Finnish Information Security Cluster Kyberala

NIS2-SOVELTAMISOPAS, 0.9 (BETA)

Kyberala ry (FISC)

Email: kyberala@teknologiateollisuus.fi

Website: www.fisc.fi

SISÄLLYSLUETTELO

LUKIJALLE

Saatesanat: Jarno Limnéll

Kyberturvallisuus on otettava vakavasti

Elämme maailmassa, jossa teknologiaa kehitetään nopeammin ja radikaalimmin kuin koskaan aikaisemmin ihmiskunnan historiassa – ja vauhti kiihtyy. Teknologian kehitys ja digitalisaatio vaikuttavat laaja-alaisesti niin koko yhteiskuntaamme ja työtehtäviimme kuin meidän jokaisen arkipäiväämme. Uusien mahdollisuuksien ja toimintatapojen ohella kehitys luo myös uudenlaisia haavoittuvuuksia ja uhkia – ja siksi kyberturvallisuus on yhä tärkeämpi asia. Tärkeää on ymmärtää, että kun teknologia kehittyy ja sitä sovelletaan jatkuvasti uusilla tavoilla, on myös kyberturvallisuus asia, mitä on jatkuvasti kehitettävä. Kyberturvallisuuden huolehtiminen ei ole projekti vaan jatkuva prosessi. Periaate koskee niin lainsäädäntötyötä eduskunnassa, julkisen sektorin ja yrityksien sekä organisaatioiden varautumista kuin meidän jokaisen oman osaamisen jatkuvaa kehittämistä.

Tähän erinomaiseen NIS2-soveltamisoppaaseen kannustan tutustumaan huolella. Euroopan unionin verkko- ja tietoturvadirektiivin eli NIS2-direktiivin kansallinen soveltaminen astuu meillä Suomessa voimaan lokakuussa 2024. Tiivistäen sanoen – tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta kriittisiksi katsottujen sektoreiden ja toimijoiden osalta.

Valitettavasti elämme turvallisuuspoliittisesti aikaa, jossa fyysisen maailman pahantahtoisuus ja epävakaus heijastuvat myös kybermaailmaan. Valtiolliset ja ei-valtiolliset toimijat pyrkivät kybermaailmassa horjuttamaan yhteiskuntaamme tai esimerkiksi saamaan taloudellista hyötyä. Hybridivaikuttamisessa keihäänkärkinä ovat usein juuri kyberhyökkäykset ja kybermaailmassa tapahtuva informaatiovaikuttaminen. On ymmärrettävä, että yhä digitaalisempi yhteiskuntamme on uudella tavalla haavoittuva.

Vastuu ja luottamus ovat kyberturvallisuudessa avainasemassa. Kyberturvallisuudesta huolehtimisessa on tunnettava oma vastuunsa, sillä kyberturvallisuudesta huolehtimisella on hyvin tärkeä merkitys luottamusyhteiskuntamme pysyvyyteen.

NIS2-direktiivissä on kyse koko yhteiskuntamme vakauden ja turvallisuuden ylläpitämisestä. Tämä soveltamisopas tarjoaa direktiivin soveltamiseen erinomaiset valmiudet maamme korkean kyberturvallisuuskulttuurin ylläpitämiseen muuttuvassa maailmassa. Yhdessä toimien.

Jarno Limnell, Kansanedustaja ja kyberturvallisuuden dosentti

Aluksi

Tämä opas on julkaistu ennen asiaa koskevan kansallisen lainsäädännön voimaantuloa ja perustuu luonnokseen Hallituksen esitykseksi eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Tästä syystä opas on nimetty versionumerolla 0.9 (Beta).

Opas päivitetään lopullista lainsäädäntöä sekä viranomaisen tulkintaohjeistoa vastaavaksi tietojen tultua saataville. Erityisen suuria muutoksia lopulliseen lainsäädäntöön ei ole odotettavissa, sillä sääntelyn pohjalla on asiaa koskeva EU-direktiivi (NIS2), jonka vähimmäissisällöstä ei voida kansallisesti poiketa.

Oppaan ”ennenaikaisen” julkaisun perusteena on varsin lyhyeksi jäävä aika soveltamisalaan kuuluville toimijoille toimeenpanna lain vaatimukset. Lain soveltaminen alkaa 18.10.204. Sääntely tuo mukanaan sekä merkittävän laajennuksen sovellettavien organisaatioiden määrään sekä kyberturvallisuuden riskienhallinnan sisällöllisiin vaatimuksiin.

NIS2- eli Network and Information Security -direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta kriittisiksi katsottujen sektoreiden ja toimijoiden osalta. Tämä toteutetaan asettamalla lain soveltamisalaan kuuluville toimijoille velvoittavia riskienhallintatoimia kyberturvallisuushäiriöiden varalta. Pahantahtoisten, laittomin keinoin toimivien yksilöiden ja ryhmien aiheuttama riski sekä verkko- ja tietojärjestelmien toiminnalle että niissä säilytettäville tiedoille on edelleen kasvamassa. Tästä syystä on edelleen perusteltua kohdistaa toimia pahantahtoisilta toimilta suojautumiseen. Yhteiskunnan toiminnan kannalta niin julkinen sektori kuin keskeisten yksityisen sektorin toimijoiden digitaalisten riskien hallintatoimet ovatkin direktiivin keskiössä. On tärkeää huomata, että Suomessa suurin osa digitaalisesta infrastruktuurista, tietojärjestelmistä sekä tiedosta on yhtiöiden hallussa.

NIS2-direktiivi vaikuttaa kaikissa EU:n jäsenvaltioissa toimivien organisaatioiden liiketoiminnan johtamiseen, teknologia- ja kumppanivalintoihin sekä operatiiviseen

valvontaan. Toimijoiden tulee muun muassa tunnistaa ja arvioida säännöllisesti kyberriskejä, toteuttaa riskiperusteiset suojaustoimet, pidettävä yllä poikkeamien hallintasuunnitelmaa ja raportoitava kyberhäiriöistä määräajassa ja -muotoisesti. Yrityksen toimiva johto vastaa kyberturvallisuuden toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Tämä tarkoittaa, että toimivan johdon yleinen vastuu ulottuu säädöksen myötä myös erikseen määritetylle kyberturvallisuuden tehtäväalueelle.

Laki määrittää sen piiriin kuuluvat toimialat, joihin kuuluvat organisaatiot jaetaan keskeisiin ja tärkeisiin toimijoihin toimialan yhteiskuntakriittisyyden ja toimijan koon mukaan. Sekä keskeisiin että tärkeisiin toimijoihin kohdistuvat samat vaatimukset, mutta keskeisiin toimijoihin kohdistetaan etukäteisvalvontaa. Myös sanktiot ovat keskeisille toimijoille kovemmat.

NIS2-direktiivin asettamat velvoitteet digitaalisten riskien hallinnan vahvistamiseksi turvaavat toimijoiden (liike)toiminnan jatkuvuutta, jolla on positiivisia vaikutuksia kannattavuuteen erityisesti pitkällä aikavälillä. Direktiivin vaatimusten täyttämisestä aiheutuu yrityksille kustannuksia, mutta kustannukset tukevat tällöin toimitusvarmuutta ja ovat luonteeltaan ennustettavia, toisin kuin puutteellisesta digitaalisten riskien hallinnasta johtuvissa ongelma- ja epäjatkuvuustilanteissa. Riskien toteutuminen aiheuttaa tyypillisesti ennustamattomia, sekä suoria että epäasuoria kustannuksia, joiden yhteydessä voi syntyä myös vahingonkorvausvelvollisuuksia. Kilpailuedun näkökulmasta etuja voidaan hahmottaa kahdella tavalla: mitä nopeammin lain vaatimukset on saavutettu, sitä todennäköisemmin asiakas suosii vaatimuksenmukaisuuden kattavasti täyttävää ja osoittavaa toimittajaa; ylittämällä direktiivin edellyttämät vähimmäisvaatimukset toimija voi myös saavuttaa kilpailuetua. Yritykset hyötyvät myös laajemmin yhteiskunnan kyberkestävyyden vahvistumisesta ja luotettavammasta ja ennakoivammasta toimintaympäristöstä, joihin direktiivi vaikuttaa myönteisesti.

Kyberala ry. on laatinut tämän dokumentin helpottamaan yrityksiä johtamaan kokonaisturvallisuuttaan ja auttamaan muuttuvien velvoitteiden täyttämisessä. Suomeen sijoittautunutta kyberturvallisuusteollisuutta edustavan yhdistyksen jäsenten yhteinen, koko toimialan laajuinen projekti NIS2-direktiivin soveltamisoppaan laatimiseksi käynnistyi syksyllä

2023. Oppaan laatimisessa on ollut mukana 18 yhtiötä monipuolisesti kyberturvallisuusalan eri sektoreilta. Kyberala on seurannut aktiivisesti NIS2-direktiivin käsittelyä ja vaikuttanut sen sisältöön. Yhdistys kannattaa vahvasti direktiivin tavoitteita ja on sitoutunut tekemään oman osuutensa sen onnistuneen toimeenpanon varmistamiseksi.

Uusien velvoitteiden tulkitseminen ja noudattaminen voi osoittautua haasteelliseksi monille direktiivin soveltamisalaan kuuluville yrityksille. Soveltamisopas valjastaa kotimaisten kyberturvallisuusalan asiantuntijoiden osaamisen ja kokemuksen apua kaipaavien toimijoiden tueksi. Soveltamisopas avaa uusien velvoitteiden sisältöä selkokielisesti ja havainnollistaa käytännön esimerkein digitaalisten riskien hallinnan sekä liiketoiminnan jatkuvuuden turvaamisen merkitystä.

Kyberturvallisuuden riskienhallinnan laiminlyöminen voi johtaa merkittäviin hallinnollisiin seuraamuksiin, kuten miljoonien eurojen sakkoihin, palvelutoiminnan keskeytyksen tai johtotehtävissä toimimisen estämiseen.

Toimivaa johtoa sitoo huolellisuusvelvoite ja se vastaa yhtiön edun mukaisesta toiminnasta. Huolimattoman toiminnan seurauksena johdon edustajat voivat joutua korvaamaan aiheuttamansa taloudellisen vahingon.

Tiivistelmä

Tietoturvallisuus tarkoittaa sekä verkko- ja tietojärjestelmien toiminnan että niissä säilytettävien tietojen suojaamista. Tieto on usein arkaluontoista tai luottamuksellista, eli niiden luonne tai paljastuminen voi vaarantaa yrityksen maineen, työntekijöiden yksityisyyden, kansallisen turvallisuuden tai valtion edut, kuten taloudellisen kestävyyden.

Kyberturvallisuus on toimintaa, jolla pyritään estämään viestintäverkkojen, tietojärjestelmien ja niiden käyttäjien vahingoittuminen, häirintä tai muu haitta. Kyberturvallisuuden riskienhallinnalla varmistetaan, että toimintaprosessien, tietoverkkojen ja -järjestelmien avulla pystytään tunnistamaan ja ehkäisemään tapahtumia, jotka uhkaavat niiden kautta saatavilla olevien palvelujen (ts. tietojen) saatavuutta, aitoutta, eheyttä tai luottamuksellisuutta. Riskienhallinnan lähtökohtana on tunnistaa luottamuksellisuuteen, eheyteen, saatavuuteen ja aitouteen liittyvät tarpeet sekä toimintojen kannalta keskeiset palvelut, järjestelmät, prosessit ja henkilöt.

Digitaaliset palvelut, kuten verkko- ja tietojärjestelmät, ovat yhteiskuntamme ja taloutemme kulmakivi. Niitä tuottavat sekä yksityiset yritykset että julkishallinto, palveluihin kohdistuu jatkuvasti uusia kyberuhkia. Kyberrikollisten motiivit voivat olla taloudelliset ja/tai poliittiset. Yksittäisen yrityksen merkitystä tai palveluiden menetyksen vaikutuksia ja seurauksia on vaikea arvioida ulkopuolelta. Siksi kaikki yritykset ovat yhtä lailla haavoittuvia kyberrikollisuudelle, paitsi se pienempi joukko toimijoita, jotka ovat erityisen kiinnostavia joko toimintansa luonteen tai asemansa takia.

NIS2-direktiivi edellyttää, että organisaatiot pystyvät tekemään määrätietoista, ohjattua ja dokumentoitua riskipohjaista päätöksentekoa oman toimintansa eri tasoilla. Päätöksenteon perusteet ja taustatiedot on kyettävä esittämään selkeästi ja ymmärrettävästi.

Toimivan johdon eli hallituksen jäsenten ja toimitusjohtajan, sekä soveltuvin osin toimitusjohtajan välittömässä alaisuudessa olevien johtajien on perehdyttävä kyberturvallisuusriskeihin ja hallintakeinoihin. Velvoitteiden täyttäminen edellyttää, että yritykset tuntevat hyvin oman toimintansa ja eri sidosryhmien merkityksen sekä vaatimukset sekä palveluiden tuottamiseen. Omaa toimintaympäristöä tulee säännöllisesti tarkastella suhteessa vaatimuksiin, jotka syntyvät sekä lainsäädännön että uhkakentän muutoksesta.

Tämä tarkoittaa, että organisaatioiden on huomioitava kyberturvallisuuden hallinnassaan mm. teknologiset, fyysiset, geopoliittiset, hallinnolliset, henkilöstö, ja liiketoiminnalliset riskit sekä niiden mahdolliset vaikutukset toimintaansa. Tämä vaatii laaja-alaista asiantuntemusta ja osaamista organisaation eri tasoilla, sekä oman toiminta- ja uhkaympäristön jatkuvaa seurantaa.

