Ohjeet 1/2021

henkilötietojen tietoturvaloukkauksesta ilmoittamista koskevista esimerkeistä

Hyväksytty 14. joulukuuta 2021

Versio 2.0

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

Versiohistoria

Versio 2.0	14.12.2021	Ohjeiden hyväksyminen julkisen kuulemisen jälkeen
Versio 1.0	14.1.2021	Ohjeiden hyväksyminen julkista kuulemista varten

Sisällysluettelo

EUROOPAN TIETOSUOJANEUVOSTO, joka

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679, jäljempänä 'yleinen tietosuoja-asetus', 70 artiklan 1 kohdan e alakohdan,

ottaa huomioon ETA-sopimuksen ja erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018[1],

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

ottaa huomioon komission Euroopan parlamentille ja neuvostolle antaman tiedonannon *Tietosuojasäännöt kansalaisten vaikutusmahdollisuuksien ja EU:n digitaalisen muutoksen edistäjänä – yleistä tietosuoja-asetusta sovellettu kaksi vuotta*[2],

ON HYVÄKSYNYT SEURAAVAT OHJEET:

1 JOHDANTO

1. Yleisessä tietosuoja-asetuksessa säädetään tietyissä tapauksissa vaatimuksesta, jonka mukaan henkilötietojen tietoturvaloukkauksesta on ilmoitettava toimivaltaiselle kansalliselle valvontaviranomaiselle, jäljempänä 'valvontaviranomainen', ja henkilöille, joiden henkilötietoihin tietoturvaloukkaus on vaikuttanut (33 ja 34 artikla).

2. 29 artiklan mukainen tietosuojatyöryhmä, jäljempänä 'tietosuojatyöryhmä', laati jo lokakuussa 2017 *yleiset* tietoturvaloukkauksista ilmoittamista koskevat ohjeet, joissa analysoidaan yleisen tietosuoja-asetuksen asiaankuuluvia jaksoja (suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta, WP 250, jäljempänä 'suuntaviivat WP 250'[3]). Näissä suuntaviivoissa ei kuitenkaan niiden luonteen ja ajoituksen vuoksi käsitelty kaikkia käytännön kysymyksiä riittävän yksityiskohtaisesti. Sen vuoksi on tarpeen laatia *käytännönläheiset ja tapauspohjaiset* ohjeet, joissa hyödynnetään valvontaviranomaisten yleisen tietosuoja-asetuksen soveltamisen aloittamisen jälkeen saamaa kokemusta.

3. Tämän asiakirjan tarkoituksena on täydentää suuntaviivoja WP 250, ja siinä otetaan huomioon ETA:n valvontaviranomaisten yhteiset kokemukset yleisen tietosuoja-asetuksen soveltamisen alkamisesta

[1] Viittauksilla "jäsenvaltioihin" tarkoitetaan tässä asiakirjassa ETA:n jäsenvaltioita.

[2] COM(2020) 264 final, 24.6.2020.

[3] 29 artiklan mukainen tietosuojatyöryhmä, WP 250 rev.01, 6. helmikuuta 2018, suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta, Euroopan tietosuojaneuvoston hyväksymät suuntaviivat (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052).

lähtien. Asiakirjan tavoitteena on auttaa rekisterinpitäjiä päättämään, miten tietoturvaloukkauksia käsitellään ja mitä tekijöitä riskinarvioinnissa otetaan huomioon.

4. Voidakseen puuttua tietoturvaloukkauksiin rekisterinpitäjän ja henkilötietojen käsittelijän olisi ensin kyettävä tunnistamaan ne. Yleisen tietosuoja-asetuksen 4 artiklan 12 kohdan mukaisesti 'henkilötietojen tietoturvaloukkauksella' tarkoitetaan "tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin".

5. Tietosuojatyöryhmä on selittänyt henkilötietojen tietoturvaloukkauksen ilmoittamisesta antamassaan lausunnossa 3/2014[4] ja suuntaviivoissaan WP 250, että tietosuojaloukkaukset voidaan luokitella seuraavien kolmen tunnetun tietoturvaperiaatteen mukaisesti:

   - "tietojen luottamuksellisuuteen vaikuttava tietoturvaloukkaus" – henkilötietojen luvaton luovuttaminen tai käyttöön antaminen
   - "tietojen eheyteen vaikuttava tietoturvaloukkaus" – henkilötietojen luvaton tai tahaton muuttaminen
   - "tietojen käytettävyyteen vaikuttava tietoturvaloukkaus" – tahaton tai luvaton henkilötietoihin pääsyn menettäminen tai henkilötietojen tuhoaminen.[5]

6. Tietoturvaloukkauksella saattaa olla useita erilaisia henkilöihin kohdistuvia haittavaikutuksia, jotka voivat aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja. Yleisen tietosuoja-asetuksen mukaan haittavaikutuksia saattavat olla muun muassa omien henkilötietojen valvomiskyvyn menettäminen tai oikeuksien rajoittaminen, syrjintä, identiteettivarkaus tai petos, taloudelliset menetykset, pseudonymisoitumisen luvaton kumoutuminen, maineen vahingoittuminen ja salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetys. Niihin saattaa sisältyä myös muuta merkittävää taloudellista tai sosiaalista vahinkoa kyseisille henkilöille. Yksi rekisterinpitäjän tärkeimmistä velvoitteista on arvioida näitä rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä ja toteuttaa asianmukaisia teknisiä ja organisatorisia toimenpiteitä niihin puuttumiseksi.

7. Näin ollen yleisessä tietosuoja-asetuksessa edellytetään, että rekisterinpitäjä

   - dokumentoi kaikki henkilötietojen tietoturvaloukkaukset, mukaan lukien henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet[6]
   - ilmoittaa henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä[7]

---

[4] 29 artiklan mukainen tietosuojatyöryhmä, 25. maaliskuuta 2014, lausunto 3/2014 henkilötietojen tietosuojaloukkauksen ilmoittamisesta, s. 6 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4).

[5] Ks. suuntaviivat WP 250, s. 8. – On otettava huomioon, että tietoturvaloukkaus voi koskea joko yhtä tai useampaa luokkaa samanaikaisesti tai yhdessä.

[6] Yleisen tietosuoja-asetuksen 33 artiklan 5 kohta.

[7] Yleisen tietosuoja-asetuksen 33 artiklan 1 kohta.

- ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisteröidylle, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille[8].

8. Tietoturvaloukkaukset ovat ongelmia itsessään, mutta ne voivat olla myös haavoittuvan ja mahdollisesti vanhentuneen tietoturvajärjestelmän oireita. Lisäksi ne voivat viitata järjestelmän heikkouksiin, joihin on puututtava. Yleisesti ottaen on aina parempi ehkäistä tietoturvaloukkauksia valmistautumalla etukäteen, sillä monet niistä johtuvat seuraukset ovat luonteeltaan peruuttamattomia. Ennen kuin rekisterinpitäjä voi *täysin* arvioida jonkinlaisen hyökkäyksen aiheuttamasta tietoturvaloukkauksesta aiheutuvan riskin, ongelman perimmäinen syy olisi yksilöitävä. Näin voidaan määrittää, ovatko poikkeamaan johtaneet haavoittuvuudet edelleen olemassa ja ovatko ne näin ollen edelleen hyödynnettävissä. Monissa tapauksissa rekisterinpitäjä pystyy havaitsemaan, että poikkeama todennäköisesti aiheuttaa riskin, ja siitä on siksi ilmoitettava. Muissakaan tapauksissa ilmoitusta ei tarvitse lykätä, kunnes tietoturvaloukkaukseen liittyvät riskit ja vaikutukset on arvioitu täysimittaisesti. Täydellinen riskinarviointi voi nimittäin tapahtua samanaikaisesti ilmoituksen kanssa, ja näin saadut tiedot voidaan toimittaa valvontaviranomaiselle vaiheittain ilman aiheetonta viivytystä.[9]

9. Tietoturvaloukkauksesta olisi ilmoitettava, kun rekisterinpitäjä katsoo sen todennäköisesti aiheuttavan riskin rekisteröidyn oikeuksille ja vapauksille. Rekisterinpitäjien olisi tehtävä tämä arviointi, kun ne saavat tiedon tietoturvaloukkauksesta. Rekisterinpitäjän ei pitäisi odottaa yksityiskohtaista rikosteknistä tutkimusta ja (varhaisia) lieventämistoimia ennen kuin se arvioi, aiheuttaako tietoturvaloukkaus todennäköisesti riskin siten, että siitä olisi ilmoitettava.

10. Jos rekisterinpitäjä itse arvioi riskin epätodennäköiseksi mutta osoittautuukin, että riski toteutuu, toimivaltainen valvontaviranomainen voi käyttää korjaavia toimivaltuuksiaan ja päättää seuraamuksista.

11. Jokaisella rekisterinpitäjällä ja henkilötietojen käsittelijällä olisi oltava käytössään suunnitelmat ja menettelyt mahdollisten tietoturvaloukkausten käsittelyä varten. Organisaatioilla olisi oltava selkeät raportointilinjat ja tietyistä palautusprosessin näkökohdista vastuussa olevat henkilöt.

12. Rekisterinpitäjien ja henkilötietojen käsittelijöiden kannalta on myös olennaisen tärkeää, että rekisterinpitäjän ja henkilötietojen käsittelijän henkilöstölle annetaan koulutusta ja tietoa tietosuojakysymyksistä siten, että keskitytään henkilötietojen tietoturvaloukkausten hallintaan (muun muassa henkilötietojen tietoturvaloukkauksen tunnistaminen ja toteutettavat jatkotoimet). Tätä koulutusta olisi toistettava säännöllisesti käsittelytoimien tyypistä ja rekisterinpitäjän koosta riippuen. Siinä olisi käsiteltävä uusimpia suuntauksia ja varoituksia, jotka johtuvat kyberhyökkäyksistä tai muista turvallisuuspoikkeamista.

13. Osoitusvelvollisuuden periaate ja sisäänrakennetun tietosuojan käsite voisivat sisältää analyysin, joka sisällytettäisiin rekisterinpitäjän ja henkilötietojen käsittelijän omaan ”henkilötietojen tietoturvaloukkausten käsittelyä koskevaan käsikirjaan”. Käsikirjan tarkoituksena olisi määrittää tosiseikat käsittelyn kullekin osa-alueelle kussakin toiminnan päävaiheessa. Tällainen etukäteen laadittu käsikirja tarjoaisi aiempaa paljon nopeamman tietolähteen. Sen avulla rekisterinpitäjät ja tietojen käsittelijät voisivat lieventää riskejä ja täyttää velvoitteet ilman aiheetonta viivytystä. Näin varmistettaisiin, että jos henkilötietojen tietoturvaloukkaus toteutuu, organisaation työntekijät tietävät, miten on toimittava. Lisäksi

[8] Yleisen tietosuoja-asetuksen 34 artiklan 1 kohta.

[9] Yleisen tietosuoja-asetuksen 33 artiklan 4 kohta.

tietoturvaloukkauksen käsittely olisi todennäköisemmin nopeampaa kuin ilman käytössä olevia lieventämistoimia tai suunnitelmaa.

14. Vaikka jäljempänä esitetyt tapaukset ovat kuvitteellisia, ne pohjautuvat tavallisiin tapauksiin, jotka perustuvat valvontaviranomaisen kollektiiviseen kokemukseen tietoturvaloukkauksia koskevista ilmoituksista. Tarjotut analyysit koskevat nimenomaisesti tarkasteltavia tapauksia, mutta niiden tavoitteena on auttaa rekisterinpitäjiä arvioimaan omia tietoturvaloukkauksiaan. Kaikki jäljempänä kuvattujen tapausten olosuhteiden muutokset voivat johtaa erilaisiin tai merkittävämpiin riskitasoihin, mikä edellyttää erilaisia toimenpiteitä tai lisätoimenpiteitä. Näissä ohjeissa tapaukset jäsennetään tiettyjen tietoturvaloukkausluokkien (esimerkiksi kiristysohjelmahyökkäykset) mukaan. Kussakin tapauksessa tarvitaan tiettyjä lieventäviä toimenpiteitä, kun on kyse tietyntyyppisistä tietoturvaloukkauksista. Näitä toimenpiteitä ei välttämättä toisteta kaikissa analysoiduissa samaan tietoturvaloukkausluokkaan kuuluvissa tapauksissa. Samaan luokkaan kuuluvien tapausten osalta esitetään ainoastaan eroavaisuudet. Sen vuoksi lukijan olisi luettava kaikki tapaukset, jotka ovat merkityksellisiä tietoturvaloukkausluokan kannalta. Näin kaikki tarvittavat toimenpiteet voidaan tunnistaa ja erottaa toisistaan.

15. Tietoturvaloukkauksen sisäinen dokumentointi on velvoite, jonka määräytyminen ei riipu tietoturvaloukkaukseen liittyvistä riskeistä. Se on toteutettava jokaisessa tapauksessa. Jäljempänä esitettyjen tapausten avulla pyritään selventämään sitä, ilmoitetaanko tietoturvaloukkauksesta valvontaviranomaiselle ja niille rekisteröidyille, joihin tietoturvaloukkaus vaikuttaa.

2 KIRISTYSOHJELMAT

16. Yleinen syy tietosuojaloukkausta koskevan ilmoituksen tekemiseen on rekisterinpitäjään kohdistunut kiristysohjelmahyökkäys. Näissä tapauksissa haitallinen koodi salaa henkilötiedot, minkä jälkeen hyökkääjä pyytää rekisterinpitäjältä lunnaita vastineeksi salauksen purkukoodista. Tällainen hyökkäys voidaan yleensä luokitella tietojen käytettävyyteen vaikuttavaksi tietoturvaloukkaukseksi, mutta usein kyseessä voi olla myös tietojen luottamuksellisuuteen vaikuttava tietoturvaloukkaus.

2.1 TAPAUS nro 1: Kiristysohjelma siten, että tapauksessa on käytössä asianmukainen varmuuskopio mutta tietoja ei ole siirretty

Pienen valmistusyrityksen tietokonejärjestelmät joutuivat kiristysohjelmahyökkäyksen kohteeksi. Näihin järjestelmiin tallennetut tiedot oli salattu. Rekisterinpitäjä käytti lepäävän datan salausta. Näin ollen kaikki tiedot, joihin kiristysohjelma pääsi, olivat salatussa muodossa. Käytössä oli uusin salausalgoritmi. Salausavain ei vaarantunut hyökkäyksessä, eli hyökkääjä ei voinut päästä siihen käsiksi eikä käyttää sitä välillisesti. Hyökkääjällä oli näin ollen pääsy ainoastaan salattuihin henkilötietoihin. Hyökkäys ei vaikuttanut myöskään yrityksen sähköpostijärjestelmään eikä asiakasjärjestelmiin, joita käytetään sinne pääsemiseen. Yritys käytti ulkopuolisen kyberturvallisuusyrityksen asiantuntemusta tapauksen selvittämiseen. Käytettävissä oli lokitietoja, joilla jäljitetään kaikki yrityksestä lähtevät tietovirrat (mukaan lukien lähtevä sähköposti). Yrityksen käyttämien havaitsemisjärjestelmien keräämien lokien ja tietojen analysoinnin jälkeen ulkoisen kyberturvayrityksen tukemassa sisäisessä tutkimuksessa todettiin *varmasti*, että hyökkääjä ainoastaan salasi tietoja, ei siirtänyt niitä. Lokitiedoissa ei näkynyt hyökkäyksen aikaista ulospäin suuntautuvaa tietovirtaa. Tietoturvaloukkauksen kohteena olevat henkilötiedot koskivat yrityksen asiakkaita ja työntekijöitä, joita oli yhteensä muutamia kymmeniä henkilöitä. Varmuuskopio oli helposti saatavilla, ja tiedot palautettiin muutaman tunnin kuluttua hyökkäyksestä. Tietoturvaloukkauksesta ei aiheutunut mitään seurauksia rekisterinpitäjän päivittäiselle toiminnalle.

