KYBERHÄIRIÖTILANTEET

VARAUTUMINEN JA TOIMINTA

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

Julkaisija:

Huoltovarmuusorganisaatio
Digipooli
Helsinki 2019

ISBN 978-952-5608-73-1

www.huoltovarmuus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeustiloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallin nonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta.

www.ficom.fi

Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry on suomalainen ICT-alan edunvalvoja, jonka tavoitteena on edistää jäsentensä liiketoimintamahdollisuuksia ja parantaa alan kilpailukykyä.

SISÄLLYSLUETTELO

KYBERHÄIRIÖTILANTEET: VARAUTUMINEN JA TOIMINTA

Huoltovarmuuskeskus ja Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry ovat päivittäneet vuonna 2017 tehdyn selvityksen kyberhäiriötilanteista ja niihin varautumisesta. Selvityksessä kartoitettiin juridista ympäristöä ja haasteita, joita huoltovarmuuskriittiset ja niille viestintä- ja IT-palveluita tarjoavat yritykset kohtaavat poikkeamia ja häiriöitä ratkaistaessa sekä sitä, miten näiltä uhilta suojautuminen tulisi etukäteen huomioida sopimuksissa, kun IT- ja viestintäpalveluita ulkoistetaan.

Päivitetyn selvityksen tavoitteena oli löytää hyviä käytäntöjä, joilla yritysten varautumista ja selviytymistä kyberhäiriötilanteissa voidaan edistää. Päivityksessä kyberhäiriöselvityksen sisältö jäsenneltiin ohjeistukseksi, jonka kohderyhmänä ovat kyberturvallisuudestaan huolehtivat yritykset, niiden tietohallinnosta ja tietoturvasta vastaavat työntekijät sekä näille yrityksille viestintä, IT- ja tietoturvapalveluita tarjoavien yritysten liiketoiminnasta vastaavat henkilöt.

Selvityksen tavoitteena oli löytää hyviä käytäntöjä, joilla yritysten varautumista ja selviytymistä kyberhäiriötilanteissa voidaan edistää.

LAINSÄÄDÄNTÖKEHYS

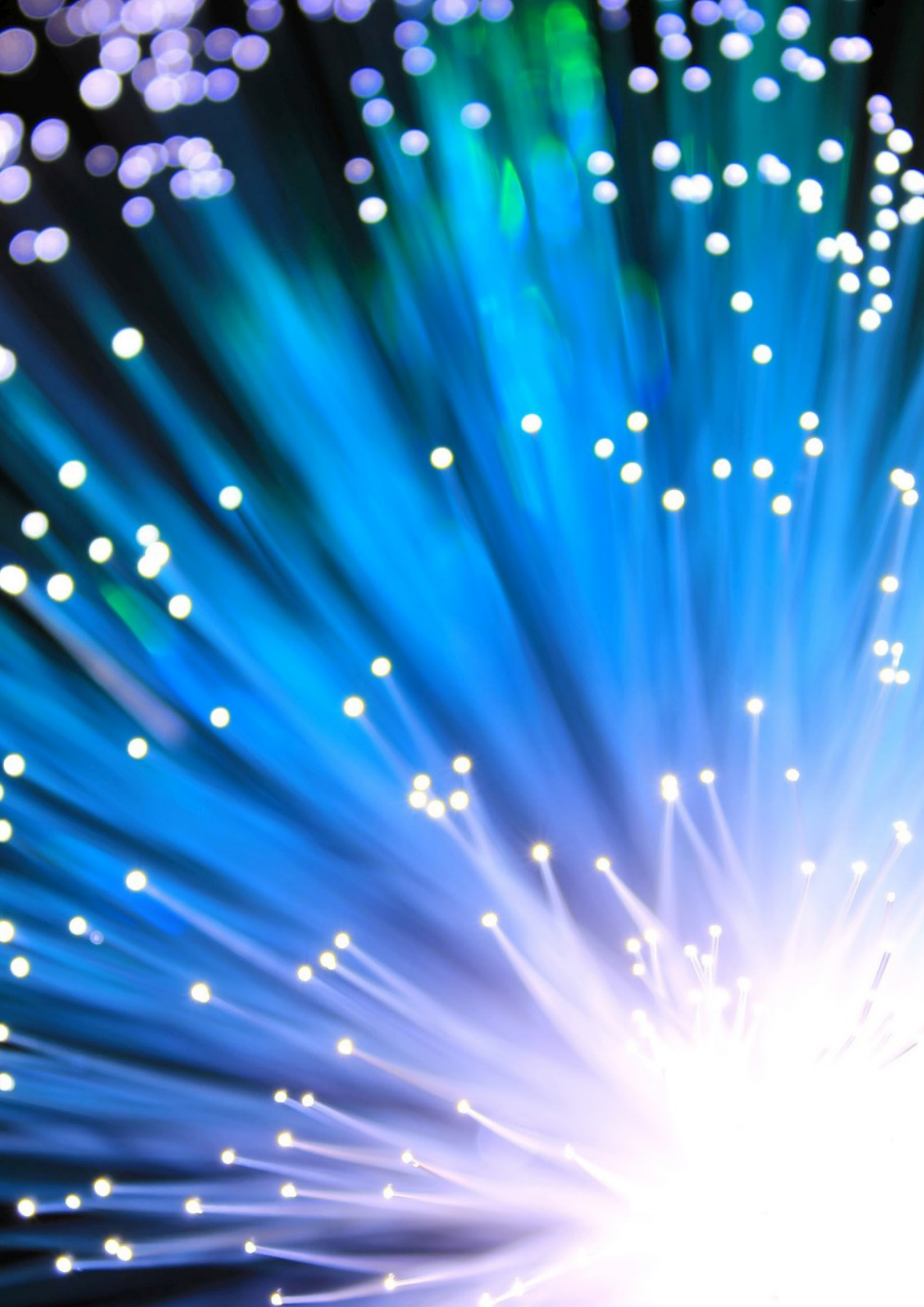
Keskeisin kyberhäiriötilanteisiin liittyvä säädös Suomessa on laki sähköisen viestinnän palveluista (917/2014), joka sisältää teleyritysten ja yhteisötilaajien viestinnän välittämiseen ja välitystietojen käsittelyyn sovellettavat säännökset.

Lisäksi tulee huomioida EU:n yleisen tietosuoja-asetuksen ((EU) 2016/679), sen myötä säädetyn tietosuojalain (1050/2018) sekä yksityisyyden suojasta työelämässä annetun lain (759/2004, työelämän tietosuojalaki) velvoitteet. Poliisin toimintaa ohjaavat rikoslaki (39/1889) ja esitutkintalaki (805/2011).

Laki julkisen hallinnon tiedonhallinnasta (906/2019) tulee voimaan 1.1.2020. Lisäksi EU:ssa valmistellaan parhaillaan sähköisen viestinnän tietosuoja-asetusta (ePrivacy) sekä sähköisen todistusaineiston rajat ylittävää saatavuutta koskevia asetusta ja direktiiviä (e-Evidence).

SUOSITUKSET

Suositukset on laadittu erikseen kyberturvallisuudestaan huolehtiville yrityksille sekä IT- ja tietoturvapalveluiden tarjoajille suunnatuiksi ohjeistuksiksi etukäteen, ennen sopimuksen allekirjoittamista huomioitavista seikoista (***Arvioi uhkia ja ymmärrä riskit***), tavanomaisessa palvelun ylläpitovaiheessa sekä varautumisessa huomioitavista seikoista (***Suojaa organisaatiosi toiminta ja turvaa jatkuvuus***) sekä häiriötilanteissa huomioitavista seikoista (***Reagoi nopeasti ja toimi suunnitelmallisesti***).



