenų valdytojo naudojama šifravimo technologija atitinka pažangiausius metodus. Iššifravimo raktas nebuvo pažeistas ir tikriausiai taip pat negalėjo būti nustatytas kitomis priemonėmis. Todėl konfidencialumo pavojai fizinių asmenų teisėms ir laisvėms sumažėja iki minimumo, nebent kriptoanalizė pažengtų tiek, kad ateityje užšifruotus duomenis būtų galima perskaityti.

21. Duomenų valdytojas turėtų apsvarstyti, kokį pavojų pažeidimas kelia asmenims[10]. Šiuo atveju atrodo, kad pavojų duomenų subjektų teisėms ir laisvėms kyla dėl nepakankamo prieinamumo prie asmens duomenų, bet asmens duomenų konfidencialumas pažeistas nebuvo[11]. Šiame pavyzdyje neigiamas pažeidimo poveikis buvo sumažintas per palyginti trumpą laikotarpį nuo pažeidimo. Taikant tinkamą atsarginių kopijų darymo sistemą[12], pažeidimo padarinių rimtumas sumažėja; šiuo atveju duomenų valdytojas ja galėjo veiksmingai pasinaudoti.

22. Kalbant apie padarinių duomenų subjektams rimtumą pažymėtina, kad nustatyti tik nedideli padariniai, nes susiję duomenys buvo atkurti per kelias valandas, pažeidimas nesutrikdė kasdienės duomenų valdytojo veiklos ir nepadarė reikšmingo poveikio duomenų subjektams (pvz., nenukentėjo mokėjimai darbuotojams arba klientų užklausų nagrinėjimas).

---

[10] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, pateiktos 29 darbo grupės Poveikio duomenų apsaugai vertinimo (PDAV) gairėse, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų, WP 248 1-oji peržiūrėta versija, patvirtinta EDAV, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.

[11] Techniniu požiūriu duomenų užšifravimo atveju įgyjama prieiga prie originalių duomenų, o išpirkos reikalavimo programinės įrangos atveju ištrinamas originalas – išpirkos reikalavimo programinės įrangos kodu reikia prieiti prie duomenų, kad juos būtų galima užšifruoti, ir pašalinti originalius duomenis. Prieš ištrindamas originalą įsilaužėlis gali padaryti jo kopiją, bet asmens duomenys išgaunami ne visada. Tęsiant duomenų valdytojo tyrimą, gali paaiškėti daugiau informacijos ir šis vertinimas gali pasikeisti. Prieiga, dėl kurios neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami asmens duomenys arba atsiranda saugumo pavojus duomenų subjektui, net jei duomenys neaiškinami, gali būti tokia reikšminga kaip ir prieiga, kurią įgijus asmens duomenys aiškinami.

[12] Atsarginio kopijavimo procedūros turėtų būti struktūrizuotos, nuoseklios ir kartotinės. Atsarginės kopijos gali būti daromos, pvz., „3 – 2 – 1“ ir „senelio – tėvo – sūnaus“ metodais. Reikėtų visada išbandyti kiekvieno metodo veiksmingumą taikymo srityje ir prireikus atkurti duomenis. Siekiant užtikrinti sistemos vientisumą, bandymus taip pat reikėtų kartoti intervalais, ypač jei pasikeičia duomenų tvarkymo operacija arba aplinkybės.

2.1.2 1 ATVEJIS. Poveikio mažinimas ir prievolės

23. Nedarant atsarginių kopijų, duomenų valdytojas turi nedaug priemonių asmens duomenų praradimui kompensuoti ir duomenis vėl reikia surinkti. Vis dėlto šiuo konkrečiu atveju išpuolio poveikį buvo galima veiksmingai apriboti, atkuriant tokią visų pažeistų sistemų būklę, kuri, kaip žinoma, nebuvo paveikta kenkėjiško kodo, pašalinant spragas ir atkuriant susijusius duomenis per trumpą laikotarpį nuo išpuolio. Nedarant atsarginių kopijų, duomenys prarandami ir padarinių rimtumas gali padidėti, nes taip pat gali padidėti pavojus arba poveikis asmenims.

24. Analizuojant pažeidimą svarbu nustatyti, ar galima laiku veiksmingai atkurti duomenis iš lengvai prieinamos atsarginės kopijos. Tinkamas pažeistų duomenų atkūrimo laikotarpis priklauso nuo išskirtinių konkretaus pažeidimo aplinkybių. BDAR nurodyta, kad apie asmens duomenų saugumo pažeidimą turi būti pranešama nepagrįstai nedelsiant ir, jei įmanoma, praėjus ne daugiau kaip 72 valandoms. Todėl būtų galima nustatyti, kad viršyti šią 72 valandų laiko ribą bet kuriuo atveju nerekomenduotina, bet didelio pavojaus atvejais gali būti laikoma, kad nepakanka laikytis net šio termino.

25. Šiuo atveju, atlikęs išsamų poveikio vertinimą ir reagavimo į incidentą procedūrą, duomenų valdytojas nusprendė, kad pavojus fizinių asmenų teisėms ir laisvėms dėl pažeidimo kilti neturėtų, todėl pranešti apie pažeidimą duomenų subjektams ir priežiūros institucijai nebūtina. Vis dėlto šis pažeidimas, kaip ir visi kiti duomenų saugumo pažeidimai, turėtų būti dokumentuojamas pagal 33 straipsnio 5 dalį. Organizacija taip pat gali turėti (arba vėliau PI gali iš jos reikalauti) atnaujinti ir ištaisyti savo organizacines ir technines asmens duomenų saugumo užtikrinimo ir rizikos mažinimo priemones bei procedūras. Jas atnaujindama ir taisydama organizacija turėtų išsamiai ištirti pažeidimą ir nustatyti priežastis bei pažeidėjo taikytus metodus, kad galėtų išvengti panašių incidentų ateityje.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	X	X

2.2 2 ATVEJIS. Išpirkos reikalavimo programinė įranga, nėra tinkamos atsarginės kopijos

Viename iš žemės ūkio bendrovės naudojamų kompiuterių įvykdytas išpirkos reikalavimo programinės įrangos išpuolis, per kurį įsilaužėlis užšifravo kompiuterio duomenis. Savo tinklo stebėseną bendrovė vykdo naudodamasi ekspertinių žinių turinčios išorės kibernetinio saugumo bendrovės pagalba. Yra žurnalai, kuriuose galima atsekti visus iš bendrovės siunčiamus duomenų srautus (įskaitant išsiunčiamąjį el. paštą). Išanalizavus žurnalus ir duomenis, kurie buvo surinkti kitomis aptikimo sistemomis, su kibernetinio saugumo bendrovės pagalba atlikto vidaus tyrimo metu buvo nustatyta, kad pažeidėjas duomenis tik užšifravo, bet jų neeksfiltravo. Iš žurnalų matyti, kad išpuolio laikotarpiu išsiunčiamųjų duomenų srautų nebuvo. Per pažeidimą nukentėję asmens duomenys susiję su bendrovės darbuotojais ir klientais – iš viso su keliasdešimt asmenų. Specialių kategorijų duomenys nenukentėjo. Atsarginių kopijų elektroniniu formatu nebuvo. Dauguma duomenų buvo atkurti iš popierinių atsarginių kopijų. Duomenų atkūrimas užtruko penkias darbo

2.2.1 2 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

26. Duomenų valdytojas turėtų būti ėmęsis tų pačių išankstinių priemonių, kurios nurodytos 2.1 dalyje ir 2.9 skirsnyje. Šis atvejis nuo pirmiau aprašyto atvejo pirmiausia skiriasi tuo, kad nėra elektroninės atsarginės kopijos ir nešifruojami ramybės būsenoje esantys duomenys. Todėl tolesni žingsniai labai skiriasi.

27. Kad galėtų išsiaiškinti galimus išpuolio padarinius, vertindamas pavojus duomenų valdytojas turėtų ištirti infiltravimo metodą ir nustatyti taikyto kenkėjiško kodo tipą. Šiame pavyzdyje asmens duomenys išpirkos reikalavimo programine įranga buvo užšifruoti, bet neeksfiltruoti. Todėl atrodo, kad pavojų duomenų

subjektų teisėms ir laisvėms kyla dėl nepakankamo prieinamumo prie asmens duomenų, bet asmens duomenų konfidencialumas pažeistas nebuvo. Siekiant nustatyti pavojų, labai svarbu išsamiai išnagrinėti užkardos žurnalus ir jų padarinius. Paprašytas duomenų valdytojas turėtų pateikti faktinius šių tyrimų rezultatus.

28. Duomenų valdytojas turi turėti omenyje, kad per sumanesnius išpuolius naudojama kenkimo programinė įranga, kurioje įdiegta žurnalų failų taisymo ir pėdsakų šalinimo funkcija. Taigi, jei žurnalai nesiunčiami į centrinį žurnalų serverį arba jame nedubliuojami, net ir po išsamaus turimo nustatęs, kad įsilaužėlis asmens duomenų neeksfiltravo, duomenų valdytojas negali tvirtinti, kad duomenys nebuvo eksfiltruoti, nes nėra žurnalo įrašo, todėl konfidencialumo pažeidimo tikimybės visiškai atmesti negalima.

29. Jei įsilaužėlis priėjo prie duomenų, duomenų valdytojas turėtų įvertinti šio pažeidimo pavojų[13]. Atlikdamas pavojų vertinimą, duomenų valdytojas taip pat turėtų atsižvelgti į pažeidimo metu nukentėjusių duomenų pobūdį, neskelbtinumą, kiekį ir kontekstą. Šiuo atveju specialių kategorijų asmens duomenys nenukentėjo, o pažeistų duomenų ir nukentėjusių duomenų subjektų nėra daug.

30. Siekiant nustatyti pavojaus lygį ir užkirsti kelią naujiems arba tolesniems išpuoliams, labai svarbu surinkti tikslią informaciją apie neleistiną prieigą. Jei duomenys nukopijuoti iš duomenų bazės, dėl to pavojus akivaizdžiai padidėjo. Jei neteisėtos prieigos specifika nelabai aiški, reikėtų apsvarstyti blogiausią scenarijų ir atitinkamai įvertinti pavojų.

31. Jei nėra atsarginės kopijos duomenų bazės, gali būti laikoma, kad pavojus didėja, atsižvelgiant į tai, kokio rimtumo padarinių gali atsirasti duomenų subjektams dėl nepakankamo prieinamumo prie duomenų.

2.2.2 2 ATVEJIS. Poveikio mažinimas ir prievolės

32. Nedarant atsarginių kopijų, duomenų valdytojas turi nedaug priemonių asmens duomenų praradimui kompensuoti ir duomenis vėl reikia surinkti, nebent yra kitų šaltinių (pvz., užsakymų patvirtinimo el. laiškai). Nedarant atsarginių kopijų, duomenys gali būti prarandami, o padarinių rimtumas priklauso nuo poveikio asmenims.

33. Jei duomenys tebėra prieinami popieriuje, juos atkurti neturėtų būti pernelyg sudėtinga[14], bet, kadangi nėra elektroninės atsarginės kopijos duomenų bazės, pranešimas priežiūros institucijai laikomas būtinu, nes duomenims atkurti prireikė laiko, galėtų būti vėluojama pristatyti užsakymus klientams ir gali būti neįmanoma susigrąžinti didelio kiekio metaduomenų (pvz., žurnalų, laiko žymų).

34. Tai, ar apie pažeidimą reikia pranešti duomenų subjektams, taip pat gali priklausyti nuo to, kiek laiko asmens duomenys yra neprieinami ir kokių dėl to atsiranda duomenų valdytojo veiklos sutrikimų (pvz., vėlavimas pervesti mokėjimus darbuotojams). Kadangi dėl šio mokėjimų ir pristatymo vėlavimo asmenys, kurių duomenys buvo pažeisti, gali patirti finansinių nuostolių, taip pat būtų galima teigti, kad dėl pažeidimo gali kilti didelis pavojus. Informuoti duomenų subjektus taip pat gali būti neišvengiama, jei reikia, kad jie padėtų atkurti užšifruotus duomenis.

---

[13] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

[14] Tai priklauso nuo asmens duomenų sudėtingumo ir struktūros. Sudėtingiausiais scenarijais duomenų vientisumui, nuoseklumui su metaduomenims atkurti, tinkamiems ryšiams su duomenų struktūromis užtikrinti ir duomenų tikslumui patikrinti gali prireikti daug išteklių ir pastangų.