17. Tässä tapauksessa henkilötietojen tietoturvaloukkauksen määritelmästä toteutuivat seuraavat seikat: tietoturvaloukkaus johti tallennettujen henkilötietojen lainvastaiseen muuttamiseen ja luvattomaan pääsyyn tietoihin.

2.1.1 TAPAUS nro 1 – Ennakkotoimenpiteet ja riskinarviointi

18. Kuten kaikkien ulkoisten toimijoiden aiheuttamien riskien kohdalla, kiristysohjelmahyökkäyksen onnistumisen todennäköisyyttä voidaan vähentää huomattavasti tiukentamalla tiedonhallintaympäristön turvallisuutta. Suurin osa näistä tietoturvaloukkauksista voidaan estää varmistamalla, että asianmukaiset organisatoriset, fyysiset ja tekniset turvallisuustoimenpiteet on toteutettu. Esimerkkejä tällaisista toimenpiteistä ovat asianmukainen ohjelmistokorjausten hallinta ja asianmukaisen haittaohjelmien havaitsemisjärjestelmän käyttö. Asianmukaisen, erillisen varmuuskopion avulla voidaan lieventää mahdollisen onnistuneen hyökkäyksen seurauksia. Lisäksi työntekijöille tarkoitettu turvallisuuskoulutus- ja valistusohjelma (SETA-ohjelma) auttaa ehkäisemään ja tunnistamaan tällaisia hyökkäyksiä (luettelo suositeltavista toimenpiteistä on kohdassa 2.5). Näistä toimenpiteistä yksi tärkeimmistä on asianmukainen ohjelmistokorjausten hallinta. Sen avulla varmistetaan, että järjestelmät ovat ajan tasalla ja että käytössä olevien järjestelmien kaikki tunnetut haavoittuvuudet on korjattu. Useimmissa kiristysohjelmahyökkäyksissä nimittäin hyödynnetään tunnettuja haavoittuvuuksia.

19. Riskejä arvioidessaan rekisterinpitäjän olisi tutkittava tietoturvaloukkaus ja yksilöitävä haitallisen koodin tyyppi. Näin voidaan ymmärtää hyökkäyksen mahdolliset seuraukset. Huomioon otettaviin riskeihin kuuluu riski siitä, että tiedot on siirretty jättämättä jälkiä järjestelmien lokitietoihin.

20. Tässä esimerkissä hyökkääjällä oli pääsy henkilötietoihin, jolloin henkilötietoja salatussa muodossa sisältävän tekstin luottamuksellisuus vaarantui. Hyökkääjä ei kuitenkaan voi ainakaan toistaiseksi lukea tai käyttää tietoja, jotka on mahdollisesti siirretty. Rekisterinpitäjän käyttämä salaustekniikka on uusinta tekniikkaa. Salausavain ei vaarantunut, eikä sitä oletettavasti voitu määrittää muillakaan keinoilla. Näin ollen luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat luottamuksellisuusriskit on minimoitu, ellei salauksen ratkomisen kehitys tee salatuista tiedoista tulevaisuudessa luettavia.

21. Rekisterinpitäjän olisi otettava huomioon tietoturvaloukkauksesta henkilöille aiheutuva riski.[10] Tässä tapauksessa vaikuttaa siltä, että rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat riskit johtuvat siitä, että henkilötietoja ei ole saatavilla, mutta henkilötietojen luottamuksellisuus ei vaarannu.[11] Tässä esimerkissä tietoturvaloukkauksen kielteisiä vaikutuksia lievennettiin melko pian tietoturvaloukkauksen jälkeen.

[10] Ohjeita todennäköisesti korkean riskin aiheuttavista käsittelytoimista on saatavilla 29 artiklan mukaisen tietosuojatyöryhmän ohjeissa tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää, ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”, WP 248 rev.01, Euroopan tietosuojaneuvoston hyväksymät ohjeet (https://ec.europa.eu/newsroom/article29/items/611236), s. 9.

[11] Teknisesti tietojen salaukseen kuuluu ”pääsy” alkuperäisiin tietoihin ja kiristysohjelmien tapauksessa alkuperäisten tietojen poistaminen – tietoihin on päästävä kiristysohjelmakoodilla, jotta ne voidaan salata ja alkuperäiset tiedot poistaa. Hyökkääjä voi tehdä kopion alkuperäisistä tiedoista ennen niiden poistamista, mutta henkilötietoja ei aina poimita. Rekisterinpitäjän tutkinnan edetessä voi tulla esiin uusia tietoja, jotka muuttavat tätä arviota. Tietoihin pääsy, joka johtaa henkilötietojen lainvastaiseen tuhoamiseen, häviämiseen, muuttamiseen tai luvattomaan luovuttamiseen taikka rekisteröidylle aiheutuvaan turvallisuusriskiin, myös ilman, että tietoja tulkitaan, voi olla merkitykseltään yhtä vakava kuin tietoihin pääsy tapauksessa, jossa henkilötietoja voidaan tulkita.

Asianmukainen varmuuskopiointijärjestelmä[12] vähentää tietoturvaloukkauksen vaikutusten vakavuutta, ja tässä tapauksessa rekisterinpitäjä pystyi hyödyntämään sitä tehokkaasti.

22. Rekisteröityihin kohdistuvien seurausten vakavuuden osalta voitiin todeta, että seuraukset olivat vähäisiä. Tiedot, joihin tietoturvaloukkaus vaikutti, palautettiin muutamassa tunnissa. Tietoturvaloukkaus ei myöskään vaikuttanut rekisterinpitäjän päivittäiseen toimintaan eikä sillä ollut merkittävää vaikutusta rekisteröityihin (esimerkiksi työntekijöiden maksuihin tai asiakaspyyntöjen käsittelyyn).

2.1.2 TAPAUS nro 1 – Lieventäminen ja velvollisuudet

23. Ilman varmuuskopiota rekisterinpitäjä voi toteuttaa vain vähän toimenpiteitä henkilötietojen katoamisen korjaamiseksi. Lisäksi tiedot on kerättävä uudelleen. Tässä nimenomaisessa tapauksessa hyökkäyksen vaikutuksia voitiin kuitenkin rajoittaa tehokkaasti. Kaikki vaarantuneet järjestelmät palautettiin puhtaaseen tilaan, jossa ei ollut haitallista koodia, haavoittuvuudet korjattiin ja vaarantuneet tiedot palautettiin pian hyökkäyksen jälkeen. Ilman varmuuskopiota tiedot häviävät ja tapauksen vakavuus voi lisääntyä, sillä myös yksilöihin kohdistuvat riskit tai vaikutukset voivat lisääntyä.

24. Tietojen tehokkaan palauttamisen nopeus helposti saatavilla olevasta varmuuskopiosta on keskeinen muuttuja tietoturvaloukkauksen analysoinnissa. Asianmukaisen aikataulun määrittäminen vaarantuneiden tietojen palauttamiseksi riippuu kyseessä olevan tietoturvaloukkauksen yksilöllisistä olosuhteista. Yleisessä tietosuoja-asetuksessa säädetään, että henkilötietojen tietoturvaloukkauksesta on ilmoitettava ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa. Sen vuoksi voidaan todeta, että 72 tunnin määräajan ylittäminen ei missään tapauksessa ole suositeltavaa. Kun käsitellään korkean riskitason tapauksia, jopa tämän määräajan noudattamista voidaan pitää epätyydyttävänä.

25. Tässä tapauksessa rekisterinpitäjä totesi yksityiskohtaisen vaikutustenarvioinnin ja tapauksen reagointiprosessin jälkeen, että tietoturvaloukkaus ei todennäköisesti aiheuta riskiä luonnollisten henkilöiden oikeuksille ja vapauksille, joten ilmoittaminen rekisteröidyille ei ole tarpeen eikä tietoturvaloukkauksesta tarvitse ilmoittaa myöskään valvontaviranomaiselle. Kuten kaikki tietoturvaloukkaukset, se olisi kuitenkin dokumentoitava 33 artiklan 5 kohdan mukaisesti. Organisaation voi myös olla tarpeen päivittää ja korjata organisatorisia ja teknisiä henkilötietojen käsittelyä ja riskinhallintaa koskevia toimenpiteitään ja menettelyjään (tai valvontaviranomainen voi myöhemmin vaatia sitä). Tämän päivityksen ja korjaamisen yhteydessä organisaation olisi tutkittava tietoturvaloukkaus perusteellisesti sekä yksilöitävä sen syyt ja hyökkääjän käyttämät menetelmät. Näin vastaavat tapahtumat voidaan estää tulevaisuudessa.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	X	X

2.2 TAPAUS nro 2: Kiristysohjelma siten, että käytettävissä ei ole asianmukaista varmuuskopiota

[12] Varmuuskopiointimenettelyjen olisi oltava jäsenneltyjä, johdonmukaisia ja toistettavissa. Esimerkkejä varmuuskopiointimenettelyistä ovat 3-2-1-menetelmä ja nk. sukupolvimenetelmä (grandfather-father-son). Kaikki menetelmät olisi aina testattava niiden kattavuuden ja tietojen palauttamisen tehokkuuden varmistamiseksi. Testaus olisi myös toistettava määräajoin ja erityisesti silloin, kun käsittelytoimi tai sen olosuhteet muuttuvat, jotta järjestelmän eheys voidaan varmistaa.

Yksi maatalousyrityksen käyttämistä tietokoneista altistui kiristysohjelmahyökkäykselle, ja hyökkääjä salasi sen tiedot. Yritys käytti ulkopuolisen kyberturvallisuusyrityksen asiantuntemusta verkkonsa seurantaan. Käytettävissä oli lokitietoja, joilla jäljitetään kaikki yrityksestä lähtevät tietovirrat (mukaan lukien lähtevä sähköposti). Lokitietojen ja muiden havaitsemisjärjestelmien keräämien tietojen analysoinnin jälkeen kyberturvallisuusyrityksen tukema sisäinen tutkinta osoitti, että hyökkääjä ainoastaan salasi tiedot, ei siirtänyt niitä. Lokitiedoissa ei näkynyt hyökkäyksen aikaista ulospäin suuntautuvaa tietovirtaa. Tietoturvaloukkauksen kohteena olevat henkilötiedot koskivat yrityksen työntekijöitä ja asiakkaita, joita oli yhteensä muutamia kymmeniä henkilöitä. Tietoturvaloukkaus ei vaikuttanut mihinkään erityisiin tietoryhmiin. Varmuuskopioita ei ollut saatavilla sähköisessä muodossa. Suurin osa tiedoista palautettiin paperisista varmuuskopioista. Tietojen palauttaminen kesti viisi työpäivää ja aiheutti pieniä viivästyksiä tilausten toimittamisessa

2.2.1 TAPAUS nro 2 – Ennakkotoimenpiteet ja riskinarviointi

26. Rekisterinpitäjän olisi pitänyt toteuttaa samat ennakkotoimenpiteet, jotka mainitaan 2.1 ja 2.5 kohdassa. Suurin ero edelliseen tapaukseen verrattuna on sähköisen varmuuskopion ja lepäävän datan salauksen puuttuminen. Tämä johtaa merkittäviin eroihin seuraavissa vaiheissa.

27. Riskejä arvioidessaan rekisterinpitäjän olisi tutkittava soluttautumismenetelmä ja yksilöitävä haitallisen koodin tyyppi, jotta voidaan ymmärtää hyökkäyksen mahdolliset seuraukset. Tässä esimerkissä kiristysohjelma salasi henkilötiedot mutta ei siirtänyt niitä. Näin ollen vaikuttaa siltä, että rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat riskit johtuvat siitä, että henkilötietoja ei ole saatavilla, mutta henkilötietojen luottamuksellisuus ei vaarannu. Palomuurin lokitietojen ja niiden merkityksen perusteellinen tarkastelu on olennaisen tärkeää riskin määrittämisen kannalta. Rekisterinpitäjän olisi pyynnöstä esitettävä näiden tutkimusten tulokset.

28. Rekisterinpitäjän on muistettava, että jos hyökkäys on hienostuneempi, haittaohjelma voi muokata lokitiedostoja ja poistaa jäljet. Näin ollen – koska lokitietoja ei välitetä tai kopioida keskitetylle lokipalvelimelle – edes sellaisen perusteellisen tutkinnan jälkeen, jossa todetaan, että hyökkääjä ei ollut siirtänyt henkilötietoja, rekisterinpitäjä ei voi todeta, että lokitietojen puuttuminen osoittaa, ettei tietoja ole siirretty. Niinpä tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen todennäköisyyttä ei voida täysin sulkea pois.

29. Rekisterinpitäjän olisi arvioitava tämän tietoturvaloukkauksen riskit[13], jos hyökkääjä on päässyt tietoihin käsiksi. Riskinarvioinnin aikana rekisterinpitäjän olisi otettava huomioon myös tietoturvaloukkaukseen liittyvien henkilötietojen luonne, arkaluonteisuus, määrä ja asiayhteys. Tässä tapauksessa tietoturvaloukkaus ei vaikuta erityisiin henkilötietoryhmiin. Lisäksi vaarantuneiden tietojen ja niiden rekisteröityjen määrä, joita asia koskee, on pieni.

30. Tarkkojen tietojen kerääminen luvattomasta pääsystä tietoihin on keskeistä riskitason määrittämiseksi ja uuden tai jatkuvan hyökkäyksen estämiseksi. Jos tiedot olisi kopioitu tietokannasta, se olisi luonnollisesti ollut riskiä lisäävä tekijä. Jos luvattoman tietoihin pääsyn erityispiirteistä ei ole varmuutta, olisi otettava huomioon huonompi skenaario ja riski olisi arvioitava sen mukaisesti.

31. Varmuuskopiotietokannan puuttumista voidaan pitää riskiä lisäävänä tekijänä sen mukaan, kuinka vakavia seurauksia rekisteröidyille aiheutuu siitä, että tietoja ei ole saatavilla.

[13] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

2.2.2 TAPAUS nro 2 – Lieventäminen ja velvollisuudet

32. Ilman varmuuskopiota rekisterinpitäjä voi toteuttaa vain vähän toimenpiteitä henkilötietojen katoamisen korjaamiseksi. Lisäksi tiedot on kerättävä uudelleen, ellei käytettävissä ole muuta lähdettä (esimerkiksi tilausten vahvistussähköpostiviestit). Ilman varmuuskopiota tietoja voidaan menettää, ja vakavuus määräytyy yksilöön kohdistuvan vaikutuksen mukaan.

33. Tietojen palauttamisen ei pitäisi osoittautua liian ongelmalliseksi[14], jos tiedot ovat edelleen saatavilla paperisina. Sähköisen varmuuskopiotietokannan puuttumisen vuoksi ilmoitusta valvontaviranomaiselle pidetään kuitenkin tarpeellisena, koska tietojen palauttaminen vie jonkin aikaa ja saattaa aiheuttaa viivästyksiä tilausten toimittamisessa asiakkaille ja koska huomattavaa määrää metatietoja (esimerkiksi lokitietoja ja aikaleimoja) ei ehkä voida palauttaa.