Direktiivin myötä toimivan johdon vastuulla on luoda ja ylläpitää kyberturvallisuutta tukevaa yrityskulttuuria. Tämä tarkoittaa tarkoituksenmukaisia, määriteltyjä ja koulutettuja toimintamalleja ja ohjeita, sekä henkilöstön pyrkimyksiä niiden noudattamiseen. Kyberhygienia eli perustason tietoturvakäytännöt (toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi) puolestaan yhdistää tietoturvallisen yrityskulttuurin turvallisiin työkaluihin ja tietojärjestelmiin. Perustason tietoturvakäytännöt ovat kokoelma laissa, ja siten myös tässä oppaassa esitetyistä vaatimuksista, ns. ydinsisältömuodossa:

1. Toimija on ohjeistanut perustason tietoturvakäytännöt henkilöstölle, alihankkijoille ja muille kumppaneille.
2. Toimija on tunnistanut kriittisimmän omaisuutensa.
3. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä.
4. Toimija on erottanut kriittiset ja haavoittuvat viestintäverkot ja tietojärjestelmät muista ympäristöistä.
5. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä haitallisia ja luvattomia ohjelmistoja vastaan.
6. Toimija on järjestänyt tunnistautumisen sisäisiin ja ulkoisiin palveluihinsa ja laitteisiinsa turvallisesti.
7. Toimija on erottanut järjestelmiensä pääkäyttäjätunnukset ja korotettujen oikeuksien tunnukset muista tunnuksista.
8. Toimija on varmistanut, että sen luottamuksellista tietoa käsitellään turvallisesti.
9. Toimija on huolehtinut, että sen järjestelmiä päivitetään säännöllisesti ja kriittiset päivitykset asennetaan viivytyksettä.
10. Toimija on huolehtinut, että sen palvelut ja laitteet on turvallisesti konfiguroitu.
11. Toimija on huolehtinut, että sen kriittiset palvelut ja tieto-omaisuus on varmuuskopioitu.
12. Toimija on varautunut, miten sen toiminta voidaan ylläpitää vakavissa poikkeamissa.
13. Toimijalla on käytössään kriittisten toimintojen tapahtumakirjaus (loki).

Ns. kyberhygienia sisältää tietoturvan ja tietotekniikan hyviä ja vakiintuneita käytäntöjä ja toimintoja, kuten tietoturvapäivitysten asentamisen, vahvojen salasanojen ja tunnistautumistapojen käyttämisen, tietoturvalokien keräämisen ja hyökkäyspinnan pienentämisen rajaamalla sallitut toiminnot ja toiminnallisuudet vain tarpeellisiin. Tämä on verrattavissa lääketieteelliseen hygieniaan, jossa eri ympäristöillä on erilaiset vaatimukset, mutta joissakin toimenpiteissä, kuten käsien pesussa, on yhteinen perustelu. NIS2-direktiivi ohjaa yrityksiä määrittämään perustellun kyberhygienian tason oman toimintansa ja yhteiskunnallisen roolinsa pohjalta. Tämä ohje antaa tukea ja ideoita tämän tehtävän suorittamiseen sekä esittää asiantuntijoiden näkemyksiä hyvän kyberhygienian minimitasosta. On hyvä huomata, että lainsäädännön kautta syntyy uusia velvoitteita lain tarkoittamien toimijoiden lisäksi myös toimitusketjun osana toimiville yrityksille, joiden tulee näin ollen myös varmistaa riittävä kyberturvallisuuden taso. Viranomaisvalvonnan kannalta luetteloa voidaan käyttää riskienhallintatoimien kattavuuden varmistamiseen, mutta on tärkeää huomata, että esimerkiksi pelkkä varmuuskopioiden olemassaolo ei välttämättä riitä suojautumaan tai palautumaan vakavalta häiriöltä, sillä usein pahantahtoiset toimijat pyrkivät estämään varmuuskopion käytön, mikäli varmuuskopiointia ei ole organisoitu laadukkaalla, kattavalla ja turvallisella tavalla.

Tässä oppaassa kuvataan, miten NIS2-direktiivin perusteella annetut kansalliset kyberturvallisuuden riskienhallinnan vaatimukset voidaan toteuttaa hyödyntäen kolmen laajalti tunnistetun tietoturvan hallintajärjestelmän sopivimpia osa-alueita. Tarkoituksena on havainnollistaa lainsäädännön vaatimusten perusteita, kuvata vaatimuksiin perustuvia kyberturvallisuuden riskitasoon tosiasiallisesti vaikuttavia keinoja ja näin tukea toimijoita täyttämään lain vaatimukset sekä saavuttamaan riskien hallinnan etuja päivittäistoiminnassaan.

Kyberturvallisuuden johtaminen voi olla erittäin haastavaa ilman toimintaa tukevaa hallintajärjestelmää, englanniksi ”Information Security Management System” (ISMS). NIS2-direktiivi ei suoraan velvoita yrityksiä minkään tietyn hallintajärjestelmän toteuttamiseen, mutta käytännössä velvoitteiden todentaminen ja vaatimusten täyttäminen on erittäin vaikeaa ilman dokumentointiin nojautuvaa järjestelmällistä hallintamallia. Kyberala suosittelee, että toimijat huomioivat kyberturvallisuuden toimintastrategiassaan ja asettavat muiden

tavoitteiden kanssa linjassa olevat kyberturvallisuuden keskeiset tavoitteet. Toimijat voivat myös laatia erillisen kyberturvallisuusstrategian, jossa on määriteltynä keskeisimmät tavoitteet kybertuvallisuudelle. Joka tapauksessa tavoitteiden tulee tukea toimijan muita strategisia tavoitteita ja olla myös mitattavia.

Kyberala on valinnut tuekseen seuraavat hallintamallit (viitekehykset): NIST Cybersecurity Framework 2.0 (NIST-CF), Cybersecurity Capability Maturity Model (C2M2) sekä ISO 27001:2022. Oppaassa on käytetty hyväksi myös Traficomin suositusta NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä (18410/09.00.02/2023). Ko. viitekehyksien mukainen lähestymistapa mahdollistaa riskienhallintakeinojen vähimmäistason ja toteutustapojen tunnistamisen sekä organisaation omien riskienhallintatavoitteiden asettamisen. Kyberala suosittelee, että tietoturvallisuuskäytänteet ja -ratkaisut jaotellaan kyberturvallisuuden hallintamallin mukaisiin osa-alueisiin. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen (NCSC-FI) kehittämän Kybermittarin mukaiset osa-alueet ovat yleisesti hyväksyttyjä ja laajaan osaamispohjaan nojautuvia käytäntöjä eri osa-alueiden turvallisuuden parantamiseen. NIST CF -viitekehys taas auttaa hahmottamaan ja määrittelemään kyberturvallisuuden hallinnan ulottuvuudet.

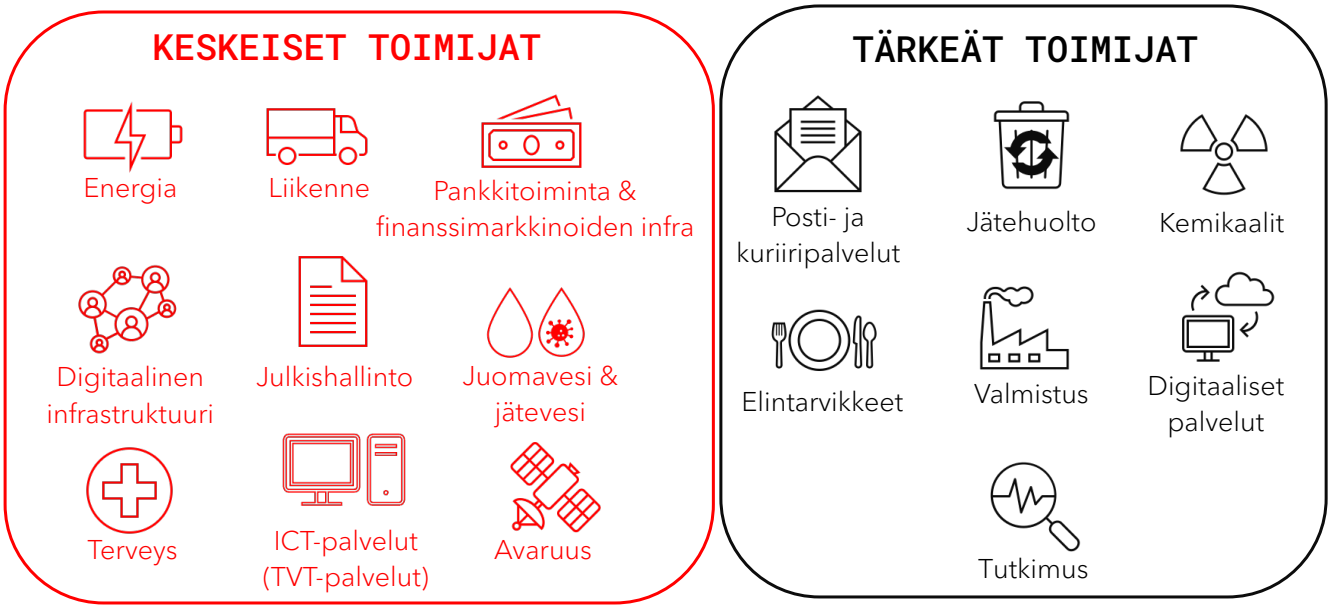
Suomessa on kehitetty Kybermittari, joka on laajalti käytetty työkalu kriittisen infrastruktuurin toimijoiden kypsyyden arviointiin. Kybermittari sisältää suurelta osin samoja tai samankaltaisia riskienhallintakeinoja kuin NIS2-direktiivi.

Alla luvussa ”Lainsäädännön vaatimukset” lain edellyttämät vähimmäisvaatimukset jaotellaan Kybermittarin osa-alueiden jäsentelymallin mukaisesti. On hyvä huomata, että Kybermittari sisältää sekä enemmän osa-alueita, että riskienhallintakeinoja, joita nyt kyseessä oleva lainsäädäntö ei edellytä. Kaikki lainsäädännön vaatimukset onkin siksi sisällytetty osa-

alueisiin ASSET, RISK, ACCESS, SITUATION, RESPONSE, THIRD PARTIES, WORKFORCE sekä ARCHITECTURE. Osa-alueet THREAT, PROGRAM sekä CRITICAL on rajattu pois, sillä vaikka näihin osa-alueisiin liittyykin joitain vaatimuksia, ne on katsottu kokonaisuuden kannalta paremmin sopiviksi muihin osa-alueisiin. Koska suuri osa toimijoista tavoittelee lain vaatimustasoa korkeampaa turvallisuustasoa, ja siten kattavampia kyberturvallisuuden hallintakeinoja, Kybermittarista, muista viitekehyksistä tai kyberturvallisuuden toimittajan suosittelemana voidaan ottaa käyttöön lisäkeinoja ilman, että menetetään ymmärrys lain edellyttämästä vähimmäistasosta.

Soveltamisala

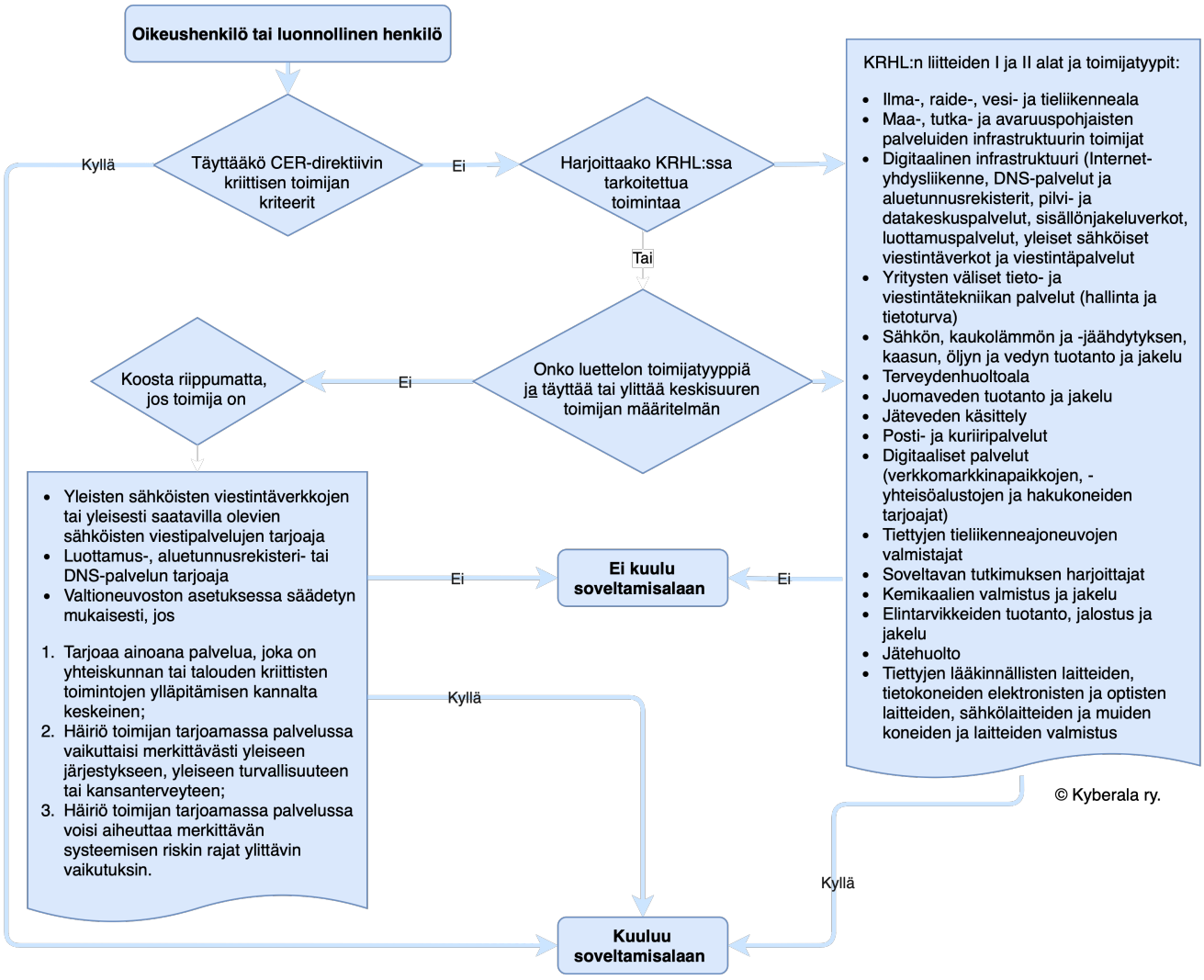
Direktiivin – ja sitä kautta kansallisen lainsäädännön – mukaan soveltamisalan tulkinta voi olla haastava tehtävä. Jokainen toimija on kuitenkin itse velvollinen selvittämään, onko toiminnassa sovellettava lain määräyksiä. Pääsääntöisesti keskeisiksi toimijoiksi katsotaan liitteen I toimialojen suuret yhtiöt ja muut ovat tärkeitä toimijoita. Alla on kuvattu yksinkertaistettu malli soveltamisalasta.