35. Šis atvejis – tai išpirkos reikalavimo programinės įrangos išpuolio pavyzdys, kai kyla pavojus duomenų subjektų teisėms ir laisvėms, bet šis pavojus nėra didelis. Šis išpuolis turėtų būti dokumentuojamas pagal 33 straipsnio 5 dalį ir apie jį turėtų būti pranešama priežiūros institucijai pagal 33 straipsnio 1 dalį. Organizacija taip pat gali turėti (arba PI gali iš jos reikalauti) atnaujinti ir ištaisyti savo organizacines ir technines asmens duomenų saugumo užtikrinimo ir rizikos mažinimo priemones bei procedūras.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	X

2.3 3 ATVEJIS. Išpirkos reikalavimo programinė įranga, yra atsarginė kopija, duomenys neeksfiltruoti – ligoninė

Naudojant išpirkos reikalavimo programinę įrangą, padarytas išpuolis prieš ligoninės / sveikatos priežiūros centro informacinę sistemą; įsilaužėlis užšifravo didelę dalį šios sistemos duomenų. Savo tinklo stebėseną bendrovė vykdo naudodamasi ekspertinių žinių turinčios išorės kibernetinio saugumo bendrovės pagalba. Yra žurnalai, kuriuose galima atsekti visus iš bendrovės siunčiamus duomenų srautus (įskaitant išsiunčiamąjį el. paštą). Išanalizavus žurnalus ir duomenis, kurie buvo surinkti kitomis aptikimo sistemomis, su kibernetinio saugumo bendrovės pagalba atlikto vidaus tyrimo metu buvo nustatyta, kad pažeidėjas duomenis tik užšifravo, bet jų neeksfiltravo. Iš žurnalų matyti, kad išpuolio laikotarpiu išsiunčiamųjų duomenų srautų nebuvo. Nukentėję asmens duomenys susiję su darbuotojais ir pacientais – tūkstančiais asmenų. Atsarginės kopijos elektroniniu formatu buvo padarytos. Dauguma duomenų buvo atkurti, tačiau tai užtruko dvi darbo dienas, todėl labai vėlavo pacientų gydymas, nes buvo atšauktos arba atidėtos operacijos, o kadangi nebuvo galima naudotis

2.3.1 3 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

36. Duomenų valdytojas turėtų būti ėmęsis tų pačių išankstinių priemonių, kurios nurodytos 2.1 dalyje ir 2.5 skirsnyje. Šis atvejis nuo pirmiau aprašyto atvejo pirmiausia skiriasi tuo, kad rimtų padarinių patyrė daug duomenų subjektų[15].

37. Pažeistų duomenų ir nukentėjusių duomenų subjektų daug, nes ligoninės paprastai tvarko didelį kiekį duomenų. Duomenų neprieinamumas daro didelį poveikį daugybei duomenų subjektų. Be to, išlieka pavojus dėl rimtų su pacientų duomenų konfidencialumu susijusių padarinių.

38. Svarbu išsiaiškinti pažeidimo pobūdį ir per pažeidimą nukentėjusių asmens duomenų rūšį, neskelbtinumą bei kiekį. Nors buvo padaryta atsarginė duomenų kopija ir duomenis buvo galima atkurti per kelias dienas,

[15] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

pavojus vis tiek yra didelis todėl, kad duomenų subjektai patyrė rimtų padarinių, nes išpuolio metu ir kelias dienas po jo nebuvo galima prieiti prie duomenų.

2.3.2 3 ATVEJIS. Poveikio mažinimas ir prievolės

39. Pranešimas priežiūros institucijai laikomas būtinu, nes pažeidimas susijęs su specialių kategorijų asmens duomenimis, duomenims atkurti gali prireikti daug laiko ir todėl gali būti labai vėluojama teikti pacientų priežiūros paslaugas. Pranešti apie pažeidimą duomenų subjektams būtina atsižvelgiant į poveikį pacientams, net po to, kai užšifruoti duomenys atkuriami. Nors buvo užšifruoti su visais per pastaruosius metus ligoninėje gydytais pacientais susiję duomenys, poveikis padarytas tik tiems pacientams, kuriuos gydyti ligoninėje buvo suplanuota tuo metu, kai kompiuterinė sistema buvo neprieinama. Šiems pacientams duomenų valdytojas apie duomenų saugumo pažeidimą turėtų pranešti tiesiogiai. Tiesioginio pranešimo kitiems pacientams, kurie ligoninėje galbūt nesilankė jau ilgiau nei dvidešimt metų, atsižvelgiant į 34 straipsnio 3 dalies c punkte nustatytą išimtį, gali nereikėti. Tokiu atveju vietoj jo turi būti skelbiamas viešas pranešimas[16] arba imamasi panašios priemonės, kuria duomenų subjektai būtų informuojami taip pat efektyviai. Šiuo atveju ligoninė turi viešai paskelbti apie išpirkos reikalavimo programinės įrangos išpuolį ir jo padarinius.

40. Šis atvejis – tai išpirkos reikalavimo programinės įrangos išpuolio pavyzdys, kai kyla didelis pavojus duomenų subjektų teisėms ir laisvėms. Jis turėtų būti dokumentuojamas pagal 33 straipsnio 5 dalį; apie jį turėtų būti pranešama priežiūros institucijai pagal 33 straipsnio 1 dalį ir duomenų subjektams pagal 34 straipsnio 1 dalį. Organizacija taip pat turi atnaujinti ir ištaisyti savo organizacines ir technines asmens duomenų saugumo užtikrinimo ir rizikos mažinimo priemones bei procedūras.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	✓

2.4 4 ATVEJIS. Išpirkos reikalavimo programinė įranga, atsarginės kopijos nėra, duomenys eksfiltruoti

Viešojo transporto bendrovės serveryje įvykdytas išpirkos reikalavimo programinės įrangos išpuolis, per kurį įsilaužėlis užšifravo serverio duomenis. Atlikus vidaus tyrimą nustatyta, kad pažeidėjas duomenis ne tik užšifravo, bet ir eksfiltravo. Pažeistų duomenų rūšis buvo klientų ir darbuotojų, taip pat kelių tūkstančių bendrovės paslaugomis besinaudojančių (pvz., bilietus internetu perkančių) žmonių asmens duomenys. Per pažeidimą nukentėjo ne tik pagrindiniai tapatybės duomenys, bet ir tapatybės kortelių numeriai ir tokie finansiniai duomenys kaip kredito kortelių informacija. Atsarginė duomenų bazė buvo sukurta, bet įsilaužėlis užšifravo ir ją.

[16] BDAR 86 konstatuojamojoje dalyje paaiškinta: *Tokie pranešimai duomenų subjektams turėtų būti pateikti kuo greičiau ir glaudžiai bendradarbiaujant su priežiūros institucija, laikantis jos ar kitų atitinkamų valdžios institucijų, tokių kaip teisėsaugos institucijos, pateiktų nurodymų. Pavyzdžiui, siekiant sumažinti tiesioginį žalos pavojų, reikėtų nedelsiant apie tai pranešti duomenų subjektams, o ilgesnį pranešimo terminą būtų galima pateisinti būtinybe įgyvendinti tinkamas priemones, kuriomis siekiama užkirsti kelią besikartojantiems ar panašiems asmens duomenų saugumo pažeidimams*.

2.4.1 4 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

41. Duomenų valdytojas turėtų būti ėmęsis tų pačių išankstinių priemonių, kurios nurodytos 2.1 dalyje ir 2.5 skirsnyje. Atsarginė kopija buvo sukurta, bet per išpuolį nukentėjo ir ji. Jau vien dėl šios aplinkybės kyla abejonių dėl duomenų valdytojo išankstinių IT saugumo priemonių kokybės; atliekant tyrimą, ją reikėtų patikrinti išsamiau, nes gerai suprojektuotoje atsarginio kopijavimo sistemoje turėtų būti saugiai laikomos kelios atsarginės kopijos, prie kurių negalima prieiti iš pagrindinės sistemos, nes kitaip jos gali būti pažeidžiamos per tą patį išpuolį. Be to išpirkos reikalavimo programinės įrangos išpuoliai gali likti nepastebėti kelias dienas ir tuo metu gali būti pamažu šifruojami retai naudojami duomenys. Taigi, kelios atsarginės kopijos gali netekti vertės, todėl atsargines kopijas taip pat reikėtų daryti periodiškai ir atskirti vieną nuo kitos. Taip būtų galima padidinti atkūrimo tikimybę, nors ir patiriant didesnių duomenų nuostolių.

42. Šis pažeidimas turi įtakos ne tik duomenų prieinamumui, bet ir jų konfidencialumui, nes įsilaužėlis galėjo pakeisti duomenis ir (arba) nukopijuoti juos iš serverio. Todėl šio pobūdžio pažeidimas kelia didelį pavojų[17].

43. Šie pavojai dar labiau didėja dėl asmens duomenų pobūdžio, neskelbtinumo ir kiekio, nes susijusių asmenų skaičius didelis ir taip pat didelis bendras susijusių asmens duomenų kiekis. Pažeisti ne tik pagrindiniai tapatybės duomenys, bet ir tapatybės dokumentai bei tokie finansiniai duomenys kaip kredito kortelių informacija. Kai pažeidžiamas šios rūšies duomenų saugumas, jau savaime kyla didelis pavojus, o jei šie duomenys tvarkomi kartu, juos būtų galima panaudoti, be kita ko, tapatybės vagystei arba sukčiavimui.

44. Dėl netinkamos serverio logikos arba netinkamų organizacinių kontrolės priemonių išpirkos reikalavimo programinė įranga paveikė atsarginių kopijų failus, todėl nebuvo galima atkurti duomenų ir pavojus padidėjo.

45. Dėl šio duomenų saugumo pažeidimo kyla didelis pavojus asmenų teisėms ir laisvėms, nes gali atsirasti tiek materialinė žala (pvz., finansiniai nuostoliai, kadangi nukentėjo kredito kortelių duomenys), tiek nematerialinė žala (pvz., tapatybės vagystė arba sukčiavimas, kadangi nukentėjo tapatybės kortelių duomenys).

2.4.2 4 ATVEJIS. Poveikio mažinimas ir prievolės

46. Labai svarbu pranešti duomenų subjektams, kad jie galėtų imtis reikiamų veiksmų, siekdami išvengti materialinės žalos (pvz., užblokuoti kredito korteles).

47. Šiuo atveju reikia ne tik dokumentuoti pažeidimą pagal 33 straipsnio 5 dalį, bet ir pranešti priežiūros institucijai (33 straipsnio 1 dalis); bet to, duomenų valdytojas taip pat privalo pranešti apie pažeidimą duomenų subjektams (34 straipsnio 1 dalis). Pranešti pastariesiems duomenų valdytojas gali asmeniškai, o asmenims, kurių kontaktinių duomenų neturi, turėtų pranešti viešai, pvz., paskelbdamas pranešimą savo svetainėje, jei jį paskelbus duomenų subjektams negalėtų atsirasti dar daugiau neigiamų padarinių. Pastaruoju atveju reikia pateikti tikslų ir aiškų, duomenų valdytojo pradžios tinklalapyje gerai matomą pranešimą, tiksliai nurodant susijusias BDAR nuostatas. Organizacija taip pat gali turėti atnaujinti ir ištaisyti savo organizacines ir technines asmens duomenų saugumo užtikrinimo ir rizikos mažinimo priemones bei procedūras.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	✓

[17] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

2.5 Išpirkos reikalavimo programinės įrangos išpuolių prevencijos / poveikio mažinimo organizacinės ir techninės priemonės

48. Tai, kad galėjo būti įvykdytas išpirkos reikalavimo programinės įrangos išpuolis, paprastai rodo vieną arba kelias duomenų valdytojo sistemos spragas. Tai pasakytina ir apie tuos išpirkos reikalavimo programinės įrangos išpuolius, per kuriuos duomenys buvo užšifruoti, bet neeksfiltruoti. Kad ir kokie būtų tyrimo rezultatai ir išpuolio padariniai, labai svarbu atminti, kad būtina visapusiškai įvertinti saugumo sistemą, itin daug dėmesio skiriant IT saugumui. Nustatytus trūkumus ir saugumo spragas reikia dokumentuoti ir nedelsiant pašalinti.