ENNEN SOPIMUKSEN ALLEKIRJOITTAMISTA HUOMIOITAVAA

ARVIOI UHKIA JA YMMÄRRÄ RISKIT

Riskiarvio

Tietoturvan tulisi olla osa yrityksen normaalia toimintaa ja prosesseja – ei sarja päälle liimattuja toimenpiteitä. Erilaisten tietoturva- ja suojausratkaisujen hankkimisen sijaan yritysten tulisi keskittyä riskien arviointiin. Riskien tunnistaminen on lähtökohta muille toimenpiteille ja niiden suunnittelulle.

Yrityksen varautuminen häiriötilanteisiin edellyttää eri tietojen merkityksen ja niitä käsittelevien järjestelmien tunnistamista. On arvioitava toimintaedellytykset tapauksissa, joissa kyseiset tiedot eivät jostain syystä ole saatavissa. Tiedon merkityksestä yrityksen toiminnalle johtuvat myös vaateet tietojen suojaamisesta ja palauttamisesta, eli käytännössä vaatimukset palvelujen ja ratkaisujen hankkimiselle, vaatimukset niiden toimittajille sekä sen varmistamiselle, että toimittaja pystyy vastaamaan vaatimuksiin.

On tärkeää ymmärtää, missä tieto säilytetään. Esimerkiksi henkilötietoja, sähköistä viestintää, maksukorttitietoja ja muita luottamuksellisia tai arkaluonteisia tietoja koskee merkittävät säilytys- ja turvallisuusvaatimukset. On hyvä huomata, että kaikkiin tietoihin ei kohdistu välttämättä samanlaisia vaatimuksia, mutta kaikkia tietoja voidaan niin halutessa säilyttää yhtä turvallisesti. Esimerkiksi henkilötietojen käsittelystä ja tietoturvasta säädetään yleisessä tietosuoja-asetuksessa (EU 2016/679), erityisesti sen artiklassa 32.

Mikä on hyväksyttävä aika sille, että tiedot eivät ole saatavissa? Tämä ratkaisee tason, jolla tiedot tai järjestelmä tai sen osa on syytä suojata ja tietojen saatavuus varmistaa. Myös tietojen luottamuksellisuuteen ja eheyteen tulee kiinnittää huomiota. Esimerkiksi tietosuoja-asetuksessa esitellyn ja edellytetyn pseudonymisoinnin soveltaminen henkilötietoihin voi vähentää asianomaisiin rekisteröityihin kohdistuvia riskejä sekä auttaa rekisterinpitäjiä ja henkilötietojen käsittelijöitä noudattamaan tietosuojavelvoitteitaan. Varautuminen onkin sarja liiketoiminnallisia (investointi)päätöksiä ja olennainen osa yrityksen palveluja ulkoistussopimuksia. Tässä tulee huomioida myös tietosuoja-asetuksen 28 artiklassa esitetty sopimussuhde palvelun tilaajan (rekisterinpitäjä) ja -tuottajan (käsittelijä) välillä.

Tietojen ja järjestelmien suojaaminen

Tarjolla on kattavasti toimivia tekniikoita, ratkaisuja ja palveluja, joilla tiedot ja järjestelmät pystytään tehokkaasti suojaamaan. Se, että asiakkaan tietojärjestelmä koostuu monen eri toimijan ratkaisuista, voi aiheuttaa sopimuksellisia ja hallinnollisia haasteita. Joissain tapauksissa palveluja hankittaessa ei häiriötilanteiden selvittämistä ole lainkaan otettu huomioon tai niihin ennalta varautuminen on ollut puutteellista. Esimerkiksi lokitietojen saatavuutta ja riittävän nopeaa pääsyä järjestelmiin ei ole varmistettu, tai ei ole rakennettu integraatiota pilvipalvelun rajapintaan, josta pääsy kirjautumislokeihin olisi saatavilla.

Järjestelmien ja tietojen suojaamisessa keskeinen tehtävä on johtaa riskiarviosta toiminnallis-teknisiä vaateita, joihin suojaaminen perustuu. Vaateiden määrittäminen perustuu pitkälti yritysten omiin hankintaprosesseihin. Riskiarvion perusteella hankintavaiheessa tulisi vähintään määritellä, miten häiriötilanteiden selvittämisessä tarvittavat lokitiedot tai pääsy tietoihin on saatavilla.

Tietoverkon käytön ohjeistus, sähköisten viestien hakeminen, yrityssalaisuuksien suojaaminen, väärinkäytösten selvittäminen ja työntekijöiden paikantaminen sekä muut teknisen valvonnan muodot edellyttävät yrityksiltä huomattavaa ennakkosuunnittelua, mukaan lukien toimintojen roolitus ja vastuuhenkilöiden nimeäminen sekä asioiden käsittely

riittävällä tarkkuudella yhteistoimintamenettelyssä. Tämän vuoksi työelämän tietosuojalaissa ja viestintäpalvelulain 18 luvussa tarkoitetut menettelyt eivät ole yrityksen käytettävissä ad hoc -pohjalta silloin, kun mahdollista tietoturvapoikkeamaa joudutaan selvittämään.

Se, millaiset tekniset hallintakeinot ja tavat löytää ja yksilöidä kyberhäiriötilanteessa saastunut laite tai järjestelmä yrityksellä on käytössään, vaikuttaa ratkaisevasti siihen, miten tietoturvapoikkeama saadaan paikallistettua. On myös tärkeää ymmärtää, miten häiriötapausten selvittäminen on hallinnoitu: kun havainto on tehty, kuinka nopeasti siihen pystytään reagoimaan, mitä prosesseja havainto käynnistää, keitä kutsutaan paikalle, millainen ryhmä asiaa ryhtyy tutkimaan jne.

EU:n toimielimissä on parhaillaan käsittelyssä sähköisen viestinnän tietosuojaa koskeva ePrivacy-asetus, joka tullee hyväksytyksi vuosien 2020 - 2021 aikana. Asetuksen sisältö ja siinä säädetyt viestinnän välitystietojen sallitut käsittelyperusteet saattavat vaikuttaa merkittävästi myös tietoturvatyöhön.

EU:n toimielimissä valmistellaan myös sähköisen todistusaineiston rajat ylittävää saatavuutta koskevia e-Evidence-asetusta ja -direktiiviä, joilla voi olla vaikutusta joidenkin palveluntarjoajien toimintaan. Lainsäädäntökokonaisuuden odotetaan valmistuvan vuoden 2020 aikana.

Valtiovarainministeriö julkaisi lokakuussa 2017 työryhmäraportin tiedonhallinnan lainsäädännön kehittämislinjauksista. Linjausten taustalla oli yleinen tietosuoja-asetus sekä havainto tiedonhallinnan toimintaympäristön perustavanlaisesta muuttumisesta keskeisten säädösten antamisen jälkeen. Työryhmä esitti julkisen hallinnon tiedonhallinnan yleislakia, joka perustuisi elinkaariajatteluun, tiedon tehokkaaseen hyödyntämiseen vakioitujen rajapintojen kautta. Eduskunta hyväksyi 18.3.2019 hallituksen esityksen julkisen hallinnon tiedonhallintalaiksi ja laki (906/2019) tulee voimaan 1.1.2020.