Lainsäädännön soveltamisalat toimialoittain jaoteltuna keskeisiin ja tärkeisiin toimijoihin.

Koska laissa soveltamisalan kriteeristö on laaja ja yksityiskohtainen, ainakin tulkinnanvaraisissa tilanteissa oman organisaation toimintaa on syytä verrata Lain kyberturvallisuuden riskienhallinnasta liitteiden I tai II tyhjentävässä luettelossa mainittuihin

soveltuviin lakeihin. Alla kuvattuna arviointimalli vuokaaviona, jonka avulla voi olla helpompi selvittää, onko harjoittaako ja oma organisaatio säänneltyä toimintaa ja täyttääkö se muutoin ominaisuuksiltaan soveltamisalaan kuulumisen kriteerit. Mikäli yksikään alla olevista ehdoista ei täyty, toimija ei kuulu soveltamisalaan.



Toimijan soveltamisalaan kuulumisen selvittämistä tukeva vuokaavio.

Kaaviota seurattaessa on tarpeen käyttää keskisuuren toimijan määritelmän täyttämisestä[1] tai ylittämisestä[2]. Askellettuun malliin viitaten yleistä suuntaa antavaa osviittaa voi saada mm. siitä, osallistuuko toimija kansallisen huoltovarmuusorganisaation (HVO) toimintaan, onko

[1] Keskisuuri toimija on yritys, jonka palveluksessa on vähintään 50 työntekijää tai jonka vuosiliikevaihto ja taseen loppusumma ylittää 10 miljoonaa euroa.
[2] Keskisuuren toimijan ylittävä yritys: palveluksessa on vähintään 250 työntekijää tai jonka vuosiliikevaihto ylittää 50 miljoonaa euroa ja taseen loppusumma ylittää 43 miljoonaa euroa.

toimija esim. jonkin huoltovarmuuspoolin jäsen, toteuttaako toimija esim. sopimuksellista varmuusvarastointia tai onko toimijalla voimassa olevia ns. tuotantovaraussopimuksia maanpuolustuksen tarkoituksiin. Kaikissa tilanteissa toimijan on viisasta pohtia oman (liike)toimintansa eli tuotantonsa häiriön vaikutusta yhteiskunnan toimintaan. Mikäli arvion mukaan vaikutus on vähäistä suurempi, kannattaa kriteeristö käydä läpi esim. perehtyneen asiantuntijan kanssa.

On hyvä huomata, että mikäli toimija on myös yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain eli ns. CER-direktiivin (Critical Entities Resilience) nojalla määritelty kriittinen toimija, direktiivin velvoitteiden valvonnasta vastaavat viranomaiset pyrkivät viran puolesta tunnistamaan soveltamisalaan kuuluvia toimijoita ja tämä voi helpottaa osaa myös NIS2-soveltamisalaan kuuluvia yhtiöitä. Lisäksi on hyvä huomata, että lain velvoitteiden näkökulmasta sillä, kuuluuko toimija liitteen I vai II luetteloon ei ole juurikaan merkitystä. Liitteessä I määritetyt toimijoita, jotka ylittävät keskisuuren yrityksen kriteerit kutsutaan laissa ”keskeisiksi” toimijoiksi ja muita toimijoita ”tärkeiksi”. Käytännön ero näiden välillä on, että keskeisiin toimijoihin voidaan kohdistaa sekä etukäteis- ja jälkikäteisvalvontaa, mutta tärkeiden toimijoiden osalta vain jälkikäteisvalvontaa.

Sääntelyn vaatimusten toimeenpanoa eli vaatimuksenmukaisuuden toteuttamista ja osoittamista ajatellen on keskeistä huomioida, että vaatimusten kohteena on organisaation toiminta eli tuotantoprosessit, ja niiden kannalta merkitykselliset viestintäverkot ja tietojärjestelmät. Tuotantoprosessien elementtien (raaka-aineet, työvaiheet, laitteet ja teknologia, työvoima, laadunvalvonta sekä logistiikka ja jakelu) keskeisimpiä tarkastelun kohteita ovat sellaiset verkot ja järjestelmät, joiden luotettavalla ja häiriöttömällä toiminnalla voidaan estää tai minimoida poikkeamien vaikutus omaan operatiiviseen toimintaan, toiminnan jatkuvuuden varmistamiseen, palvelujen vastaanottajiin ja muihin palveluihin. Huomio on siis erityisesti prosesseissa ja palveluissa, joiden häiriöllä on toimijaan nähden myös ulkopuolinen vaikutus, kuten toimitushäiriö tai toimitusverkoston muihin toimijoihin etenevä poikkeama. Asianomaiselle toimijalle itselleen taloudellisia tappioita aiheuttavaa häiriötä voitaneen pitää itsestään selvänä huomion kohteena. Kaikilta osin tietoturvallisuuden perusta, eli tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistaminen riskien kannalta hyväksyttävällä tasolla on myös tämän sääntelyn ydin.

Monikansallisten toimijoiden osalta NIS2-direktiivin asetelmaa on pidetty osittain monimutkaisempana yksinomaan kansallisesti toimiviin organisaatioihin verrattuna. Koska direktiivi edellyttää omaa, kansallisesta lainsäädäntöä kussakin EU:n jäsenvaltiossa, direktiivien vaatimukset toimeenpaneva sääntely voi erota jopa merkittävästi jäsenvaltioiden välillä – vaikka riskienhallinnan vaatimukset ovat kaikille yhteiset. Monikansallisesti toimivien organisaatioiden onkin suositeltavaa tarkastella eri jäsenvaltioiden sääntelyn noudattamista sekä oikeudellisen rakenteensa (konsernirakenne ja tytäryhtiöt), että sääntelyn kohteena olevien viestintäverkkojen ja tietojärjestelmien hallintamallin näkökulmista.

Konserni- ja tytäryhtiörakennetta mukaillen toimijan kannattaa tarkastella ainakin seuraavia seikkoja:

- Ovatko pääkonttorin ulkopuolella sijaitsevat yksiköt paikallisesti rekisteröityjä oikeushenkilöitä, vai ainoastaan toisessa jäsenvaltioissa työskenteleviä tiimejä tai henkilöitä?
- Millainen on tytäryhtiöiden ja niiden toimivan johdon asema konsernirakenteessa? Onko niillä itsenäistä toimivaltaa kyberturvallisuusriskien hallintapäätöksiin, vai ovatko ne sidoksissa pääkonttorin ohjaukseen?
- Harjoittaako tytäryhtiö sijaintivaltiossaan yhteiskunnan toiminnan kannalta kriittisiksi katsottua toimintaa direktiivin tarkoituksessa?
- Mikä taho vastaa direktiivin kannalta toimijan viestintäverkkojen ja tietojärjestelmien hallinnasta, kehittämisestä ja riskeistä? Ovatko esimerkiksi tietohallinnon keskeiset resurssit pääkonttorin ohjauksessa? Minne tietohallinnon aineellinen ja konsernin aineeton omaisuus on kirjattu (tase) tai muuten liitetty[3]?

Yllä mainitut kysymykset voivat antaa tukea johtopäätöksille sille, katsooko monikansallinen toimija riittäväksi, että se noudattaa pääkonttorinsa sijaintivaltion kansallista lainsäädäntöä, vai onko sen lisäksi tutkittava yksityiskohtaisemmin, miten konsernin muiden osien sijaintivaltion sääntely eroaa edellisestä. Mitä keskitetympi viestintäverkkojen ja tietojärjestelmien hallintaan liittyvät suoritteet ja kontrollit ovat, sitä selkeämmin pääkonttorin

[3] Miten konserniyhtiöt suorittavat ja kontrolloivat toimintoja liittyen aineettoman omaisuuden kehittämiseen (Development), parantamiseen (Enhancement), ylläpitoon (Maintenance), suojaamiseen (Protection) tai hyödyntämiseen (Exploitation).

sijaintivaltion sääntelyn yksinomaista noudattamista voinee perustella. On kuitenkin tärkeää huomata, että toimijat, esimerkiksi ICT-palveluiden toimittajat, joilla voi tyypillisesti olla asiakkaita usean eri EU-jäsenvaltion alueella on otettava asiakkaan mahdolliset kansalliset velvoitteet huomioon.

Lopuksi on tärkeää huomioida, että vaikka toimija ei kuuluisikaan lain soveltamisalaan, voi sille kohdistua velvoitteita sopimusperustaisesti silloin, kun toimijan asiakas kuuluu soveltamisalaan (kotimaassa tai toisessa EU-jäsenvaltiossa). Koska direktiiviin sisältyy vaatimuksia toimijalle hallita oman välittömän toimitusketjunsa kyberturvallisuusriskejä, siirretään näitä velvoitteita tyypillisesti sopimusperustaisesti asiakkaalle. Toimitusketjuun liittyvistä velvoitteista tarkemmin osioissa ”Riskienhallinta ja johtaminen (RISK)” sekä ” Toimitusketjun ja ulkoisten riippuvuuksien hallinta (DEPENDENCIES/THIRD PARTIES)”.

Lain vaatimusten kohteena ovat organisaation tuotantoprosessit, ja niiden kannalta merkitykselliset viestintäverkot ja tietojärjestelmät: tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistaminen hyväksyttävällä riskitasolla.

Soveltamisalaan kuuluvien toimijoiden viranomaisvalvonnan vastuunjako on ehdotettu järjestettäväksi alla taulukossa[4] esitetyllä tavalla. Eri toimialat on jaettu vasemmassa sarakkeessa esitettyjen viranomaisten välille. Toimijat voivat taulukon avulla tunnistaa sen viranomaisen, jonka puoleen tulisi ensisijaisesti kääntyä lain soveltamisen kysymyksissä ja joiden kautta voidaan antaa myös tarkempia ohjeita esim. toiminnallisista käytänteistä.

Valvova viranomainen	Toimiala
Liikenne- ja viestintävirasto	Ilmaliikenne, raideliikenne, vesiliikenne, tieliikenne, avaruus, digitaalinen infrastruktuuri, TVT-palvelujen hallinta, kuriiri- ja postipalvelun tarjoajat, digitaalisen palvelun tarjoajat, valmistus (moottoriajoneuvojen, perävaunujen ja puoliperävaunujen

[4] Liikenne- ja viestintäministeriö, 9.10.2023.

	valmistusta harjoittavat toimijat, muiden kulkuneuvojen valmistusta harjoittavat toimijat, tutkimusorganisaatiot, julkishallinto
Energiavirasto	Sähkö, kaukolämmityksen tai kaukojäähdytyksen haltijat, kaasu (jakelu- ja siirtoverkonhaltijat)
Turvallisuus- ja kemikaalivirasto	Kaasu (maakaasun toimittajat, varastointilaitteiston haltijat, maakaasun käsittelylaitteiston haltijat, maakaasualan yritykset sekä maakaasun jalostus- ja käsittelylaitteistojen haltijat), öljy, vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat, aineiden valmistusta ja aineiden tai seosten jakelua harjoittavat yritykset sekä yritykset, jotka tuottavat esineitä aineista tai seoksista, tietokoneiden, elektronisten ja optisten laitteiden valmistajat, sähkölaitteiden valmistajat sekä muiden koneiden ja laitteiden valmistajat
Sosiaali- ja terveydenalan lupa- ja valvontavirasto	Terveydenhuolto
Etelä-Savon ELY-keskus	Juomavesi, jätevesi ja jätehuolto
Ruokavirasto	Elintarvikeyritykset, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta
Lääkealan turvallisuus- ja kehittämiskeskus	Lääkinnällisiä laitteita valmistavat toimijat ja In vitro -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita valmistavat toimijat
Finanssivalvonta	Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri

Toimialat jaoteltuna valvovan sektoriviranomaisten suhteen.

LAINSÄÄDÄNNÖN VAATIMUKSET

Euroopan parlamentin ja neuvoston kyberturvallisuusdirektiivin (EU) 2022/2555[5] eli ns. NIS2-direktiivi on EU-lainsäädäntöä, joka saatetaan osaksi kunkin jäsenvaltion oikeutta antamalla direktiivistä kansallista lainsäädäntöä. Suomessa direktiivin perusteella annetaan yksi uusi laki ja muutetaan useita muita lakeja.

Direktiivin vaatimukset toteutetaan seuraavien kansallisten lakien kautta:

1. Laki kyberturvallisuuden riskienhallinnasta (uusi laki)
2. Laki julkisen hallinnon tiedonhallinnasta (lakia muutetaan)
3. Laki sähköisen viestinnän palveluista (lakia muutetaan).

Lisäksi edellisen direktiivin, ns. NIS1-täytäntöönpanosäännökset kumotaan sektorikohtaisista laeista, kuten sähköisen viestinnän palveluista annetusta laista, ilmailu-, raideliikenne-, sähkömarkkina- sekä vesihuoltolaista. Tiivistäen voidaan sanoa, että uusi laki kyberturvallisuuden riskienhallinnasta (KRHL) koskee ensisijaisesti yrityksiä, laki julkisen hallinnon tiedonhallinnasta (TiHL) julkishallintoa eli viranomaisia, virastoja, korkeakouluja sekä liikelaitoksia. Sähköisen viestinnän palvelulaki (SVPL) koskee viranomaisten lisäksi mm. teleyrityksiä ja muita mm. digitaalisen infrastruktuurin toimijoita, verkkotunnusten välittäjiä ja myyjiä.