49. Rekomenduojamos priemonės:

(Toliau išvardytų priemonių sąrašas jokiu būdu nėra vienintelis galimas arba išsamus. Siekiama tik pasiūlyti prevencijos idėjų ir galimus sprendimus. Kiekviena duomenų tvarkymo veikla skiriasi, todėl duomenų valdytojas turėtų nuspręsti, kurios priemonės geriausiai tinka konkrečiai situacijai.)

- nuolat atnaujinti aparatinę programinę įrangą, operacinę sistemą ir programinę įrangą serveriuose, kliento kompiuterius, aktyviuosius tinklo komponentus ir visus kitus tame pačiame vietiniame tinkle (LAN) esančius kompiuterius (įskaitant vietinio belaidžio tinklo prietaisus); užtikrinti, kad būtų taikomos tinkamos IT saugumo priemonės ir jos būtų veiksmingos, reguliariai jas naujinti tvarkant duomenis arba pasikeitus ar besikeičiant aplinkybėms; taip pat turėtų būti saugomi išsamūs žurnalai apie taikomas pataisas ir jų laiko žymas;
- projektuoti ir organizuoti tokias duomenų tvarkymo sistemas ir infrastruktūrą, kuriose būtų suskirstomi į segmentus arba atskiriami tinklai ir duomenų sistemos, kad būtų galima išvengti kenkimo programų platinimo organizacijoje ir išorės sistemose;
- taikyti aktualią saugią ir išbandytą atsarginio kopijavimo procedūrą; vidutinės trukmės ir ilgalaikėms atsarginėms kopijoms (pvz., kasdienei prieauginei atsarginei kopijai ir kassavaitinei išsamiai atsarginei kopijai) skirtos laikmenos turėtų būti saugomos atskirai nuo veiklai vykdyti naudojamų duomenų atminties įtaisų ir tokioje vietoje, prie kurios negalėtų prieiti trečiosios šalys, net sėkmingo išpuolio atveju;
- taikyti / įsigyti tinkamą naujausią veiksmingą ir integruotą apsaugos nuo kenkimo programinę įrangą;
- taikyti tinkamą naujausią veiksmingą ir integruotą užkardą ir įsilaužimų aptikimo bei prevencijos sistemą; nukreipti tinklo srautą per užkardą / įsilaužimų aptikimo sistemą, net dirbant iš namų arba naudojantis mobiliaisiais prietaisais (pvz., jungiantis prie interneto, naudoti virtualiojo privačiojo tinklo prisijungimą prie organizacijos saugumo mechanizmų);
- mokyti darbuotojus IT išpuolių atpažinimo ir prevencijos metodų; duomenų valdytojas turėtų suteikti priemones, kuriomis naudojantis būtų galima nustatyti, ar el. laiškai ir kitomis ryšio priemonėmis gauti pranešimai yra autentiški ir patikimi; darbuotojai turėtų būti mokomi atpažinti, kada toks išpuolis įvykdytas, kaip iš tinklo pašalinti galinį punktą, ir informuojami apie jų prievolę nedelsiant pranešti apie išpuolį saugumo pareigūnui;
- atkreipti dėmesį į būtinybę nustatyti kenkėjiško kodo tipą, siekiant išsiaiškinti išpuolio padarinius ir rasti tinkamas pavojaus mažinimo priemones; jei įvykdytas sėkmingas išpirkos reikalavimo programinės įrangos išpuolis, atgauti duomenis būtų galima naudojantis, pvz., projekto *no more ransom* (nomoreransom.org) priemonėmis; vis dėlto, jei buvo padaryta saugi atsarginė kopija, duomenis patartina atkurti iš jos;
- persiųsti visus žurnalus į centrinį žurnalų serverį arba dubliuoti žurnalus šiame serveryje (galbūt taip pat užtikrinti, kad žurnalo įrašai būtų pasirašomi ir arba žymimi kriptografinėmis laiko žymomis);
- taikyti patikimą šifravimą ir daugiaveiksnį tapatumo nustatymą, ypač administracinei prieigai prie IT sistemų, tinkamas raktų ir slaptažodžių valdymas;
- reguliariai atlikti pažeidžiamumo ir skverbimosi testavimą;

- įsteigti organizacijoje reagavimo į kompiuterių saugumo incidentus tarnybą (CSIRT) arba kompiuterinių incidentų tyrimo tarnybą (CERT) arba bendrą CSIRT / CERT; parengti reagavimo į incidentus planą, veiklos atkūrimo po ekstremaliųjų įvykių planą bei veiklos tęstinumo planą ir užtikrinti, kad jie būtų kruopščiai išbandomi;
- vertinant atsakomąsias priemones, reikėtų peržiūrėti, išbandyti ir atnaujinti pavojų analizę.

3 DUOMENŲ EKSFILTRAVIMO IŠPUOLIAI

50. Išpuoliai, kuriuos vykdant išnaudojamos duomenų valdytojų trečiosioms šalims internetu teikiamų paslaugų spragos ir kurie vykdomi, pvz., įterpimo (SQL įterpimo, katalogų apėjimo ir pan.), svetainės pažeidimo ir panašiais metodais, gali būti panašūs į išpirkos programinės įrangos vykdomus išpuolius, nes pavojus sukeliamas neteisėtais trečiosios šalies veiksmais, bet vykdant šiuos išpuolius paprastai siekiama nukopijuoti, eksfiltruoti asmens duomenis ir jais piktnaudžiauti kokiu nors kenkėjišku tikslu. Taigi, tai daugiausia yra konfidencialumo ir galbūt duomenų vientisumo pažeidimai. Vis dėlto, jei duomenų valdytojas žino šio pobūdžio pažeidimų ypatybes, jis gali naudotis daugybe priemonių, kuriomis galima labai sumažinti sėkmingo išpuolio įvykdymo pavojų.

3.1 5 ATVEJIS. Darbo paraiškų duomenų eksfiltravimas iš svetainės

Įdarbinimo agentūra patyrė kibernetinį išpuolį, per kurį į jos svetainę buvo įterptas kenkėjiškas kodas. Šis kenkėjiškas kodas prieigos teisių neturinčiam asmeniui (-ims) suteikė prieigą prie internetinėse darbo paraiškų formose pateiktų ir svetainės serveryje saugomų asmens duomenų. Spėjama, kad nukentėjo 213 formų. Išanalizavus susijusius duomenis nustatyta, kad specialių kategorijų duomenys per pažeidimą nenukentėjo. Konkretus įdiegtas kenkimo programinės įrangos priemonių rinkinys pasižymėjo tokiomis funkcijomis, kuriomis naudodamasis įsilaužėlis galėjo pašalinti eksfiltravimo istoriją, stebėti duomenų tvarkymą serveryje ir fiksuoti asmens duomenis. Šis priemonių rinkinys buvo

3.1.1 5 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

51. Duomenų valdytojo aplinkos saugumas atlieka itin svarbų vaidmenį, nes daugumos tokių pažeidimų galima išvengti užtikrinant, kad visos sistemos būtų nuolat naujinamos, neskelbtini duomenys būtų užšifruojami, o taikomosios programos kuriamos laikantis aukštų saugumo standartų, pvz., užtikrinant patikimą tapatumo nustatymą, imantis kovos su brutaliąja jėga ir išpuoliais priemonių, taikant naudotojų įvedinių atmetimo arba apvalymo metodus[18] ir pan. Taip pat reikia periodiškai atlikti IT saugumo auditą, pažeidžiamumo vertinimus ir skverbimosi testavimą, kad tokio pobūdžio pažeidžiamas vietas būtų galima aptikti iš anksto ir pašalinti. Šiuo konkrečiu atveju kodo injekciją galbūt būtų buvę lengviau nustatyti generavimo aplinkoje taikant failų vientisumo stebėsenos priemones. (Rekomenduojamų priemonių sąrašas pateiktas 3.7 skirsnyje.)

52. Siekdamas nustatyti, kokių priemonių reikia imtis, duomenų valdytojas, pradėdamas tirti pažeidimą, visada pirmiausia turėtų nustatyti išpuolio pobūdį ir metodus. Kad veikti būtų galima sparčiai ir veiksmingai, duomenų valdytojas turi būti parengęs reagavimo į incidentus planą, kuriame nurodyta, kokių veiksmų būtina skubiai imtis, siekiant suvaldyti incidentą. Šiuo konkrečiu atveju pavojus padidėjo dėl pažeidimo pobūdžio,

[18] Naudotojų įvedinių atmetimas (angl. *escaping*) arba apvalymas (angl. *sanitizing*) yra toks įvedinių patvirtinimas, kuriuo užtikrinama, kad į informacinę sistemą būtų įtraukiami tik tinkamai suformatuoti duomenys.

nes buvo ne tik pažeistas duomenų konfidencialumas – infiltruotojas taip pat turėjo priemonių pakeisti sistemą, todėl abejotinas tapo ir duomenų vientisumas.

53. Siekiant nustatyti, kaip pažeidimas pakenkė duomenų subjektams, reikėtų įvertinti per pažeidimą nukentėjusių duomenų pobūdį, neskelbtinumą ir kiekį. Nors specialių kategorijų asmens duomenys nenukentėjo, duomenyse, prie kurių įgyta prieiga, pateikta labai daug iš internetinių formų gautos informacijos apie asmenis ir šiais duomenimis būtų galima įvairiai piktnaudžiauti (teikti jiems nepageidaujamą rinkodaros informaciją, pavogti jų tapatybę ir pan.), taigi, dėl padarinių rimtumo turėtų padidėti pavojus duomenų subjektų teisėms ir laisvėms[19].

3.1.2 5 ATVEJIS. Poveikio mažinimas ir prievolės

54. Išsprendus problemą, duomenų bazę, jei įmanoma, reikėtų palyginti su saugioje atsarginėje kopijoje saugoma duomenų baze. Į aiškinantis pažeidimą įgytą patirtį reikėtų atsižvelgti atnaujinant IT infrastruktūrą. Duomenų subjektas turėtų atkurti tokią visų susijusių IT sistemų būklę, kuri, kaip žinoma, nebuvo paveikta, pašalinti spragą ir įgyvendinti naujas saugumo priemones, kad išvengtų panašių duomenų saugumo pažeidimų ateityje, pvz., tikrinti failų vientisumą ir atlikti saugumo auditus. Jei asmens duomenys buvo ne tik eksfiltruoti, bet ir ištrinti, duomenų valdytojas turi imtis sistemingų veiksmų, kad atkurtų prieš pažeidimą buvusios būsenos asmens duomenis. Gali prireikti naudoti išsamias atsargines kopijas, prieauginius pakeitimus ir galbūt iš naujo atlikti duomenų tvarkymą, kuris buvo atliktas nuo tada, kai buvo padaryta paskutinė prieauginė atsarginė kopija, o norėdamas tai padaryti duomenų valdytojas turi turėti galimybę atkartoti nuo paskutinio atsarginio kopijavimo padarytus pakeitimus. Šiuo tikslu gali reikėti, kad duomenų valdytojas turėtų sistemą, kurioje būtų galima išsaugoti kasdienius įvedinių failus, jei juos prireiktų tvarkyti iš naujo, ir reikia taikyti patikimą saugojimo metodą ir tinkamą saugojimo politiką.

55. Atsižvelgiant į tai, kas išdėstyta pirmiau, kadangi dėl pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, apie jį neabejotinai reikėtų pranešti duomenų subjektams (34 straipsnio 1 dalis), o tai, žinoma, reiškia, kad taip pat reikėtų įtraukti atitinkamą (-as) priežiūros instituciją (-as), pateikiant jai (joms) pranešimą apie duomenų saugumo pažeidimą. Dokumentuoti pažeidimą privaloma pagal BDAR 33 straipsnio 5 dalį; remiantis šia dokumentacija lengviau vertinti situaciją.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	✓

3.2 6 ATVEJIS. Maišos metodu užšifruoto slaptažodžio eksfiltravimas iš svetainės

Pasinaudojant pažeidžiamumu SQL injekcijai, buvo prisijungta prie patiekalų svetainės serverio duomenų bazės. Naudotojams buvo leista kaip naudotojų vardus pasirinkti tik pseudonimus. Buvo raginama šiuo tikslu nenaudoti el. pašto adresų. Duomenų bazėje saugomi slaptažodžiai buvo užšifruoti maišos metodu, taikant patikimą algoritmą; druska nebuvo pažeista. Nukentėję duomenys – maišos metodu užšifruoti 1 200 naudotojų slaptažodžių. Siekdamas užtikrinti saugą, duomenų valdytojas el. paštu informavo duomenų subjektus apie pažeidimą ir paprašė jų pasikeisti

[19] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

3.2.1 6 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

56. Šiuo konkrečiu atveju pažeistas duomenų konfidencialumas, bet duomenų bazėje saugoti slaptažodžiai buvo užšifruoti maišos funkcija, taikant šiuolaikines technologijas atitinkantį metodą, todėl su asmens duomenų pobūdžiu, neskelbtinumu ir kiekiu susijęs pavojus galėtų sumažėti. Šiuo atveju pavojus duomenų subjektų teisėms ir laisvėms nekyla.