34. Tietoturvaloukkauksesta ilmoittaminen rekisteröidyille voi riippua myös siitä, kuinka kauan henkilötiedot eivät ole saatavilla, ja tästä kestosta rekisterinpitäjän toiminnalle mahdollisesti aiheutuvista vaikeuksista (esimerkiksi työntekijöiden maksujen siirron viivästymisestä). Koska nämä maksujen ja toimitusten viivästykset voivat aiheuttaa taloudellisia menetyksiä henkilöille, joiden tiedot ovat vaarantuneet, voidaan katsoa, että tietoturvaloukkauksesta aiheutuu todennäköisesti korkea riski. Saattaa myös olla mahdotonta välttää ilmoittamasta rekisteröidyille, jos heidän osallistumistaan tarvitaan salattujen tietojen palauttamiseen.

35. Tämä tapaus toimii esimerkkinä kiristysohjelmahyökkäyksestä, johon liittyy sellainen rekisteröityjen oikeuksiin ja vapauksiin kohdistuva riski, joka ei kuitenkaan ole korkea. Se olisi dokumentoitava 33 artiklan 5 kohdan mukaisesti, ja siitä olisi ilmoitettava valvontaviranomaiselle 33 artiklan 1 kohdan mukaisesti. Organisaation voi myös olla tarpeen päivittää ja korjata organisatorisia ja teknisiä henkilötietojen käsittelyä ja riskinhallintaa koskevia toimenpiteitään ja menettelyjään (tai valvontaviranomainen voi vaatia sitä).

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	X

[14] Tämä määräytyy henkilötietojen monimutkaisuuden ja rakenteen mukaan. Monimutkaisimmissa skenaarioissa tietojen eheyden palauttaminen, johdonmukaisuus metatietojen kanssa, tietorakenteiden sisäisten oikeiden suhteiden varmistaminen ja tietojen oikeellisuuden tarkistaminen voivat vaatia huomattavia määriä resursseja ja työtä.

2.3 TAPAUS nro 3: Kiristysohjelma sairaalassa siten, että tapauksessa on käytössä varmuuskopio mutta tietoja ei ole siirretty

Sairaalan/terveyskeskuksen tietojärjestelmä altistui kiristysohjelmahyökkäykselle, ja hyökkääjä salasi huomattavan osan sen tiedoista. Yritys käytti ulkopuolisen kyberturvallisuusyrityksen asiantuntemusta verkkonsa seurantaan. Käytettävissä oli lokitietoja, joilla jäljitetään kaikki yrityksestä lähtevät tietovirrat (mukaan lukien lähtevä sähköposti). Lokitietojen ja muiden havaitsemisjärjestelmien keräämien tietojen analysoinnin jälkeen kyberturvallisuusyrityksen tukema sisäinen tutkinta osoitti, että hyökkääjä ainoastaan salasi tiedot, ei siirtänyt niitä. Lokitiedoissa ei näkynyt hyökkäyksen aikaista ulospäin suuntautuvaa tietovirtaa. Tietoturvaloukkauksen kohteena olevat henkilötiedot liittyivät työntekijöihin ja potilaisiin, joita oli yhteensä tuhansia henkilöitä. Varmuuskopiot olivat saatavilla sähköisessä muodossa. Suurin osa tiedoista saatiin palautettua, mutta toimenpide kesti kaksi työpäivää ja johti huomattaviin viivästyksiin potilaiden hoidossa. Leikkauksia peruttiin tai lykättiin, ja palvelutaso laski järjestelmien toimimattomuuden vuoksi.

2.3.1 TAPAUS nro 3 – Ennakkotoimenpiteet ja riskinarviointi

36. Rekisterinpitäjän olisi pitänyt toteuttaa samat ennakkotoimenpiteet, jotka mainitaan 2.1 ja 2.5 kohdassa. Suurin ero edelliseen tapaukseen verrattuna on se, että seuraukset ovat erittäin vakavia merkittävälle osalle rekisteröidyistä.[15]

37. Tietoturvaloukkauksen kohteena olevien tietojen määrä ja niiden rekisteröityjen määrä, joihin tietoturvaloukkaus vaikuttaa, on suuri, sillä sairaalat käsittelevät yleensä suuria tietomääriä. Sillä, että tietoja ei ole saatavilla, on suuri vaikutus merkittävään osaan rekisteröityjä. Lisäksi potilastietojen luottamuksellisuuteen kohdistuva riski on erittäin vakava.

38. Tietoturvaloukkauksen tyyppi ja tietoturvaloukkauksen kohteena olevien henkilötietojen luonne, arkaluonteisuus ja määrä ovat tärkeitä. Vaikka tiedot oli varmuuskopioitu ja ne voitiin palauttaa muutamassa päivässä, riski on edelleen korkea, sillä rekisteröidyille aiheutui vakavia seurauksia siitä, että tietoja ei ollut saatavilla hyökkäyshetkellä ja sitä seuraavina päivinä.

2.3.2 TAPAUS nro 3 – Lieventäminen ja velvollisuudet

39. Ilmoitusta valvontaviranomaiselle pidetään tarpeellisena, koska asiaan liittyy erityisiä henkilötietoryhmiä ja tietojen palauttaminen voi kestää kauan, mikä johtaa huomattaviin viivästyksiin potilaiden hoidossa. Tietoturvaloukkauksesta ilmoittaminen rekisteröidyille on tarpeen potilaille aiheutuvien vaikutusten vuoksi myös salattujen tietojen palauttamisen jälkeen. Koska kaikkia sairaalassa viime vuosina hoidettuja potilaita koskevat tiedot on salattu, vaikutukset kohdistuivat ainoastaan niihin potilaisiin, joita oli tarkoitus hoitaa sairaalassa silloin, kun tietokonejärjestelmä ei ollut käytettävissä. Rekisterinpitäjän olisi ilmoitettava tietoturvaloukkauksesta suoraan kyseisille potilaille. Yleisen tietosuoja-asetuksen 34 artiklan 3 kohdan c alakohdassa säädetyn poikkeuksen vuoksi suoraa ilmoitusta muille potilaille, joista osa ei välttämättä ole ollut sairaalassa yli 20 vuoteen, ei ehkä vaadita. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa[16]

[15] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

[16] Yleisen tietosuoja-asetuksen johdanto-osan 86 kappaleessa selitetään, että *”[t]ällainen ilmoitus rekisteröidylle olisi tehtävä niin pian kuin se on kohtuudella mahdollista ja tiiviissä yhteistyössä valvontaviranomaisen kanssa noudattaen*

tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla. Tässä tapauksessa sairaalan olisi julkistettava kiristysohjelmahyökkäys ja sen vaikutukset.

40. Tämä tapaus toimii esimerkkinä kiristysohjelmahyökkäyksestä, johon liittyy rekisteröityjen oikeuksiin ja vapauksiin kohdistuva korkea riski. Se olisi dokumentoitava 33 artiklan 5 kohdan mukaisesti, minkä lisäksi siitä olisi ilmoitettava valvontaviranomaiselle 33 artiklan 1 kohdan mukaisesti ja rekisteröidyille 34 artiklan 1 kohdan mukaisesti. Organisaation on myös päivitettävä ja korjattava organisatorisia ja teknisiä henkilötietojen käsittelyä ja riskinhallintaa koskevia toimenpiteitään ja menettelyjään.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	✓

2.4 TAPAUS nro 4: Kiristysohjelma siten, että tapauksessa ei ole käytössä varmuuskopiota ja tietoja on siirretty

Joukkoliikenneyrityksen palvelin altistui kiristysohjelmahyökkäykselle, ja hyökkääjä salasi palvelimen tiedot. Sisäisen tutkinnan tulosten mukaan hyökkääjä ei ainoastaan salannut tietoja vaan myös siirsi ne. Tietoturvaloukkauksen kohteena olleet tiedot olivat tyypiltään asiakkaiden ja työntekijöiden sekä niiden tuhansien henkilöiden henkilötietoja, jotka käyttivät yrityksen palveluja (esimerkiksi ostamalla lippuja verkossa). Perushenkilötietojen lisäksi tietoturvaloukkaukseen liittyi henkilökorttien numeroita ja taloudellisia tietoja, kuten luottokorttitietoja. Varmuuskopiotietokanta oli olemassa, mutta hyökkääjä salasi myös sen tiedot.

2.4.1 TAPAUS nro 4 – Ennakkotoimenpiteet ja riskinarviointi

41. Rekisterinpitäjän olisi pitänyt toteuttaa samat ennakkotoimenpiteet, jotka mainitaan 2.1 ja 2.5 kohdassa. Vaikka käytössä oli varmuuskopio, hyökkäys vaikutti myös siihen. Jo tämä järjestely herättää kysymyksiä rekisterinpitäjän aiempien tietoteknisten turvallisuustoimenpiteiden laadusta, ja sitä olisi tutkittava tarkemmin tutkinnan aikana. Hyvin suunnitellussa varmuuskopiointijärjestelmässä on tallennettava useita varmuuskopioita turvallisesti siten, ettei niihin pääse käsiksi pääjärjestelmästä, sillä muutoin ne voivat vaarantua samassa hyökkäyksessä. Lisäksi kiristysohjelmahyökkäykset voivat jäädä huomaamatta päiväkausiksi siten, että harvoin käytettyjä tietoja salataan hitaasti. Tämä voi tehdä monista varmuuskopioista hyödyttömiä, joten varmuuskopiot olisi tehtävä säännöllisesti ja eristettävä. Tämä lisäisi palauttamisen todennäköisyyttä, joskin tietojen menetys lisääntyisi.

42. Tämä tietoturvaloukkaus ei koske ainoastaan tietojen käytettävyyttä vaan myös luottamuksellisuutta, sillä hyökkääjä on saattanut muuttaa ja/tai kopioida palvelimen tietoja. Näin ollen tietoturvaloukkauksen tyyppi aiheuttaa korkean riskin.[17]

valvontaviranomaisen tai muiden asiaankuuluvien viranomaisten (kuten lainvalvontaviranomaisten) antamia ohjeita. Esimerkiksi tarve lieventää välittömien haittojen riskiä edellyttää sitä, että rekisteröidyille ilmoitetaan viipymättä, kun taas tarve toteuttaa asianmukaiset toimenpiteet tietoturvaloukkauksen jatkumisen tai vastaavien henkilötietojen tietoturvaloukkausten estämiseksi voivat olla perusteena pidemmälle ilmoitusajalle."

[17] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

43. Henkilötietojen luonne, arkaluonteisuus ja määrä lisäävät riskejä entisestään, koska niiden henkilöiden määrä, joihin vaikutukset kohdistuvat, on suuri, samoin kuin niiden henkilötietojen kokonaismäärä, joihin vaikutukset kohdistuvat. Perushenkilötietojen lisäksi kyse on henkilötodistuksista ja taloudellisista tiedoista, kuten luottokorttitiedoista. Tällaisia tietoja koskeva tietoturvaloukkaus aiheuttaa korkean riskin itsessään ja, jos tietoja käsitellään yhdessä, niitä voidaan käyttää muun muassa identiteettivarkauksiin tai petoksiin.

44. Joko virheellisen palvelinlogiikan tai organisaation valvonnan vuoksi kiristysohjelma vaikutti varmuuskopiotiedostoihin, mikä esti tietojen palauttamisen ja lisäsi riskiä.

45. Tämä tietoturvaloukkaus aiheuttaa korkean riskin henkilöiden oikeuksille ja vapauksille, sillä se voi todennäköisesti aiheuttaa sekä aineellisia (esimerkiksi taloudelliset menetykset siitä, että luottokorttitietoihin kohdistuu vaikutuksia) että aineettomia vahinkoja (esimerkiksi identiteettivarkaus tai petos, joka johtuu luottokorttitietoihin kohdistuvista vaikutuksista).

2.4.2 TAPAUS nro 4 – Lieventäminen ja velvollisuudet

46. Ilmoittaminen rekisteröidyille on olennaisen tärkeää, jotta he voivat toteuttaa tarvittavat toimenpiteet aineellisten vahinkojen välttämiseksi (esimerkiksi kuolettaa luottokorttinsa).

47. Sen lisäksi, että tietoturvaloukkaus dokumentoidaan 33 artiklan 5 kohdan mukaisesti, myös ilmoitus valvontaviranomaiselle on tässä tapauksessa pakollinen (33 artiklan 1 kohta). Lisäksi rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidyille (34 artiklan 1 kohta). Rekisterinpitäjän ilmoitus voidaan tehdä henkilöittäin. Niille henkilöille, joiden yhteystietoja ei ole saatavilla, rekisterinpitäjän olisi tehtävä julkinen ilmoitus esimerkiksi verkkosivustollaan. Tämä edellyttää, että kyseinen ilmoitus ei voi aiheuttaa rekisteröityihin kohdistuvia lisähaittoja. Tapauksessa edellytetään täsmällistä ja selkeää ilmoitusta, joka on selvästi nähtävissä rekisterinpitäjän kotisivulla ja jossa on tarkat viittaukset asianmukaisiin yleisen tietosuoja-asetuksen säännöksiin. Organisaation saattaa myös olla tarpeen päivittää ja korjata organisatorisia ja teknisiä henkilötietojen käsittelyä ja riskinhallintaa koskevia toimenpiteitään ja menettelyjään.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	✓

2.5 Organisatoriset ja tekniset toimenpiteet kiristysohjelmahyökkäysten vaikutusten ehkäisemiseksi tai lieventämiseksi

48. Se, että kiristysohjelmahyökkäys olisi voinut tapahtua, on yleensä merkki yhdestä tai useammasta haavoittuvuudesta rekisterinpitäjän järjestelmässä. Tämä koskee myös kiristysohjelmatapauksia, joissa henkilötiedot on salattu mutta niitä ei ole siirretty. Hyökkäyksen tuloksesta ja seurauksista riippumatta ei voida korostaa riittävästi tietoturvajärjestelmän kattavaa arviointia, jossa painotetaan erityisesti tietotekniikan turvallisuutta. Havaitut puutteet ja turvallisuuden aukot on dokumentoitava, ja niihin on puututtava viipymättä.

49. Suositeltavat toimenpiteet:

(Seuraavien toimenpiteiden luettelo ei ole missään tapauksessa poissulkeva tai kattava. Tavoitteena on pikemminkin tarjota ennaltaehkäisyä koskevia ideoita ja mahdollisia ratkaisuja. Kaikki käsittelytoimet ovat erilaisia, joten rekisterinpitäjän olisi tehtävä päätös siitä, mitkä toimenpiteet sopivat parhaiten kulloiseenkin tilanteeseen.)

- Pidetään palvelinten, asiakaspäätteiden, aktiivisten verkkokomponenttien ja muiden saman lähiverkon laitteiden (mukaan lukien WiFi-laitteet) laiteohjelmistot, käyttöjärjestelmät ja sovellusohjelmistot ajan

tasalla. Varmistetaan asianmukaisten tietoteknisten turvallisuustoimenpiteiden käyttö ja tehokkuus. Pidetään nämä toimenpiteet säännöllisesti ajan tasalla käsittelyn tai olosuhteiden muuttuessa. Tähän kuuluu yksityiskohtaisten lokitietojen säilyttäminen siitä, mitkä ohjelmistokorjaukset on asennettu milläkin aikaleimalla.