NIS2-direktiivin velvoitteissa on pääosin kyse yksityiskohtaisesta ja vähimmäisharmonisoivasta sääntelystä, millä tarkoitetaan sitä, että kaikissa jäsenvaltioissa (vaihtelevin lainsäädönkeinoin) kaikille soveltamisalaan kuuluvien organisaatioiden, lain kielellä toimijoiden, on täytettävä yhteisesti asetetut vaatimukset.

[5] Direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa.

Riskienhallinta ja johtaminen (RISK)

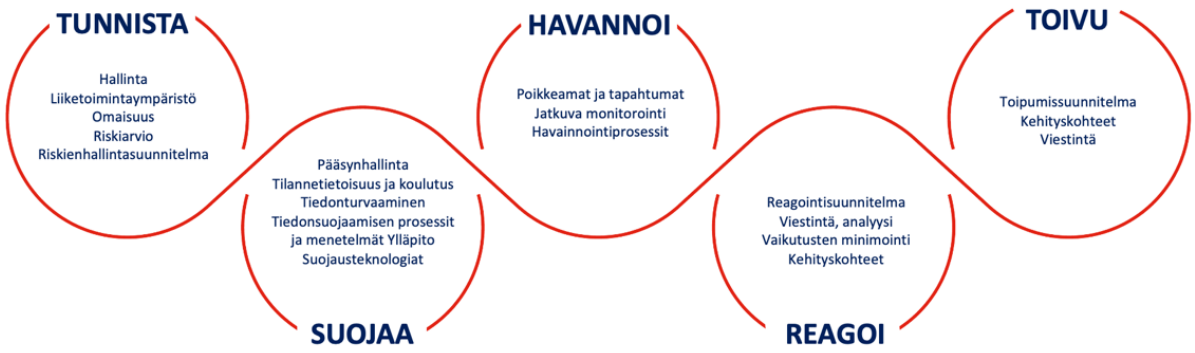
Toimijan lainsäädännölliset velvoitteet:

- **Tunnistettava, arvioitava ja hallittava riskejä**, joita kohdistuu organisaation toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuuden **riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus** toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin.
- Huomioitava **toimitusketjuhäiriön vaikutus** sen omaan toimintaan sekä varautua mahdolliseen toimitushäiriöön.
- **Tunnistettava ja huomioitava fyysiset ympäristöt sekä fyysisen ympäristön tekijät**, joiden turvallisuus on viestintäverkkojen ja tietojärjestelmien toiminnan kannalta tärkeää ja **suojattava näitä** toimintaan vaikuttavien uhkien vaikutukselta ja häiriöiltä.
- Oltava ajantasainen **kyberturvallisuuden riskienhallinnan toimintamalli, toimintaperiaatteet ja toimenpiteiden vaikuttavuuden arviointi** viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta. Toimintamallissa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit kaikki vaaratekijät huomioivan lähestymistavan mukaisesti.
- Toimintamallissa on **määritettävä ja kuvattava toimenpiteet**, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan riskeiltä ja poikkeamilta (jäljempänä hallintatoimenpiteet).
- Oltava **kirjalliset** viestintäverkkojen ja tietojärjestelmien **turvallisuutta koskevat toimintaperiaatteet ja menettelyt**.
- **Toteutettava turvallisuus- ja riskienhallintatoimenpiteet**, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin sekä viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.
- Varmistettava, että **johto vastaa kyberturvallisuuden** riskienhallinnan toteuttamisen ja valvonnan **järjestämisestä** sekä **hyväksyy** riskienhallinnan **toimintamallin** ja **valvoo** sen toteuttamista.

Riskienhallinta on keskeinen elementti liiketoiminnan jatkuvuuden turvaamisessa. Se auttaa oikeasuhtaisten hallintatoimenpiteiden suunnittelussa ja resurssien kohdistamisessa sinne, missä niillä on eniten vaikutusta. Tämä edellyttää muun muassa, että kaikki henkilöstöryhmät saavat laadukasta koulutusta, noudattavat selkeitä ohjeita ja ovat motivoituneita toimimaan määriteltyjen toimintatapojen mukaisesti. Näin riskienhallinnan keinot toteutuvat käytännössä eikä vain paperilla. Erityisen tärkeää on, että myös operatiivinen henkilöstö ilmoittaa

eteenpäin havaitsemistaan poikkeamista tai huolistaan, sillä kaikkea ei voida havaita ja hallita pelkästään teknisellä valvonnalla.

Lainsäädännön vaatimusten myötä toimijoilla on oltava kyvykkyys tunnistaa ja hallita (liike)toimintaansa kohdistuvia kyberturvallisuusriskejä. Toimijoiden tulee luoda ja ylläpitää koko toiminnan kattava riskienhallintaohjelmaa; tunnistaakseen, arvioidakseen ja hallitakseen kyberturvallisuuden riskejä. Toimijoiden on arvioitava omaa kyvykkyyttään ja kypsyyttään suhteessa uhkiin sekä tunnistettuihin riskeihin. Tämä auttaa tunnistamaan heikkoudet ja vahvuudet sekä määrittämään oikeasuhtaiset riskienhallintakeinot. Arviointityön tulee olla kokonaisvaltaista, systemaattista ja tosiasioihin perustuvaa. Toimijat voivat hyödyntää valmiita työkaluja kuten Traficomin Kybermittaria tai ulkopuolisia palveluntuottajia tukemaan arviointityötään. Arviointityössä on tärkeää varmistaa, että riittävä osaaminen on käytettävissä ja tämä on myös jälkikäteen todennettavissa. Toimijoiden tulee dokumentoida riskienhallinnan toimenpiteet ja löydökset, sekä säilytettävä ne asianmukaisesti. Toimijan tulee käyttää riskienhallinnassa yhteismitallisia ja luotettavia mittareita, jotka kuvaavat sen kyberturvallisuuden todellista tilaa ja kehitystä.



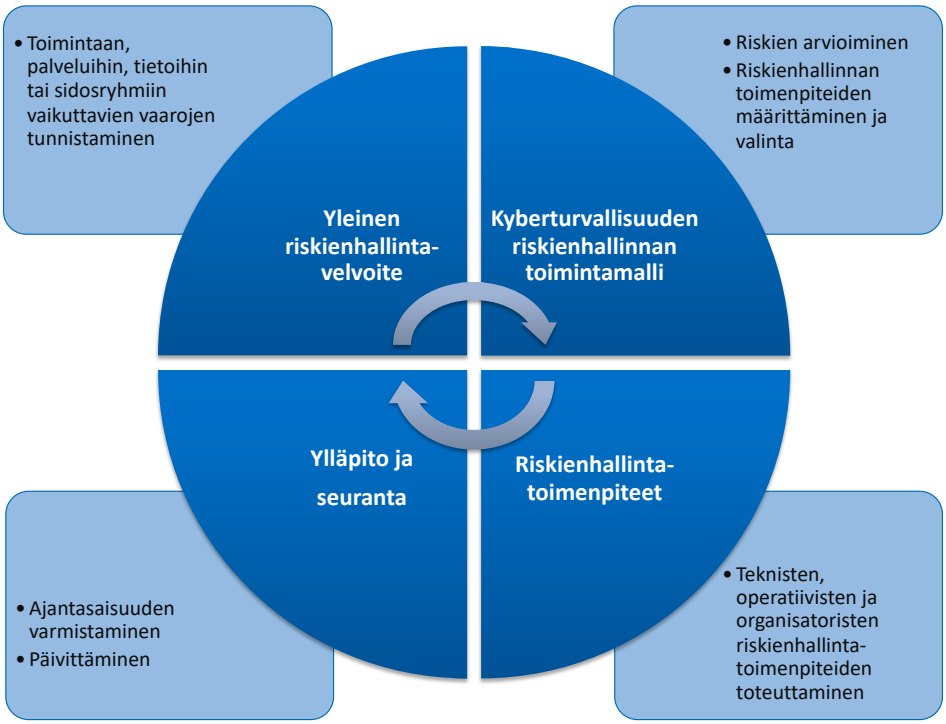
Kyberturvallisuuden hallinnan prosessimalli.

Roolit, vastuut ja prosessit

Organisaation on määriteltävä selkeästi roolit ja vastuut kyberturvallisuudelle sekä sisäisesti että ulkoisesti toimitusketjun osalta. Toimivan johdon tulee mahdollistaa riskienhallinnan toteuttaminen ja valvoa toteutusta. Organisaation on dokumentoitava riskit, riippuvuudet, tunnistetut uhat tai haavoittuvuudet ja arvioitava näiden vaikutuksia. Vaikutusten arviointi toteutetaan huomioiden käytössä olevat riskienhallintakeinot. Organisaation on valvottava tuotteiden ja -palveluiden kyberturvallisuutta koko niiden elinkaaren ajan sekä tehtävä

yhteistyötä sisäisten ja ulkoisten sidosryhmien kanssa jakamalla tietoa sekä parhaita käytänteitä. Riskienhallinnalla tarkoitetaan toiminnan tai palveluntarjonnan kannalta merkityksellisiin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien kyberriskien tunnistamista, riskien vakavuuksien arvioimista sekä riittävien toimenpiteiden toteuttamista riskien hallitsemiseksi.

Riskien tunnistaminen: Organisaation on tunnistettava uhat ja riskit, jotka voivat vaikuttaa sen toimintaan, palveluihin, tietoihin tai sidosryhmiin.
Riskien arviointi: Organisaation on arvioitava riskien todennäköisyys ja vaikutus, jolloin on mahdollista käsitellä syntyneiden riskien priorisointi niiden kriittisyyden mukaan.
Riskien käsittely: Organisaation on valittava ja toteutettava sopivat riskienhallintakeinot eli toimeenpanna asianmukaiset tekniset, operatiiviset ja hallinnolliset kyberturvallisuuden hallintatoimenpiteet. Toimenpiteiden tulee olla oikeasuhtaisia ja ajantasaisia toimijan tarpeisiin nähden. Sopivien menettelyiden valinnassa on syytä huomioida liiketoiminnalliset tarpeet ja tunnistetut kyberturvallisuusriskit.
Riskien seuranta: Organisaation on seurattava ja tarkasteltava riskienhallintakeinojen tehokkuutta ja tarvittaessa tehtävä korjaavia toimenpiteitä.



Kyberturvallisuuden riskien käsittelymalli.

Esimerkki: *Organisaatio voi nimetä kyberturvallisuudesta vastaavan henkilön tai yksikön, joka koordinoi ja ohjaa kyberturvallisuuden toimintaa. Organisaatio voi myös laatia toimitusketjun kartan, joka näyttää sen keskeiset toimittajat, alihankkijat ja palveluntarjoajat sekä niiden mahdollistamat uudet kyberturvallisuuden riskit.*

Esimerkki: *Organisaatio voi myös seurata tuotteiden ja -palveluiden kyberturvallisuuden tilaa ja kehitystä esimerkiksi tietoturvapäivitysten, haavoittuvuusskannauksien ja tietoturvalokien avulla.*

Esimerkki: *Organisaatio voi tehdä yhteistyötä kumppanin kanssa, joka auttaa riskienhallinnan toimenpiteiden jalkauttamisessa. Organisaatio voi myös osallistua kyberturvallisuuden yhteisöihin ja verkostoihin, joissa se voi vaihtaa tietoa ja kokemuksia muiden toimijoiden kanssa.*

Toimintaperiaatteet

Organisaatioiden on laadittava selkeät toimintaperiaatteet viestintäverkkojen ja tietojärjestelmien turvallisuudelle, riskienhallinnasta nousseiden havaintojen perusteella. Toimintaperiaatteet kuvastavat organisaation näkemystä tietoturvan tavoitteista, periaatteista ja toteutuksesta koko elinkaaren ajalle. Toimintaperiaatteet voivat koskea esimerkiksi:

- **Hallinnollista turvallisuutta:** Organisaation on määriteltävä tietoturvan roolit, vastuut, valtuudet ja raportointikäytännöt, sekä noudatettava tietoturvan lainsäädäntöä ja standardeja.
- **Henkilöstöturvallisuutta:** Organisaation on huolehdittava henkilöstön tietoturvaosaamisesta, koulutuksesta ja valvonnasta sekä estettävä henkilöstön aiheuttamat tietoturvaloukkaukset.
- **Laitteistoturvallisuutta:** Organisaation on hankittava, asennettava, ylläpidettävä ja hävitettävä tieto-omaisuutta sisältävät laitteet asianmukaisesti.

Esimerkki*: Toimija tunnistaa ne tietojärjestelmät, jotka vaikuttavat sen ydinliiketoimintaan. Tämän jälkeen toimija arvioi, miten mahdolliset häiriöt tai häirinnät näissä järjestelmissä voisivat vaikuttaa sen kykyyn tuottaa palveluita tai toteuttaa liiketoimintaansa. Tämän riskin hallitsemiseksi toimija tunnistaa useita kontrollikeinoja. Näitä ovat esimerkiksi*

tietoturvapäivitysten ajantasainen asentaminen, käyttöoikeuksien tiukka hallinta ja kehittyneen haittaohjelmasuojauksen ylläpito palvelimilla. Koska näiden kontrollikeinojen ylläpito on osa toimijan päivittäistä IT-toimintaa, se sopii säännöllisestä seurantaraportoinnista. Tämän ansiosta toimija, joka kantaa kyber- ja liiketoimintariskejä, saa säännöllisesti vahvistuksen siitä, että riskikontrollit toteutetaan suunnitellusti. Tämän tiedon avulla toimija voi arvioida omistamansa riskin todellisen tilan sekä jäännösriskien todennäköisyyden perustuen tarkkaan tietoon. Tämä auttaa toimijaa tekemään tietoon perustuvia päätöksiä ja hallitsemaan riskejä tehokkaasti.