57. Be to, nebuvo pažeista kontaktinė duomenų subjektų informacija (pvz., el. pašto adresai arba telefono numeriai), todėl nekyla didelio pavojaus, kad į duomenų subjektus gali būti nukreipiami bandymai sukčiauti (pvz., jie galėtų gauti duomenų viliojimo el. laiškus arba nesąžiningus tekstinius pranešimus ir telefono skambučius). Specialių kategorijų asmens duomenys nenukentėjo.

58. Kai kuriuos naudotojų vardus būtų galima laikyti asmens duomenimis, bet iš svetainės turinio negalima daryti neigiamų konotacijų. Vis dėlto pažymėtina, kad pavojų vertinimas gali pasikeisti[20], jei dėl svetainės tipo (pvz., politinės partijos arba profsąjungos svetainė) ir gautų duomenų galėtų paaiškėti specialių kategorijų asmens duomenys. Neigiamus pažeidimo padarinius būtų galima sumažinti taikant pažangiausiais metodais grindžiamą šifravimą. Apribojus leidžiamą prisijungimo bandymų skaičių, bus užkirstas kelias sėkmingiems brutaliojo prisijungimo išpuoliams, todėl labai sumažės naudotojų vardus jau žinančių įsilaužėlių keliami pavojai.

3.2.2 6 ATVEJIS. Poveikio mažinimas ir prievolės

59. Pranešimas duomenų subjektams kai kada gali būti laikomas poveikio mažinimo veiksniu, nes duomenų subjektai taip pat gali imtis reikiamų veiksmų, siekdami išvengti tolesnės su pažeidimu susijusios žalos, pvz., pasikeisti slaptažodžius. Šiuo atveju pranešti apie pažeidimą nebuvo privaloma, bet daugeliu atvejų pranešimas gali būti laikomas gerąja praktika.

60. Duomenų valdytojas turėtų pašalinti spragą ir įgyvendinti naujas saugumo priemones, kad išvengtų panašių duomenų saugumo pažeidimų ateityje, pvz., sistemingai atlikti svetainės saugumo auditą.

61. Pažeidimas turėtų būti dokumentuojamas pagal 33 straipsnio 5 dalį, bet pranešti apie jį nereikia.

62. Be to, apie su slaptažodžiais susijusį pažeidimą bet kuriuo atveju labai patartina pranešti duomenų subjektams, net jei saugomi slaptažodžiai buvo užšifruoti maišos ir druskos įterpimo metodais, taikant pažangiausią algoritmą. Pirmenybė teiktina tokiems tapatumo nustatymo metodams, kuriuos taikant nereikia tvarkyti slaptažodžių serveryje. Duomenų subjektams turėtų būti suteikiama galimybė imtis tinkamų su jų slaptažodžiais susijusių priemonių.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	X	X

3.3 7 ATVEJIS. Kredencialų vagystės išpuolis bankininkystės svetainėje

[20] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

Bankas vienoje savo bankininkystės svetainėje patyrė kibernetinį išpuolį. Per išpuolį siekta nustatyti visus galimus prisijungimo naudotojų identifikatorius, naudojantis nesudėtingu fiksuotuoju slaptažodžiu. Slaptažodžius sudaro 8 skaitmenys. Pasinaudojant svetainės pažeidžiamumu, kai kuriais atvejais pas įsilaužėlį nutekėjo su duomenų subjektais susijusi informacija (vardas, pavardė, lytis, gimimo data ir vieta, mokesčių mokėtojo kodas, naudotojų identifikavimo kodai), net jei naudotas slaptažodis buvo neteisingas arba banko sąskaita buvo nebeaktyvi. Nukentėjo apie 100 000 duomenų subjektų. Įsilaužėliui pavyko prisijungti prie maždaug 2 000 su jais susijusių paskyrų, kurioms buvo naudojami paprasti įsilaužėlio išbandyti slaptažodžiai. Po šio incidento duomenų valdytojui pavyko nustatyti visus neteisėtus bandymus prisijungti. Duomenų valdytojas galėjo patvirtinti, kad išpuolio metu šiose paskyrose sandorių neįvykdyta. Bankas apie duomenų saugumo pažeidimą sužinojo todėl, kad jo saugumo operacijų centras nustatė daug į svetainę išsiųstų prisijungimo užklausų. Į tai atsakydamas duomenų valdytojas sustabdė galimybę prisijungti prie svetainės, ją išjungdamas, ir privertė pasikeisti pažeistų paskyrų slaptažodžius. Duomenų valdytojas apie pažeidimą pranešė tik tiems naudotojams, kurių paskyros buvo pažeistos, t. y. tiems naudotojams, kurių slaptažodžiai buvo

3.3.1 7 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

63. Svarbu pažymėti, kad itin asmeninio pobūdžio duomenis[21] tvarkantiems duomenų valdytojams tenka didesnė atsakomybė užtikrinti tinkamą duomenų saugumą, pvz., įsteigti saugumo operacijų centrą ir taikyti kitas incidentų prevencijos, aptikimo ir atsako į juos priemones. Nesilaikant šių aukštesnių standartų, atliekant PI tyrimą tikrai bus taikomos griežtesnės priemonės.

64. Pažeidimas susijęs su finansiniais duomenimis, kuriuos sudaro daugiau nei tapatybės ir naudotojo identifikavimo informacija, todėl jis yra itin rimtas. Nukentėjusių asmenų skaičius didelis.

65. Tai, kad pažeidimas galėjo būti padarytas tokioje jautrioje aplinkoje, rodo dideles duomenų valdytojo sistemos duomenų saugumo spragas ir gali rodyti, kad pagal BDAR 24 straipsnio 1 dalį, 25 straipsnio 1 dalį ir 32 straipsnio 1 dalį *būtina* peržiūrėti ir atnaujinti susijusias priemones. Naudojantis pažeistais duomenimis, galima nustatyti atskirų duomenų subjektų tapatybę ir gauti kitokios informacijos apie juos (įskaitant lytį, gimimo datą ir vietą); be to, jais naudodamasis įsilaužėlis gali bandyti atspėti klientų slaptažodžius arba surengti į banko klientus nukreiptą personalizuoto duomenų viliojimo kampaniją.

66. Dėl šių priežasčių laikyta, kad dėl duomenų saugumo pažeidimo gali kilti didelis pavojus visų susijusių duomenų subjektų teisėms ir laisvėms[22]. Todėl jie gali patirti materialinę žalą (pvz., finansinių nuostolių) ir nematerialinę žalą (pvz., gali būti pavogta jų tapatybė).

3.3.2 7 ATVEJIS. Poveikio mažinimas ir prievolės

67. Aprašant atvejį nurodytos duomenų valdytojo priemonės yra tinkamos. Po pažeidimo jis taip pat pašalino svetainės spragas ir ėmėsi kitų veiksmų, siekdamas išvengti panašių duomenų saugumo pažeidimų ateityje,

[21] Ši duomenų subjektų informacija buvo susijusi su mokėjimo metodais, pvz., kortelių numeriais, banko sąskaitomis, mokėjimais internetu, darbo užmokesčiais, banko išrašais, ekonominiais tyrimais arba kita informacija, iš kurios galima gauti su duomenų subjektais susijusios ekonominės informacijos.

[22] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

pvz., nukentėjusioje svetainėje nustatė dviveiksnį tapatumo nustatymą ir pradėjo taikyti patikimą klientų tapatumo nustatymą.

68. Tai, ar dokumentuoti pažeidimą pagal BDAR 33 straipsnio 5 dalį ir pranešti apie jį priežiūros institucijai, šiame scenarijuje rinktis negalima. Be to pagal BDAR 34 straipsnį duomenų valdytojas turėtų informuoti visus 100 000 duomenų subjektų (įskaitant tuos duomenų subjektus, kurių paskyros nebuvo pažeistos).

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	✓

3.4 Programišių išpuolių prevencijos / poveikio mažinimo organizacinės ir techninės priemonės

69. Tokiais atvejais, kaip ir išpirkos reikalavimo programinės įrangos išpuolių atveju, būtina iš naujo įvertinti IT saugumą, kad ir kokie būtų rezultatai ir išpuolio padariniai.

70. Rekomenduojamos priemonės:[23]

(Toliau išvardytų priemonių sąrašas jokiu būdu nėra vienintelis galimas arba išsamus. Siekiama tik pasiūlyti prevencijos idėjų ir galimus sprendimus. Kiekviena duomenų tvarkymo veikla skiriasi, todėl duomenų valdytojas turėtų nuspręsti, kurios priemonės geriausiai tinka konkrečiai situacijai.)

- taikyti pažangiausiais metodais grindžiamą šifravimą ir raktų valdymą, ypač jei tvarkomi slaptažodžiai, neskelbtini arba finansiniai duomenys; kriptografiniam slaptos informacijos (slaptažodžių) šifravimui maišos ir druskos įterpimo metodais visada teiktina pirmenybė prieš slaptažodžių šifravimą; pirmenybė teiktina tokiems tapatumo nustatymo metodams, kuriuos taikant nereikia tvarkyti slaptažodžių serveriuose;
- nuolat atnaujinti sistemą (programinę ir aparatinę programinę įrangą); užtikrinti, kad būtų taikomos visos IT saugumo priemonės ir jos būtų veiksmingos, reguliariai jas naujinti tvarkant duomenis arba pasikeitus ar besikeičiant aplinkybėms; kad pagal BDAR 5 straipsnio 2 dalį galėtų įrodyti atitiktį 5 straipsnio 1 dalies f punktui, duomenų valdytojas turėtų saugoti įrašus apie visus atliktus atnaujinimus, įskaitant įrašus apie jų laiką;
- taikyti patikimus tapatumo nustatymo metodus, pvz., dviveiksnį tapatumo nustatymą ir tapatumo nustatymo serverius, papildant šias priemones aktualia slaptažodžių politika;
- taikyti saugaus kūrimo standartus, pvz., naudotojų įvedinių filtravimą (kiek įmanoma, baltųjų sąrašų sudarymą), naudotojų įvedinių atmetimą ir brutaliosios jėgos prevencijos priemones (pvz., apribojant didžiausią leistiną bandymų skaičių); veiksmingai taikyti šį metodą gali būti lengviau naudojantis saityno taikomųjų programų užkardomis;
- taikyti patikimą naudotojų privilegijų ir prieigos kontrolės valdymo politiką;
- taikyti tinkamas naujausias veiksmingos ir integruotas užkardos, įsilaužimo aptikimo ir kitas juosiamosios gynybos sistemas;
- sistemingai atlikti IT saugumo auditus ir pažeidžiamumo vertinimus (skverbimosi testavimą);
- atlikti reguliarią peržiūrą ir testavimą siekiant užtikrinti, kad atsargines kopijas būtų galima naudoti bet kuriems pažeisto vientisumo arba prieinamumo duomenims atkurti;
- universaliuosiuose adresuose nenaudoti seansų identifikatorių grynuoju tekstu.

[23] Dėl saugių saityno taikomųjų programų kūrimo taip pat žr. https://www.owasp.org/index.php/Main_Page.

4 VIDINIS ŽMOGAUS KELIAMO PAVOJAUS ŠALTINIS

71. Reikia atkreipti dėmesį į žmogaus klaidų vaidmenį asmens duomenų saugumo pažeidimų srityje, nes tokių klaidų pasitaiko dažnai. Šio pobūdžio pažeidimai gali būti tiek tyčiniai, tiek netyčiniai, todėl duomenų valdytojams labai sunku nustatyti spragas ir imtis šių pažeidimų prevencijos priemonių. Per Tarptautinę duomenų apsaugos ir privatumo priežiūros pareigūnų konferenciją buvo pripažinta, kad atsižvelgti į šiuos žmogaus veiksnius svarbu, o 2019 m. spalio mėn. buvo priimta rezoliucija dėl atsižvelgimo į žmogaus klaidos vaidmenį asmens duomenų saugumo pažeidimų srityje[24]. Šioje rezoliucijoje pabrėžiama, kad, siekiant išvengti žmogaus klaidų, reikėtų imtis tinkamų apsaugos priemonių, ir pateiktas nebaigtinis šių apsaugos priemonių ir metodų sąrašas.