Standardointi

Vallitseva standardiperhe on Tietoturvallisuuden hallintajärjestelmä ISO27000, jonka lisäksi alalla noudatettavista vakioehdoista (IT2018, JIT2015) löytyy elementtejä poikkeus- ja häiriötilanteiden selvittämiseen. Joillakin julkishallinnon toimijoilla pohjana voi olla tiettyjä ehtoja, esimerkiksi VAHTI, Katakri ja

PiTuKri. Kyberturvallisuuskeskus suosittelee lisäksi Huoltovarmuuskeskuksen SOPIVA-suositusten huomioimista. Todellista tarvetta korkeamman standardin vaatiminen kaiken tiedon käsittelyyn voi kuitenkin aiheuttaa yritykselle vain tarpeettomia lisäkuluja.

Standardien lisäksi varautumisessa tulee usein huomioida esimerkiksi Amazon Web Services- ja Azure-sertifioinnit. Yrityksillä on myös omia tietoturvallisuusvaateita, joissa osassa on hyödynnetty Information Security Forumin (ISF) Standard of Good Practice for Information Security -käytäntöjä.

Käytännön muutostarpeet

Toimintaympäristön muutoksella on merkitystä häiriöihin varautumisessa ja niihin vastaamisessa, oli kyse sitten pilvipalveluista, robotisaatiosta, Big Datasta, IoT:stä tai muista viime aikojen muutoksista toimintaympäristössä. Muutostarpeita aiheutuu mm. organisatorisille järjestelyille, tietohallinnolle sekä hankintamenettelylle. Palveluja ja ratkaisuja hankittaessa ostajan tulee paitsi tietää, mitä on hankkimassa, myös varmistua siitä, että toimittaja pystyy käytännössä toimimaan siltä edellytetyllä tavalla ja että yrityksen sopimuskäytännöissä huomioidaan lainsäädännön vaatimukset. Työn tekemisen tapojen ja teknisen toimintaympäristön muuttuessa on entistä tärkeämpää huolehtia tietoturvasta osana yrityksen normaaleja toimintatapoja ja yrityskulttuuria.

Yksityisyyden suojasta työelämässä annettu laki (759/2004)

Yksityisyyden suojasta työelämässä annetussa laissa (759/2004, työelämän tietosuojalaki) säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta. Teknisenä valvontana pidetään myös työntekijöiden paikantamista.

Työelämän tietosuojalaki on työelämäkysymysten erityislaki, ja sitä sovelletaan työntekijän ja eräiltä osin työnhakijan asemassa olevien henkilöiden tietojen käsittelyyn. Sellaisiin kysymyksiin, joista siinä ei ole säädetty, sovelletaan yleisen tietosuoja-asetuksen, tietosuojalain sekä viestintäpalvelulain säännöksiä. Lakia ei sovelleta yhtiöoikeudellisiin johtajiin (TSV 22.11.2006), vaan ainoastaan työ- tai virkasuhteessa oleviin työntekijöihin. Laki täsmentää tietosuoja-asetuksen ja tietosuojalain säännöksiä henkilötietojen käsittelystä ja antaa puitteet kameravalvonnan ja työnantajalle kuuluvien sähköisten viestien hakemiseen.

Laki ohjaa toimimaan huolellisesti, koska asiat on käsiteltävä yhteistoimintamenettelyssä. Lain 21 § mukaan työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja valvonnassa käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely ovat työnantajan ja henkilöstön välisessä yhteistoimintamenettelyssä käsiteltäviä asioita.

Työnantajan tulee siis ennalta varautua laissa säädettyjen menetelmien käyttöön ja käsiteltävä esimerkiksi tietoverkon käyttöön liittyvät ohjeet ja toimintatavat yhteistoimintamenettelyssä.

Työ- ja elinkeinoministeriö asetti 21.9.2017 työryhmän tarkastelemaan työelämän tietosuojalainsäädännön ja EU:n yleisen tietosuoja-asetuksen välistä suhdetta. Työryhmän ehdotusten pohjalta yksityisyyden suojasta työelämässä annettuun lakiin tehdyt muutokset tulivat voimaan 1.4.2019.

Laki sähköisen viestinnän palveluista, 18 luku – yhteisötilaajaa koskeva erityissääntely

Sähköisen viestinnän palveluista annetun lain 18 luku sisältää sähköisen viestinnän tietosuojalakiin vuonna 2009 lisätyt yhteisötilaajiin sovellettavat säännökset välitystietojen käsittelystä viestintäpalvelujen luvattoman käytön ja yrityssalaisuuksien paljastamisen tapauksissa. Säännökset tulivat tunnetuiksi Lex Nokiana. Yhteisötilaajalla tarkoitetaan viestintä- tai lisäarvopalvelun asiakasyritystä tai -yhteisöä, joka käsittelee viestintäverkossaan käyttäjien viestejä, välitys- tai sijaintitietoja.

Luvun säännökset antavat yhteisötilaajalle oikeuden käsitellä viestinnän välitystietoja väärinkäytöksien selvittämiseksi. Luvun säännösten käyttäminen edellyttää yrityksiltä suunnitelmallisuutta: teknisten valmiuksien lisäksi yhteisötilaajan huolehtimisvelvollisuuteen kuuluu 147 § mukaan huolehtia asianmukaisesta tietoturvasta ja määritellä, millaisia sähköisiä viestejä sen viestintäverkon kautta saa välittää ja hakea sekä miten sen viestintäverkkoa ja viestintäpalvelua saa muutoin käyttää ja esimerkiksi millaisiin kohdeosoitteisiin sähköpostia ei saa lähettää. Yrityssalaisuuksien osalta yhteisötilaajan on

ensin määriteltävä yrityssalaisuutensa ja suojattava sekä ne että verkkonsa asianmukaisesti. Lisäksi yhteisötilaajan on määriteltävä, miten yrityssalaisuuksia saa viestintäverkossa siirtää, luovuttaa tai muutoin käsitellä.

Yhteisötilaajan on myös suunniteltava toiminta nimeämällä henkilöt, joiden tehtäviin käsittely kuuluu ja käsiteltävä välitystietojen käsittelyn perusteet ja käytännöt yhteistoimintamenettelyssä henkilöstön kanssa. Ennen toiminnan aloittamista tulee siitä tehdä ennakkoilmoitus myös säännösten noudattamista valvovalle tietosuojavaltuutetun toimistolle.

Säännösten mukaan välitystietoja saa käsitellä ensi sijassa automaattisen hakutoiminnon avulla ja siinä havaitun poikkeaman ja eräiden muiden perusteiden nojalla myös manuaalisesti. Yhteisötilaajalle on asetettu vuosittainen tiedonantovelvollisuus työntekijöiden edustajalle säännöksissä tarkoitetusta välitystietojen käsittelystä. Lisäksi yhteisötilaajan on informoitava käsittelystä myös kyseistä käyttäjää määrämuotoisella selvityksellä.

Sähköisen viestinnän palveluista annetun lain 18 luvun mukaisen mekanismin käyttöön liittyy siinä määrin menettelyllisiä vaatimuksia ja valvontaviranomaiselle tehtävän ennakkoilmoituksen muodossa riskejä yrityksen julkisuuskuvalle, että yritykset eivät ole ottaneet laajasti luvussa tarkoitettua mahdollisuutta käyttöön.