- Suunnitellaan ja organisoidaan käsittelyjärjestelmiä ja -infrastruktuuria tietojärjestelmien ja -verkkojen segmentoimiseksi tai eristämiseksi, jotta vältetään haittaohjelmien leviäminen organisaation sisällä ja ulkoisiin järjestelmiin.
- Ylläpidetään ajantasaista, turvallista ja testattua varmuuskopiointimenettelyä. Keskipitkän ja pitkän aikavälin varmuuskopiointivälineet olisi pidettävä erillään tallennetuista operatiivisista tiedoista ja kolmansien osapuolten ulottumattomissa myös siinä tapauksessa, että hyökkäys onnistuu (kuten päivittäinen lisävarmuuskopiointi ja viikoittainen täysi varmuuskopiointi).
- Hankitaan asianmukaiset, ajantasaiset, tehokkaat ja integroidut haittaohjelmien torjuntaohjelmistot.
- Hankitaan asianmukainen, ajantasainen, tehokas ja integroitu palomuuri ja tunkeutumisen havaitsemis- ja ehkäisyjärjestelmä. Verkkoliikenne ohjataan palomuurin tai hyökkäysten havaitsemisen kautta, myös kotitoimistossa tai liikkuvassa työssä (esimerkiksi käyttämällä VPN-yhteyksiä organisaation turvallisuusmekanismeihin internetiä käytettäessä).
- Koulutetaan työntekijöitä tietoteknisten hyökkäysten tunnistamisessa ja ehkäisemisessä. Rekisterinpitäjän olisi tarjottava keinot, joilla voidaan määrittää, ovatko muilla viestintävälineillä saadut sähköpostiviestit ja muut viestit aitoja ja luotettavia. Työntekijät olisi koulutettava tunnistamaan, milloin tällainen hyökkäys on toteutunut, miten päätepistelaite poistetaan verkosta ja miten heidän on ilmoitettava siitä välittömästi turvallisuusvastaavalle.
- Korostetaan tarvetta määrittää haitallisen koodin tyyppi, jotta voidaan havaita hyökkäyksen seuraukset ja löytää oikeat toimenpiteet riskin lieventämiseksi. Jos kiristysohjelmahyökkäys on onnistunut eikä käytettävissä ole varmuuskopiota, tietojen palauttamiseen voidaan käyttää esimerkiksi No More Ransom -hankkeen (nomoreransom.org) tarjoamia välineitä. Jos käytettävissä kuitenkin on turvallinen varmuuskopio, on suositeltavaa palauttaa tiedot siitä.
- Välitetään tai kopioidaan kaikki lokitiedot keskitetylle lokipalvelimelle (mahdollisesti mukaan lukien lokimerkintöjen allekirjoittaminen tai salausaikaleimaus).
- Käytetään vahvaa salausta ja monivaiheista todentamista, erityisesti kun on kyse hallinnollisesta pääsystä tietojärjestelmiin sekä asianmukaisesta avainten ja salasanojen hallinnasta.
- Testataan haavoittuvuutta ja tietoturvallisuuden tasoa säännöllisesti.
- Perustetaan organisaation sisälle tietoturvaloukkauksiin reagoiva ja niitä tutkiva yksikkö (CSIRT) tai tietotekniikan kriisiryhmä (CERT) tai liitytään yhteiseen CSIRT- tai CERT-ryhmään. Laaditaan häiriötilanteisiin reagoimista koskeva suunnitelma, palautumissuunnitelma ja toiminnan jatkuvuussuunnittelu ja varmistetaan, että ne testataan perusteellisesti.
- Myös riskianalyysi olisi tarkistettava, testattava ja saatettava ajan tasalle vastatoimenpiteitä arvioitaessa.

3 TIETOJENSIIRTOHYÖKKÄYKSET

50. Hyökkäykset, joissa hyödynnetään rekisterinpitäjän kolmansille osapuolille internetissä tarjoamien palvelujen haavoittuvuuksia, esimerkiksi injektiohyökkäysten (kuten SQL-injektointi ja hakemistopuun läpikulku (path traversal), verkkosivuston vaarantamisen ja vastaavien menetelmien avulla, voivat muistuttaa kiristysohjelmahyökkäyksiä siten, että riski aiheutuu luvattoman kolmannen osapuolen toiminnasta. Näillä hyökkäyksillä pyritään kuitenkin tavallisesti kopioimaan, siirtämään ja väärinkäyttämään henkilötietoja johonkin haitalliseen tarkoitukseen. Näin ollen kyse on pääasiassa luottamuksellisuuden ja mahdollisesti myös tietojen eheyden loukkauksista. Jos rekisterinpitäjä on tietoinen tällaisten tietoturvaloukkausten

ominaispiirteistä, käytettävissä on useita toimenpiteitä, joilla voidaan merkittävästi vähentää hyökkäyksen onnistumisen riskiä.

3.1 TAPAUS nro 5: Työhakemuksia koskevien tietojen siirtäminen verkkosivustolta

Työvoimatoimisto joutui kyberhyökkäyksen kohteeksi: hyökkäys asetti työvoimatoimiston verkkosivustolle haitallisen koodin. Tämä haitallinen koodi mahdollisti sen, että verkossa olevilla työnhakulomakkeilla toimitetut, verkkopalvelimelle tallennetut henkilötiedot olivat asiaankuulumattomien henkilöiden saatavilla. Vaikutukset olivat voineet kohdistua 213 tällaiseen lomakkeeseen. Niiden tietojen analysoinnin jälkeen, joihin tietoturvaloukkaus vaikuttaa, todettiin, ettei tietoturvaloukkaus vaikuttanut mihinkään erityisiin tietoryhmiin. Asennetussa haittaohjelmatyökalusarjassa oli toimintoja, joiden avulla hyökkääjä pystyi poistamaan kaiken

3.1.1 TAPAUS nro 5 – Ennakkotoimenpiteet ja riskinarviointi

51. Rekisterinpitäjän ympäristön turvallisuus on erittäin tärkeää. Suurin osa näistä tietoturvaloukkauksista voidaan estää varmistamalla, että kaikkia järjestelmiä päivitetään jatkuvasti, arkaluonteiset tiedot salataan ja sovellukset kehitetään tiukkojen turvallisuusstandardien mukaisesti käyttämällä muun muassa vahvaa todentamista, väsytyshyökkäysten torjuntatoimenpiteitä sekä käyttäjän syötteiden ”keskeyttämistä” (escaping) tai ”sanitointia”[18]. Tällaisten haavoittuvuuksien havaitseminen ja korjaaminen edellyttää myös määräaikaisia tietoturvatarkastuksia, haavoittuvuusarviointeja ja koehyökkäyksiä. Tässä nimenomaisessa tapauksessa tuotantoympäristön tiedostojen eheyden seurantavälineet olisivat saattaneet auttaa havaitsemaan koodin injektoinnin (luettelo suositeltavista toimenpiteistä on kohdassa 3.7).

52. Rekisterinpitäjän olisi aina aloitettava tietoturvaloukkauksen tutkiminen määrittämällä hyökkäyksen tyyppi ja menetelmät. Näin voidaan arvioida, mitä toimenpiteitä on toteutettava. Jotta määrittäminen olisi nopeaa ja tehokasta, rekisterinpitäjällä olisi oltava käytössä häiriötilanteisiin reagoimista koskeva suunnitelma, jossa yksilöidään nopeat tarvittavat toimenpiteet häiriön hallitsemiseksi. Tässä nimenomaisessa tapauksessa tietoturvaloukkauksen tyyppi oli riskiä lisäävä tekijä, sillä sen lisäksi, että tietojen luottamuksellisuutta rajoitettiin, hyökkääjällä oli keinot tehdä muutoksia järjestelmään, joten myös tietojen eheys muuttui kyseenalaiseksi.

53. Tietoturvaloukkauksen kohteena olevien henkilötietojen luonne, arkaluonteisuus ja määrä olisi arvioitava sen määrittämiseksi, missä määrin tietoturvaloukkaus vaikutti rekisteröityihin. Vaikka vaikutukset eivät kohdistuneet erityisiin henkilötietoryhmiin, niihin tietoihin, joihin päästiin käsiksi, sisältyi huomattavia määriä henkilöiden verkkolomakkeissa olleita tietoja. Näitä tietoja voitaisiin käyttää väärin monin tavoin (muun muassa ei-toivottuun markkinointiin ja identiteettivarkauksiin), joten seurausten vakavuuden pitäisi lisätä rekisteröityjen oikeuksiin ja vapauksiin kohdistuvaa riskiä.[19]

3.1.2 TAPAUS nro 5 – Lieventäminen ja velvollisuudet

54. Ongelman ratkaisemisen jälkeen tietokantaa olisi mahdollisuuksien mukaan verrattava suojattuun varmuuskopioon tallennettuun tietokantaan. Tietoturvaloukkauksesta saatuja kokemuksia olisi hyödynnettävä tietoteknisen infrastruktuurin päivittämisessä. Rekisterinpitäjän olisi palautettava kaikki

[18] Käyttäjien syötteiden keskeyttäminen tai sanitointi on syötteiden validoinnin muoto, jolla varmistetaan, että tietojärjestelmään syötetään ainoastaan asianmukaisesti muotoiltuja tietoja.

[19] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

asianomaiset tietotekniset järjestelmät puhtaaseen tilaan, korjattava haavoittuvuus ja toteutettava uusia turvallisuustoimenpiteitä, kuten tiedostojen eheystarkastuksia ja tietoturvatarkastuksia, vastaavien tietoturvaloukkausten välttämiseksi tulevaisuudessa. Jos henkilötietoja ei ole ainoastaan siirretty vaan myös poistettu, rekisterinpitäjän on ryhdyttävä järjestelmällisiin toimiin henkilötietojen palauttamiseksi siihen tilaan, jossa ne olivat ennen tietoturvaloukkausta. Saattaa olla tarpeen käyttää täydellisiä varmuuskopioita ja lisäysmuutoksia ja viimeisimmän lisäyskopioinnin jälkeen mahdollisesti toteuttaa käsittely uudelleen. Tämä edellyttää, että rekisterinpitäjä pystyy toistamaan viimeisimmän varmuuskopion jälkeen tehdyt muutokset. Tämä saattaa edellyttää, että rekisterinpitäjällä on järjestelmä, joka on suunniteltu säilyttämään päivittäiset syöttötiedostot siltä varalta, että niitä on käsiteltävä uudelleen. Lisäksi se edellyttää vankkaa säilytysmenetelmää ja sopivaa säilytyskäytäntöä.

55. Edellä esitetyn perusteella ja koska tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisteröidyille olisi ehdottomasti ilmoitettava siitä (34 artiklan 1 kohta). Tämä tarkoittaa tietenkin sitä, että myös asianomainen valvontaviranomainen (tai asianomaiset valvontaviranomaiset) olisi otettava mukaan lähettämällä sille (tai niille) tietoturvaloukkausta koskeva ilmoitus. Tietoturvaloukkauksen dokumentointi on yleisen tietosuoja-asetuksen 33 artiklan 5 kohdan mukaisesti pakollista, ja se helpottaa tilanteen arviointia.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	✓

3.2 TAPAUS nro 6: Hajautetun salasanan siirtäminen verkkosivustolta

Ruoanlaittosivuston palvelimen tietokantaan pääsemiseksi hyödynnettiin SQL-injektiohaavoittuvuutta. Käyttäjät saivat valita käyttäjänimiksi ainoastaan satunnaisia salanimiä. Sähköpostiosoitteiden käyttöä tähän tarkoitukseen ei suositeltu. Tietokantaan tallennetut salasanat oli hajautettu vahvalla algoritmilla, eikä suola vaarantunut. Tietoturvaloukkaus vaikutti 1 200 käyttäjän hajautettuihin salasanoihin. Turvallisuuden vuoksi rekisterinpitäjä ilmoitti rekisteröidyille tietoturvaloukkauksesta sähköpostitse ja pyysi heitä vaihtamaan salasanansa, erityisesti jos he

3.2.1 TAPAUS nro 6 – Ennakkotoimenpiteet ja riskinarviointi

56. Tässä nimenomaisessa tapauksessa tietojen luottamuksellisuus on vaarantunut mutta tietokannan salasanat on hajautettu ajantasaisella menetelmällä. Tämä vähentäisi henkilötietojen luonteeseen, arkaluonteisuuteen ja määrään liittyvää riskiä. Tämä tapaus ei aiheuta rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä.

57. Lisäksi rekisteröityjen yhteystietoja (esimerkiksi sähköpostiosoitteita tai puhelinnumeroita) ei vaarannettu. Niinpä rekisteröityjen kannalta ei ole merkittävää riskiä siitä, että he joutuisivat petosyritysten (esimerkiksi verkkourkintasähköpostien tai vilpillisten tekstiviestien tai puhelujen) kohteiksi. Tietoturvaloukkaukseen ei liittynyt erityisiä henkilötietoryhmiä.

58. Joitakin käyttäjänimiä voidaan pitää henkilötietoina, mutta verkkosivuston aihe ei johda kielteisiin mielleyhtymiin. On kuitenkin huomattava, että riskinarviointi voi muuttua[20], jos verkkosivuston tyyppi ja saatavilla olevat tiedot voivat paljastaa erityisiä henkilötietoryhmiä (esimerkiksi poliittisen puolueen tai ammattiliiton verkkosivusto). Uusimman tekniikan mukainen salaus voisi lieventää tietoturvaloukkauksen

[20] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

haitallisia vaikutuksia. Sen varmistaminen, että kirjautumisyrityksiä sallitaan ainoastaan rajoitettu määrä, estää väsytyskirjautumishyökkäyksen onnistumisen ja vähentää näin suurelta osin riskejä, joita käyttäjätunnukset tuntevat hyökkääjät aiheuttavat.

3.2.2 TAPAUS nro 6 – Lieventäminen ja velvollisuudet

59. Rekisteröidyille ilmoittamista voitaisiin joissakin tapauksissa pitää lieventävänä tekijänä, koska rekisteröidyillä on mahdollisuus toteuttaa tarvittavat toimenpiteet tietoturvaloukkauksesta aiheutuvien lisävahinkojen välttämiseksi esimerkiksi vaihtamalla salasanansa. Tässä tapauksessa ilmoittaminen ei ollut pakollista, mutta sitä voidaan pitää hyvänä käytäntönä monissa tapauksissa.

60. Rekisterinpitäjän olisi korjattava haavoittuvuus ja toteutettava uusia turvallisuustoimenpiteitä, kuten verkkosivuston järjestelmälliset turvallisuustarkastukset, vastaavien tietoturvaloukkausten välttämiseksi tulevaisuudessa.