Eräs keino riskienhallintatoimia koskevaan päätöksentekoon, mukaan lukien priorisoimiseen on ns. ROM-laskelma (Return on Mitigation) eli riskienhallinnan tuotto. Kyse ei ole kuitenkaan varsinaisesta tuotosta, vaan ROM-laskelma tarkoittaa potentiaalisten tappioriskien ja tehokkaiden hallintakeinojen potentiaalisen positiivisen vaikutuksen välistä suhdetta. Se auttaa muuntamaan riskit ja vaikutukset taloudellisesti vertailtavaan muotoon, mikä omalta osaltaan tukee keskeisiä suorituskykyindikaattoreita (KPI) ja oman pääoman tuoton (ROI) laskelmia. ROM-arvo laskemalla tietoturvapoikkeaman mahdolliset kustannukset ja tappiot sekä vertaamalla niitä hallintakeinon kustannuksiin. Esimerkiksi keskeisen tietojärjestelmän vakavan toimintahäiriön kustannukset voisivat olla:

- liikevaihdon menetys 300k€
- aineellisen ja aineettoman omaisuuden korvaaminen 100k€
- mainehaitta ja asiakasluottamuksen menetys 150k€
- lain vaatimuksen laiminlyönnistä määrättävä hallinnollinen seuraamusmaksu 70 k€

Menetyksen kokonaiskustannus olisi 620k€. Tehokkaiden riskienhallintakeinojen toteuttaminen täysimittaisen vahingon välttämiseksi (esim. huolellinen varmuuskopiointi, tietoturvapoikkeaman elpymissuunnitelmat ja säännölliset turvallisuustestaus) kustannuksen ollessa esim. 40k€, jää ROI-arvoksi 580 k€ (620 k€ – 40k€). Mitä suurempi riskienhallintakeinon ja vahingon kokonaiskustannuksen välinen ero on, sitä kannattavampaa riskin hallitsemiseen investoiminen on. Joidenkin riskienhallintakeinojen käyttöönoton kustannus on marginaalinen, jopa lähellä nollaa.

Toimintaympäristö

Organisaation on huomioitava kyberturvallisuusuhkien monialainen ja monitahoinen luonne sekä toimitusketjujen rooli sen toiminnassa. Organisaation on tunnistettava ja hallittava toimitusketjuista ja toimittajista aiheutuvat riskit. Organisaation on sisällytettävä kyberturvallisuustoimenpiteitä sopimuksiinsa, joita se tekee välittömien toimittajiensa ja palveluntarjoajiensa kanssa. NIS2-direktiivi edellyttää, että organisaatio varmistaa koko toimitusketjun turvallisuuden. Toimitusketjun hallinta on osa riskienhallinnan kokonaisuutta. Riskienhallinnan käytännöt on integroitava saumattomasti organisaation eri toimintoihin niiden vaatimusten mukaisesti.

- **Toimitusketjut:** Organisaation on varmistettava, että sen toimittajat ja alihankkijat noudattavat riittäviä kyberturvallisuuden standardeja ja sopimuksia. Kyberhygienian varmistaminen toimittajasopimuksin, sekä arvioinnein.
- **Tekninen valvonta:** Organisaation on käytettävä tehokkaita ja ajantasaisia teknisiä ratkaisuja, kuten palomuureja, virustorjuntaa, salauksia ja varmuuskopioita, suojaamaan tietojärjestelmiään ja tietojaan. Toimijoiden tulee huolehtia, että toimittajat noudattavat hyviä kyberturvallisuuden käytänteitä.
- **Päätöksenteon läpinäkyvyys:** Organisaation on oltava huolellinen ja totuudenmukainen kyberturvallisuuden riskienhallinnastaan ja raportoitava siitä säännöllisesti.

Esimerkki: *Organisaatio voi vaatia toimittajiltaan ja palveluntarjoajiltaan, että ne noudattavat tiettyjä kyberturvallisuuden standardeja, kuten ISO 27001 tai NIST CSF. Organisaatio voi myös tarkistaa toimittajiensa ja palveluntarjoajiensa kyberturvallisuuden tilan ja kehityksen säännöllisesti. Organisaatio voi myös sopia toimittajiensa ja palveluntarjoajiensa kanssa kyberturvallisuuteen liittyvistä vastuista, velvoitteista ja ilmoitusmenettelyistä.*

Esimerkki*: Yrityksellä on käytössä etätyön tekoon virtuaalityöpöytäratkaisu, johon kirjaudutaan suoraan internetistä vahvaa tunnistautumista käyttäen. Kyberturvakeskus antaa kyseisen valmistajan tuotteesta korkean prioriteetin varoituksen, koska siitä on löytynyt toistaiseksi paikkaamaton etäkäytön mahdollistava tekninen haavoittuvuus, jota hyökkääjät käyttävät aktiivisesti hyväksi. Yrityksen riskienhallinta tekee tilanteesta pikaisen arvion tietotekniikasta vastaavien tiimien kanssa. Yrityksen toiminta vaatii etätyön tekemisen mahdollisuutta, mutta tietomurron riski on tällä hetkellä liian ilmeinen. Päätetään tehdä*

järjestelmien reititysmuutoksia niin että etätyöpöydän käytön muutos sallitaan VPN yhteyden avulla, ja niin että asennetaan myöhemmän tietomurtoyritysten havaitsemiseksi erillinen sensori (ns. IDS-laite) korkean haavoittuvuuden omaavan laitteen internet-liikennettä varten. . Tämä vaikeuttaa ja hidastaa väliaikaisesti työntekijöiden sisäänkirjautumista ja etätyön tekemistä jonkun verran, mutta kuitenkaan mahdollistaa sen jatkumisen turvallisesti. Poikkeustilanne ohjeistetaan käyttäjille sähköpostilla ja toteutetaan välittömästi. Kun myöhemmin etätyöpöydän valmistaja julkaisee korjaavan tietoturvapäivityksen, voidaan poikkeusjärjestely purkaa ja järjestelmän käyttö suoraan internetistä taas sallia.

***Tapaus**: Organisaatiossa tehty riskienhallinta kattoi lähinnä taloudelliset ja kilpailutilanteeseen liittyvät riskit. Yksittäisiä puutteita ja kyberriskejä oli kyllä tunnistettu organisaation alemmilla tasoilla mutta niitä ei ollut järjestelmällisesti kerätty ja raportoitu. Tämän vuoksi yrityksen johdolla ei ollut riittävää ymmärrystä yrityksen kyberriskeistä. Tietoturvaloukkauksen tapahduttua yrityksen johdolle tuli täytenä yllätyksenä IT-järjestelmiin ja kyberturvaan liittyvä korkea riskitaso. Liiketoimintayksiköillä ja yrityksen johdolla oli ollut käsitys, että "IT-yksikkö vastaa kyberturvasta". IT-palvelujen ja niihin liittyvien vaarojen tunnistaminen ei valitettavasti tuo riittävää varmuutta kyberturvaan. Kyberriskien osalta vastuun tulee olla myös liiketoiminnalla, ei pelkästään tietohallinnolla.*

Näin liikkeelle:

- Tunnista ja hallitse riskejä, jotka uhkaavat toimintaa ja viestintäverkkoja, varmistaen toiminnan jatkuvuuden ja minimoiden häiriöiden vaikutukset.
- Ota huomioon toimitusketjun häiriöiden vaikutus toimintaan ja valmistaudu mahdollisiin häiriöihin.
- Ylläpidä yllä ajantasaista kyberturvallisuuden riskienhallintamallia, joka suojaa viestintäverkkoja ja tietojärjestelmiä riskeiltä.
- Varmista, että johto vastaa kyberturvallisuuden riskienhallinnan toimenpiteiden toteuttamisesta ja seuraa niiden tehokkuutta.

HUOM! Huolehdi, että vaatimusten **perustaso** toteutuu: tekniset kontrollit (tai vähintään kirjalliset käytännöt) ohjelmistojen asentamiseen ja haittaohjelmilta suojautumista vastaan (esimerkiksi kalastelusähköpostit, tuntemattomat ulkoiset tallennusmediat, piraattisovellukset, haitalliset verkkovierailut) on otettu käyttöön.

Toimijalla on käytännöt, joilla määritetään tiedon luottamuksellisuus sekä kirjalliset ohjeet tiedon käsittelyyn, kuten miten ja missä luottamuksellista tietoa säilytetään, käsitellään, siirretään eri järjestelmien välillä ja tuhotaan.

Omaisuuden, muutoksen ja konfiguraation hallinta (ASSET)

Toimijan lainsäädännölliset velvoitteet:

- Oltava **säännölliset ja dokumentoidut omaisuudenhallinnan menettelyt ja ohjeet**.
- **Tunnistettava** viestintäverkkoihin ja tietojärjestelmiin liittyvä **omaisuus ja luokiteltava ne suojaustarpeiden perusteella**.
- **Ylläpidettävä** omaisuudesta **ajantasaista luetteloa**.
- Huolehdittava viestintäverkkojen ja tietojärjestelmien **hankinnan, kehittämisen ja ylläpidon** turvallisuudesta koko niiden elinkaaren ajan.
- Hankittavien järjestelmien tulee olla toiminnan tarpeiden perusteella **riittävän turvallisia** ainakin eheyden, saatavuuden ja luottamuksellisuuden suhteen ja niiden on **kyettävä suojautumaan tavallisimpia hyökkäyksiä** vastaan.
- Järjestelmien **turvallinen konfiguraatio tulee määritellä ja dokumentoida,** sekä huomioida erityisesti päivitysten aikana.
- **Konfiguraatio- ja ohjelmistopäivitysten tulee olla dokumentoituja, muutoshallintaprosessien mukaisesti suunniteltuja, kattavia** sekä kohteen ominaispiirteiden **ja** päivitysten kriittisyyden kannalta **oikea-aikaisia**. Luvattomien tai haitallisten muutosten tekeminen tulee estää.
- Turvallisuuden kannalta **kriittisimmät kohteet tulee tunnistaa** ja näiden turvallisuudesta tulisi huolehtia lisäksi **prosessien säännöllisen tarkastelun tai teknisten testausten avulla**.

HUOM! Mikäli toimija tuottaa viestintäverkko- tai tietojärjestelmäpalveluita, on huolehdittava myös näiden turvallisuudesta. Toimijan on varmistettava, että näiden turvallinen konfiguraatio on mahdollista ja niille tuotetaan turvallisuuspäivityksiä.

Suojattavan omaisuuden tunnistaminen ja hallinta on olennaista liiketoiminnan turvallisuudelle. Yrityksen on tiedettävä, mikä sille tuottaa liiketoimintaa sekä -arvoa ja määrittää miten tätä omaisuutta halutaan suojata, jotta oikeamittaiset suojatoimenpiteet voidaan toteuttaa. Ydinasia on, että toimija on tunnistanut toimintansa kannalta kriittiset kohteet. Nämä kohteet ovat sellaisia, joita ilman ei voi toimia tai niihin kohdistuu muutoin esim. toimialakohtaisia lakisääteisiä velvoitteita, tai niihin kohdistunut tietoturvaloukkaus voi aiheuttaa suurta vahinkoa. Kohteet voivat olla esimerkiksi laitteita, ohjelmistoja, sovelluksia tai toiminnan kannalta välttämätöntä dataa.

Omaisuuden hallinnan toteutuksessa on usein hyväksyttävä, ettei luettelointi ole välttämättä täydellinen ja se voi perustua useisiin rekistereihin, joita toimija käyttää osana toimintojaan. Näitä ovat esimerkiksi päätelaitteiden laitehallinta- ja tietoturvasovellukset, HR-rekisterit henkilöiden oikeuksista, taloushallinnon käyttöomaisuusluettelot sekä tietosuojan

käsittelytoimien selosteet tietojärjestelmille ja tietovarannoille. Myös ulkopuolisten palvelujen ostot, näiden raportoinnit ja sopimustenhallinta, sekä teollisuuslaitteiden, kiinteistöjen ja tilojen tai huollon laiterekisterit voivat myös olla osa kokonaisuutta. Jos näitä rekistereitä ylläpidetään hyvin, niitä voidaan hyödyntää tehokkaasti omaisuuden luetteloinnissa ja riskienhallinnassa.

Suojattavaan omaisuuteen kohdistuvia riskejä on arvioitava ja hallittava. Pääsynhallinta on yksi tapa kohdentaa suojatoimenpiteet oikeisiin kohteisiin. Muutoksen ja konfiguraation hallinta on toinen tapa varmistaa, että suojattavan omaisuuden tiedot ovat ajan tasalla ja yhteydessä muihin toimintoihin, kuten HR:ään ja talouteen.

Muutos- ja konfiguraatiohallinta

Muutos- ja konfiguraatiohallinnalla tarkoitetaan sitä, että suojattava omaisuus pysyy ajantasaisena ja toimivana. Muutos- ja konfiguraatiohallinta kattaa omaisuuden koko elinkaaren ja sen kytkennät muihin toimintoihin, kuten hankintaan. Muutos- ja konfiguraatiohallintaan liittyy esimerkiksi:

- Käyttöomaisuusluettelo, joka sisältää taloushallinnon tiedot omaisuudesta.
- Tietosuojan käsittelytoimien seloste, joka sisältää tietojärjestelmien ja tietovarantojen tiedot.
- IT- ja pilvipalveluiden sekä tilausten hallinta, joka sisältää ostojen ja sopimustenhallinnan tiedot.
- Huollon laiterekisteri ja kunnossapito, joka sisältää teollisuuslaitteiden, kiinteistöjen ja tilojen tiedot.

Esimerkki: *jos organisaatiolla on useita erilaisia tietojärjestelmiä, laitteita, lisenssejä ja sopimuksia, sen on pidettävä niistä luetteloa, joka on ajan tasalla ja helposti saatavilla. Näin organisaatio voi seurata omaisuutensa tilaa, käyttöä ja elinkaarta. Omaisuuden hallinnan avulla organisaatio voi myös varmistaa, että sillä on riittävät oikeudet ja valtuudet omaisuuteensa, ja että se noudattaa kaikkia sovellettavia lakeja ja säädöksiä.*

Tapaus*: Yhtiö käytti tuotekehitykseen epävirallista, dokumentoimatonta palvelinta, joka ei ollut virallisen ylläpidon piirissä. Aikojen saatossa palvelimelle oli asennettu kaikenlaista tuotekehityksen tarvitsemaa ohjelmistoa ja monenlaisia aputyökaluja.*
Kun sitten yöllinen vesivahinko tuhosi palvelimen, ei mistään löytynytkään sen enempää kunnollista varmuuskopiota kuin mitään dokumentaatiota, joiden pohjalta palvelimen uudelleenasennus olisi voitu tehdä. Erilaisten itsetehtyjen ohjelmistojen, konfiguraatiotiedostojen, skriptien ja aputyökalujen kokoaminen ja järjestelmän uudelleen

rakentaminen vei niin paljon aikaa, että yrityksen tuotekehitykselle ja sitä kautta liiketoiminnalle aiheutui merkittäviä häiriöitä.