SUOSITUKSIA KYBERTURVALLISUUDESTAAN HUOLEHTIVILLE YRITYKSILLE

- Ymmärrä, mitä olet palveluntarjoajalta hankkimassa.
- Varmistu siitä, että palvelun toimittaja pystyy käytännössä toimimaan siltä edellytetyllä tavalla.
- Varmista, että yrityksen sopimuskäytännöissä huomioidaan lainsäädännön vaatimukset.
- Ota sopimuksissa huomioon, millaisia standardeja organisaatiossasi tulee noudattaa.
- Tiedosta, mitä tietoja palveluun ollaan tallentamassa, miten tieto on luokiteltu ja mikä sen merkitys on yrityksesi toiminnan kannalta.
- Tunnista tietojen käsittelyyn ja tallennukseen liittyvät vaatimukset ja lainsäädäntö.
- Varmista, että palveluntarjoaja pystyy turvaamaan tietojen eheyden ja saatavuuden.
- Sovi lokien pääsyn hallinnasta ja lokien käytön toimenpiteistä.
- Varmista, että yhteys lokeihin on toteutettu niin, että käytännöt ovat lainsäädännön mukaiset ja että lokituksen osalta on määritetty, mitä lokitetaan ja kuinka kauan.
- Varmista, että oikeudet järjestelmiin on annettu työntekijän roolin ja tarpeen mukaisesti, tarvittaessa myös ulkopuoliselle palveluntarjoajalle tai viranomaiselle. Huomioi lokitietojen hyödyntämisessä siirrettävyys sekä luottamuksellisuus.
- Varmista, että lokien hallintaan liittyvät tarpeet, esimerkiksi datan luovuttamisen määräajat viranomaispyyntöjen vuoksi, on katettu sopimuksessa.
- Huomioi hankintaprosessissa myös edellä mainittujen seikkojen varmistus ja esimerkiksi integraatioiden rakentaminen palveluntarjoajan lokitietoihin.
- Huomioi sopimuksessa mahdolliset auditointivaatimukset, kuten ennakkoilmoitukset, auditointikriteeristö sekä kustannusjako.

SUOSITUKSIA IT- JA TIETOTURVAPALVELUIDEN PALVELUNTARJOAJILLE

- Tiedosta, mitä tietoja asiakas haluaa palveluun tallentaa, miten tieto on asiakasyrityksessä luokiteltu ja mikä sen merkitys on asiakkaan toiminnan kannalta.
- Tunnista tietojen käsittelyyn ja tallennukseen liittyvä lainsäädäntö ja vaatimukset, esim. henkilötietojen osalta tietosuojalaki ja -asetus
- Varmista, että asiakasyrityksen tietojen eheys sekä saatavuus pystytään turvaamaan ja että asiakkaan vaatima taso on selkeästi määritelty.

- Sovi asiakasyrityksen kanssa lokien pääsyn hallinnasta ja lokien käytön toimenpiteistä.

- Varmista, että yhteys lokeihin on toteutettu niin, että lokituskäytännöt ovat lainsäädännön mukaiset ja että lokituksen osalta on määritetty, mitä lokitetaan ja kuinka kauan.

- Varmista, että oikeudet järjestelmiin on annettu käyttäjän roolin ja tarpeen mukaisesti, tarvittaessa myös muulle palveluntarjoajalle tai viranomaiselle. Huomioi lokitietojen hyödyntämisessä niiden siirrettävyys sekä luottamuksellisuus.

- Varmista, että lokien hallintaan liittyvät tarpeet, esimerkiksi datan luovuttamisen määräajat viranomaispyyntöjen vuoksi, on katettu sopimuksessa. Huomioi myös tarjottava palveluympäristö.

- Varmista, että asiakkaan varautumisessa on huomioitu mahdolliset auditointivaatimukset, esim. ennakkoilmoitukset, auditointikriteeristö ja kustannusjako.

PALVELUN YLLÄPITOVAIHEESSA JA VARAUTUMISESSA HUOMIOITAVAA

SUOJAA ORGANISAATIOSI TOIMINTA JA TURVAA JATKUVUUS

Organisatoriset järjestelyt

Tietojen ja järjestelmien suojaamisessa yrityksen henkilöstöllä on tärkeä asema. Työelämän tietosuojalaki edellyttää, että henkilöstölle annetaan ennalta ohjeet tietoverkon ja järjestelmien käytöstä ja kerrotaan teknisen valvonnan menetelmistä. Ohjeistus ja valvonnan perusteet voidaan käsitellä yhteistoimintamenettelyssä, mutta ne voidaan antaa myös muunlaisena sisäisenä ohjeistuksena. Valvontakäytännöt kannattaa käydä läpi säännöllisesti henkilöstön edustajien kanssa, eikä vain silloin, kun suunnitellaan ja otetaan uutta käyttöön. Oma roolinsa tässä on myös organisaation mahdollisella tietosuojavastaavalla. Tietosuojavaltuutetun toimisto on myös julkaissut toimintaohjeet yksityisyyden tarkistamiseksi työpaikalla.

Laissa sähköisen viestinnän palveluista, sen 17 luvussa säädetään sähköisen viestin ja välitystietojen käsittelystä. Sääntelyn lähtökohta, viestinnän luottamuksellisuus, esitellään 136 §:ssä. Sen mukaan viestinnän osapuolilla on toisistaan riippumaton oikeus käsitellä omia viestejään ja niiden välitystietoja. Muita sähköisiä viestejä kuin yleisesti vastaanotettavaksi tarkoitettua radioviestintää saa käsitellä vain viestinnän osapuolen suostumuksella tai jos laissa niin säädetään.

Viestien ja välitystietojen käsittelyperiaatteita on linjattu lain 137 §:ssä, jonka mukaan sähköisten viestien ja välitystietojen käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa, eikä sillä saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Käsittelyn jälkeen sähköiset viestit ja välitystiedot on hävitettävä tai välitystiedot tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, jollei laissa toisin säädetä.

Viestinnän tietoja saa luovuttaa ainoastaan tahoille, joilla on oikeus niitä käsitellä. Viestinnän tietoja saa käsitellä vain viestinnän välittäjän tai tilaajan lukuun toimiva henkilö.

Viestien ja välitystietojen käsittely on luonnollisesti sallittu viestinnän välittämiseksi, sovitun palvelun toteuttamiseksi sekä tietoturvasta huolehtimiseksi (138 §). Muita sallittuja käsittelyperusteita ovat laskutus, markkinointi, tekninen kehittäminen, tilastollisen analyysin tuottaminen, väärinkäytöstapaukset, käsittely virheen tai teknisen vian havaitsemiseksi.

Lain 145 § mukaan viestinnän välittäjän on tallennettava yksityiskohtaiset tapahtumatiedot luottamuksellisuuden ja yksityisyyden suojan kannalta keskeisiä välitystietoja sisältävissä tietojärjestelmissä tapahtuvasta välitystietojen käsittelystä, jos se on teknisesti ja ilman kohtuuttomia kustannuksia mahdollista. Tapahtumatiedoista on käytävä ilmi käsittelyn ajankohta, kesto ja käsittelijä. Tapahtumatiedot on säilytettävä kaksi vuotta niiden tallentamisesta.

Niin sanotun varjo-IT:n eli esimerkiksi henkilöstön käyttämien kuluttajapalveluiden (iCloud, Dropbox, Slack, Trello jne.) tai muuten itsenäisesti hankittujen palveluiden osalta on huomioitava niiden käyttöehdot sekä tietosuoja- ja turvallisuuslupaukset. Suositeltavaa onkin joko mahdollisuuksien mukaan ohjeistaa henkilöstöä käyttämään työtehtävissä muita kuin kuluttajapalveluita tai vähintäänkin neuvoa niiden käytössä tai hankkia palveluille yrityslisenssi.

Havainnointikyvyn kohentaminen

Tietoturvaloukkauksien selvittämisen ja yrityksen toiminnan jatkamisen turvaamisen kannalta on tärkeää varmistaa, että loukkaus havaitaan mahdollisimman nopeasti. Tällöin yrityksen tulee määritellä, mitkä tekijät ovat hälyttäviä: esimerkiksi se, että Kyberturvallisuuskeskuksen huoltovarmuuskriittisille toimijoille ja valtionhallinnolle suunnatun

tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä HAVARO antaa ilmoituksen. On kuitenkin syytä huomioida myös muut viitteet tavallisesta poikkeavasta käytöstä. Valvonta- eli SOC-palvelut (Security Operations Center -palvelut) edellyttävät usein merkittävää panostusta, mutta ovat edellytys tehokkaalle varautumiselle. Mikäli yrityksen käsittelemillä tiedoilla ei ole maantieteellisiä rajoituksia, voi SOC-palvelun hankkia myös ulkomaiselta toimijalta.