61. Tietoturvaloukkaus on dokumentoitava 33 artiklan 5 kohdan mukaisesti, mutta siitä ei tarvitse ilmoittaa.

62. On erittäin suositeltavaa ilmoittaa salasanoihin liittyvästä tietoturvaloukkauksesta rekisteröidyille joka tapauksessa myös silloin, kun salasanoja on tallennettu käyttämällä suolattua tiivistettä, jossa on uusimman tekniikan mukainen algoritmi. On suositeltavaa käyttää todentamismenetelmiä, joiden avulla salasanoja ei tarvitse käsitellä palvelinpuolella. Rekisteröidyille olisi annettava mahdollisuus toteuttaa omia salasanojaan koskevat asianmukaiset toimenpiteet.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	X	X

3.3 TAPAUS nro 7: Pankin verkkosivustoon kohdistuva kirjautumistietojen täyttöhyökkäys

Pankkiin kohdistui kyberhyökkäys yhtä sen verkkopankkisivustoa vastaan. Hyökkäyksen tarkoituksena oli luetella kaikki mahdolliset käyttäjien kirjautumistunnukset, joissa käytettiin kiinteää triviaalia salasanaa. Salasanoissa oli kahdeksan numeroa. Verkkosivuston haavoittuvuuden vuoksi hyökkääjä sai joissakin tapauksissa tietoja rekisteröidyistä (etu- ja sukunimi, sukupuoli, syntymäaika ja -paikka, verotunnus sekä käyttäjätunnukset), vaikka käytetty salasana ei ollut oikea tai pankkitili ei ollut enää aktiivinen. Tämä koski noin 100 000:ta rekisteröityä. Hyökkääjä kirjautui onnistuneesti noin 2 000 tilille, jotka käyttivät hyökkääjän kokeilemaa triviaalia salasanaa. Tämän jälkeen rekisterinpitäjä pystyi tunnistamaan kaikki laittomat kirjautumisyritykset. Rekisterinpitäjä pystyi vahvistamaan, että petostentorjuntatarkastusten mukaan näillä tileillä ei tehty tapahtumia hyökkäyksen aikana. Pankki oli tietoinen tietoturvaloukkauksesta, koska sen turvallisuuskeskus havaitsi suuren määrän sivustolle kohdistuvia sisäänkirjautumispyyntöjä. Vastauksena rekisterinpitäjä poisti mahdollisuuden kirjautua verkkosivustolle kytkemällä sen pois päältä ja pakotti ne tilit, joiden salasanat olivat vaarantuneet, vaihtamaan salasanaa. Rekisterinpitäjä ilmoitti tietoturvaloukkauksesta ainoastaan niille käyttäjille, joiden tilit olivat vaarantuneet, eli niille

3.3.1 TAPAUS nro 7 – Ennakkotoimenpiteet ja riskinarviointi

63. On tärkeää mainita, että erittäin henkilökohtaisia tietoja[21] käsittelevillä rekisterinpitäjillä on suurempi vastuu riittävän tietoturvan takaamisesta, esimerkiksi turvallisuuskeskuksen ja muiden häiriöiden ehkäisy-, havaitsemis- ja vastaustoimenpiteiden toteuttamisesta. Näiden tiukempien vaatimusten noudattamatta jättäminen johtaa varmasti vakavampiin toimenpiteisiin valvontaviranomaisen tutkinnan aikana.

64. Tietoturvaloukkaus koskee henkilöllisyys- ja käyttäjätunnustietojen lisäksi myös muita taloudellisia tietoja, minkä vuoksi se on erityisen vakava. Vaikutusten kohteena olevien henkilöiden määrä on suuri.

65. Se, että tietoturvaloukkaus saattoi tapahtua näin arkaluonteisessa ympäristössä, viittaa merkittäviin tietoturva-aukkoihin rekisterinpitäjän järjestelmässä. Se voi olla osoitus siitä, että asianomaiset toimenpiteet tulee tarkistaa ja päivittää yleisen tietosuoja-asetuksen 24 artiklan 1 kohdan, 25 artiklan 1 kohdan ja 32 artiklan 1 kohdan mukaisesti. Tietoturvaloukkauksen kohteena olevat tiedot mahdollistavat rekisteröityjen yksilöllisen tunnistamisen ja sisältävät muita tietoja heistä (mukaan lukien sukupuoli sekä syntymäaika ja -paikka). Lisäksi hyökkääjä voi käyttää niitä arvatakseen asiakkaiden salasanat tai toteuttaakseen pankin asiakkaille suunnatun kohdennetun verkkourkintakampanjan.

66. Näistä syistä tietoturvaloukkauksen katsottiin todennäköisesti aiheuttavan korkean riskin kaikkien asianomaisten rekisteröityjen oikeuksille ja vapauksille.[22] Näin ollen mahdollisia seurauksia ovat aineelliset (esimerkiksi taloudelliset tappiot) ja aineettomat vahingot (esimerkiksi identiteettivarkaudet tai petokset).

3.3.2 TAPAUS nro 7 – Lieventäminen ja velvollisuudet

67. Tapauskuvauksessa mainitut rekisterinpitäjän toimenpiteet ovat riittäviä. Tietomurron jälkeen rekisterinpitäjä korjasi verkkosivuston haavoittuvuuden ja ryhtyi muihin toimiin estääkseen vastaavat tietoturvaloukkaukset tulevaisuudessa, kuten lisäämällä kaksivaiheisen todennuksen kyseiselle verkkosivustolle ja siirtymällä vahvaan asiakastodennukseen.

68. Yleisen tietosuoja-asetuksen 33 artiklan 5 kohdan mukainen tietoturvaloukkauksen dokumentointi ja siitä ilmoittaminen valvontaviranomaiselle eivät ole tässä skenaariossa vapaaehtoisia. Lisäksi rekisterinpitäjän olisi ilmoitettava asiasta yleisen tietosuoja-asetuksen 34 artiklan mukaisesti kaikille 100 000 rekisteröidylle (mukaan lukien rekisteröidyt, joiden tilit eivät vaarantuneet).

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	✓

3.4 Organisatoriset ja tekniset toimenpiteet hakkerihyökkäysten vaikutusten ehkäisemiseksi tai lieventämiseksi

69. Samoin kuin kiristysohjelmahyökkäyksissä, rekisterinpitäjien on vastaavissa tapauksissa pakollista arvioida tietoteknistä turvallisuutta uudelleen hyökkäyksen tuloksesta ja seurauksista riippumatta.

[21] Tällaisia ovat esimerkiksi rekisteröityjen tiedot, jotka liittyvät maksutapoihin, kuten korttinumeroihin, pankkitileihin, verkkomaksuihin, palkkalistoihin, tiliotteisiin, taloustutkimuksiin tai muihin tietoihin, jotka voivat paljastaa rekisteröityihin liittyviä taloudellisia tietoja.

[22] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

70. Suositeltavat toimenpiteet[23]:

(*Seuraavien toimenpiteiden luettelo ei ole missään tapauksessa poissulkeva tai kattava. Tavoitteena on pikemminkin tarjota ennaltaehkäisyä koskevia ideoita ja mahdollisia ratkaisuja. Kaikki käsittelytoimet ovat erilaisia, joten rekisterinpitäjän olisi tehtävä päätös siitä, mitkä toimenpiteet sopivat parhaiten kulloiseenkin tilanteeseen.*)

- Käytetään uusimman tekniikan mukaista salausta ja avainten hallintaa, erityisesti kun käsitellään salasanoja taikka arkaluonteisia tai taloudellisia tietoja. Salaisten tietojen (salasanojen) kryptografinen hajauttaminen ja suolaaminen on aina suositeltavampaa kuin salasanojen salaus. On suositeltavaa käyttää todentamismenetelmiä, joiden avulla salasanoja ei tarvitse käsitellä palvelinpuolella.
- Pidetään järjestelmä (ohjelmistot ja laiteohjelmistot) ajan tasalla. Varmistetaan kaikkien tietoteknisten turvallisuustoimenpiteiden käyttö ja tehokkuus. Pidetään nämä toimenpiteet säännöllisesti ajan tasalla käsittelyn tai olosuhteiden muuttuessa. Pystyäkseen osoittamaan 5 artiklan 1 kohdan f alakohdan noudattamisen yleisen tietosuoja-asetuksen 5 artiklan 2 kohdan mukaisesti rekisterinpitäjän olisi pidettävä kirjaa kaikista tehdyistä päivityksistä, myös ajankohdasta, jolloin päivitykset tehtiin.
- Käytetään vahvoja todentamismenetelmiä, kuten kaksivaiheista todentamista ja todentamispalvelimia, joita täydennetään ajantasaisella salasanakäytännöllä.
- Sisällytetään turvallisiin kehittämisstandardeihin käyttäjän syötteiden suodattaminen (käyttäen mahdollisuuksien mukaan valkolistaamista), käyttäjien syötteiden keskeyttäminen ja väsytyshyökkäysten ehkäisytoimenpiteet (kuten uudelleenyritysten enimmäismäärän rajoittaminen). Verkkosovellusten palomuurit voivat auttaa tämän tekniikan tehokkaassa käytössä.
- Käytetään vahvoja käyttäjäoikeuksia ja käytönvalvontakäytäntöä.
- Käytetään asianmukaisia, ajantasaisia, tehokkaita ja integroituja palomuureja, tunkeutumisen havaitsemisjärjestelmiä ja muita ympäryspuolustusjärjestelmiä.
- Tehdään järjestelmällisiä tietoteknisiä turvallisuustarkastuksia ja haavoittuvuusarviointeja (penetraatiotestaus).
- Tehdään säännöllisiä tarkistuksia ja testejä sen varmistamiseksi, että varmuuskopioita voidaan käyttää sellaisten tietojen palauttamiseen, joiden eheys tai käytettävyys on heikentynyt.
- Ei käytetä URL-osoitteessa selväkielitekstinä olevaa istuntotunnistetta.

4 SISÄINEN INHIMILLINEN RISKINLÄHDE

71. Inhimillisten virheiden merkitystä henkilötietojen tietoturvaloukkauksissa on korostettava, sillä ne ovat yleisiä. Koska tämäntyyppiset tietoturvaloukkaukset voivat olla sekä tahallisia että tahattomia, rekisterinpitäjien on hyvin vaikea tunnistaa haavoittuvuudet ja toteuttaa toimenpiteitä niiden välttämiseksi. Kansainvälinen tietosuojaviranomaisten maailmankokous on tunnustanut, että tällaisiin inhimillisiin tekijöihin on tärkeää puuttua. Se hyväksyi lokakuussa 2019 päätöslauselman[24], jossa käsitellään inhimillisen virheen merkitystä henkilötietojen tietoturvaloukkauksissa. Päätöslauselmassa korostetaan, että olisi

[23] Suojattujen verkkosovellusten kehittämisestä on saatavilla tietoja osoitteessa https://www.owasp.org/index.php/Main_Page

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

toteutettava asianmukaisia suojatoimenpiteitä inhimillisten virheiden ehkäisemiseksi. Lisäksi siinä esitetään ei-tyhjentävä luettelo tällaisista suojatoimista ja lähestymistavoista.

4.1 TAPAUS nro 8: Työntekijän toteuttama yritystietojen siirtäminen

Yrityksen työntekijä kopioi irtisanomisaikanaan liiketoimintatietoja yrityksen tietokannasta. Työntekijällä oli oikeus tutustua tietoihin ainoastaan tehtäviensä hoitamista varten. Kuukausia myöhemmin, lopetettuaan yrityksessä työskentelyn, hän käytti näin saamiaan tietoja (perusyhteystietoja) uudessa tietojenkäsittelyssä, jonka rekisterinpitäjänä hän toimi, ottaakseen yhteyttä yrityksen asiakkaisiin ja houkutellakseen heidät uuteen yritykseensä.

4.1.1 TAPAUS nro 8 – Ennakkotoimenpiteet ja riskinarviointi

72. Tässä nimenomaisessa tapauksessa ei toteutettu mitään ennakkotoimenpiteitä sen estämiseksi, että työntekijä voisi kopioida yrityksen asiakaskunnan yhteystietoja. Työntekijä tarvitsi laillisen pääsyn näihin tietoihin työtehtäviään varten, ja hänellä oli tällainen pääsy. Koska useimpien asiakassuhteiden hoitaminen edellyttää työntekijöiden pääsyä henkilötietoihin, näitä tietoturvaloukkauksia voi olla kaikkein vaikeinta ehkäistä. Pääsyn laajuutta koskevat rajoitukset voivat rajoittaa työtä, jota kyseinen työntekijä voi tehdä. Hyvin harkitut käyttökäytännöt ja jatkuva valvonta voivat kuitenkin auttaa estämään tällaisia tietoturvaloukkauksia.

73. Kuten tavallista, riskinarvioinnissa on otettava huomioon tietoturvaloukkauksen tyyppi sekä tietoturvaloukkauksen kohteena olevien henkilötietojen luonne, arkaluonteisuus ja määrä. Tällaiset tietoturvaloukkaukset ovat tavallisesti luottamuksellisuuteen kohdistuvia tietoturvaloukkauksia, sillä tietokanta jätetään yleensä ennalleen ja sen sisältö ”ainoastaan” kopioidaan myöhempää käyttöä varten. Tietojen määrä on yleensä vähäinen tai keskisuuri. Tässä nimenomaisessa tapauksessa tietoturvaloukkaus ei vaikuttanut erityisiin henkilötietoryhmiin, vaan työntekijä ainoastaan tarvitsi asiakkaiden yhteystietoja ottaakseen heihin yhteyttä yrityksestä poistuttuaan. Näin ollen kyseiset tiedot eivät ole arkaluonteisia.

74. Vaikka tietoja pahantahtoisesti kopioineen entisen työntekijän ainoa tavoite saattaa rajoittua yrityksen asiakaskunnan yhteystietojen hankkimiseen työntekijän omia kaupallisia tarkoituksia varten, rekisterinpitäjä ei voi pitää rekisteröityihin kohdistuvaa riskiä vähäisenä, koska rekisterinpitäjällä ei ole minkäänlaista varmuutta työntekijän aikeista. Vaikka tietoturvaloukkauksen seuraukset saattaisivat rajoittua entisen työntekijän asiattomaan itsemarkkinointiin, varastettujen tietojen myöhempi ja vakavampi väärinkäyttö ei ole poissuljettua riippuen entisen työntekijän toteuttaman käsittelyn tarkoituksesta.[25]

4.1.2 TAPAUS nro 8 – Lieventäminen ja velvollisuudet

75. Tietoturvaloukkauksen haitallisten vaikutusten lieventäminen edellä mainitussa tapauksessa on vaikeaa. Se saattaa edellyttää välittömiä oikeustoimia, joilla estetään entistä työntekijää käyttämästä tietoja väärin ja levittämästä niitä edelleen. Seuraavaksi olisi pyrittävä välttämään vastaavia tilanteita tulevaisuudessa. Rekisterinpitäjä voi yrittää määrätä entisen työntekijän lopettamaan tietojen käytön, mutta tämän toimenpiteen onnistuminen on parhaimmillaankin kyseenalaista. Asianmukaiset tekniset toimenpiteet, kuten tietojen kopioinnin tai lataamisen mahdottomuus irrotettaville laitteille, voivat auttaa.

76. Tällaisiin tapauksiin ei ole olemassa yhtä ainoaa ratkaisua, mutta järjestelmällinen lähestymistapa voi auttaa ehkäisemään niitä. Yritys voi esimerkiksi harkita mahdollisuuksien mukaan tiettyjen käyttöoikeuksien peruuttamista työntekijöiltä, jotka ovat ilmoittaneet aikomuksestaan irtisanoutua, tai käyttölokien

[25] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

käyttöönottoa, jotta ei-toivottu käyttö voidaan kirjata ja merkitä. Työntekijöiden kanssa allekirjoitetussa sopimuksessa olisi oltava lausekkeita, jotka kieltävät tällaiset toimet.