4.1 8 ATVEJIS. Darbuotojas eksfiltruoja verslo duomenis

Įspėjimo apie atleidimą iš darbo laikotarpiu bendrovės darbuotojas iš bendrovės duomenų bazės nukopijuoja verslo duomenis. Naudotis duomenų baze darbuotojui leidžiama tik vykdant su darbu susijusias užduotis. Išėjęs iš darbo jis po kelių mėnesių naudoja taip gautus duomenis (pagrindinius kontaktinius duomenis) vykdydamas naują duomenų tvarkymo veiklą, kurios atžvilgiu jis yra duomenų valdytojas, kad galėtų susisiekti su bendrovės klientais, norėdamas privilioti juos į savo

4.1.1 8 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

72. Šiuo konkrečiu atveju nebuvo imtasi išankstinių priemonių, kad darbuotojas negalėtų nukopijuoti kontaktinės bendrovės klientų informacijos, nes jam reikėjo teisėtos prieigos prie šios informacijos, kad galėtų vykdyti savo darbo užduotis, ir jis šią prieigą turėjo. Kadangi dirbant daugumą su klientų santykiais susijusių darbų darbuotojams reikia turėti tam tikrą prieigą prie asmens duomenų, išvengti tokių duomenų saugumo pažeidimų gali būti itin sudėtinga. Apribojus prieigą, gali būti apribotas darbas, kurį galėtų atlikti konkretus darbuotojas. Vis dėlto gerai apgalvota prieigos politika ir nuolatinė kontrolė gali padėti išvengti šių pažeidimų.

73. Atliekant pavojų vertinimą, kaip įprastai, reikia atsižvelgti į pažeidimo pobūdį ir nukentėjusių asmens duomenų rūšį, neskelbtinumą bei kiekį. Tokie pažeidimai paprastai yra konfidencialumo pažeidimai, nes duomenų bazė paprastai lieka nepažeista – jos turinys „tik“ nukopijuojamas tolesniam naudojimui. Paprastai ir susijusių duomenų kiekis yra nedidelis arba vidutinis. Šiuo konkrečiu atveju specialių kategorijų asmens duomenys nenukentėjo, nes darbuotojui tereikėjo klientų kontaktinės informacijos, kad galėtų susisiekti su jais išėjęs iš bendrovės. Todėl susiję duomenys nėra neskelbtini duomenys.

74. Nors vienintelis duomenis kenkėjiškai nukopijavusio buvusio darbuotojo tikslas gali būti tik bendrovės klientų kontaktinės informacijos gavimas savo komerciniais tikslais, duomenų valdytojas negali manyti, kad pavojus susijusiems duomenų subjektams yra mažas, nes neturi jokio patvirtinimo dėl darbuotojo ketinimų. Todėl, nors pažeidimo padariniai gali būti tik netinkamos buvusio darbuotojo savirinkodaros poveikis, neatmetama, kad pavogtais duomenimis gali būti piktnaudžiaujama toliau ir didesniu mastu, atsižvelgiant į tai, kokiu tikslu buvęs darbuotojas tvarko duomenis[25].

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

[25] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

4.1.2 8 ATVEJIS. Poveikio mažinimas ir prievolės

75. Sumažinti neigiamą poveikį pirmiau aprašytu atveju sudėtinga. Siekiant užkirsti kelią tolesniam buvusio darbuotojo piktnaudžiavimui duomenimis ir jų platinimui, gali prireikti nedelsiant imtis teisinių veiksmų. Imantis tolesnių veiksmų, turėtų būti stengiamasi išvengti panašių situacijų ateityje. Duomenų valdytojas galėtų bandyti nurodyti buvusiam darbuotojui nustoti naudoti duomenis, bet šių veiksmų sėkmė geriausiu atveju yra abejotina. Galėtų praversti tinkamos techninės priemonės, kurias taikant, pvz., būtų neįmanoma nukopijuoti arba atsisiųsti duomenų į keičiamuosius prietaisus.

76. Nėra vieno sprendimo, kuris visada tiktų tokiais atvejais, bet jų išvengti gali būti lengviau laikantis sisteminio požiūrio. Pavyzdžiui, įmonė galėtų apsvarstyti galimybę, jei įmanoma, panaikinti tam tikrą savo darbuotojų, kurie yra išreiškę savo ketinimą išeiti iš darbo, prieigą arba naudoti prieigos žurnalus, kuriuose būtų registruojama ir žymima nepageidaujama prieiga. Į su darbuotojais pasirašomas sutartis reikėtų įtraukti nuostatas, kuriomis tokie veiksmai draudžiami.

77. Apskritai tariant, kadangi dėl šio konkretaus pažeidimo didelis pavojus fizinių asmenų teisėms ir laisvėms nekils, pakaks pranešti priežiūros institucijai. Vis dėlto duomenų valdytojui taip pat gali būti pravartu informuoti ir duomenų subjektus, nes gali būti geriau, jei jie apie duomenų nutekėjimą išgirs iš bendrovės, o ne iš buvusio darbuotojo, kuris bandys su jais susisiekti. Duomenų saugumo pažeidimo dokumentavimas pagal 33 straipsnio 5 dalį yra teisinė prievolė.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	X

4.2 9 ATVEJIS. Netyčinis duomenų perdavimas patikimai trečiajai šaliai

Draudimo agentas pastebėjo, kad jis – dėl netinkamų el. paštu gauto *Excel* failo nuostatų – gavo prieigą prie informacijos, susijusios su keliomis dešimtimis į jo veiklos sritį nepatenkančių klientų. Jis yra įpareigotas laikytis profesinės paslapties ir buvo vienintelis el. laiško gavėjas. Pagal duomenų valdytojo ir draudimo agento susitarimą draudimo agentas privalo nepagrįstai nedelsdamas pranešti apie asmens duomenų saugumo pažeidimą duomenų valdytojui. Todėl agentas iškart pranešė apie klaidą duomenų valdytojui, o šis ištaisė failą, išsiuntė jį dar kartą ir paprašė agento ankstesnį pranešimą ištrinti. Pagal pirmiau nurodytą susitarimą agentas turi patvirtinti ištrynimą rašytiniu pareiškimu – tai jis ir padarė. Gautoje informacijoje specialių kategorijų asmens duomenų nėra – ją sudaro tik kontaktiniai duomenys ir duomenys apie draudimą (draudimo rūšis, suma). Išanalizavęs per pažeidimą nukentėjusius asmens duomenis, duomenų valdytojas nenustatė jokių specialių su asmenimis arba duomenų valdytoju susijusių ypatybių, kurios galėtų turėti įtakos pažeidimo poveikio dydžiui.

4.2.1 9 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

78. Šiuo atveju pažeidimas padarytas ne tyčiniais darbuotojo veiksmais, bet per netyčinę žmogaus klaidą dėl neatidumo. Tokio pobūdžio pažeidimų galima išvengti arba jų dažnumą galima sumažinti: a) įgyvendinant mokymo, švietimo ir informuotumo didinimo programas, per kurias darbuotojai geriau suprastų asmens duomenų apsaugos svarbą, b) mažinant keitimąsi failais el. paštu ir vietoj to, pvz., taikant specialias klientų duomenims tvarkyti skirtas sistemas, c) prieš siunčiant dar kartą patikrinant failus, d) atskiriant failų kūrimo ir siuntimo veiklą.

79. Šis duomenų saugumo pažeidimas susijęs tik su duomenų konfidencialumu, o jų vientisumas ir prieinamumas liko nepažeisti. Duomenų saugumo pažeidimas buvo susijęs tik su keliomis dešimtimis klientų, todėl galima laikyti, kad susijusių duomenų kiekis buvo nedidelis. Be to, susijusiuose asmens duomenyse nebuvo neskelbtinų duomenų. Tai, kad duomenų tvarkytojas susisiekė su duomenų valdytoju iškart, kai sužinojo apie duomenų saugumo pažeidimą, gali būti laikoma pavojų mažinančiu veiksniu. (Taip pat reikėtų įvertinti, ar duomenys galėjo būti išsiųsti kitiems draudimo agentams, ir, jei tai pasitvirtintų, reikėtų imtis tinkamų priemonių.) Kadangi po duomenų saugumo pažeidimo buvo imtasi tinkamų veiksmų, pažeidimas tikriausiai nedarys poveikio duomenų subjektų teisėms ir laisvėms.

80. Dėl visų šių aplinkybių – susijusių asmenų skaičius buvo nedidelis, pažeidimas buvo aptiktas iš karto ir buvo imtasi jo poveikio mažinimo priemonių – šiuo konkrečiu atveju pavojus nekyla.

4.2.2 9 ATVEJIS. Poveikio mažinimas ir prievolės

81. Be to, svarbų vaidmenį atlieka kitos riziką mažinančios aplinkybės: agentas įpareigotas laikytis profesinės paslapties, jis pats pranešė apie problemą duomenų valdytojui ir paprašytas ištrynė failą. Išvengti panašių atvejų ateityje tikriausiai bus lengviau didinant informuotumą ir į dokumentų, kuriuose yra asmens duomenų, tikrinimą galbūt įtraukiant papildomų veiksmų.

82. Nereikia imtis jokių kitų veiksmų, išskyrus pažeidimo dokumentavimą pagal 33 straipsnio 5 dalį.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	X	X

4.3 Vidinių žmogaus pavojaus šaltinių prevencijos / poveikio mažinimo organizacinės ir techninės priemonės

83. Sumažinti panašių pažeidimų pasikartojimo tikimybę būtų galima lengviau, derinant toliau nurodytas priemones; jos turėtų būti taikomos atsižvelgiant į konkrečias atvejo ypatybes.

84. Rekomenduojamos priemonės:

(Toliau išvardytų priemonių sąrašas jokiu būdu nėra vienintelis galimas arba išsamus. Siekiama tik pasiūlyti prevencijos idėjų ir galimus sprendimus. Kiekviena duomenų tvarkymo veikla skiriasi, todėl duomenų valdytojas turėtų nuspręsti, kurios priemonės geriausiai tinka konkrečiai situacijai.)

- periodiškai įgyvendinti darbuotojams skirtas mokymo, švietimo ir informuotumo didinimo programas su privatumu ir saugumu susijusių jų pareigų ir grėsmių asmens duomenų saugumui aptikimo bei pranešimo apie jas klausimais[26]; parengti informuotumo didinimo programą, siekiant priminti darbuotojams apie dažniausiai pasitaikančias klaidas, dėl kurių atsiranda asmens duomenų saugumo pažeidimų, ir apie tai, kaip šių klaidų išvengti;
- nustatyti patikimas ir veiksmingas duomenų apsaugos ir privatumo praktiką, procedūras ir sistemas[27];
- vertinti privatumo praktiką, procedūras ir sistemas, siekiant užtikrinti nuolatinį jų veiksmingumą[28];
- parengti tinkamą prieigos kontrolės politiką ir priversti naudotojus laikytis taisyklių;
- įgyvendinti metodus, pagal kuriuos prieigą prie neskelbtinų asmens duomenų būtų galima gauti tik patvirtinus naudotojo tapatumą;
- išjungti su įmone susijusią naudotojo paskyrą iškart, kai tik asmuo palieka bendrovę;
- tikrinti neįprastus duomenų srautus tarp serverio ir darbuotojų darbo stočių;
- nustatyti įvesties ir išvesties sąsajos saugumą BIOS sistemoje arba naudojant programinę įrangą, kuria tikrinamas kompiuterinių sąsajų naudojimas (užrakinti arba atrakinti, pvz., USB / CD / DVD ir pan.);
- peržiūrėti darbuotojų prieigos politiką (pvz., žurnaluose registruoti prieigą prie neskelbtinų duomenų ir reikalauti iš naudotojo įvesti veiklos priežastį, kad šia informacija būtų galima naudotis atliekant auditus);
- išjungti atviras debesijos paslaugas;
- uždrausti prieigą prie žinomų atviryjų pašto paslaugų arba užkirsti kelią šiai prieigai;
- išjungti ekrano kopijos funkciją operacinėje sistemoje;
- užtikrinti tvarkingos darbo vietos politikos laikymąsi;
- po tam tikros neveikimo trukmės automatiškai užrakinti visus kompiuterius;
- bendrai naudojamoje aplinkoje naudoti greito naudotojų perjungimo mechanizmus (pvz., (belaidį) prieigos raktą, kuriuo būtų galima prisijungti prie užrakintų paskyrų ir (arba) jas atverti);
- taikyti specialias asmens duomenų valdymo sistemas, kuriose taikomi tinkami prieigos kontrolės mechanizmai ir užkertamas kelias žmogaus klaidoms, pvz., pranešimų išsiuntimui nepageidaujamam subjektui; naudojimasis skaičiuoklėmis ir kitais *Office* dokumentais nėra tinkamas klientų duomenų valdymo būdas.