Yrityksen on kyettävä huomaamaan ja yksilöimään poikkeukselliset kirjautumiset sen eri järjestelmiin. Keskitetty lokijärjestelmä auttaa lokitietojen saamisessa ja saastuneen työaseman nopeassa tunnistamisessa.

Tietoturvasta huolehtiminen

Laki sähköisen viestinnän palveluista ja sen 272 § sallii verrattain joustavat mahdollisuudet teleyrityksille, yhteisötilaajille ja lisäarvopalvelun tarjoajille ryhtyä välttämättömiin toimiin tietoturvasta huolehtimiseksi.

Pykälän mukaan toimijoilla on oikeus ryhtyä välttämättömiin toimiin

1. viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi

2. viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi tai

3. viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.

Tietoturvatoimet voivat käsittää

1. viestin sisältöä koskevan automaattisen selvittämisen

2. viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen

3. tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä ja

4. muut 1–3 kohdassa tarkoitettuihin rinnastettavat teknisluonteiset toimenpiteet.

Pykälä sallii myös viestin sisällön käsittelyn manuaalisesti. Tällöin tulee olla ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn. Tähän voidaan päätyä viestin tyypin, muodon tai muun vastaavan seikan perusteella. Lisäksi manuaalisen käsittelyn edellytyksenä on, että sisällön automaattisella selvittämisellä ei pystytä turvaamaan tietoturvan toteutumista.

Lokituskäytännöt

Nopea reagointi tietoturvaloukkaukseen sekä ymmärrys siitä, mihin tietoihin ja järjestelmiin loukkaajalla on ollut pääsy, edellyttää keskitettyä lokijärjestelmää. Palvelun hankintavaiheessa tulisi vähintään määritellä, miten häiriötilanteiden selvittämisessä tarvittavat lokitiedot tai pääsy niihin ovat saatavilla.

Jos keskitetyssä palomuurissa ja palvelinympäristössä myös lokit on keskitetty, voi palveluntarjoajan olla haastavaa eritellä yhden asiakkaan lokeja muista. Lisäksi on mahdollista, että joku muu toimija kuin lokijärjestelmän toimittaja ylläpitää järjestelmää, jolloin toimittajalle esitettyyn palvelupyyntöön reagoiminen edellyttää lokitietoihin pääsyn oikeuksien selvittämistä. Asiakasorganisaation näkökulmasta olennaista on, mitä saa lokittaa, kuinka kauan lokitietoja saa tai täytyy säilyttää ja kuka mahdolliseen omaan lokijärjestelmään pääsee.

Kriittisistä järjestelmistä on kerättävä lokia, josta pystyy selvittämään, mitä palvelussa tapahtuu. Yritysten tulee tunnistaa toimintansa kannalta kriittiset palvelut ja se, miten ne toimivat, ketkä niitä käyttävät ja mitä tietoa niihin kertyy. Myös mahdollisesti jaettujen ympäristöjen vaikutukset lokien hallintaan tulee huomioida. Relevanttia tietoa tulee säilyttää riittävän kauan. Yritysten tulisikin sopia, kuka vastaa lokituksesta, sen säilytyksestä ja siitä, miten siihen pääsee käsiksi. Vastaavasti myös varmuuskopioinnin toimivuus ja se, miten pitkältä ajalta varmuuskopiot säilytetään, on oltava sovittuna. Usein yritykset huomaavat tietoturvaloukkauksen liian myöhään, eikä kyseiseltä ajalta ole enää lokitietoja saatavissa.

On tärkeää, että ulkopuoliset eivät pääse käsiksi lokitietoihin ja että ne ovat mahdollista tuomioistuinkäsittelyä varten muutenkin oikeuskelpoiset. Todistelun

luotettavuuden takaamiseksi on pystyttävä osoittamaan, etteivät lokitiedot ole altistuneet tahattomille muutoksille, manipuloinnille tai hävittämiselle.

Kriittisiä kohtia määriteltäessä kannattaa palvelusopimuksissa huomioida myös vasteajat eli esimerkiksi, kuinka nopeasti tietyn ajanjakson lokit tulee olla saatavilla. Jos vasteajoista ei ole sovittu, ei niitä voi palveluntarjoajalta myöskään vaatia. Jos yrityksen omaan toimintaan, esimerkiksi järjestelmien korjausaikoihin, kohdistuu sääntelyä, kannattaa tämä huomioida myös sopimuksissa palveluntarjoajan kanssa.

Riippuen siitä, millainen yrityksen lokienhallinnan tarve on, saattaa olla aiheellista harkita erillisen SIEM -järjestelmän (Security Information and Event Management) hankkimista. SIEM-järjestelmän päätehtävät ovat ympäristön havainnointi, tiedon prosessointi ja havaintojen jatkokäsittely sekä kerätyn syötteen tallentaminen.

Datan käyttöön ja tiedon jakamiseen liittyvät haasteet

Kun yritys määrittelee osto- ja ulkoistamisprosessien vaatimuksiaan, sen tulee ottaa huomioon tietoturva sekä tietojen käytettävyys- ja turvaamisvaatimukset käytettäville palveluille. Vaatimukset voivat koskea muun muassa tietojen käytettävyyttä ja tallennuspaikkaa, yhteistyökumppanin pääsyä tietoihin ja tarkastusoikeutta.

Käytettävien palveluiden reunaehtoja sekä tietojen käytettävyys- ja turvaamisvaatimuksia määritellessä yritysten on huomioitava lainsäädännön mukanaan tuomat rajoitteet. Varsinaisten palveluntarjoajien lisäksi on huolehdittava, että vastuu ulottuu myös alihankkijoihin.

Data Loss Prevention -ratkaisujen tarkoitus on estää tahaton yrityksen luottamuksellisten tietojen paljastuminen. Näiden ratkaisujen sekä esimerkiksi verkon reunalla salauksen purkavien palomuurien tai Office365:n hallinnan mahdollistamien tietoturvaratkaisujen sallittuus lainsäädännön näkökulmasta riippuu pitkälti niiden toteuttamistavasta. Tarve ratkaisuille kasvaa samalla kun pilvipalvelujen tarjonta laajenee.

Koska tämäntyyppisiin ratkaisuihin liittyy lainsäädännöllisiä rajoitteita, eikä ennakoivaa ohjetta ole, voi olla tarpeen kysyä tulkintaa valvovalta viranomaiselta eli Kyberturvallisuuskeskukselta. Tällöin on syytä valmistella tekninen kuvaus siitä, kuka tekee, mitä tekee ja miksi haluaa viestintäpalvelulain tulkintaa. Konkreettisesti tällainen voi olla esimerkiksi yksinkertainen piirros tiedosta, sen käsittelystä sekä

käsittelyn perusteesta. Tulkintaa mietittäessä Kyberturvallisuuskeskuksessa joudutaan purkamaan sekä tekninen toteutus että asiakkaan ja palveluntarjoajan roolit kussakin tilanteessa.