Näin liikkeelle:

- Kehitä kattavat menettely omaisuuden hallintaan, tunnista viestintäverkkojen ja tietojärjestelmien omaisuus, ja pidä niistä ajan tasalla olevaa luetteloa.
- Varmista järjestelmien hankinta- ja ylläpitoprosessien turvallisuus niiden koko elinkaaren ajan, mukaan lukien riittävä suojaus yleisimpiä hyökkäyksiä vastaan.
- Laadi ja ylläpidä turvalliset järjestelmäkonfiguraatiot, ja toteuta päivitykset hallitusti estäen luvattomat muutokset.
- Tunnista turvallisuuden kannalta kriittiset osat ja varmista niiden turvallisuus säännöllisin tarkastuksin ja testauksin.

HUOM! Huolehdi, että vaatimusten **perustaso** toteutuu: kriittiset kohteet on tunnistettu, viestintäverkkojen ja tietojärjestelmien turvallisuuteen liittyvien toimintaperiaatteiden mukaiset käytännöt ja ohjeet omaisuudenhallintaan on laadittu, viestitty ja ovat saatavilla. Viestintäverkoista ja tietojärjestelmistä ylläpidetään vähintään yksinkertaista dokumentaatiota, kuten verkkokuvia ja -kaavioita.

Toimijalla on käytännöt, joiden perusteella se poistaa järjestelmistään tarpeettomat ominaisuudet, mukaan lukien ylimääräisten palveluiden tai laitteiden sammutus tai poistaminen käytöstä. Toimija on muuttanut järjestelmiensä tai laitteidensa oletusasetukset kuten oletussalasanat ja säilyttää päivitetyt salasanat turvallisesti. Mikäli toimija on luonut tunnuksia hätätilanteita varten, on niiden suojaamisesta, käyttöperusteista ja saatavuudesta hätätilanteiden yhteydessä huolehdittu. Järjestelmien tarjoamat turvallisuustoiminnot on otettu käyttöön, kuten automaattiset ohjelmistopäivitykset, turvalliset tunnistusmenetelmät, salaus ja tapahtumakirjausten (loki).

Ohjelmistojen asentamista ja suorittamista sekä tallennusmedioiden käyttöä tulisi hallita automaattisesti (esimerkiksi Windows Defender Application Control WDAC, AppLocker, AppArmor, SELinux).

Toimijalla on käytännöt, joilla se seuraa käyttämiensä käyttöjärjestelmien, sovellusten ja laiteohjelmistojen kriittisiä turvallisuuspäivityksiä ja asentaa ne viivytyksettä riskiarvion perusteella, esimerkiksi automaattisilla päivityksillä. Järjestelmiä, joita ei voi päivittää, tulee suojata muilla menetelmillä ja päivitykset tulee asentaa hallitusti silloin kun se on mahdollista. Myös muita kuin kriittisiä turvallisuuspäivityksiä tehdään säännöllisin väliajoin, esimerkiksi kuukausittain, kun järjestelmän toimittaja julkaisee uudet päivitykset.

Organisaation on tunnistettava ja tunnettava toimintansa kannalta kriittiset prosessit ja kohteet sekä varmistettava näiden riittävä turvallisuustaso.

Identiteetin- ja pääsynhallinta (ACCESS)

Toimijan lainsäädännölliset velvoitteet:

- Oltava **menettelyt käyttäjätunnusten ja käyttöoikeuksien koko elinkaaren ajalle** ja **käyttöoikeuksia on hallittava ja valvottava** niiden mukaisesti.
- Oltava **pääsynhallintaan liittyvät määrittelyt ja käytännöt**, joilla varmistetaan kattavasti luotettava tunnistaminen ja joilla sallitaan pääsy vain tarvittaviin viestintäverkkoihin ja tietojärjestelmiin, suojattaviin tietoihin, muihin resursseihin sekä fyysistä pääsyä edellä mainittuja ylläpitäviin laitteisiin ja tiloihin.
- Pääsynhallinnan menettelyiden tulee kattaa **väärinkäytösten estäminen**, kuten vaarallisten työyhdistelmien tunnistaminen ja välttäminen, työtehtäväkierto, sekä työsuhteen tai sopimuksen päättymisen. Mikäli työtehtävien ja vastuiden katsotaan vaativan erityistä luotettavuutta, henkilölle tulee voida tehdä tarkoituksenmukainen **taustatarkistus**.
- Oltava **menettelyt vahvojen oikeuksien käyttäjätilien ja pääkäyttäjätilien hallintaan**. Pääkäyttäjäoikeudet tulisi rajoittaa mahdollisimman pienelle käyttäjäjoukolle ja näitä tunnuksia on suojattava vahvoin menetelmin.
- Pääsynhallinnan ja todentamisen **menettelyiden tulee koskea sekä luonnollisia käyttäjiä** kuten henkilöstöä ja ulkoisia toimijoita, **että järjestelmätunnuksia** kuten laitteiden, ohjelmistojen, rajapintojen ja muiden oleellisten resurssien käyttämiä tunnuksia.
- Pääsynhallinnan tulee koskea **sekä ohjelmistolla todennettavaa pääsyä, että fyysistä pääsyä (esim. päätelaitteille)**. Menettelyiden tulee perustua liiketoimintavaatimuksiin sekä tietoverkkoja ja tietojärjestelmiä koskeviin vaatimuksiin järjestelmien erityispiirteet huomioon ottaen.
- Käyttöoikeuksista ja -rooleista on **pidettävä ajantasaista kirjaa** ja käyttäjille on **annettava vain ne oikeudet, jotka ovat työtehtävien suorittamisen vuoksi välttämättömiä** (vähimpien oikeuksien periaate).
- Valittavien todentamiskäytäntöjen ja -tekniikoiden tulee perustua tietojen saatavuutta koskeviin vaatimuksiin ja todentamisen menettelyihin. **Todennusmenetelmien tulee olla riittävän turvallisia** niin, että oikeudeton käyttö on mahdollisuuksien mukaan estetty. Tarvittaessa todennusmenetelmänä tulisi käyttää vahvaa tunnistusta, monivaiheista todentamista (MFA) tai jatkuvaa todentamista, mikäli niiden käyttö on mahdollista.

Pääsynhallinta on olennainen osa kyberturvallisuutta, koska se auttaa suojaamaan organisaation tärkeitä resursseja. Jos haitalliset tahot saavat fyysisen- tai loogisen pääsyn yrityksen järjestelmiin, he voivat vaikuttaa yrityksen liiketoiminnan luottamuksellisuuteen, eheyteen tai saatavuuteen. Heikko pääsynhallinta johtaa laitteiden, ohjelmistojen ja tiedon luvattomaan käyttöön, julkistamiseen, tuhoamiseen sekä peukalointiin. Lisäksi se nostaa tarpeettomasti organisaation riskitasoa. Pääsynhallinnan avulla varmistetaan, että vain oikeutetut henkilöt voivat käyttää tiloja, laitteita, järjestelmiä, tietokantoja tai tuotantojärjestelmiä, jotka ovat organisaation toiminnan kannalta keskeisiä.

Lainsäädännön vaatimusten myötä organisaatioilla on oltava kyky hallita ja rajoittaa loogista ja fyysistä pääsyä suojattavaan omaisuuteen. Pääsyä tulee hallita suhteessa toimintaan

kohdistuviin riskeihin ja organisaation yleisiin tavoitteisiin. Tässä yhteydessä loogisen pääsynhallinnan suojausmekanismeja sovelletaan toiminnon kannalta tärkeisiin laitteisiin, ohjelmistoihin ja tietoon. Fyysisen pääsynhallinnan suojausmekanismeja sovelletaan toiminnon kannalta tärkeisiin laitteisiin ja tiloihin. Automatisoituja suojausmekanismeja sovelletaan sekä loogisen että fyysisen pääsynhallinnan yhteydessä. Tavoitteena on kokonaisvaltainen ja systemaattinen fyysisien sekä digitaalisien identiteettien ja käyttöoikeuksien hallinta.

Toimijat ovat vastuussa siitä, että heillä on hallussaan ja valvonnassaan kaikki pääsytiedot ja -oikeudet. Omaisuus, kuten laitteet, tietojärjestelmät, data ja informaatio tunnistetaan ja luokitellaan niiden kriittisyyden mukaan. Mitä kriittisempi omaisuus on kyseessä, sitä tarkemmin pääsyjä tulee valvoa ja hallita. Pääsynhallinnan menettelyiden tulisi perustua liiketoimintavaatimuksiin sekä tietoverkkoja ja tietojärjestelmiä koskeviin vaatimuksiin. Pääsynhallinnan tulisi kattaa sekä ohjelmistolla todennettava pääsy että fyysinen pääsy. Pääsynhallinnassa tulisi ottaa huomioon oikeuksien myöntäminen, muuttaminen ja poistaminen sekä asianmukainen valvonta. Pääsynhallinnan tulisi kattaa koko yrityksen kriittinen infrastruktuuri ja tilat sekä arkaluonteiset tiedot. Omaisuudenhallinnan tulisi kattaa sekä fyysinen että aineeton omaisuus.

Identiteetinhallinta

Identiteetinhallinta varmistaa, että käyttäjät, laitteet, sovellukset ja koneet on tunnistettu. Valtuudet määritellään sen perusteella, kenellä on oikeus mihinkin tietoon; tämä voi olla myös roolipohjaista. Pääsyoikeudet luodaan identiteeteille näiden valtuuksien pohjalta; mitä kriittisempi resurssi, sitä rajatumpi joukko identiteettejä siihen on valtuutettu. Kukaan ei pääse käyttämään resursseja tunnistautumatta tai jälkeä jättämättä.

Hallintaperiaatteet

Pääsyoikeuksia kohteisiin rajoitetaan minimitasolle toimenpiteen vaatimusten mukaisesti. Esimerkiksi palvelimella olevan sovelluksen päivittämiseen tarvitaan valtuudet vain kyseiseen sovellukseen, ei koko palvelimeen. Varmistetaan, että istunnoista jää lokitiedosto. Erityisen kriittisten resurssien osalta toimenpiteitä voidaan valvoa reaaliaikaisesti ja tallentaa; esimerkkeinä voivat olla potilastietokannan ylläpitotoimet tai tehtaan säätöjärjestelmien kalibrointi. Kriittiset yhteydet tulee voida katkaista reaaliaikaisesti tarvittaessa. Yhteyksiä

kriittisiin järjestelmiin ei pidetä aina auki; ne avataan organisaation sisältä vain tarvittaessa. Tunnisteiden hallinta (salasanat ja digitaaliset avaimet) on keskeistä turvallisuuden kannalta.

Monivaiheinen tunnistautuminen tarkoittaa, että käyttäjän on todistettava henkilöllisyytensä useammalla kuin yhdellä tavalla, esimerkiksi salasanalla ja kertakäyttöisellä koodilla. Tämä vaikeuttaa huomattavasti (joidenkin lähteiden mukaan jopa 99,9 %) luvattoman pääsyn saamista järjestelmiin. Esimerkiksi henkilö- tai potilastietojen vuotaminen, tuotantolaitosten häiritseminen tai tuhoaminen, tietopääoman tai tiedon (IPR) anastaminen sekä erilaisten haittaohjelmien asentaminen ovat mahdollisia seurauksia pääsynhallinnan pettämisestä. Pääsy kohteisiin rajoitetaan minimitasolle vaatimusten mukaisesti; esimerkiksi palvelimella olevan sovelluksen päivittämiseen tarvitaan valtuudet vain kyseiseen sovellukseen, ei koko palvelimeen. Lisäksi varmistetaan, että istunnoista jää lokitiedosto jälkiselvitykseen.