[26] Rezoliucijos dėl atsižvelgimo į žmogaus klaidos vaidmenį asmens duomenų saugumo pažeidimų srityje 2 dalies i punktas.

[27] Rezoliucijos dėl atsižvelgimo į žmogaus klaidos vaidmenį asmens duomenų saugumo pažeidimų srityje 2 dalies ii punktas.

[28] Rezoliucijos dėl atsižvelgimo į žmogaus klaidos vaidmenį asmens duomenų saugumo pažeidimų srityje 2 dalies iii punktas.

5 PRARASTI ARBA PAVOGTI PRIETAISAI IR POPIERINIAI DOKUMENTAI

85. Nešiojamieji prietaisai prarandami arba pavagiami dažnai. Šiais atvejais duomenų valdytojas turi atsižvelgti į duomenų tvarkymo operacijos aplinkybes, pvz., į tai, kokių rūšių duomenys saugomi prietaise, taip pat į papildomus įrenginius ir priemones, kurių imtasi prieš pažeidimą, siekiant užtikrinti tinkamą saugumo lygį. Visi šie aspektai turi įtakos galimam duomenų saugumo pažeidimo poveikiui. Įvertinti pavojus gali būti sudėtinga, nes prietaiso nebėra.

86. Šio pobūdžio pažeidimus visada galima priskirti prie konfidencialumo pažeidimų. Vis dėlto, jei nėra atsarginės pavogtos duomenų bazės kopijos, pažeidimo pobūdis taip pat gali būti prieinamumo pažeidimas ir vientisumo pažeidimas.

87. Iš toliau aprašytų scenarijų matyti, kokią įtaką pirmiau nurodytos aplinkybės turi duomenų saugumo pažeidimo tikimybei ir rimtumui.

5.1 10 ATVEJIS. Pavogtas turtas, kuriame saugoti užšifruoti asmens duomenys

Įsilaužus į vaikų dienos priežiūros centrą, buvo pavogti du planšetiniai kompiuteriai. Šiuose planšetiniuose kompiuteriuose buvo įdiegta programėlė, kurioje saugoti asmens duomenys apie dienos priežiūros centrą lankančius vaikus. Tai buvo vaikų asmenvardžiai, gimimo datos ir asmens duomenys apie ugdymą. Tiek abu užšifruoti planšetiniai kompiuteriai, kurie įsilaužimo metu buvo užšifruoti, tiek programėlė buvo apsaugoti patikimu slaptažodžiu. Duomenų valdytojas galėjo veiksmingai iš karto gauti atsarginės kopijos duomenis. Sužinojęs apie įsilaužimą, dienos priežiūros centras nuotoliniu būdu davė komandą iš planšetinių kompiuterių ištrinti informaciją ir ji buvo

5.1.1 10 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

88. Šiuo konkrečiu atveju duomenų valdytojas ėmėsi tinkamų priemonių, siekdamas išvengti galimo duomenų saugumo pažeidimo ir sumažinti jo poveikį, nes naudojosi prietaisų šifravimo funkcija, nustatė tinkamą apsaugą slaptažodžiu ir užtikrino, kad būtų padaryta atsarginė planšetiniuose kompiuteriuose saugomų duomenų kopija. (Rekomenduojamų priemonių sąrašas pateiktas 5.7 skirsnyje.)

89. Sužinojęs apie pažeidimą, duomenų valdytojas turėtų įvertinti pavojaus šaltinį, pagalbines duomenų tvarkymo sistemas, susijusių asmens duomenų rūšį ir galimą duomenų saugumo pažeidimo poveikį susijusiems asmenims. Pirmiau aprašytas duomenų saugumo pažeidimas galėjo pakenkti susijusių duomenų konfidencialumui, prieinamumui ir vientisumui, bet dėl tinkamų duomenų valdytojo procedūrų prieš duomenų saugumo pažeidimą ir po jo nė vienu iš šių aspektų pakenkta nebuvo.

5.1.2 10 ATVEJIS. Poveikio mažinimas ir prievolės

90. Prietaisuose saugotų asmens duomenų konfidencialumas pažeistas nebuvo, nes abu planšetiniai kompiuteriai ir abi programėlės buvo apsaugoti patikimais slaptažodžiais. Planšetiniai kompiuteriai buvo sukonfigūruoti taip, kad nustatant slaptažodį taip pat būtų užšifruojami prietaise esantys duomenys. Šis poveikis dar labiau sustiprintas duomenų valdytojo pastangomis nuotoliniu būdu iš pavogtų prietaisų ištrinti viską, kas juose buvo.

91. Dėl taikytų priemonių taip pat buvo apsaugotas duomenų konfidencialumas. Be to, atsarginiu kopijavimu užtikrintas nuolatinis asmens duomenų prieinamumas, todėl negalėjo atsirasti galimo neigiamo poveikio.

92. Atsižvelgiant į šias aplinkybes, pavojus duomenų subjektų teisėms ir laisvėms dėl pirmiau aprašyto duomenų saugumo pažeidimo kilti neturėjo, todėl pranešti priežiūros institucijai arba susijusiems duomenų subjektams nereikėjo. Vis dėlto šį duomenų saugumo pažeidimą taip pat būtina dokumentuoti pagal 33 straipsnio 5 dalį.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	X	**X**

5.2 11 ATVEJIS. Pavogtas turtas, kuriame saugoti neužšifruoti asmens duomenys

Buvo pavogtas elektroninis skreitinis paslaugų teikimo bendrovės darbuotojo kompiuteris. Pavogtame skreitiniame kompiuteryje saugoti daugiau kaip 100 000 klientų vardai, pavardės, lytis, adresai ir gimimo datos. Dėl neprieinamumo prie pavogto prietaiso nebuvo galima nustatyti, ar taip pat nukentėjo kitų kategorijų asmens duomenys. Prieiga prie skreitinio kompiuterio standžiojo disko nebuvo apsaugota slaptažodžiu. Asmens duomenis buvo galima atkurti iš esamų

5.2.1 11 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

93. Duomenų valdytojas nesiėmė išankstinių saugos priemonių, todėl pavogtame skreitiniame kompiuteryje saugoti asmens duomenys buvo lengvai prieinami vagiui arba kitam vėliau prietaisą gavusiam asmeniui.

94. Šis duomenų saugumo pažeidimas susijęs su pavogtame prietaise saugotų duomenų konfidencialumu.

95. Šiuo atveju skreitinis kompiuteris, kuriame saugoti asmens duomenys, buvo pažeidžiamas, nes jis nebuvo nei apsaugotas slaptažodžiu, nei užšifruotas. Nesiimant pagrindinių saugumo priemonių didėja pavojus susijusiems duomenų subjektams. Be to, taip pat sudėtinga nustatyti susijusius duomenų subjektus, todėl didėja pažeidimo rimtumas. Dėl didelio susijusių asmenų skaičiaus pavojus didėja, bet specialių kategorijų asmens duomenys per šį duomenų saugumo pažeidimą nenukentėjo.

96. Atlikdamas pavojų vertinimą[29], duomenų valdytojas turėtų atsižvelgti į galimus konfidencialumo pažeidimo padarinius ir neigiamą jo poveikį. Dėl pažeidimo, naudojantis pavogtame prietaise esančiais duomenimis, iš susijusių duomenų subjektų gali būti pavogta tapatybė, todėl laikoma, kad pavojus yra didelis.

5.2.2 11 ATVEJIS. Poveikio mažinimas ir prievolės

97. Jei būtų buvęs įjungtas prietaiso šifravimas, o saugota duomenų bazė būtų buvusi apsaugota patikimu slaptažodžiu, pavojus duomenų subjektų teisėms ir laisvėms dėl duomenų saugumo pažeidimo galbūt nebūtų kilęs.

98. Atsižvelgiant į šias aplinkybes, reikia pranešti priežiūros institucijai; taip pat būtina pranešti susijusiems duomenų subjektams.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	✓

[29] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

5.3 12 ATVEJIS. Pavogtos popierinės bylos, kuriose buvo neskelbtinų duomenų

Iš narkotikų priklausomybės reabilitacijos įstaigos pavogtas popierinis žurnalas. Šiame žurnale buvo surašyti pagrindiniai į reabilitacijos įstaigą priimtų pacientų tapatybės ir sveikatos duomenys. Duomenys buvo saugomi tik popieriuje; atsarginės kopijos, kuria galėtų pasinaudoti pacientus gydantys medikai, nebuvo. Žurnalas nebuvo laikomas užrakintame stalčiuje arba kabinete, duomenų valdytojas nesinaudojo nei prieigos kontrolės sistema, nei kokiomis nors kitomis popierinių dokumentų apsaugos

5.3.1 12 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

99. Duomenų valdytojas nesiėmė išankstinių saugos priemonių, todėl žurnalą radęs asmuo galėjo lengvai prieiti prie šiame žurnale saugotų asmens duomenų. Be to, atsarginės duomenų kopijos stoka, atsižvelgiant į žurnale saugotų asmens duomenų pobūdį, yra labai rimtas pavojaus veiksnys.

100. Šis atvejis – tai didelį pavojų keliančio duomenų saugumo pažeidimo pavyzdys. Nesiimant tinkamų su sauga susijusių atsargumo priemonių, buvo prarasti neskelbtini sveikatos duomenys pagal BDAR 9 straipsnio 1 dalį. Šiuo atveju taip pat nukentėjo specialių kategorijų asmens duomenys, todėl taip pat padidėjo galimi pavojai susijusiems duomenų subjektams, – į tai duomenų valdytojas, atlikdamas pavojų vertinimą, taip pat turėtų atsižvelgti[30].

101. Šis pažeidimas turi įtakos susijusių asmens duomenų konfidencialumui, prieinamumui ir vientisumui. Dėl pažeidimo sulaužytas įsipareigojimas saugoti medicininę paslaptį, o leidimo neturinčios trečiosios šalys galėjo įgyti prieigą prie privačios pacientų medicininės informacijos – tai gali turėti didelį poveikį asmeniniam pacientų gyvenimui. Prieinamumo pažeidimas taip pat gali pakenkti pacientų gydymo tęstinumui. Kadangi negalima atmesti dalies žurnalo turinio pakeitimo arba panaikinimo, taip pat pažeistas asmens duomenų vientisumas.

5.3.2 12 ATVEJIS. Poveikio mažinimas ir prievolės

102. Vertinant apsaugos priemones, taip pat reikėtų atsižvelgti į papildomų įrenginių pobūdį. Kadangi pacientų žurnalas buvo fizinis dokumentas, jį reikėjo apsaugoti kitaip nei elektroninį prietaisą. Duomenų saugumo pažeidimo būtų buvę galima išvengti pseudoniminant pacientų asmenvardžius, laikant žurnalą apsaugotose patalpose ir užrakintame stalčiuje arba kabinete ir taikant tinkamą prieigos kontrolę, pagal kurią, prieš suteikiant prieigą prie žurnalo, būtų reikalaujama patvirtinti tapatumą.

103. Pirmiau aprašytas duomenų saugumo pažeidimas gali padaryti didelį poveikį susijusiems duomenų subjektams; todėl privaloma pateikti pranešimą priežiūros institucijai ir pranešti apie pažeidimą susijusiems duomenų subjektams.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	✓

5.4 Prietaisų praradimo arba vagystės prevencijos / poveikio mažinimo organizacinės ir techninės priemonės

104. Sumažinti panašių pažeidimų pasikartojimo tikimybę būtų galima lengviau, derinant toliau nurodytas priemones; jos turėtų būti taikomos atsižvelgiant į konkrečias atvejo ypatybes.

[30] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

105. Rekomenduojamos priemonės:

(Toliau išvardytų priemonių sąrašas jokiu būdu nėra vienintelis galimas arba išsamus. Siekiama tik pasiūlyti prevencijos idėjų ir galimus sprendimus. Kiekviena duomenų tvarkymo veikla skiriasi, todėl duomenų valdytojas turėtų nuspręsti, kurios priemonės geriausiai tinka konkrečiai situacijai.)