Usein kysymys on myös työelämän tietosuojasta ja henkilötiedoista, jolloin ohjeistusta kannattaa hakea tietosuojavaltuutetun toimistosta. Tietosuoja-asetuksen 35 artiklassa säädetään tilanteista, joissa rekisterinpitäjän olisi tehtävä tietosuojaa koskeva vaikutusarviointi ja sen perusteella asian niin edellyttäessä myös kuultava tietosuojavaltuutettua. Tietosuojavaltuutettu voi muutenkin antaa yksittäisiin rekisterinpitäjien oikeudellisiin kysymyksiin sitovia vastauksia, ellei asiassa ole kysymys johonkin nimenomaiseen tietosuoja-asetuksen tai muun lain kohtaan perustuvasta syystä.

SUOSITUKSIA KYBERTURVALLISUUDESTAAN HUOLEHTIVILLE YRITYKSILLE

- Viestitä henkilöstöllesi, miten häiriö- tai poikkeamatilanteessa tulee toimia. Sen voi tehdä esimerkiksi tietoverkon käytöstä annetulla erillisellä ohjeella tai YT-menettelyssä.
- Huomioi tietoturvaohjeistuksessa ja käyttäjille annetuissa ohjeissa myös mobiililaitteet sekä se, käytetäänkö eri laitteita yrityksen sisäisissä vai ulkoisissa, julkisissa verkoissa.
- Harjoittele toimintatavat häiriötilanteiden varalle ja huomioi harjoittelu sekä harjoittelukustannukset palveluntarjoajan kanssa tehtävässä sopimuksessa.
- Seuraa palvelun tietoturvaa esimerkiksi pitämällä säännöllisiä palvelunseurantakokouksia.

SUOSITUKSIA IT- JA TIETOTURVAPALVELUIDEN PALVELUNTARJOAJILLE

- Huolehdi siitä, että yrityksesi henkilöstöllä on selkeät toimintaohjeet asiakasyritykseen kohdistuvan häiriö- tai poikkeustilanteen varalle.
- Huomioi tietoturvaohjeissa ja käyttäjille annetuissa ohjeissa se, käytetäänkö eri laitteita sisäisissä verkoissa vai ulkoisissa, julkisissa verkoissa. Huomioi myös mobiililaitteet.
- Harjoittele toimintatavat häiriötilanteiden varalle ja huomioi harjoittelu sekä harjoittelukustannukset sopimuksessa.

HÄIRIÖTILANTEISSA HUOMIOITAVAA

REAGOI NOPEASTI JA TOIMI SUUNNITELMALLISESTI

Tietoturvaloukkaukseen vastaaminen

Loukkaukseen vastaamisessa keskeistä on saada mahdollisimman nopeasti ymmärrys siitä, mihin tietoihin ja järjestelmiin loukkaajalla on ollut pääsy. Tämä edellyttää usein sekä viestintään liittyvien tietojen että järjestelmien kirjautumislokien käsittelyä. Yrityksen tulee jo ennakolta kartoittaa, minkälaisia tietoja missäkin järjestelmässä käsitellään: ovatko tiedot puhtaasti tietohallinnollisia, teknisiä tietoja vai mahdollisesti henkilötietoja, viestinnän välitystietoja tai viestinnän sisältöjä? Henkilötietojen osalta tulee määrittää ennen käsittelyn aloittamista tietojen tietosuoja-asetuksen mukainen käsittelyperuste.

Viestinnän sääntelyn kannalta on tärkeä tiedostaa:

1. Onko kyse sähköisestä viestinnästä?

2. Ketkä ovat viestinnän osapuolet? Mikä on yrityksen rooli? Käsitelläänkö tietoja viestinnän välittäjänä?

3. Mikä on sähköisen viestinnän palveluista annetun lain mukainen peruste käsitellä tietoja, jos roolina on viestinnän välittäjä?

4. Onko tietojen käsittely tarpeen tietoturvaloukkauksen selvittämiseksi?

Viestinnän osapuolella on oikeus käsitellä omaa viestintäänsä ja siihen liittyviä välitystietoja. Jos käsiteltäväksi tulee työntekijän viestintä, vaikuttaa sovellettavaan lainsäädäntöön se, mitä, miten ja miksi viestintää käsitellään. Esimerkiksi sähköisen viestinnän palveluista annetun lain 247 §:ssä säädetään viestinnän välittäjän, kuten yhteisötilaajan, velvollisuuksista ja lain 272 §:ssä taas oikeuksista tietoturvasta huolehtimiseksi. Työnantajan oikeutta lukea työntekijän sähköpostiviestejä säädellään muussa lainsäädännössä. Yrityksessä on suositeltavaa määritellä ja ottaa tietoverkon käytöstä annettavaan ohjeeseen esimerkkitilanteita, joissa välitystietojen tietoturvaperusteinen käsittely on tarpeen.

Tietohallinnon keinot

1. Ovatko loukkauksen selvittämiseksi tarvittavat lokitiedot saatavilla?

2. Kuinka nopeasti ja kuinka monen järjestelmän tietojen avulla esimerkiksi haitalliseen osoitteeseen yhteydessä oleva laite voidaan yksilöidä?

3. Kuinka nopeasti ja minkä tietojen perusteella voidaan selvittää, mihin järjestelmiin tai tietoihin saastunut laite on vaikuttanut?

4. Kuinka nopeasti mahdolliselle ulkopuoliselle palveluntarjoajalle on annettavissa pääsy selvittämään asioita?

Jos yrityksen oma havaintokyky on puutteellinen tai järjestelmälokeja katsotaan vain silloin, kun jotain sattuu, ei poikkeuksia pystytä välttämättä havaitsemaan. Asiaa pitää ehdottomasti harjoitella. On myös tärkeää etukäteen suunnitella ja harjoitella sitä, miten häiriöistä viestitään asiakkaille ja muille sidosryhmille.

Organisatoriset järjestelyt

Keskeistä tietoturvaloukkauksen selvittämisessä on yhteistyö yritysten liiketoiminnan, tietohallinnon, lakimiesten ja viestinnän kesken. Toimintakyvyn turvaamiseksi on suositeltua perustaa laaja-alainen ryhmä tietoturvapoikkeamien hallitsemiseksi ja harjoitella toimintaa säännöllisesti. Tietoturvaloukkauksen havaitsemisessa olennaista on, pystytäänkö teknisesti ja käyttäjäraportoinnin osalta tunnistamaan mahdollinen uhka, josta voi tulla tunnistamattomana

loukkaus: pystytäänkö tietoturvaloukkaus havaitsemaan 1) ennakkoon, 2) tilanteen ollessa jo päällä ja 3) jälkikäteen, ja ymmärtääkö yrityksen henkilöstö, että sen tulee olla tarkkana.

Tietoturvatyössä korostuvat tyypillisesti tekninen näkökulma ja erilaiset teknisluonteiset ratkaisut. Työn tekemisen tapojen ja teknisen toimintaympäristön muuttuessa on entistä tärkeämpää pystyä ottamaan tietoturva osaksi yrityksen normaaleja toimintatapoja ja yrityskulttuuria. Ymmärrettävät ja yrityksen toiminnan keskeisiin prosesseihin nivoutuvat tietoturvaohjeistukset ja -käytännöt sekä niistä tiedottaminen henkilöstölle luovat hyvät ja selkeät edellytykset tehokkaalle varautumiselle.