77. Koska kyseinen tietoturvaloukkaus ei aiheuta korkeaa riskiä luonnollisten henkilöiden oikeuksille ja vapauksille, ilmoitus valvontaviranomaiselle riittää. Rekisteröidyille ilmoittamisesta voi kuitenkin olla hyötyä myös rekisterinpitäjälle, sillä saattaa olla parempi, että he kuulevat tietovuodosta yritykseltä kuin entiseltä työntekijältä, joka yrittää ottaa heihin yhteyttä. Tietoturvaloukkauksen dokumentointi 33 artiklan 5 kohdan mukaisesti on oikeudellinen velvoite.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	X

4.2 TAPAUS nro 9: Tietojen tahaton välittäminen luotetulle kolmannelle osapuolelle

Eräs vakuutusasiamies huomasi, että sähköpostitse saamansa Excel-tiedoston virheellisten asetusten ansiosta hän pääsi käsiksi noin 20 asiakkaan tietoihin, jotka eivät liittyneet hänen työtehtäviinsä. Häntä sitoi salassapitovelvollisuus, ja hän oli sähköpostin ainoa vastaanottaja. Rekisterinpitäjän ja vakuutusasiamiehen välinen järjestely velvoitti vakuutusasiamiehen ilmoittamaan henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä. Näin ollen vakuutusasiamies ilmoitti välittömästi virheestä rekisterinpitäjälle, joka korjasi tiedoston ja lähetti sen uudelleen sekä pyysi vakuutusasiamiestä poistamaan aiemman viestin. Edellä mainitun järjestelyn mukaan vakuutusasiamiehen oli vahvistettava poisto kirjallisella lausunnolla, minkä hän teki. Saadut tiedot eivät sisältäneet erityisiä henkilötietoryhmiä vaan ainoastaan yhteystietoja ja itse vakuutusta koskevia tietoja (vakuutustyyppi ja -määrä). Analysoituaan henkilötiedot, joihin tietoturvaloukkaus vaikutti, rekisterinpitäjä ei havainnut henkilöiden tai rekisterinpitäjän osalta mitään sellaisia erityispiirteitä, jotka voisivat vaikuttaa

4.2.1 TAPAUS nro 9 – Ennakkotoimenpiteet ja riskinarviointi

78. Tässä tapauksessa tietoturvaloukkaus ei johdu työntekijän tahallisesta toiminnasta vaan tahattomasta inhimillisestä virheestä, joka johtuu tarkkaamattomuudesta. Tällaiset tietoturvaloukkaukset voidaan välttää tai niiden esiintymistiheyttä voidaan vähentää a) toteuttamalla koulutus- ja valistusohjelmia, jotta työntekijät ymmärtävät paremmin henkilötietojen suojan merkityksen, b) vähentämällä sähköpostitse tapahtuvaa tiedostojen vaihtoa ja käyttämällä sen sijaan esimerkiksi asiakastietojen käsittelyyn tarkoitettuja järjestelmiä, c) tarkistamalla tiedostot kahdesti ennen niiden lähettämistä taikka d) erottamalla tiedostojen luominen ja lähettäminen toisistaan.

79. Tämä tietoturvaloukkaus koskee ainoastaan tietojen luottamuksellisuutta. Niiden eheys ja käytettävyys pysyvät muuttumattomina. Tietoturvaloukkaus koski ainoastaan noin 20:tä käyttäjää, joten tietojen määrää, johon se vaikuttaa, voidaan pitää vähäisenä. Kyseiset henkilötiedot eivät myöskään sisältäneet arkaluonteisia tietoja. Sitä, että henkilötietojen käsittelijä otti välittömästi yhteyttä rekisterinpitäjään saatuaan tiedon tietoturvaloukkauksesta, voidaan pitää riskiä lieventävänä tekijänä (olisi myös arvioitava, onko tietoja mahdollisesti lähetetty muille vakuutusasiamiehille, ja jos se vahvistetaan, olisi ryhdyttävä asianmukaisiin toimenpiteisiin). Koska tietoturvaloukkauksen jälkeen on toteutettu asianmukaiset toimenpiteet, sillä ei todennäköisesti ole vaikutusta rekisteröityjen oikeuksiin ja vapauksiin.

80. Kun otetaan huomioon tietoturvaloukkauksen kohteeksi joutuneiden henkilöiden vähäinen määrä sekä tietoturvaloukkauksen havaitseminen välittömästi ja sen vaikutusten minimoimiseksi toteutetut toimenpiteet, tässä tapauksessa ei ole riskiä.

4.2.2 TAPAUS nro 9 – Lieventäminen ja velvollisuudet

81. Lisäksi on olemassa muita riskiä lieventäviä tekijöitä: vakuutusasiamiehellä oli salassapitovelvollisuus, hän itse ilmoitti ongelmasta rekisterinpitäjälle ja hän poisti tiedoston pyynnöstä. Tietoisuuden lisääminen ja mahdollisesti lisätoimien sisällyttäminen henkilötietoihin liittyvien asiakirjojen tarkastamiseen auttaa todennäköisesti välttämään vastaavia tapauksia tulevaisuudessa.

82. Muita toimia ei tarvita sen lisäksi, että tietoturvaloukkaus dokumentoidaan 33 artiklan 5 kohdan mukaisesti.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	X	X

4.3 Organisatoriset ja tekniset toimenpiteet sisäisten inhimillisten riskinlähteiden vaikutusten ehkäisemiseksi tai lieventämiseksi

83. Jäljempänä mainittujen toimenpiteiden yhdistelmän, jota sovelletaan tapauksen ainutlaatuisten piirteiden mukaan, pitäisi auttaa pienentämään samankaltaisen tietoturvaloukkauksen toistumisen mahdollisuutta.

84. Suositeltavat toimenpiteet:

(*Seuraavien toimenpiteiden luettelo ei ole missään tapauksessa poissulkeva tai kattava. Tavoitteena on pikemminkin tarjota ennaltaehkäisyä koskevia ideoita ja mahdollisia ratkaisuja. Kaikki käsittelytoimet ovat erilaisia, joten rekisterinpitäjän olisi tehtävä päätös siitä, mitkä toimenpiteet sopivat parhaiten kulloiseenkin tilanteeseen.*)

- Toteutetaan säännöllisesti työntekijöille suunnattuja koulutus- ja valistusohjelmia, jotka koskevat heidän yksityisyyttä ja turvallisuutta koskevia velvollisuuksiaan sekä henkilötietojen turvallisuuteen kohdistuvien uhkien havaitsemista ja niistä ilmoittamista.[26] Kehitetään tiedotusohjelma, jolla työntekijöitä muistutetaan yleisimmistä virheistä, jotka johtavat henkilötietojen tietoturvaloukkauksiin, ja siitä, miten niitä voidaan välttää.
- Luodaan vankat ja tehokkaat tietosuoja- ja yksityisyyskäytännöt, -menettelyt ja -järjestelmät.[27]
- Arvioidaan yksityisyyden suojaa koskevia käytäntöjä, menettelyjä ja järjestelmiä tehokkuuden varmistamiseksi.[28]
- Huolehditaan asianmukaisista käytönvalvontakäytännöistä ja pakotetaan käyttäjät noudattamaan sääntöjä.
- Otetaan käyttöön menetelmät, joilla käyttäjä pakotetaan tunnistautumaan arkaluontoisiin henkilötietoihin pääsemiseksi.
- Poistetaan käyttäjän yritykseen liittyvä tili käytöstä heti, kun henkilö poistuu yrityksen palveluksesta.
- Tarkastetaan tiedostopalvelimen ja työntekijöiden työasemien välinen epätavallinen tiedonkulku.
- Määritetään I/O-rajapintojen suojaus BIOSissa tai tietokoneen rajapintojen käyttöä ohjaavien ohjelmistojen avulla (muun muassa USB-, CD- tai DVD-rajapinnan lukitus tai avaaminen).
- Tarkistetaan työntekijöiden käyttöoikeuskäytännöt (esimerkiksi arkaluontoisiin tietoihin pääsyn kirjaaminen ja käyttäjän velvoittaminen syöttämään liiketoimintaperuste, jotta se on käytettävissä tarkastuksia varten).
- Poistetaan käytöstä avoimet pilvipalvelut.
- Kielletään ja estetään tunnettujen avointen postipalvelujen käyttö.
- Poistetaan käyttöjärjestelmän kuvankaappaustoiminto käytöstä.
- Valvotaan puhtaan työpöydän käytäntöä.
- Lukitaan kaikki tietokoneet automaattisesti, kun ne ovat olleet käyttämättöminä tietyn aikaa.
- Käytetään mekanismeja (esimerkiksi [langatonta] tunnistevälinettä lukituille tileille kirjautumiseksi tai niiden avaamiseksi), joiden avulla käyttäjävaihdokset yhteisissä ympäristöissä voidaan tehdä nopeasti.
- Käytetään sellaisia henkilötietojen hallintaan tarkoitettuja järjestelmiä, joissa sovelletaan asianmukaisia pääsynvalvontamekanismeja ja joilla estetään inhimilliset virheet, kuten viestien lähettäminen väärälle

[26] Kansainvälisen tietosuojaviranomaisten maailmankokouksen inhimillisten virheiden merkitystä henkilötietojen tietoturvaloukkauksissa koskevan päätöslauselman 2 kohdan i alakohta.

[27] Kansainvälisen tietosuojaviranomaisten maailmankokouksen inhimillisten virheiden merkitystä henkilötietojen tietoturvaloukkauksissa koskevan päätöslauselman 2 kohdan ii alakohta.

[28] Kansainvälisen tietosuojaviranomaisten maailmankokouksen inhimillisten virheiden merkitystä henkilötietojen tietoturvaloukkauksissa koskevan päätöslauselman 2 kohdan iii alakohta.

henkilölle. Laskentataulukoiden ja muiden toimistoasiakirjojen käyttö ei ole asianmukainen tapa hallita asiakastietoja.

5 KADONNEET TAI VARASTETUT LAITTEET JA PAPERIASIAKIRJAT

85. Yleinen tapaustyyppi on kannettavien laitteiden katoaminen tai varastaminen. Tällaisissa tapauksissa rekisterinpitäjän on otettava huomioon käsittelytoimen olosuhteet, kuten laitteeseen tallennettujen tietojen tyyppi ja niitä tukevat resurssit, sekä ennen tietoturvaloukkausta toteutetut toimenpiteet asianmukaisen turvallisuustason varmistamiseksi. Kaikki nämä tekijät vaikuttavat tietoturvaloukkauksen mahdollisiin vaikutuksiin. Riskinarviointi voi olla vaikeaa, koska laite ei ole enää käytettävissä.

86. Tällaiset tietoturvaloukkaukset voidaan aina luokitella luottamukseen vaikuttavaksi tietoturvaloukkaukseksi. Jos varastetusta tietokannasta ei ole varmuuskopiota, tietoturvaloukkauksen tyyppi voi olla myös tietojen käytettävyyteen tai eheyteen vaikuttava tietoturvaloukkaus.

87. Jäljempänä esitetyt skenaariot osoittavat, miten edellä mainitut olosuhteet vaikuttavat tietoturvaloukkauksen todennäköisyyteen ja vakavuuteen.

5.1 TAPAUS nro 10: Varastettu materiaali, johon on tallennettu salattuja henkilötietoja

Lasten päiväkotiin kohdistuneessa murrossa varastettiin kaksi taulutietokonetta. Taulutietokoneissa oli sovellus, jossa oli päiväkodissa käyvien lapsien henkilötietoja. Kyse oli nimestä, syntymäajasta ja lasten kasvatusta koskevista henkilötiedoista. Molemmat salatut taulutietokoneet olivat murtohetkellä pois päältä, ja sovellus oli suojattu vahvalla salasanalla. Varmuuskopiotiedot olivat tehokkaasti ja helposti rekisterinpitäjän käytettävissä. Pian murron paljastumisen jälkeen päiväkoti antoi etäyhteyden välityksellä komennon pyyhkiä taulutietokoneet.

5.1.1 TAPAUS nro 10 – Ennakkotoimenpiteet ja riskinarviointi

88. Tässä nimenomaisessa tapauksessa rekisterinpitäjä toteutti riittävät toimenpiteet mahdollisen tietoturvaloukkauksen estämiseksi ja lieventämiseksi käyttämällä laitteen salausta, ottamalla käyttöön riittävän salasanansuojauksen ja varmistamalla taulutietokoneisiin tallennettujen tietojen varmuuskopioinnin (luettelo suositeltavista toimenpiteistä on kohdassa 5.7).

89. Saatuaan tiedon tietoturvaloukkauksesta rekisterinpitäjän olisi arvioitava riskin lähde, tietojen käsittelyä tukevat järjestelmät, asiaan liittyvien henkilötietojen tyyppi ja tietoturvaloukkauksen mahdolliset vaikutukset asianomaisiin henkilöihin. Edellä kuvattu tietoturvaloukkaus olisi koskenut kyseisten tietojen luottamuksellisuutta, käytettävyyttä ja eheyttä, mutta rekisterinpitäjän ennen tietoturvaloukkausta ja sen jälkeen toteuttamien asianmukaisten menettelyjen ansiosta mitään näistä ei kuitenkaan tapahtunut.

5.1.2 TAPAUS nro 10 – Lieventäminen ja velvollisuudet

90. Laitteilla olevien henkilötietojen luottamuksellisuus ei vaarantunut, sillä sekä taulutietokoneissa että sovelluksissa oli vahva salasanasuoja. Taulutietokoneet oli määritetty siten, että salasanan asettaminen tarkoitti myös laitteen tietojen salaamista. Tätä tehosti myös se, että rekisterinpitäjä yritti pyyhkiä kaikki varastettujen laitteiden tiedot etäyhteyden avulla.

91. Toteutettujen toimenpiteiden vuoksi myös tietojen luottamuksellisuus säilyi muuttumattomana. Lisäksi varmuuskopioinnilla varmistettiin henkilötietojen jatkuva käytettävyys, joten mahdollisia kielteisiä vaikutuksia ei olisi voinut esiintyä.

92. Näiden seikkojen vuoksi edellä kuvattu tietoturvaloukkaus ei todennäköisesti aiheuta riskiä rekisteröityjen oikeuksille ja vapauksille, joten siitä ei tarvinnut ilmoittaa valvontaviranomaiselle tai asianomaisille rekisteröidyille. Tämä tietoturvaloukkaus on kuitenkin dokumentoitava 33 artiklan 5 kohdan mukaisesti.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	X	X

5.2 TAPAUS nro 11: Varastettu materiaali, johon on tallennettu salaamattomia henkilötietoja

Palveluntarjoajayrityksen työntekijän kannettava tietokone varastettiin. Varastettu kannettava tietokone sisälsi yli 100 000 asiakkaan nimet, sukunimet, sukupuolet, osoitteet ja syntymäajat. Koska varastettu laite ei ollut käytettävissä, ei ollut mahdollista määrittää, vaikuttiko tietoturvaloukkaus myös muihin henkilötietoryhmiin. Kannettavan tietokoneen kiintolevyä ei ollut suojattu salasanalla. Henkilötiedot voitiin palauttaa päivittäisistä varmuuskopioista.

5.2.1 TAPAUS nro 11 – Ennakkotoimenpiteet ja riskinarviointi

93. Rekisterinpitäjä ei ollut toteuttanut ennalta turvallisuustoimenpiteitä, joten varastettuun kannettavaan tietokoneeseen tallennetut henkilötiedot olivat helposti varkaan tai kenen tahansa muun sellaisen henkilön saatavilla, joka sai laitteen myöhemmin haltuunsa.

94. Tämä tietoturvaloukkaus koskee varastettuun laitteeseen tallennettujen tietojen luottamuksellisuutta.

95. Henkilötietoja sisältävä kannettava tietokone oli tässä tapauksessa haavoittuva, sillä siinä ei ollut salasanansuojausta tai salausta. Perusturvallisuustoimenpiteiden puuttuminen nostaa asianomaisiin rekisteröityihin kohdistuvan riskin tasoa. Lisäksi asianomaisten rekisteröityjen tunnistaminen on ongelmallista, mikä myös lisää tietoturvaloukkauksen vakavuutta. Asianomaisten henkilöiden huomattava määrä lisää riskiä, mutta tietoturvaloukkaus ei kuitenkaan koskenut erityisiä henkilötietoryhmiä.

96. Riskinarvioinnin[29] aikana rekisterinpitäjän olisi otettava huomioon tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja kielteiset vaikutukset. Tietosuojaloukkauksen seurauksena asianomaisiin rekisteröityihin voi kohdistua identiteettipetoksia, jotka perustuvat varastetusta laitteesta saatavilla oleviin tietoihin, joten riskin katsotaan olevan korkea.