***Tapaus**: Kriittisen infrastruktuurin yrityksessä on tunnistettu operatiivisten toimintaympäristöjen käyttöoikeuksien hallinnan olevan yksi merkittävimmistä tietoturvakontrolleista. Ympäristöjen normaali operointi edellyttää tarkkaan valvotun käyttöoikeuden omistamista, monivaiheista tunnistautumista ja sisäänkirjautumista vain yrityksen omistamista laitteista VPN yhteyttä käyttäen. Tarkastuksessa todetaan kuitenkin teknisen henkilöstön sopineen IT osaston kanssa epävirallisesta käytännöstä, jossa päivystäjällä on käytössä erityisasennettu kannettava tietokone, josta on jatkuva yhteys operatiiviseen ympäristöön, palomuureihin tehdyn poikkeussäännön kautta. Kannettavan tietokoneen avaamiseen vaadittava salasana on tiedossa kaikilla päivystäjillä, eikä operointi vaadi muita tunnistautumisia koska yhteyden käytön nopeutta ja toimintavarmuutta priorisoidaan. Tietoturva perustui tässä tapauksessa siis lähinnä päivystäjän kannettavan tietokoneen fyysiseen turvallisuuteen, eikä ollut operatiiviset riskit omistavan tahon tiedossa.*

***Tapaus**: Organisaation ylläpitäjillä oli tapana käyttää vain yksiä tunnuksia kaikkeen ylläpitotyöhön. Yrityksellä oli julkisessa verkossaan palvelin, jota ei ylläpidetty. Palvelimen ohjelmistossa oli haavoittuvuuksia, joita hyväksikäyttäen palvelin saatiin murrettua. Tämän jälkeen murtautuja asettui odottamaan. Kun järjestelmän ylläpitäjät aikaan kirjautuivat sisään järjestelmään organisaation pääkäyttäjän ylläpitotunnuksilla (AD-ylläpitäjä), aktivoituivat murtautujat välittömästi ja saivat haltuunsa pääkäyttäjätunnuksen ja sitä kautta nopeasti koko IT-ympäristön.*

***Tapaus**: Käyttäjätunnuksiin liittyy myös tunnuksia, jotka on alistettu ainoastaan tietokoneen ja sen sovelluksen käyttöön. Kyseille käyttäjätunnukselle pyydettiin vain lukuoikeudet kaikkiin muihin järjestelmässä oleviin resursseihin (käyttöjärjestelmätiedot, sovellustiedot yms.). Pyynnön laati tietoturvasta vastaava henkilö ja toteutti IT-järjestelmien ylläpito-organisaatio. Myöhemmin ilmeni, että kaikki pyydetyt käyttövaltuustasot oli toteutettu niin, että kaikille vain lukuoikeuksia pyytäneille oli annettu järjestelmien korkeimmat käyttövaltuudet.*

***Tapaus**: On useita tapauksia, joissa "aina avoimet" yhteydet eri verkkojen segmenttien tai jopa eri yksikköjen välillä ovat auttaneet hyökkääjää saamaan jalansijaa kriittisiin järjestelmiin. Hyökkääjä löytää todennäköisesti myös sellaisia yhteyksiä, jotka eivät ole näkyvissä tavalliselle käyttäjälle, koska hyökkääjällä on työkaluja, jotka löytävät kaikki verkossa olevat yhteydet.*

Näin liikkeelle:

- Käyttäjätunnusten ja käyttöoikeuksien elinkaaren ajaksi tulee olla menettelyt, jotka tukevat niiden hallintaa ja valvontaa.
- Pääsynhallintakäytäntöjen tulee olla sellaiset, että ne mahdollistavat luotettavan käyttäjien tunnistamisen ja rajoittavat pääsyn vain niihin viestintäverkkoihin ja tietojärjestelmiin, joihin on tarvetta.
- Pääkäyttäjätileille ja muille vahvojen oikeuksien käyttäjätileille tulee olla omat hallintamenettelyt, ja niiden käyttö tulee rajoittaa vain välttämättömille henkilöille.
- Pääsynhallinnan ja todentamisen käytännöt ja menettelyt tulee kattaa kaikki käyttäjät ja järjestelmätunnukset, ja niiden tulee perustua (liike)toimintavaatimuksiin sekä järjestelmien turvallisuusvaatimuksiin.

HUOM! Huolehdi, että vaatimusten **perustaso** toteutuu: ei-luotetuista viestintäverkoista tulevan haitallisen tai ei-toivotun liikenteen estävä ratkaisu on käytössä, kuten palomuuri (erillislaitteena tai ohjelmistona) tai pääsylista (access control list, ACL).

Toimija on rajannut pääsyn palveluihinsa vähimpien oikeuksien periaatteella esimerkiksi rajaamalla pääsyn julkisissa viestintäverkoissa sijaitseviin palveluihin (rajapinnat, puhepalvelut, tiedostojaot, hallintapalvelut) identiteettien, käyttäjäryhmien, IP-osoitteiden, porttien tai protokollien perusteella. Vähimpien oikeuksien periaatetta ylläpidetään koko viestintäverkon elinkaaren ajan muutostenhallinnan avulla. Käytännöt löytyvät myös pääkäyttäjätunnusten ja korotettujen oikeuksien tunnusten myöntämiselle ja ylläpidolle.

Toimijalla on salasanakäytännöt, jotka edellyttävät valitsemaan turvallisia ja yksilöllisiä käyttäjätunnuksia sekä salasanoja, sekä ilmoittamaan tunnusten vaarantumisesta. Turvallisten ja yksilöllisten käyttäjätunnusten ja salasanojen käyttöä voi edistää salasananhallintaohjelman avulla. Järjestelmät, joissa voi ja tulee ottaa käyttöön vahvemmat tunnistus- ja todennusmenetelmät, kuten monivaiheinen tunnistautuminen (MFA) on tunnistettu.

Uhka- ja tilannekuva (SITUATION)

Toimijan lainsäädännölliset velvoitteet:

- Viestintäverkkoja ja tietojärjestelmiä tulee **valvoa ja niitä tulee suojata** luvattomalta fyysiseltä pääsyltä, vahingoilta ja häiriöiltä.
- Poikkeamien havainnointia ja käsittelyä varten toimijalla tulee olla **dokumentoidut menettelyt, roolit, vastuut sekä raportointikanavat** sisäisille ja ulkoisille toimijoille poikkeamien ehkäisemistä ja havainnoimista varten sekä vakavista ja muihin toimijoihin ulottuvista **poikkeamista varoittamiseksi**.
- Oltava **työkalut ja prosessit** tapahtumien kirjaamiseen ja havainnointiin. Havainnointi- ja analysointikyvyn kannalta on välttämätöntä, että toimijalla on **kerättynä ja käytettävissä riittävät lokitiedot** esimerkiksi ylläpidosta, muutoksista, käytöstä ja virheistä.
- **Arvioitava tapahtumat** sen selvittämiseksi, aiheuttavatko ne poikkeaman, mukaan lukien käytännöt, joilla poikkeaman vakavuus ja vaikutukset voidaan arvioida ja tarvittaessa **luokitella**.
- Poikkeamien käsittelyn tulee sisältää myös **menettelyt tiedon jakamiseen niin, ettei se vaaranna toimijaa tai muuta organisaatiota**.
- Poikkeamien käsittelyn **menettelyjä tulee ylläpitää ja kehittää koko elinkaaren ajan**, ja niitä tulee kehittää.

HUOM! Mikäli toimija ei tuota viestintäverkko- tai tietojärjestelmäpalveluja itse, ei sen tarvitse myöskään itse käsitellä haavoittuvuusilmoituksia tai julkistaa haavoittuvuuksia.

Laki tuo organisaatiolle velvoitteen seurata kyberturvallisuuden uhka- ja tilannekuvaa. Organisaatiolla on oltava kyky määritellä tilannekuva ja ylläpitää sitä. Organisaation tulee määritellä ja ylläpitää prosesseja ja teknisiä ratkaisuja operatiivisen ja kyberturvallisuustiedon keräämiseen, analysointiin, hälytysten nostamiseen, esittämiseen ja käyttämiseen, hyödyntäen muissa Kybermittarin osioissa mainittua informaatiota. Tilannekuva muodostetaan sekä organisaation toiminnan, että kyberturvallisuuden tasosta. Tavoitteena on lokien hallinnan ja monitoroinnin toteuttaminen sekä tilannekuvan muodostaminen.

Operatiivisen tietoturvan päätavoitteena on torjua pyrkimykset vaarantaa suojattavan tietojen luottamuksellisuutta, eheyttä tai saatavuutta, sekä minimoida onnistuneen hyökkäyksen/murron mahdollinen vaikutus ja saada palauduttua normaaliin toimintaan mahdollisimman lyhyellä häiriöajalla. Operatiivisen tietoturvan tehokkaan toimivuuden keskeinen elementti on mahdollisimman reaaliaikainen näkyvyys suojattaviin tietovarantoihin ja -järjestelmiin, sekä niiden teknisten tietoturvakontrollien tilaan. Näitä kontrolleja ovat esimerkiksi palomuurit, tunkeutumisen havaitsemisjärjestelmät, käyttöjärjestelmien ja ohjelmien turvallisuuslokit sekä erilaiset päätelaitteiden suojaohjelmistot. Yksi tämän

kyvykkyyden ehdoton edellytys on kyky keskitetystä analysoida turvallisuustapahtumia ja muodostaa hälytyksiä niistä.

Tämänkaltaisen näkyvyyden rakentuminen jakautuu useisiin prosesseihin ja vaiheisiin, joista ensimmäinen on kyvykkyys kerätä tilatietoja ja tapahtumalokeja kaikista toiminnalle merkittävistä järjestelmistä ja ohjelmistoista. Seuraava on kyvykkyys tunnistaa kerätystä lokimassasta poikkeavuuksia ja murron merkkejä, sekä muodostaa niistä hälytyksiä. Kolmas vaihe on arvioida hälytykset ja tarvittaessa laukausta liikkeelle korjaavia, rajaavia tai suojaavia toimenpiteitä.

Nykyisessä monimutkaisessa tietojärjestelmäarkkitehtuurissa tämänkaltaisen kyvyn saavuttaminen käytännössä vaatii automatisoituja ratkaisuja ja jatkuvan valvonta- ja ylläpitotyön vastuiden ja resurssien määrittämistä. Tehokkaan analysointikyvyn aikaansaamiseksi analyysityökalut vaativat laajalla kirjolla eri teknologioista kerättävien lokitietojen vastaanottoa ja käsittelyä, mikä kasvattaa käsiteltävän datan määrää nopeasti sekä edellyttää kaikkien eri teknologoista vastaavien tahojen, toimijoiden ja tiimien yhteistyötä.

Tapahtumien jäljittämiskyky, poikkeavuuksien tunnistaminen ja niihin reagoiminen ovat olennainen osa tietojärjestelmissä olevan tiedon suojaamista. Vaatimus tämän kyvyn rakentamiselle juontaa juurensa sekä kriittisten liiketoimintojen turvaamisesta, että GDPR:n (yleinen tietosuoja-asetus) ja muiden yksityisyyttä koskevien lakien asettamista vaatimuksista.

Lokienhallinta

Lokienhallinnan käytännön haaste yrityksille on teknisen käytännön toteutuksen suunnittelu niin että näkyvyys tapahtumiin on tarpeeksi kattava. Lokien käyttötarkoituksen huomioon ottaen olisi syytä pystyä yhdistämään tietoturvatapahtumia mahdollisimman laajalti kaikista käytössä olevissa teknologioista. Lokeja kerättäessä usein unohtuvat esimerkiksi tietoverkkojen aktiivilaitteet (kuormantasaajat, palomuuria ja erilaiset pääsyhallinnan laitteet), applikaatiotaso (webbiserverit, julkaisualustat, virtualisointikerrokset ja vaikkapa nimipalvelin sekä DHCP palvelu) ja työasemien lokit.

Lokien kerääminen muodostaa ytimen tietoturvatapahtumien valvonnalle ja poikkeamien tunnistamiselle. Tietomurron tapahtuessa tallennetut lokit, ajalta ennen murtoa, murron hetkellä ja reaaliaikaisesti hyökkäyksentorjunnan aikana, toimivat puolustavien tahojen tärkeimpänä ja usein ainoana tiedonlähteenä johon tutkimus, tilanteen arviointi ja vastatoimenpiteiden suunnittelu perustuu. Tästä syystä lokienhallinnan teknisesti kattava ja turvallinen toteutus on ydinkysymyksiä yrityksen kyvykkyydessä tunnistaa ja torjua tietoturvapoikkeamia.

Lokeja tulee kerätä kaikista toiminnalle tarpeellisista lähteistä, mieluiten vähän liikaa kuin liian vähän. Murtotutkimuksen aikana on tarvetta pystyä rakentamaan tapahtumaketjuja ja korrelaatioita eri teknologioissa tapahtuneiden asioiden välillä, jolloin eri lokilähteistä kerättyjen lokien aikaleimojen, kirjoitusformaattien ja sisältämän tiedon tulisi olla keskenään harmonisoitua. Tällä tarkoitetaan käytännössä esimerkiksi sitä, että lokitiedoissa tulisi aina olla luettavissa mistä järjestelmästä tapahtuma kirjattiin, mistä käyttäjätunnuksesta on kyse, mistä IP-osoitteesta pyyntö tuli ja oliko kyseessä sallittu vai estetty tapahtuma. Tapahtumakirjauksen olisi syytä vastata ainakin seuraaviin kysymyksiin mahdollisuuksien mukaan: kuka, mitä, mistä, milloin, mihin.

Pahantahtoinen toimija pystyy usein tuhoamaan tai vääristämään palvelimien paikallisia lokitietoja. Tästä syystä lokienhallinta tulisi rakentaa teknisesti niin, että muodostuneet lokit kerättäisiin erilliseen, suojattuun lokipalvelimeen niin, että niihin voitaisiin kohdistaa hakuja, vaikka alkuperäiset lokit tuhottaisiin hyökkäyksen alle joutuneelta palvelimelta hyökkääjän toimesta. Lokipalvelun turvallisessa toteutuksessa tulee ottaa huomioon nykyaikaisten hyökkäysten toteutuksen tavat, jossa usein tuotantoympäristöjen palvelimiin yhdistetyt varmennus-, lokienhallinta- ja muut ylläpidon käyttämät palvelimet tunnistetaan ennen varsinaisen hyökkäyksen toteuttamista, ja niiden toiminta lamaannutetaan tai estetään samanaikaisesti. Lokien hallinnan palvelu kannattaa tästä syystä eriyttää muista ympäristöistä kaikin mahdollisin tavoin, verkkoteknisesti ja käyttöoikeuksien puolesta.

Uhkatiedon hankinta ja hyödyntäminen riskienhallinnassa

Yrityksen tulee tunnistaa omaan toimiympäristöönsä vaikuttavien ulkopuolisten uhkien kehittymistä ja mukauttaa omia turvallisuuden hallintakeinoja ja toimintamallejaan niiden mukaisesti. Tietoisuutta asioista, jotka uhkaavat tai voivat uhata yrityksen toimintaa on

olemassa yleistä ei-tietojärjestelmäspesifistä sekä hyvin täsmällistä tietoturvauhkiin liittyvää ns. ”uhkatietoa”. Uhkatietoa tulee käytännössä kerätä eri tietolähteistä, kuten haavoittuvuustietoja organisaation omista tietovarannoista, viranomaistiedotteista sekä teknologiatoimittajien julkaisuista. On muistettava, että laissa edellytetään myös muiden kuin viestintäverkkojen ja tietojärjestelmien sisäisten uhkien tunnistamista ja arviointia. Esimerkiksi fyysisiä uhkia ovat luonnolliset ja yhteiskunnalliset tapahtumat, kuten tulipalot, tulvat ja levottomuudet.