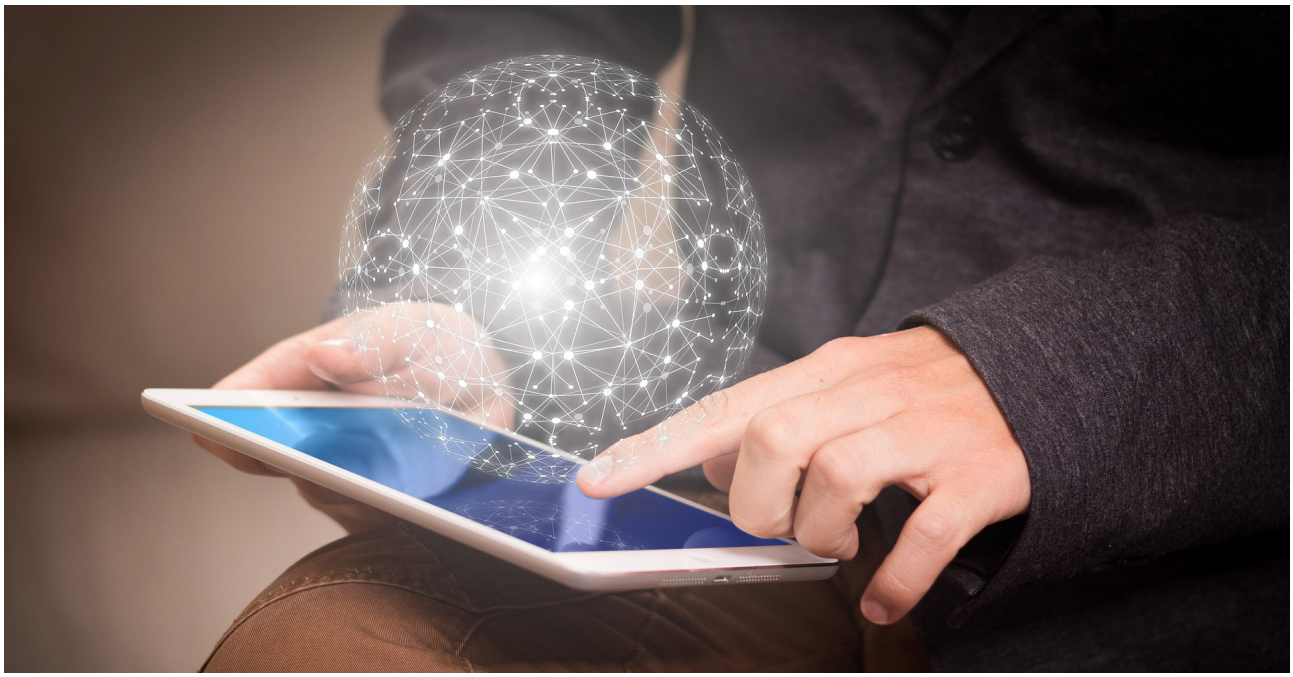
Yleisen tietosuoja-asetuksen 5 artiklan mukaan rekisterinpitäjä vastaa itse siitä, että henkilötietojen suhteen on noudatettu tietosuoja-asetuksen vaatimuksia. Rekisterinpitäjän on myös pystyttävä osoittamaan noudattaneensa asetuksen vaatimuksia, mikä tulee huomioida varautumisessa.

Tietojen käytettävyys- ja turvaamisvaatimukset on syytä viedä kiinteästi yrityksen osto- ja ulkoistamisprosesseihin. Yrityksen tulee omissa vaatimuksissaan määritellä tietoturvan reunaehdot käytettäville palveluille. Vaatimukset voivat koskea mm. tietojen käytettävyyttä ja tallennuspaikkaa, lokitietojen saatavuutta, yhteistyökumppanin pääsyoikeuksia, käyttöoikeuksia, sopimusvelvoitteisiin liittyvää tarkastusoikeutta ja muita vastaavia seikkoja. Ostoprosessin määrittelyssä hyvä käytäntö on tehdä kiinteää yhteistyötä liiketoiminnan ja lakiosaston välillä, jotta varmistetaan vaatimusten huomioiminen osana yrityksen sopimuskäytäntöjä.

Nopean pääsyn turvaaminen työasemalle tai muulle päätelaitteelle

Varsin monessa yrityksessä sovelletaan menettelyä, jossa työasemalla olevien tietojen käsittelyyn hankitaan työntekijältä aina erillinen suostumus. Menettely on tietoturvapalveluita tarjoavan yrityksen toimintatapana perusteltu tapa kontrolloida vastuita. Yrityksen toimintakyvyn varmistamiseksi parempi tapa olisi kertoa noudatettavasta menettelystä työelämän tietosuojalaissa tarkoitetussa tietoverkon käytöstä annettavassa ohjeistuksessa. Tällöin menettelytavat käytäisiin henkilöstön kanssa läpi myös YT-menettelyssä, mikä antaa luontevan pohjan integroida tietoturvatoimenpiteet osaksi yrityksen normaaleja toimintatapoja.

Etukäteen tapahtuva menettelytapojen kuvaaminen edistäisi tietoturvatoimenpiteiden arkipäiväistämistä, ja keskeisin hyöty olisi menettelyn nopeutuminen. Työtapojen monimuotoistuessa ja pilvipalveluiden yleistyessä tietoturvan painopiste siirtyy yritysten verkoista yhä enemmän käyttäjien päätelaitteisiin. Tällöin ohjeistuksessa on syytä huomioida mahdollisuus laitteiden etävalvontaan. Toisaalta päätelaitteita ei voi eritellä toisistaan niiden tyypin mukaan, vaan olennaisempaa on, onko kyseessä yrityksen



omistama vai työntekijän henkilökohtainen laite. Tärkeää on myös se, missä verkossa laitetta käytetään – omien tilojen ulkopuolella julkisessa verkossa, mahdollisesti myös ulkomailla, vai pelkästään toimitilojen sisäisessä verkossa.

Työasema tulisi ymmärtää laajasti niin, että se kattaisi myös pilviympäristössä työntekijän käyttöön annetut resurssit sekä ulottaa tietoturvaohjelmat ja -ohjeistukset myös älypuhelimiin.

Viranomaisyhteistyö

Velvollisuus korjata häiriö

Sähköisen viestinnän palveluista annetun lain 273 §:n mukaan teleyrityksen tai muun verkon tai laitteen haltijan on välittömästi ryhdyttävä toimenpiteisiin tilanteen korjaamiseksi, jos viestintäverkko, viestintäpalvelu tai laite aiheuttaa merkittävää haittaa tai häiriötä viestintäverkolle, viestintäpalvelulle, viestintäverkkoon liitetylle muulle palvelulle, laitteelle, viestintäverkon käyttäjälle tai muulle henkilölle. Jos häiriötä ei saada korjatuksi, tulee häiriötä aiheuttava laite, palvelu tai verkko irrottaa viestintäverkosta.

Euroopan unionin verkko- ja tietoturvadirektiivin (NIS-direktiivi, (EU) 2016/1148) täytäntöönpanon myötä joillekin yhteiskunnan toiminnan kannalta keskeisten digitaalisten palveluiden tarjoajille säädettiin tietoturvallisuuteen liittyvää riskienhallintaa ja häiriöiden raportointia koskevia velvoitteita. Lisäksi säädettiin näiden velvoitteiden valvonnasta, viranomaisten välisestä tietojen vaihdosta sekä yleisestä tietoturvallisuuteen liittyvästä viranomaistoiminnasta.

Häiriöistä ilmoittaminen

Sähköisen viestinnän palveluista annetun lain (SVPL) 275 §:n mukaan teleyrityksen on ilmoitettava viipymättä Liikenne- ja viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus tai muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Teleyrityksen on ilmoitettava myös ilman aiheetonta viivästystä häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään. Liikenne- ja viestintävirasto toimittaa EU-komissiolle sekä Euroopan verkko- ja tietoturvavirastolle vuosittain tiivistelmäraportin ilmoituksista.