5.2.2 TAPAUS nro 11 – Lieventäminen ja velvollisuudet

97. Laitteen salauksen käyttöönotto ja tallennetun tietokannan vahvan salasanasuojan käyttö olisivat voineet estää tietoturvaloukkausta aiheuttamasta rekisteröityjen oikeuksiin ja vapauksiin kohdistuvaa riskiä.

98. Näistä olosuhteista johtuen valvontaviranomaiselle on ilmoitettava asiasta, minkä lisäksi myös asianomaisille rekisteröidyille on ilmoitettava asiasta.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	✓

5.3 TAPAUS nro 12: Varastetut paperiasiakirjat, joissa on arkaluonteisia tietoja

[29] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

Huumevieroituslaitokselta varastettiin paperinen lokikirja. Kirja sisälsi vieroituslaitoksessa olevien potilaiden henkilöllisyyttä ja terveyttä koskevia perustietoja. Tiedot oli tallennettu ainoastaan paperille, eikä potilaita hoitavilla lääkäreillä ollut käytettävissään varmuuskopiota. Kirjaa ei säilytetty lukitussa laatikossa tai huoneessa. Rekisterinpitäjällä ei ollut pääsynvalvontajärjestelmää eikä mitään muuta paperiasiakirjojen turvaamistoimenpidettä.

5.3.1 TAPAUS nro 12 – Ennakkotoimenpiteet ja riskinarviointi

99. Rekisterinpitäjä ei toteuttanut ennalta turvallisuustoimenpiteitä, joten tähän kirjaan tallennetut henkilötiedot olivat helposti kirjan löytäneen henkilön saatavilla. Lisäksi kirjaan tallennettujen henkilötietojen luonne tekee varmuuskopioitujen tietojen puuttumisesta erittäin vakavan riskitekijän.

100. Tämä tapaus on esimerkki korkean riskin tietoturvaloukkauksesta. Asianmukaisten turvallisuusvarotoimien epäonnistumisen vuoksi yleisen tietosuoja-asetuksen 9 artiklan 1 kohdan mukaiset arkaluonteiset terveyttä koskevat tiedot menetettiin. Koska tässä tapauksessa kyse oli erityisestä henkilötietoryhmästä, asianomaisiin rekisteröityihin kohdistuvat mahdolliset riskit kasvoivat, mikä rekisterinpitäjän olisi otettava huomioon riskiä arvioidessaan.[30]

101. Tietoturvaloukkaus koskee kyseisten henkilötietojen luottamuksellisuutta, käytettävyyttä ja eheyttä. Tietoturvaloukkauksen seurauksena lääketieteellinen salassapitovelvollisuus rikkoutuu, ja asiattomat kolmannet osapuolet voivat päästä käsiksi potilaiden yksityisiin lääketieteellisiin tietoihin, millä voi olla vakavia vaikutuksia potilaan henkilökohtaiseen elämään. Tietojen käytettävyyteen vaikuttava tietoturvaloukkaus voi myös häiritä potilaiden hoidon jatkuvuutta. Koska kirjan sisällön osien muuttamista tai poistamista ei voida sulkea pois, myös henkilötietojen eheys vaarantuu.

5.3.2 TAPAUS nro 12 – Lieventäminen ja velvollisuudet

102. Suojatoimenpiteitä arvioitaessa olisi otettava huomioon myös tukena olevan resurssin tyyppi. Koska potilaslokikirja oli fyysinen asiakirja, sen suojaaminen olisi pitänyt järjestää eri tavalla kuin sähköisen laitteen suojaaminen. Potilaiden nimien pseudonymisointi, kirjan säilyttäminen suojatuissa tiloissa ja lukitussa laatikossa tai huoneessa sekä asianmukainen pääsynvalvonta ja -todentaminen sen käytön yhteydessä olisivat voineet estää tietoturvaloukkauksen.

103. Edellä kuvatulla tietoturvaloukkauksella voi olla vakavia vaikutuksia asianomaisiin rekisteröityihin, joten tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle ja asianomaisille rekisteröidyille on pakollista.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	✓

5.4 Organisatoriset ja tekniset toimenpiteet laitteiden katoamisen tai varastamisen vaikutusten ehkäisemiseksi tai lieventämiseksi

104. Jäljempänä mainittujen toimenpiteiden yhdistelmän, jota sovelletaan tapauksen ainutlaatuisten piirteiden mukaan, pitäisi auttaa pienentämään samankaltaisen tietoturvaloukkauksen toistumisen mahdollisuutta.

105. Suositeltavat toimenpiteet:

[30] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

(*Seuraavien toimenpiteiden luettelo ei ole missään tapauksessa poissulkeva tai kattava. Tavoitteena on pikemminkin tarjota ennaltaehkäisyä koskevia ideoita ja mahdollisia ratkaisuja. Kaikki käsittelytoimet ovat erilaisia, joten rekisterinpitäjän olisi tehtävä päätös siitä, mitkä toimenpiteet sopivat parhaiten kulloiseenkin tilanteeseen.*)

- Otetaan käyttöön laitteen salaus (kuten Bitlocker, Veracrypt tai DM-Crypt).
- Käytetään salasanaa kaikissa laitteissa. Kaikki kannettavat laitteet salataan siten, että salauksen purku edellyttää monimutkaisen salasanan syöttämistä.
- Käytetään monivaiheista todentamista.
- Otetaan käyttöön erittäin kevyiden kannettavien laitteiden toiminnot, joiden avulla ne voidaan paikantaa, jos ne katoavat tai joutuvat väärään paikkaan.
- Käytetään kannettavien laitteiden hallintaa koskevaa MDM-ohjelmistoa tai -sovellusta ja paikantamista. Käytetään häikäisysuodattimia. Suljetaan kaikki valvomattomat laitteet.
- Henkilötietoja ei tallenneta kannettavalle laitteelle vaan keskitetylle taustatietopalvelimelle, jos se on mahdollista ja kyseisen tietojenkäsittelyn kannalta tarkoituksenmukaista.
- Jos työasema on liitetty yrityksen lähiverkkoon, tehdään automaattinen varmuuskopiointi työkansioista, jos on väistämätöntä, että niihin tallennetaan henkilökohtaisia tietoja.
- Käytetään suojattua VPN-yhteyttä (joka esimerkiksi edellyttää erillistä kaksivaiheista todentamisavainta turvallisen yhteyden luomiseksi) kannettavien laitteiden yhdistämiseksi taustatietopalvelimiin.
- Tarjotaan työntekijöille fyysiset lukot, jotta he voivat turvata käyttämänsä kannettavat laitteet fyysisesti, kun ne ovat valvomattomia.
- Säännellään laitteiden käytön asianmukaisuutta yrityksen ulkopuolella.
- Säännellään laitteiden käytön asianmukaisuutta yrityksen sisäpuolella.
- Käytetään kannettavien laitteiden hallintaa koskevaa MDM-ohjelmistoa tai -sovellusta ja otetaan käyttöön etäpyyhintätoiminto.
- Käytetään keskitettyä laitehallintaa siten, että loppukäyttäjille annetaan vähimmäisoikeudet ohjelmistojen asentamiseen.
- Asennetaan fyysiset pääsynvalvontalaitteet.
- Vältetään arkaluonteisten tietojen tallentamista kannettaville laitteille tai kiintolevyille. Jos yrityksen sisäiseen järjestelmään on tarpeen päästä, olisi käytettävä suojattuja kanavia, kuten edellä todetaan.

6 VIRHEELLINEN POSTITUS

106. Myös tässä tapauksessa riskin lähde on sisäinen inhimillinen virhe, mutta tässä tietoturvaloukkaukseen ei ole johtanut mikään pahantahtoinen toiminta. Se on seurausta tarkkaamattomuudesta. Rekisterinpitäjä voi toteuttaa ainoastaan vähän toimia sen jälkeen, kun virhe on tapahtunut, joten ennaltaehkäisy on näissä tapauksissa vielä tärkeämpää kuin muissa tietoturvaloukkaustyypeissä.

6.1 TAPAUS nro 13: Postitusvirhe

Vähittäismyyntiyritys pakkasi kaksi kenkiä sisältävää tilausta. Inhimillisen erehdyksen vuoksi kaksi pakkauslaskua menivät sekaisin, minkä seurauksena tuotteet ja niihin liittyvät pakkauslaskut lähetettiin väärille henkilöille. Tämä tarkoittaa sitä, että nämä kaksi asiakasta saivat toistensa tilaukset, mukaan lukien toisen henkilön henkilötiedot sisältävän pakkauslaskun. Saatuaan tiedon tietoturvaloukkauksesta rekisterinpitäjä pyysi lähettämään tilaukset takaisin ja lähetti ne oikeille

6.1.1 TAPAUS nro 13 – Ennakkotoimenpiteet ja riskinarviointi

107. Laskut sisälsivät onnistuneen toimituksen edellyttämät henkilötiedot (nimi ja osoite sekä ostettu tavara ja sen hinta). On tärkeää selvittää, miten inhimillinen virhe on voinut tapahtua ja olisiko se voitu estää jollakin tavalla. Tässä nimenomaisessa tapauksessa riski on pieni, koska siihen ei liity erityisiä henkilötietoryhmiä tai muita tietoja, joiden väärinkäyttö voisi johtaa huomattaviin kielteisiin vaikutuksiin. Tietoturvaloukkaus ei myöskään johdu rekisterinpitäjän tekemästä järjestelmällisestä virheestä, vaan se koskee ainoastaan kahta henkilöä. Henkilöihin ei voitu tunnistaa kohdistuneen kielteisiä vaikutuksia.

6.1.2 TAPAUS nro 13 – Lieventäminen ja velvollisuudet

108. Rekisterinpitäjän olisi huolehdittava siitä, että tuotteet ja niiden mukana olevat laskut palautetaan maksutta. Sen olisi myös pyydettävä vääriä vastaanottajia tuhoamaan tai poistamaan kaikki mahdolliset kopiot laskuista, jotka sisältävät toisen henkilön henkilötietoja.

109. Vaikka tietoturvaloukkaus itsessään ei aiheuta korkeaa riskiä niiden henkilöiden oikeuksille ja vapauksille, joihin vaikutukset kohdistuvat, eikä yleisen tietosuoja-asetuksen 34 artiklan mukaisesti siten edellytä ilmoittamista rekisteröidyille, tietoturvaloukkauksesta ilmoittamista ei voida välttää, sillä riskin lieventämiseksi tarvitaan rekisteröityjen yhteistyötä.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	X	X

6.2 TAPAUS nro 14: Erittäin luottamukselliset henkilötiedot, jotka lähetetään postitse erehdyksessä

Erään julkishallinnon viraston työllisyysosasto lähetti sähköpostiviestin tulevista koulutuksista henkilöille, jotka olivat rekisteröityneet työnhakijoiksi sen järjestelmään. Tähän sähköpostiviestiin liitettiin erehdyksessä asiakirja, joka sisälsi kaikki näiden työnhakijoiden henkilötiedot (nimi, sähköpostiosoite, postiosoite ja sosiaaliturvatunnus). Tietoturvaloukkauksen vaikutukset kohdistuivat yli 60 000 henkilöön. Tämän jälkeen virasto otti yhteyttä kaikkiin vastaanottajiin ja pyysi heitä poistamaan edellisen viestin ja olemaan käyttämättä sen sisältämiä tietoja.

6.2.1 TAPAUS nro 14 – Ennakkotoimenpiteet ja riskinarviointi

110. Tällaisten viestien lähettämiseen olisi pitänyt soveltaa tiukempia sääntöjä. On harkittava uusien valvontamekanismien käyttöönottoa.

111. Niiden henkilöiden määrä, joihin vaikutukset kohdistuvat, on huomattava, ja heidän sosiaaliturvatunnuksensa ja muut perushenkilötietonsa lisäävät riskiä, joka voidaan todeta korkeaksi riskiksi.[31] Rekisterinpitäjä ei voi estää sitä, että joku vastaanottajista mahdollisesti jakaa tietoja.

6.2.2 TAPAUS nro 14 – Lieventäminen ja velvollisuudet

112. Kuten edellä mainitaan, keinot lieventää tehokkaasti samankaltaisen tietoturvaloukkauksen riskejä ovat rajalliset. Vaikka rekisterinpitäjä pyysi viestin poistamista, se ei voi pakottaa vastaanottajia poistamaan viestiä eikä se näin ollen voi olla varma, että vastaanottajat noudattavat pyyntöä.

[31] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

113. Tämänkaltaisessa tapauksessa kaikkien kolmen jäljempänä mainitun toimen toteuttamisen olisi oltava itsestään selvää.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	✓

6.3 TAPAUS nro 15: Henkilötiedot, jotka lähetetään postitse erehdyksessä

Hotellissa järjestettävän viiden päivän pituisen oikeusalan englannin kurssin osallistujaluettelo lähetettiin vahingossa hotellin sijasta 15:lle kurssin entiselle osallistujalle. Luettelo sisälsi 15 osallistujan nimet, sähköpostiosoitteet ja ruokatoiveet. Vain kaksi osallistujaa oli täyttänyt ruokatoiveet ja ilmoittanut, että heillä on laktoosi-intoleranssi. Yhdelläkään osallistujista ei ollut suojattua henkilöllisyyttä. Rekisterinpitäjä havaitsi virheen välittömästi luettelon lähettämisen jälkeen. Hän ilmoitti erehdyksestä vastaanottajille ja pyysi heitä poistamaan luettelon.

6.3.1 TAPAUS nro 15 – Ennakkotoimenpiteet ja riskinarviointi

114. Henkilötietoja sisältävien viestien lähettämiseen olisi pitänyt soveltaa tiukkoja sääntöjä. On harkittava uusien valvontamekanismien käyttöönottoa.

115. Henkilötietojen luonteesta, arkaluonteisuudesta, määrästä ja asiayhteydestä johtuvat riskit ovat vähäisiä. Henkilötiedot sisältävät arkaluonteisia tietoja kahden osallistujan ruokatoiveista. Vaikka tieto siitä, että jollain on laktoosi-intoleranssi, on terveyttä koskeva tieto, riski siitä, että tätä tietoa käytetään haitallisella tavalla, olisi katsottava suhteellisen vähäiseksi. Vaikka terveyteen liittyvien tietojen tapauksessa yleensä oletetaan, että tietoturvaloukkaus aiheuttaa todennäköisesti korkean riskin rekisteröidylle[32], tässä nimenomaisessa tapauksessa ei kuitenkaan ole havaittavissa riskiä siitä, että tietoturvaloukkaus aiheuttaisi rekisteröidylle fyysistä, aineellista tai aineetonta vahinkoa, joka johtuisi laktoosi-intoleranssia koskevien tietojen luvattomasta luovuttamisesta. Toisin kuin eräät muut ruokatoiveet, laktoosi-intoleranssia ei yleensä voida yhdistää mihinkään uskonnolliseen tai filosofiseen vakaumukseen. Myös niiden tietojen määrä, joihin tietoturvaloukkaus kohdistuu, ja niiden rekisteröityjen määrä, joihin vaikutus kohdistuu, on hyvin pieni.

6.3.2 TAPAUS nro 15 – Lieventäminen ja velvollisuudet

116. Yhteenvetona voidaan todeta, että tietoturvaloukkauksella ei ollut merkittävää vaikutusta rekisteröityihin. Lieventävänä seikkana voidaan pitää sitä, että rekisterinpitäjä otti välittömästi yhteyttä vastaanottajiin saatuaan tiedon virheestä.