- įjungti prietaiso šifravimą (pvz., *Bitlocker*, *Veracrypt* arba *DM-Crypt*);
- visuose prietaisuose taikyti prieigos kodą / slaptažodį; užšifruoti visus mobiliuosius elektroninius prietaisus taip, kad, norint juos iššifruoti, reikėtų įvesti sudėtingą slaptažodį;
- taikyti daugiaveiksnį tapatumo nustatymą;
- įjungti labai mobilių prietaisų funkcijas, kuriomis būtų galima nustatyti šių prietaisų buvimo vietą, jei jie būtų prarasti arba atsidurtų netinkamoje vietoje;
- naudoti mobiliųjų įrenginių valdymo (angl. *Mobile Devices Management*, MDM) programinę įrangą / programėlę ir vietos nustatymo funkciją; taikyti ekrano filtrus; laikyti prietaisus išjungtus tuo metu, kai jais nesinaudojama;
- jei įmanoma ir tinkama atsižvelgiant į konkretų duomenų tvarkymą, saugoti asmens duomenis ne mobiliajame prietaise, bet centriniame vidiniame serveryje;
- jei darbo stotis prijungta prie organizacijos vietinio tinklo, daryti automatines kopijas iš darbo aplankų, jei juose neišvengiamai būtina saugoti asmens duomenis;
- jungiantis mobiliaisiais prietaisais prie vidinių serverių, naudoti saugų virtualųjį privatųjį tinklą (pvz., kuriame, norint užmegzti saugų ryšį, reikalaujama atskiro tapatumo nustatymo antruoju veiksniu rakto);
- aprūpinti darbuotojus fiziniais užraktais, kad savo naudojamus mobiliuosius prietaisus jie galėtų apsaugoti fiziškai tol, kol jais nesinaudoja;
- nustatyti tinkamas prietaisų naudojimo už bendrovės teritorijos taisykles;
- nustatyti tinkamas prietaisų naudojimo bendrovės teritorijoje taisykles;
- naudoti mobiliųjų įrenginių valdymo (angl. *Mobile Devices Management*, MDM) programinę įrangą / programėles ir įjungti nuotolinio ištrynimo funkciją;
- taikyti centralizuotą prietaisų valdymą, suteikiant galutiniams naudotojams minimalias programinės įrangos diegimo teises;
- įdiegti fizinės prieigos kontrolės priemones;
- stengtis nesaugoti neskelbtinos informacijos mobiliuosiuose prietaisuose arba standžiuosiuose diskuose; prireikus jungtis prie bendrovės vidaus sistemos, reikėtų taikyti pirmiau nurodytus saugumo kanalus.

6 PAŠTO IŠSIUNTIMAS KLAIDINGIEMS ADRESATAMS

106. Šiuo atveju pavojaus šaltinis taip pat yra vidinė žmogaus klaida, bet šiuo atveju pažeidimas nepiktavališkai. Jis įvyko dėl neatidumo. Įvykus tokiam pažeidimui, duomenų valdytojas nedaug ko gali imtis, todėl šiais atvejais, kitaip nei dėl kito pobūdžio pažeidimų, dar svarbesnė yra prevencija.

6.1 13 ATVEJIS. Siuntimo paštu klaida

Mažmeninės prekybos bendrovė supakavo du batų užsakymus. Dėl žmogaus klaidos pakuočių sąskaitos faktūros buvo sukeistos, todėl abu gaminiai ir susijusios pakuočių sąskaitos faktūros buvo išsiųstos klaidingiems adresatams. Todėl abu klientai gavo vienas kito užsakymus, įskaitant pakuotės sąskaitas faktūras, kuriose buvo asmens duomenų. Sužinojęs apie pažeidimą, duomenų valdytojas užsakymus atšaukė ir išsiuntė juos teisingiems gavėjams.

6.1.1 13 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

107. Sąskaitose faktūrose buvo nurodyti sėkmingam pristatymui reikiami asmens duomenys (pavardė, adresas, taip pat pirktas daiktas ir jo kaina). Pirmiausia svarbu išsiaiškinti, kodėl galėjo įvykti žmogaus klaida ir ar jos kaip nors būtų buvę galima išvengti. Šiuo konkrečiu aprašytu atveju pavojus yra nedidelis, nes nenukentėjo specialių kategorijų asmens duomenys arba kiti duomenys, kuriais piktnaudžiaujant būtų galima padaryti didelį neigiamą poveikį, pažeidimas įvyko ne dėl sisteminės duomenų valdytojo klaidos ir buvo susijęs tik su dviem asmenimis. Neigiamo poveikio asmenims nenustatyta.

6.1.2 13 ATVEJIS. Poveikio mažinimas ir prievolės

108. Duomenų valdytojas turėtų sudaryti sąlygas nemokamai grąžinti daiktus bei susijusias sąskaitas faktūras ir taip pat turėtų paprašyti, kad neteisingi gavėjai sunaikintų arba ištrintų visas galimas sąskaitų faktūrų, kuriose pateikta asmens duomenų, kopijas.

109. Nors dėl paties pažeidimo didelio pavojaus susijusių asmenų teisėms ir laisvėms nekyla ir todėl pranešti duomenų subjektams pagal BDAR 34 straipsnį neprivaloma, šio pranešimo jiems išvengti nepavyko, nes, norint sumažinti poveikį, reikėjo, kad jie bendradarbiautų.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	X	X

6.2 14 ATVEJIS. Per klaidą el. paštu išsiųsti labai konfidencialūs asmens duomenys

Viešojo administravimo įstaigos užimtumo skyrius asmenims, kurie jo sistemoje buvo užregistruoti kaip ieškantys darbo, el. paštu išsiuntė pranešimą apie būsimus mokymus. Per klaidą prie šio el. laiško buvo pridėtas dokumentas su visų šių darbo ieškančių žmonių asmens duomenimis (asmenvardžiais, el. pašto adresais, pašto adresais, socialinio draudimo numeriais). Susijusių asmenų daugiau nei 60 000. Vėliau įstaiga, susisiekusi su visais gavėjais, paprašė, kad jie ištrintų ankstesnį pranešimą ir nenaudotų jame pateiktos informacijos.

6.2.1 14 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

110. Reikėjo įgyvendinti griežtesnes tokių pranešimų siuntimo taisykles. Reikia apsvarstyti galimybę nustatyti papildomus kontrolės mechanizmus.

111. Susijusių asmenų skaičius didelis, o dėl jų socialinio draudimo numerių, kartu su kitais, bendresnio pobūdžio asmens duomenimis, pavojus dar labiau padidėja ir galima laikyti, kad jis yra didelis[31]. Duomenų valdytojas nieko negali padaryti, kad kuris nors gavėjas vėliau neišplatintų duomenų.

6.2.2 14 ATVEJIS. Poveikio mažinimas ir prievolės

112. Kaip nurodyta pirmiau, galimybės veiksmingai sumažinti panašaus pažeidimo pavojus yra ribotos. Nors duomenų valdytojas paprašė ištrinti pranešimą, jis negali priversti gavėjų to padaryti, todėl negali būti visiškai tikras tuo, kad jie šį prašymą įvykdys.

113. Savaime suprantama, kad tokiu atveju, kaip šis, reikėtų imtis visų trijų toliau nurodytų veiksmų.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams

[31] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

✓	✓	✓

6.3 15 ATVEJIS. Per klaidą el. paštu išsiunčiami asmens duomenys

Viešbutyje penkias dienas truksiančių teisinės anglų kalbos kursų dalyvių sąrašas per klaidą išsiunčiamas penkiolikai buvusių kursų dalyvių. Šiame sąraše nurodyti šių penkiolikos dalyvių asmenvardžiai, el. pašto adresai ir pageidavimai dėl maisto. Pageidavimus dėl maisto pateikė tik du dalyviai: jie nurodė, kad netoleruoja laktozės. Nė vienam dalyviui netaikoma tapatybės apsauga. Duomenų valdytojas klaidą pastebi iškart, kai tik išsiunčia sąrašą, informuoja gavėjus apie klaidą ir prašo, kad jie šį sąrašą ištrintų.

6.3.1 15 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

114. Turėjo būti įgyvendintos griežtos pranešimų, kuriuose yra asmens duomenų, siuntimo taisyklės. Reikia apsvarstyti galimybę nustatyti papildomus kontrolės mechanizmus.

115. Pavojai, kylantys dėl asmens duomenų pobūdžio, neskelbtinumo, kiekio ir konteksto, yra nedideli. Asmens duomenys apima neskelbtinus duomenis, susijusius su dviejų dalyvių pageidavimais dėl maisto. Nors informacija apie laktozės netoleravimą yra sveikatos duomenys, pavojus, kad jie bus panaudoti pakenkiant, turėtų būti laikomas palyginti mažu. Nors su sveikata susijusių duomenų atveju paprastai daroma prielaida, kad dėl pažeidimo duomenų subjektui gali kilti didelis pavojus[32], šiuo konkrečiu atveju negalima nustatyti pavojaus, kad dėl pažeidimo neleistinai atskleidus informaciją apie laktozės netoleravimą duomenų subjektas patirs fizinę, materialinę arba nematerialinę žalą. Kitaip nei kitų pageidavimų dėl maisto atveju, laktozės netoleravimo paprastai negalima susieti su religiniais arba filosofiniais įsitikinimais. Pažeistų duomenų ir susijusių duomenų subjektų taip pat yra labai nedaug.

6.3.2 15 ATVEJIS. Poveikio mažinimas ir prievolės

116. Apibendrinant galima teigti, kad pažeidimas duomenų subjektams nepadarė didelio poveikio. Faktas, kad duomenų valdytojas susisiekė su gavėjais iškart, kai tik sužinojo apie klaidą, gali būti laikomas pavojų mažinančiu veiksniu.

117. Jei el. laiškas išsiunčiamas neteisingam / neįgaliotam gavėjui, rekomenduojama, kad duomenų valdytojas, naudodamasis nematomosios kopijos funkcija, išsiųstų nepageidaujamiems gavėjams dar vieną el. laišką ir jame atsiprašytų, pareikalautų ištrinti el. laišką, kuriuo buvo padarytas pažeidimas, ir paaiškintų gavėjams, kad jie neturi teisės toliau naudoti jiems atskleistų el. pašto adresų.

118. Atsižvelgiant į šias aplinkybes, pavojus duomenų subjektų teisėms ir laisvėms dėl šio duomenų saugumo pažeidimo kilti neturėjo, todėl pranešti priežiūros institucijai arba susijusiems duomenų subjektams nereikėjo. Vis dėlto šį duomenų saugumo pažeidimą taip pat būtina dokumentuoti pagal 33 straipsnio 5 dalį.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	X	X

6.4 16 ATVEJIS. Siuntimo paštu klaida

[32] Žr. Gaires WP 250, p. 23.

Draudimo įmonių grupė siūlo automobilių draudimą. Šiuo tikslu ji paštu siunčia reguliariai tikslinamus draudimo įmokų polisus. Be draudėjo asmenvardžio ir adreso, laiške nurodomas transporto priemonės registracijos numeris, neužmaskuojant skaitmenų, einamųjų ir kitų draudžiamųjų metų draudimo įmokos, apytikslė metinė rida ir draudėjo gimimo data. Sveikatos duomenys pagal BDAR 9 straipsnį, mokėjimo duomenys (banko rekvizitai), ekonominiai ir finansiniai duomenys neįtraukiami.

Laiškai pakuojami automatizuotais pakavimo į vokus aparatais. Dėl mechaninės klaidos dviem skirtingiems draudėjams skirti laiškai įdedami į vieną voką ir paštu išsiunčiami vienam draudėjui. Draudėjas namie atplėšia voką ir mato jam teisingai pristatytą laišką ir neteisingai pristatytą kitam draudėjui skirtą laišką.

6.4.1 16 ATVEJIS. Išankstinės priemonės ir pavojų vertinimas

119. Neteisingai pristatytame laiške nurodytas asmenvardis, adresas, gimimo data, neužmaskuotas transporto priemonės registracijos numeris ir einamųjų bei kitų metų draudimo įmokos klasifikacija. Poveikis susijusiam asmeniui laikytinas vidutiniu, nes leidimo neturinčiam gavėjui atskleista tokia viešai neprieinama informacija kaip gimimo data arba neužmaskuoti draudimo registracijos numeriai ir informacija apie draudimo įmokų padidėjimą. Įvertinta, kad piktnaudžiavimo šiais duomenimis tikimybė yra nuo mažos iki vidutinės. Vis dėlto, nors gavėjai ne jiems skirtus laiškus dažniausiai išmeta, atskirais atvejais negalima visiškai atmesti, kad laiškas bus paskelbtas socialiniuose tinkluose arba kad bus susisiekta su draudėju.