SVPL:n lisäksi vastaavat säännökset on lisätty ilmailu-, rautatie- ja alusliikennepalvelulakeihin, alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin, liikenteen palveluista annettuun lakiin, sähkö- ja maakaasumarkkinalakeihin sekä vesihuoltolakiin. Vastaavasti toimivalta valvoa riskienhallinta- ja häiriöraportointivelvoitteita on Liikenne- ja viestintäviraston lisäksi muillakin sektorikohtaisilla valvontaviranomaisilla eli Energiavirastolla, Finanssivalvonnalla sekä ELY-keskuksilla.

Vaatimus viranomaisille ilmoittamisesta kohdistuu aina asiakasyritykseen, mutta käytännön toteutus on usein ulkoistettu. Liikesalaisuudet ovat suurin ongelma, mutta muutenkin on mietittävä ennakkoon, minkä tyyppisestä tiedosta (luottamukselliset tiedot, välitystiedot, henkilötiedot tms.) on kyse. On siis tunnistettava, mitä tietoa käsitellään, millä oikeuksilla niitä käsitellään, mistä tietoa kerääntyy, mihin sitä käytetään sekä mitä alihankkija saa milläkin tiedolla tehdä tai mihin sen luovuttaa. Tämä riippuu paljon siitä, millä alalla asiakas toimii.

Sääntelyssä on usein tarkastuslista erilaisista teknisistä seikoista. Esimerkiksi EU-komission digitaalisten palvelujen tarjoajia koskevalla täytäntöönpanoasetuksella ((EU) 2018/151) tarkennetaan NIS-direktiivin vaatimuksia digitaalisille palveluille. Sääntelystä ei selviä vaadittava ICT-suoritustaso kaikkeen mahdolliseen, mutta palveluita sekä ostaessa että myytäessä kannattaa listatut asiat, esimerkiksi tilaturvallisuus ja testaus, ottaa huomioon.

Palveluntarjoajan ei pidä tehdä ilmoitusta Kyberturvallisuuskeskukselle eikä luovuttaa asiakasdataa tai vastata sen mahdollisiin kysymyksiin ilman asiakasyrityksen siunausta. Jos yritys haluaa antaa luvan luovuttaa tietoja Kyberturvallisuuskeskukselle, kannattaa tästä sopia palveluntarjoajan kanssa etukäteen. Tällöin säästyy aikaa itse asiaan, eli tietoturvatilanteen selvittämiseen.

Kyberturvallisuuskeskus ei tee yritysten tai yhteisöjen puolesta rikosilmoituksia. Se ei myöskään lähtökohtaisesti luovuta sille annettuja tietoja esimerkiksi poliisille, ellei ilmoituksen tekijä tähän nimenomaisesti anna lupaa. Keskukselle ilmoitusta tehdessä voi määritellä, voiko ilmoituksen tietoja jakaa poliisin kanssa. Kyberturvallisuuskeskus kehottaa usein tekemään loukkauksesta rikosilmoituksen.

NIS-direktiivin ilmoitusvelvollisuus ei hyödytä poliisia, joten olisi hyvä, että yrityksillä olisi harjoiteltu prosessi siitä, miten eri ilmoitusten kanssa toimitaan. Poliisin kanssa tehtävää yhteistyötä helpottaa paljonkin se, että tietoturvaloukkauksen selvitystyössä käytettävä työkopio tehdään niin, että se kelpaa sellaisenaan myös poliisin tekniseen tutkintaan.

Tietosuojavaltuutetun toimisto on julkaissut oman ohjeistuksensa tilanteista, joissa tietosuojaloukkaus edellyttää ilmoittamista viranomaiselle tai rekisteröidylle itselleen. Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava ilman aiheetonta viivytystä myös rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille.

Rikoslain 38 luvun 10 § mukaan syyttäjä ei saa nostaa syytettä viestintäsalaisuuden loukkauksesta, törkeästä viestintäsalaisuuden loukkauksesta, tietojärjestelmän häirinnästä, tietomurrosta tai suojauksen purkujärjestelmärikoksesta, ellei asianomistaja tee rikosilmoitusta tai ellei rikoksentekijä rikosta tehdessään ole ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa tai ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista. Kyseiset rikokset ovat asianomistajarikoksia, joiden tutkittavaksi ottaminen edellyttää asianomistajan tutkintapyyntöä sekä rangaistusvaatimusta.

Viranomaisille tehtävissä ilmoituksissa on prosessien lisäksi otettava huomioon myös yhteyskäytännöt ja rajapinnat. Käytännön harjoittelun osana tulee olla myös se, mihin konkreettisesti otetaan yhteyttä. Määritellyn ja harjoitellun prosessin tuloksena saattaa olla yhteydenottotarve viranomaiseen.

Yhteyskäytäntöjen määrittely ei myöskään koske pelkästään viranomaisia, vaan on myös muita sidosryhmiä, joille kaikille tulee olla paikalliset yhteystiedot. Koska trendinä on rajapinnan yhdenmukaistaminen, yhteyskäytäntöjä pitäisi ulottaa laajemminkin sidosryhmiin pelkkien yhteystietojen vaihtamisen lisäksi. Etukäteen pitäisi sopia, millaisesta asiasta ja milloin tiedotetaan, kuka hoitaa julkisen tiedotuksen ja niin edelleen. Monitoimittajaympäristössä toimittajien välisten viestiketjujen on oltava kunnossa. Jos kaikilla toimijoilla on erilaiset käytännöt, täytyy häiriönhallinta synkronoida viimeistään ennen tuotantovaihetta.

Kaikilla tulee olla tiedossa, kuka johtaa ja mikä on prosessin etenemisjärjestys. Viestintää kannattaa harjoitella ja tarkastella, toimiko viestintäprosessi niin kuin oli suunniteltu. Hyvänä käytäntönä on esimerkiksi eräänlainen tilannepäiväkirja toimista.

SUOSITUKSIA KYBERTURVALLISUUDESTAAN HUOLEHTIVILLE YRITYKSILLE

- Selvitä etukäteen, mitä tietoja yritykseesi kohdistuvassa häiriö- tai loukkaustilanteessa voidaan käsitellä, kenen toimesta ja millä perusteella.
- Varmista, että yrityksessäsi on kyky havaita siihen kohdistettu tietoturvaloukkaus tai sen uhka.
- Varmista, että saastunut tunnus, laite tai järjestelmä pystytään yksilöimään ja että kyberloukkaukseen pystytään reagoimaan mahdollisimman nopeasti.
- Määrittele prosessit asiakkaille, sidosryhmille, palveluntarjoajille sekä eri viranomaisille tehtäviä ilmoituksia varten.

SUOSITUKSIA IT- JA TIETOTURVAPALVELUIDEN PALVELUNTARJOAJILLE

- Selvitä etukäteen, mitä tietoja asiakasyrityksesi häiriö- tai loukkaustapauksessa voidaan käsitellä, kenen toimesta ja millä perusteella.
- Varmista, että asiakasyritykseen tai omiin järjestelmiin kohdistettu tietoturvaloukkaus tai sen uhka on mahdollista havaita.
- Varmista, että saastunut tunnus, laite ja/tai järjestelmä pystytään yksilöimään ja että kyberloukkaukseen pystytään reagoimaan mahdollisimman nopeasti.
- Määrittele prosessit asiakkaille, sidosryhmille sekä eri viranomaisille tehtäviä ilmoituksia varten. Esim. henkilötietoihin kohdistuvasta tietosuojaloukkauksesta tulee tehdä ilmoitus rekisteröidylle viipymättä ja tietosuojavaltuutetun toimistolle 72 tunnin kuluessa.

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

FiCom
TIETOLIIKENTEEN
JA TIETOTEKNIIKAN
KESKUSLIITTO FiCom ry