117. Jos sähköpostiviesti lähetetään väärälle tai valtuuttamattomalle vastaanottajalle, on suositeltavaa, että rekisterinpitäjä lähettää tahattomille vastaanottajille piilokopiona lisäsähköpostiviestin, jossa pyydetään anteeksi, kehotetaan poistamaan sääntöjenvastainen sähköpostiviesti ja ilmoitetaan vastaanottajille, että heillä ei ole oikeutta käyttää heille paljastuneita sähköpostiosoitteita.

118. Näiden seikkojen vuoksi tämä tietoturvaloukkaus ei todennäköisesti aiheuta riskiä rekisteröityjen oikeuksille ja vapauksille, joten siitä ei tarvinnut ilmoittaa valvontaviranomaiselle tai asianomaisille rekisteröidyille. Tämä tietoturvaloukkaus on kuitenkin lisäksi dokumentoitava 33 artiklan 5 kohdan mukaisesti.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille

[32] Ks. suuntaviivat WP 250, s. 25.

✓	X	X

6.4 TAPAUS nro 16: Postitusvirhe

Vakuutusyritysryhmä tarjosi autovakuutuksia. Tätä varten se lähetti postitse säännöllisesti mukautettuja maksutietoja. Kirjeessä oli vakuutuksenottajan nimen ja osoitteen lisäksi ajoneuvon rekisterinumero ilman peitettyjä numeroita, kuluvan ja seuraavan vakuutusvuoden vakuutusmaksut, likimääräinen vuotuinen ajokilometrimäärä ja vakuutuksenottajan syntymäaika. Tietoihin ei sisältynyt yleisen tietosuoja-asetuksen 9 artiklan mukaisia terveyttä koskevia tietoja, maksutietoja (pankkitiedot) taikka talous- ja rahoitustietoja.

Kirjekuoret pakattiin automaattisilla kuorituskoneilla. Mekaanisen virheen vuoksi kaksi eri vakuutuksenottajille osoitettua kirjettä laitettiin samaan kirjekuoreen ja lähetettiin yhdelle vakuutuksenottajalle kirjepostina. Vakuutuksenottaja avasi kirjeen kotonaan ja tarkasteli sekä asianmukaisesti toimitettua kirjettä että toisen vakuutuksenottajan virheellisesti toimitettua kirjettä.

6.4.1 TAPAUS nro 16 – Ennakkotoimenpiteet ja riskinarviointi

119. Virheellisesti toimitettu kirje sisältää nimen, osoitteen, syntymäajan, ajoneuvon peittämättömän rekisterinumeron sekä kuluvan ja seuraavan vuoden vakuutusmaksuluokituksen. Vaikutuksia asianomaiseen henkilöön on pidettävä keskisuurina, koska luvattomalle vastaanottajalle paljastuu tietoja, jotka eivät ole julkisesti saatavilla, kuten syntymäaika tai ajoneuvojen peittämättömät rekisterinumerot ja tiedot vakuutusmaksujen korotuksista. Näiden tietojen väärinkäytön todennäköisyyden arvioidaan olevan pieni tai keskisuuri. Vaikka monet vastaanottajat todennäköisesti hävittävät virheellisesti saadun kirjeen roskana, yksittäistapauksissa ei kuitenkaan voida täysin sulkea pois sitä, että kirje julkaistaan sosiaalisissa verkostoissa tai että vakuutuksenottajaan otetaan yhteyttä.

6.4.2 TAPAUS nro 16 – Lieventäminen ja velvollisuudet

120. Rekisterinpitäjän olisi palautettava alkuperäinen asiakirja itselleen omalla kustannuksellaan. Väärälle vastaanottajalle olisi myös ilmoitettava, ettei hän saa käyttää lukemiaan tietoja väärin.

121. Täysin automatisoitujen koneiden avulla ei luultavasti koskaan pystytä täysin estämään postitusvirheitä massapostituksissa. Jos esiintymistiheys kuitenkin kasvaa, on tarpeen tarkistaa, onko kuorituskoneet asetettu ja huollettu riittävän oikein tai onko jokin muu järjestelmään liittyvä ongelma johtanut tällaiseen tietoturvaloukkaukseen.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	X

6.5 Organisatoriset ja tekniset toimenpiteet postitusvirheiden vaikutusten ehkäisemiseksi tai lieventämiseksi

122. Jäljempänä mainittujen toimenpiteiden yhdistelmän, jota sovelletaan tapauksen ainutlaatuisten piirteiden mukaan, pitäisi auttaa pienentämään samankaltaisen tietoturvaloukkauksen toistumisen mahdollisuutta.

123. Suositeltavat toimenpiteet:

(*Seuraavien toimenpiteiden luettelo ei ole missään tapauksessa poissulkeva tai kattava. Tavoitteena on pikemminkin tarjota ennaltaehkäisyä koskevia ideoita ja mahdollisia ratkaisuja. Kaikki käsittelytoimet ovat erilaisia, joten rekisterinpitäjän olisi tehtävä päätös siitä, mitkä toimenpiteet sopivat parhaiten kulloiseenkin tilanteeseen.*)

- Asetetaan tarkat standardit kirjeiden tai sähköpostien lähettämiselle siten, että niissä ei ole tulkinnanvaraa.
- Koulutetaan henkilöstö asianmukaisesti kirjeiden tai sähköpostien lähettämiseen.
- Luetellaan sähköpostiviestien vastaanottajat oletusarvoisesti piilokopiokentässä, kun sähköpostiviestejä lähetetään useille vastaanottajille.
- Tarvitaan lisävahvistus, kun sähköpostiviestejä lähetetään useille vastaanottajille ja vastaanottajia ei luetella piilokopiokentässä.
- Sovelletaan neljän silmän periaatetta.
- Käytetään automaattista osoitusta manuaalisen osoituksen sijasta siten, että tiedot poimitaan käytettävissä olevasta ja ajantasaisesta tietokannasta, minkä lisäksi automaattista osoitusjärjestelmää olisi tarkistettava säännöllisesti piilevien virheiden ja virheellisten asetusten varalta.
- Käytetään viestiviivettä (esimerkiksi viesti voidaan poistaa tai sitä voidaan muokata tietyn ajan kuluessa lähetyspainikkeen napsauttamisesta).
- Poistetaan automaattinen täydentäminen käytöstä sähköpostiosoitteita kirjoitettaessa.
- Järjestetään tiedotustilaisuuksia yleisimmistä virheistä, jotka johtavat henkilötietojen tietoturvaloukkaukseen.
- Järjestetään koulutustilaisuuksia ja julkaistaan käsikirjoja siitä, miten henkilötietojen tietoturvaloukkaukseen johtavia tapauksia käsitellään ja kenelle asiasta on ilmoitettava (tietosuojavastaavan osallistuminen).

7 MUUT TAPAUKSET – KÄYTTÄJÄN MANIPULOINTI

7.1 TAPAUS nro 17: Identiteettivarkaus

Televiestintäyrityksen yhteyskeskus vastaanotti puhelun henkilöltä, joka esiintyi asiakkaana. Oletettu asiakas pyysi yritystä muuttamaan sähköpostiosoitteen, johon laskutustiedot pitäisi tästä lähtien lähettää. Yhteyskeskuksen työntekijä varmisti asiakkaan henkilöllisyyden kysymällä tiettyjä henkilötietoja, jotka on määritelty yrityksen menettelyissä. Soittaja ilmoitti oikein pyydetyn asiakkaan verotunnuksen ja postiosoitteen (koska hänellä oli pääsy näihin tietoihin). Vahvistuksen jälkeen työntekijä teki pyydetyn muutoksen, ja siitä lähtien laskutustiedot lähetettiin uuteen sähköpostiosoitteeseen. Menettelyyn ei sisältynyt ilmoitusta aiempaan sähköpostiosoitteeseen. Seuraavassa kuussa oikea asiakas otti yhteyttä yritykseen ja tiedusteli, miksi hän ei saa laskuja sähköpostiosoitteeseensa. Hän kiisti soittaneensa ja vaatineensa sähköpostiosoitteen muuttamista. Yritys ymmärsi, että tiedot oli lähetetty väärälle käyttäjälle, ja perui muutoksen.

7.1.1 TAPAUS nro 17 – Riskinarviointi, lieventäminen ja velvollisuudet

124. Tämä tapaus on esimerkki ennakkotoimenpiteiden merkityksestä. Riskinäkökulmasta katsottuna tietoturvaloukkaukseen liittyy korkea riski[33], sillä laskutustiedot voivat antaa tietoa rekisteröidyn yksityiselämästä (esimerkiksi tottumukset ja yhteystiedot) ja johtaa aineelliseen vahinkoon (esimerkiksi

[33] Ohjeet todennäköisesti korkean riskin aiheuttavista käsittelytoimista, ks. edellä oleva alaviite 10.

vainoaminen ja fyysisen koskemattomuuden vaarantuminen). Hyökkäyksen aikana saatuja henkilötietoja voidaan käyttää myös helpottamaan tilin haltuunottoa tämän organisaation osalta tai käyttämään hyväksi muiden organisaatioiden muita todentamistoimenpiteitä. Nämä riskit huomioon ottaen ”asianmukaisen” todentamistoimenpiteen olisi täytettävä korkea vaatimustaso sen mukaan, mitä henkilötietoja voidaan käsitellä todentamisen seurauksena.

125. Tämän vuoksi rekisterinpitäjältä tarvitaan sekä ilmoitus valvontaviranomaiselle että ilmoitus rekisteröidylle.

126. Aiempaa asiakkaiden todentamisprosessia on selvästi tarkennettava tämän tapauksen perusteella. Todentamisessa käytetyt menetelmät eivät olleet riittäviä. Pahantahtoinen osapuoli pystyi esiintymään tarkoitettuna käyttäjänä käyttämällä julkisesti saatavilla olevia tietoja ja niitä tietoja, joihin hänellä oli muutoin pääsy.

127. Tämäntyyppisen staattiseen tietoon perustuvan todentamisen (jossa vastaus ei muutu ja jossa tiedot eivät ole ”salaisia” kuten salasanan tapauksessa olisi) käyttöä ei suositella.

128. Sen sijaan organisaation olisi käytettävä todentamistapaa, jonka avulla päästäisiin suureen luottamukseen siitä, että todennettu käyttäjä on tarkoitettu henkilö eikä kukaan muu. Ongelma voitaisiin ratkaista ottamalla käyttöön kaistan ulkopuolinen monivaiheinen todentamismenetelmä, jolla voitaisiin esimerkiksi todentaa muutosvaatimus lähettämällä vahvistuspyyntö entiseen yhteystietoon, tai lisäämällä lisäkysymyksiä ja vaatimalla tietoja, jotka näkyvät ainoastaan aiemmissa laskuissa. Rekisterinpitäjän vastuulla on päättää, mitä toimenpiteitä se ottaa käyttöön, sillä se tuntee parhaiten sisäisen toimintansa yksityiskohdat ja vaatimukset.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	✓

7.2 TAPAUS nro 18: Sähköpostien siirtäminen

Eräs hypermarketketju havaitsi kolme kuukautta konfiguroinnin jälkeen, että joitakin sähköpostitilejä oli muutettu. Lisäksi oli luotu sääntöjä, joiden mukaan jokainen sähköpostiviesti, joka sisälsi tiettyjä ilmaisuja (esimerkiksi ”lasku”, ”maksu”, ”pankkisiirto”, ”luottokorttitodennus” tai ”pankkitilitiedot”), siirrettiin käyttämättömään kansioon ja välitettiin ulkoiseen sähköpostiosoitteeseen. Paljastumiseen mennessä oli myös jo tehty käyttäjän manipulointihyökkäys, eli hyökkääjä oli esiintynyt tavarantoimittajana ja muuttanut tavarantoimittajan pankkitilin tiedot omikseen. Tuohon mennessä oli lähetetty useita väärennettyjä laskuja, joihin sisältyi uusi pankkitilitieto. Sähköpostialustan seurantajärjestelmä antoi lopulta kansioita koskevan hälytyksen. Yhtiö ei pystynyt määrittämään, miten hyökkääjä oli alun perin saanut pääsyn sähköpostitileihin. Yhtiö oletti, että pääsy maksuista vastaavaan käyttäjäryhmään mahdollistui saastuneen sähköpostin välityksellä.

Sähköpostien avainsanapohjaisen välittämisen ansiosta hyökkääjä sai seuraavat tiedot 99 työntekijästä: nimi ja tietyn kuukauden palkka 89 rekisteröidyn osalta sekä nimi, siviilisääty, lasten lukumäärä, palkka, työtunnit ja muut jäämätiedot kymmenen sellaisen työntekijän palkkatuloista, joiden työsuhde oli päättynyt. Rekisterinpitäjä ilmoitti tietoturvaloukkauksesta ainoastaan viimeksi mainittuun ryhmään kuuluville kymmenelle työntekijälle.

7.2.1 TAPAUS nro 18 – Riskinarviointi, lieventäminen ja velvollisuudet

129. Vaikka hyökkääjän tarkoituksena ei todennäköisesti ollut kerätä henkilötietoja, henkilötietojen tietoturvaloukkauksesta voi aiheutua sekä aineellista (esimerkiksi taloudellinen menetys) että aineetonta vahinkoa (esimerkiksi identiteettivarkaus tai petos). Lisäksi tietoja voidaan käyttää muiden hyökkäysten

(esimerkiksi tietojenkalasteluhyökkäys) helpottamiseen. Niinpä henkilötietojen tietoturvaloukkauksesta aiheutuu todennäköisesti korkea riski luonnollisten henkilöiden oikeuksille ja vapauksille. Näin ollen tietoturvaloukkauksesta olisi ilmoitettava kaikille 99 työntekijälle eikä ainoastaan niille kymmenelle työntekijälle, joiden palkkatiedot vuosivat.

130. Saatuaan tietoonsa tietoturvaloukkauksen rekisterinpitäjä pakotti vaihtamaan vaarantuneiden tilien salasanat, esti sähköpostiviestien lähettämisen hyökkääjän sähköpostitilille, ilmoitti hyökkääjän käyttämän sähköpostin palveluntarjoajalle hyökkääjän toimista, poisti hyökkääjän asettamat säännöt ja kehitti seurantajärjestelmän hälytyksiä siten, että järjestelmä antaa hälytyksen automaattisen säännön luomisesta välittömästi. Vaihtoehtoisesti rekisterinpitäjä voisi poistaa käyttäjiltä oikeuden asettaa edelleenlähetyssääntöjä, jolloin tietotekniikkapalveluryhmä voisi tehdä sen vain pyynnöstä. Se myös voisi ottaa käyttöön käytännön, jonka mukaan käyttäjien olisi tarkistettava tileilleen asetetut säännöt ja raportoitava niistä kerran viikossa tai useammin aloilla, joilla käsitellään taloustietoja.

131. Se, että tietoturvaloukkaus saattoi tapahtua ja olla havaitsematta niin pitkään ja että pidemmän ajan kuluessa käyttäjän manipulointia olisi voitu käyttää useampien tietojen muuttamiseen, toi esiin merkittäviä ongelmia rekisterinpitäjän tietoteknisessä turvallisuusjärjestelmässä. Niihin olisi puututtava viipymättä, esimerkiksi painottamalla automaatiotarkastuksia ja muutosvalvontaa, poikkeamien havaitsemista sekä reagointitoimenpiteitä. Muun muassa arkaluonteisia ja taloudellisia tietoja käsittelevillä rekisterinpitäjillä on suurempi vastuu riittävän tietoturvan tarjoamisesta.

Tunnistettuihin riskeihin perustuvat tarvittavat toimet		
Sisäinen dokumentointi	Ilmoitus valvontaviranomaiselle	Ilmoitus rekisteröidyille
✓	✓	✓