6.4.2 16 ATVEJIS. Poveikio mažinimas ir prievolės

120. Duomenų valdytojas turėtų pasirūpinti, kad originalus dokumentas būtų grąžintas duomenų valdytojo sąskaita. Neteisingas gavėjas taip pat turėtų būti informuojamas apie tai, kad jis negali piktnaudžiauti perskaityta informacija.

121. Siunčiant paštą masiškai ir naudojantis visiškai automatizuotais aparatais, visiškai išvengti pašto pristatymo klaidų tikriausiai niekada nebus įmanoma. Vis dėlto, jei klaidų padaugėja, būtina patikrinti, ar pakavimo į vokus aparatai pakankamai gerai nustatyti ir prižiūrimi, arba išsiaiškinti, ar šie pažeidimai galbūt įvyksta dėl kitos sisteminės problemos.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	X

6.5 Pašto išsiuntimo klaidingiems adresatams prevencijos / poveikio mažinimo organizacinės ir techninės priemonės

122. Sumažinti panašių pažeidimų pasikartojimo tikimybę būtų galima lengviau, derinant toliau nurodytas priemones; jos turėtų būti taikomos atsižvelgiant į konkrečias atvejo ypatybes.

123. Rekomenduojamos priemonės:

(Toliau išvardytų priemonių sąrašas jokiu būdu nėra vienintelis galimas arba išsamus. Siekiama tik pasiūlyti prevencijos idėjų ir galimus sprendimus. Kiekviena duomenų tvarkymo veikla skiriasi, todėl duomenų valdytojas turėtų nuspręsti, kurios priemonės geriausiai tinka konkrečiai situacijai.)

- nustatyti tikslius ir vienareikšmiškus laiškų / el. laiškų siuntimo standartus;
- tinkamai išmokyti darbuotojus, kaip siųsti laiškus / el. laiškus;
- nustatyti, kad, siunčiant el. laiškus keliems gavėjams, jie pagal numatytuosius parametrus būtų įtraukiami į nematomosios kopijos lauką;

- nustatyti, kad, jei el. laiškai siunčiami keliems gavėjams ir gavėjai nurodomi ne nematomosios kopijos lauke, reikėtų papildomo patvirtinimo;
- taikyti „keturių akių“ principą;
- naudotis ne rankiniu, bet automatiniu adresavimu, imant duomenis iš esamos aktualios duomenų bazės; automatinio adresavimo sistema turėtų būti reguliariai peržiūrima, siekiant patikrinti, ar nėra užslėptųjų klaidų ir netinkamų nustatymų;
- taikyti pranešimų išsiuntimo atidėjimo funkciją (pvz., spustelėjus siuntimo mygtuką, pranešimą kurį laiką dar galima ištrinti arba pataisyti);
- išjungti automatinio el. pašto adresų užbaigimo, juos įvedant, funkciją;
- rengti informuotumo didinimo kursus dažniausiai pasitaikančių klaidų, dėl kurių įvyksta asmens duomenų saugumo pažeidimai, klausimais;
- organizuoti mokymo kursus ir parengti vadovus, kaip elgtis įvykus incidentui, dėl kurio pažeidžiami asmens duomenys, ir ką informuoti (įtraukti duomenų apsaugos pareigūną).

7 KITI ATVEJAI. SOCIALINĖ INŽINERIJA

7.1 17 ATVEJIS. Tapatybės vagystė

Į telekomunikacijų įmonės ryšių centrą paskambina klientu apsimetantis asmuo. Tariamas klientas prašo bendrovės pakeisti el. pašto adresą, kuriuo nuo šiol norėtų gauti sąskaitų informaciją. Ryšių centro darbuotojas, laikydamasis nustatytų bendrovės procedūrų, patikrina kliento tapatybę, paprašydamas nurodyti tam tikrus asmens duomenis. Paskambinęs asmuo teisingai nurodo prašomą kliento mokesčių mokėtojo numerį ir pašto adresą (nes turėjo prieigą prie šių duomenų). Patvirtinęs tapatybę, operatorius pakeičia prašytus duomenis ir nuo tada sąskaitų informacija siunčiama naujuoju el. pašto adresu. Pagal procedūrą nenumatyta išsiųsti pranešimo ankstesniam el. pašto adresatui. Kitą mėnesį tikrasis klientas susisiekia su bendrove. Jis klausia, kodėl negauna sąskaitos savo el. pašto adresu, ir tvirtina, kad neskambino ir neprašė pakeisti kontaktinio el. pašto adreso. Vėliau bendrovė supranta, kad informacija buvo išsiųsta neteisėtam naudotojui ir pakeitimą atšaukia.

7.1.1 17 ATVEJIS. Pavojų vertinimas, poveikio mažinimas ir prievolės

124. Šis atvejis rodo, kaip svarbu imtis išankstinių priemonių. Kalbant apie pavojų pažymėtina, kad pažeidimas kelia didelį pavojų33, nes iš sąskaitų duomenų galima gauti informacijos apie duomenų subjekto asmeninį gyvenimą (pvz., jo įpročius, kontaktinius asmenis), o jais naudojantis galima padaryti materialinės žalos (pvz., duomenų subjektas gali būti persekiojamas, kyla pavojus fizinei jo neliečiamybei). Naudojantis per šį išpuolį gautais asmens duomenimis, taip pat būtų galima lengviau perimti paskyrą šioje organizacijoje arba pasinaudoti tolesnėmis tapatybės patvirtinimo priemonėmis kitose organizacijose. Atsižvelgiant į šiuos pavojus, tinkamai tapatybės patvirtinimo priemonei turėtų būti taikomi griežti reikalavimai, atsižvelgiant į tai, kokius asmens duomenis galima tvarkyti patvirtinus tapatybę.

[33] Gairės dėl duomenų tvarkymo operacijų, kurios *gali sukelti didelį pavojų*, nurodytos pirmiau 10 išnašoje.

125. Todėl duomenų valdytojas turi pranešti apie pažeidimą tiek priežiūros institucijai, tiek duomenų subjektui.

126. Atsižvelgiant į šį atvejį, akivaizdu, kad reikia patobulinti išankstinį klientų patvirtinimo procesą. Taikyti tapatybės patvirtinimo metodai buvo nepakankami. Piktavalis galėjo apsimesti tikruoju naudotoju, pasinaudodamas viešai prieinama ir informacija ir informacija, kurią galėjo gauti kitu būdu.

127. Taikyti tokį statinėmis žiniomis grindžiamą tapatybės patvirtinimo metodą (kai atsakymas nesikeičia ir kai informacija nėra tokia slapta, koks būtų slaptažodis) nerekomenduojama.

128. Vietoj jo organizacija turėtų taikyti tokį tapatybės patvirtinimo metodą, kuriuo būtų galima labai patikimai užtikrinti, kad naudotojas, kurio tapatybė patvirtinama, iš tikrųjų yra tas konkretus asmuo, o ne kas nors kitas. Problemą būtų galima išspręsti taikant daugiaveiksnį tapatybės patvirtinimo metodą ne pagrindiniu bendravimo kanalu, pvz., siekiant patikrinti pakeitimo užklausą, būtų galima išsiųsti patvirtinimo užklausą buvusiam adresatui, arba būtų galima įtraukti papildomų klausimų ir prašyti informacijos, kuri matyti tik ankstesnėse sąskaitose. Atsakomybė nuspręsti, kokias priemones nustatyti, tenka duomenų valdytojui, nes jis geriausiai žino savo vidaus veiklos informaciją ir reikalavimus.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	✓

7.2 18 ATVEJIS. El. pašto eksfiltravimas

Prekybos centrų tinklas po trijų mėnesių nuo konfigūracijos nustatė, kad buvo pakeistos kai kurios el. pašto paskyros ir nustatytos tokios taisyklės, pagal kurias kiekvienas el. laiškas, kuriame yra tam tikrų žodžių ir žodžių junginių (pvz., *sąskaita*, *mokėjimas*, *banko pervedimas*, *kredito kortelės autentiškumo patvirtinimas*, *banko sąskaitos duomenys*), būtų perkeltas į nenaudojamą aplanką ir persiųstas išorės el. pašto adresu. Be to, tuo metu jau buvo įvykdytas socialinės inžinerijos išpuolis, t. y. įsilaužėlis, apsimesdamas tiekėju, pasirūpino tuo, kad tiekėjo banko sąskaitos informacija būtų pakeista į jo paties informaciją. Galiausiai tuo metu buvo išsiųstos kelios sąskaitos faktūros, kuriose buvo nurodyti naujos banko sąskaitos duomenys. Galiausiai el. pašto platformos stebėsenos sistema pateikė įspėjimą dėl aplankų. Bendrovei nepavyko nustatyti, kaip įsilaužėlis iš pradžių galėjo įgyti prieigą prie el. pašto paskyrų, bet spėjo, kad prieiga prie naudotojų, atsakingų už mokėjimus, grupės gauta atsiuntus užkrėstą el. laišką.

Taikydamas raktažodžiais grindžiamą el. laiškų persiuntimo metodą, įsilaužėlis gavo informaciją apie 99 darbuotojus: su 89 duomenų subjektais susijusius asmenvardžius bei konkretaus mėnesio atlyginimus ir 10 darbuotojų, kurių sutartys buvo nutrauktos, asmenvardžius, civilinę būklę, vaikų skaičių, atlyginimą, darbo valandas ir priminimus apie gautą atlyginimą. Duomenų valdytojas informavo tik dešimt pastarajai grupei priklausančių darbuotojų.

7.2.1 18 ATVEJIS. Pavojų vertinimas, poveikio mažinimas ir prievolės

129. Net jei įsilaužėlis galbūt nesiekė rinkti asmens duomenų, dėl jų saugumo pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, nes gali atsirasti tiek materialinė žala (pvz., finansiniai nuostoliai), tiek nematerialinė žala (pvz., tapatybės vagystė arba sukčiavimas), arba naudojantis duomenimis gali būti lengviau įvykdyti kitus išpuolius (pvz., duomenų viliojimo). Todėl apie pažeidimą reikėtų informuoti ne tik 10 darbuotojų, kurių atlyginimo informacija nutekėjo, bet visus 99 darbuotojus.

130. Sužinojęs apie pažeidimą, duomenų valdytojas privertė pasikeisti pažeistų paskyrų slaptažodžius, užblokavo el. laiškų siuntimą į įsilaužėlio el. pašto paskyrą, pranešė įsilaužėlio naudojamo el. pašto paslaugų tiekėjui apie įsilaužėlio veiksmus, pašalino įsilaužėlio nustatytas taisykles ir patikslino stebėsenos sistemos įspėjimus, kad įspėjimas būtų duodamas iškart, kai sukuriama automatinė taisyklė. Duomenų valdytojas taip pat galėtų

panaikinti naudotojų teisę nustatyti persiuntimo taisykles, užtikrinti, kad, tai galėtų atlikti tik IT paslaugų grupės darbuotojai gavę prašymą, arba nustatyti tokią politiką, pagal kurią naudotojai turėtų tikrinti jų paskyrose nustatytas taisykles ir pranešti apie šias taisykles kartą per savaitę arba finansinių duomenų tvarkymo srityse – dažniau.

131. Iš to, kad galėjo būti padarytas pažeidimas, kad jis liko nepastebėtas tiek ilgai ir kad ilgainiui naudojantis socialine inžinerija būtų buvę galima pakeisti daugiau duomenų, matyti didelės duomenų valdytojo IT saugumo sistemos problemos. Jos turėtų būti sprendžiamos nedelsiant, pvz., turėtų būti atkreipiamas dėmesys į automatizavimo peržiūrą ir pakeitimų kontrolę, taip pat taikomos incidentų nustatymo ir reagavimo į juos priemonės. Neskelbtinus duomenis, finansinę ir panašią informaciją tvarkantiems duomenų valdytojams tenka didesnė atsakomybė užtikrinti tinkamą duomenų saugumą.

Nustatytais pavojais grindžiami būtini veiksmai		
Vidaus dokumentavimas	Pranešimas priežiūros institucijai	Pranešimas duomenų subjektams
✓	✓	✓