Viestintäverkkoihin ja tietojärjestelmiin liittyvän uhkatiedon tulee olla oikea-aikaista, käyttökelpoista ja konkreettisia toimia tuottavaa. Uhkatiedon avulla organisaatio voi priorisoida riskienhallintatoimia niihin toimintoihin, joihin uhkat todennäköisimmin kohdistuvat ja joiden vaikutus on kriittisin. Toimijaan mahdollisesti kohdistuvista vaaroista ja riskien arviointiin liittyvistä seikoista on mahdollista saada suhteellisen pienellä vaivalla hyödyllistä tietoja valmiiksi jäsenneltynä ja analysoituna alla mainituista luotettavista lähteistä:

- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen tuotteet: Kybersää-tilannekatsaukset, haavoittuvuustiedotteet sekä toimialakohtainen tilannekuva
- Huoltovarmuuskeskuksen julkaisut sekä huoltovarmuuden tilannekatsaukset (edellyttää käyttöoikeuksia HVO Extranet:iin)
- Euroopan unionin kyberturvallisuusvirasto ENISAn uhkakatsaukset (englanniksi)
- Kyberturvallisuuden tapahtumia, uhkatietoja sekä pahantahtoisia toimijoita seuraavien Kyberala ry:n jäsenorganisaatioiden kausittaiset katsaukset (verkkosivuilla ja esim. LinkedIn-palvelussa)

***Esimerkki**: Lokienhallinta tulee ensisijaisesti ajatella yrityksen vastuullisuuden kautta syntyvänä velvoitteena, jolla mahdollistetaan tiedon keruu useista toisistaan riippumattomista tietojärjestelmistä tai -lähteistä. Lokitietoa tarvitaan selvittämään, mitä, miksi ja milloin jotakin tapahtui. Ilman lokitietoa organisaatioilla on erittäin heikot mahdollisuudet palautua kyberturvahäiriöistä.*

***Esimerkki**: Lokitiedot ovat ennen kaikkea todistusaineistoa digitaalisista tapahtumista ja näihin tulee suhtautua kuten perinteisiin tositteisiin. Lokitietoa tulee kerätä sellaisista laitteista, ohjelmistoista ja tietovarannoista, joita voidaan käyttää hyökkääjän tavoitteiden*

saavuttamiseen. Mitä kriittisempi valvontakohde eli lokilähde on kyseessä, sitä merkittävämpää on lokitiedon kerääminen ja varmistaminen.

Näin liikkeelle:

- Viestintäverkot ja tietojärjestelmät on suojattava luvattomalta pääsyltä, vahingoilta ja häiriöiltä. Valvonta vaatii dokumentoituja menettelytapoja, rooleja, vastuita ja raportointikanavia sekä poikkeamien ehkäisyyn että havainnointiin ja niistä ilmoittamiseen.
- Tapahtumien kirjaaminen ja havainnointi on välttämätöntä, ja siihen tarvitaan riittävät lokitiedot, kuten ylläpidosta ja muutoksista. Poikkeamien arviointi ja niiden vakavuuden sekä vaikutusten luokittelu on olennaista.
- Poikkeamien käsittelyprosessien on oltava jatkuvasti ylläpidettyjä ja päivitettäviä, ja ne tulee suunnitella siten, etteivät ne vaaranna toimijaa tai muita organisaatioita. Mikäli toimija ei itse tuota viestintäverkko- tai tietojärjestelmäpalveluita, ei sen tarvitse käsitellä haavoittuvuusilmoituksia tai julkistaa haavoittuvuuksia.

HUOM! Huolehdi, että vaatimusten **perustaso** toteutuu: riskienhallintaan perustuen tunkeutumisen havaitsemis- tai estämisjärjestelmiä, tunkeilijan havaitsemisjärjestelmä (IDS), murron estämisjärjestelmä (IPS), päätelaitteiden turvallisuuspalveluita (EDR/XDR) sekä palvelunestohyökkäyksiä rajoittavia palveluita on käytössä.

Kriittisiin toimintoihin liittyvistä tapahtumista kerätään tapahtumakirjauksia, kuten pääkäyttäjien tekemistä toimenpiteistä ja käyttöoikeuksiin liittyvistä muutoksista, sekä mahdollisuuksien mukaan kaikista turvallisuuteen liittyvistä tapahtumista koko viestintäverkon ja tietojärjestelmän laajuudella. Tapahtumakirjauksia kerätään myös luottamuksellisen tiedon käsittelystä perustuen esimerkiksi lainsäädännön vaatimuksiin. Tapahtumaloki on suojattu muutoksilta ja sitä hallinnoidaan erillisillä käyttäjätunnuksilla ja varmuuskopioitu säännöllisin väliajoin tai kopioitu erilliseen järjestelmään.

Tietoturvallisuuspoikkeamien toteutustavat muuttuvat jatkuvasti, joten on tärkeää seurata kyberturvallisuuden yleistilannetta sekä omien tietoverkkojen ja -järjestelmien toimintaa. Riittävä lokien kerääminen on avainasemassa mahdollisista poikkeamista toipumiseen.

Tapahtumien ja häiriötilanteiden hallinta (RESPONSE)

Toimijan lainsäädännölliset velvoitteet:

- **Poikkeamat tulee käsitellä** turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi
- Poikkeaman käsittelyssä tulee olla **käytännöt myös niihin reagoimiseksi**, joihin liittyy myös toimet poikkeaman **rajoittamiseksi, selvittämiseksi ja vaikutusten poistamiseksi**. Poikkeaman jälkeen tulee arvioida poikkeamaan johtaneet syyt ja oppia kokemuksista, jotta vastaavan poikkeaman uhkaan voidaan varautua jatkossa paremmin.
- Oltava **dokumentoidut menettelyt toiminnan jatkuvuuden ja häiriötilanteista palautumisen osalta** – eli suunnitelma häiriötilanteiden hallinnan ja toiminnan jatkamisen sekä takaisin toimintakuntoon saattamisen osalta ennalta määritellyllä hyväksyttävällä tasolla. Jatkuvuus tulee varmistaa riskienhallinnan perusteella luodulla jatkuvuussuunnitelmalla sekä toipumissuunnitelmalla.
- **Haitallinen** tekninen **liikenne** viestintäverkossa **tulee kyetä havaitsemaan ja estämään**.
- Suunnitelmien tulee sisältää **vähintään kriisinhallintamenettelyt erittäin vakavien poikkeamien varalta**.
- Muun riskienhallinnan mukaisesti **suunnitelmia tulee ylläpitää ja kehittää säännöllisesti** sekä niiden mukaista toimintaa harjoitella.
- Toimijan on **määritettävä varmuuskopioinnin käytänteet:** miltä osin varmuuskopioita on otettava järjestelmistä sekä varajärjestelmistä, niiden tiheys, säilytysaika, suojaus ja palautuksen testaaminen tilanteessa, jossa alkuperäinen järjestelmä ei olisi käytettävissä.
- Mikäli riskiarvion mukaan on todettu välttämättömäksi varmistaa viestintäkanavat myös silloin, kun tavanomaisesti käytössä olevat järjestelmät (esim. puhelin, sähköposti, pikaviestimet) eivät ole käytettävissä, tulee toimijan määrittää myös **suojatut varaviestintäjärjestelmät**, niiden tarve sekä käyttöönottotavat.
- Mikäli toimija tuottaa viestintäverkko- tai tietojärjestelmäpalveluita, tulee varmistua myös ylläpidon turvallisuudesta sekä määrittää tarvittavat **menettelyt haavoittuvuuksien käsittelyyn ja julkistamiseen.**

Organisaatiolla on oltava kyky hallita, reagoida ja palautua kybertapahtumista ja -häiriöistä. Organisaation tulee määritellä ja ylläpitää suunnitelmia, prosesseja ja teknologiaa kyberturvallisuuteen liittyvien tapahtumien ja häiriöiden havaitsemiseksi, analysoimiseksi, niihin vastaamiseksi ja niistä palautumiseksi suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin. Tavoitteena kybertapahtumien ja -häiriöiden havainnointi ja analysointi sekä niihin reagointi.

Reagointi

Kyberhäiriöiden hallinta, analysointi, dokumentointi ja raportointi ovat tärkeitä velvoitteita, ja näihin toimintoihin onkin olemassa ennalta määriteltyjä prosesseja ja ohjeita. Kyberhäiriöiden

hallintasuunnitelma sisältää yksityiskohtaisen viestintäsuunnitelman, joka kattaa kaikki oleelliset sisäiset ja ulkoiset sidosryhmät.

Organisaatio seuraa aktiivisesti kybertapahtumia ja raportoi havaitut häiriöt määriteltyjen toimintaohjeiden mukaisesti vastuullisille henkilöille tai rooleille. Kaikki tapahtumat ja häiriöt kirjataan huolellisesti rekisteriin, jota seurataan jatkuvasti. Sidosryhmät, kuten johto, viranomaiset, kumppanit ja asiakkaat on tunnistettu etukäteen. Heitä informoidaan säännöllisesti kyberturvallisuustilanteesta raportointivaatimusten mukaisesti.

Lain mukaan toimijan on toimitettava valvovalle viranomaiselle 24 tunnin kuluessa ensi-ilmoitus tietoturvapoikkeaman havaitsemisesta ja 72 tunnin kuluessa jatkoilmoitus. Poikkeamatilanteen päätyttyä toimijan on toimitettava valvovalle viranomaiselle loppuraportti. Kolmivaiheisen ilmoitusvelvollisuuden tavoitteena on toisaalta varmistaa poikkeamien nopea ilmoittaminen ja ajantasaisen tilannekuvan muodostaminen sekä toisaalta mahdollistaa toimijan resurssien suuntaaminen ensisijaisesti poikkeamien käsittelyyn liittyviin toimintoihin. Jatkoilmoituksessa toimijan on esitettävä alustava arvio merkittävästä poikkeamasta, sen vakavuudesta ja vaikutuksista sekä vaarantumista kuvaavat indikaattorit (Indicator of Compromise) eli IoC-tieto, jos sellaisia on saatavilla. IoC-tiedolla tarkoitetaan eroteltavaa tietoa esim. poikkeuksellisesta ulkoverkkoon ohjautuvasta dataliikenteestä, käyttäjätunnusten pääsy- tai käyttöoikeuksien laajentamispyrkimyksiä, poikkeavia tietojärjestelmien rekisterimuutoksia tai maantieteellisen sijainnin kannalta poikkeavia kirjautumisyrityksiä.

On syytä huomata, että mikäli toimija havaitsee merkittävän poikkeaman jonkun muun, esimerkiksi välittömän alihankkijan toiminnassa, olisi toimijan ilmoitettava tällaisesta poikkeamasta myös silloin, jos kyseinen poikkeama (voi) aiheuttaa vakavan toimintahäiriön toimijan omissa palveluissa taikka huomattavaa aineellista tai aineetonta vahinkoa toimijalle.

Varmistaminen

Organisaatio harjoittelee kyberhäiriöihin reagointia säännöllisin väliajoin varmistaakseen valmiuden todellisiin tilanteisiin. Häiriöiden juurisyitä analysoidaan perusteellisesti ja toteutetaan korjaavia toimenpiteitä sekä päivitetään toimintasuunnitelmia tarvittaessa. Jatkuvuussuunnitelmat ovat keskeinen osa organisaation strategiaa varmistamaan toiminnan jatkuminen kybertapahtuman tai -häiriön sattuessa. Suunnitelmissa otetaan huomioon kaikki

kriittiset resurssit sekä testataan ja arvioidaan niitä säännöllisesti varmistaakseen niiden toimivuuden. Tiedoista pidetään varmuuskopioita ja niiden palauttamista varmuuskopioilta testataan säännöllisesti.

Jatkuvuudenhallinta

Kyberhäiriöiden hallintaan, analysointiin, dokumentointiin ja raportointiin on ennalta määritelty prosessi ja toimintaohjeet. Kyberhäiriöiden hallintasuunnitelma sisältää viestintäsuunnitelman, joka kattaa sekä sisäiset että ulkoiset sidosryhmät. Kybertapahtumia seurataan ja havaitut kyberhäiriöt raportoidaan toimintaohjeen mukaisesti tietyille henkilöille tai roolien haltijoille.

Raportointi esitutkintaviranomaiselle (poliisi)

Tietojärjestelmiin tai muuhun tietotekniseen ympäristöön kohdistuneiden rikosten selvittämisessä eli esitutkinnassa hyödynnetään samankaltaisia tietoja kuin teknisen häiriötilanteen selvittämisessäkin. Tietoverkkoihin kohdistuvia rikoksia ovat esimerkiksi palvelunestohyökkäykset, tietomurrot ja datavahingonteot, joissa rikostutkinnan tukena toimivat hyvin erilaiset lokit sekä havainnot haittaohjelmien toiminnasta. Useat organisaatiot joutuvat myös erilaisten tietojenkalasteluiden ja huijausten kohteiksi. Tietojenkalastelulla pyritään pääsemään käsiksi organisaation dataan tai järjestelmään. Tietomurtojen yhteydessä kyseeseen saattaa tulla myös kiristys, jossa kohdetta kiristetään uhkaamalla julkaista saatua dataa. Kohdetta voidaan kiristää myös pyytämällä rahaa vastineeksi salauksenpurkuavaimesta, jolla salattu data saadaan avattua. Usein myös näitä molempia kiristyskeinoja hyödynnetään samanaikaisesti.

Mikäli epäilee rikoksen tai tietoturvaloukkauksen tapahtuneen, on asiasta perusteltua ilmoittaa poliisille epäselvissäkin tapauksissa. Poliisi arvioi ilmoituksen jälkeen, täyttääkö teko jonkin rikoksen tunnusmerkistön. Tietoturvaloukkausta koskevan rikoksen (kyberrikoksen) esitutkinnan aloittamista varten poliisi tarvitsee mahdollisimman tarkan kuvauksen siitä, mitä on tapahtunut ja keitä asia koskee. Asianomistaja on rikoksen osallinen, johon teko on kohdistunut. Asianomistajaa voidaan kutsua myös joissakin rikostyypeissä uhriksi.

Asianomistajalta selvitetään esimerkiksi:

- tarkat tiedot rikoksen kohteesta

- aiheutuneet vahingot
- vaaditaanko asiassa rangaistusta
- mahdolliset korvausvaatimukset
- tiedossa oleva näyttö (todistusaineisto).

***Tapaus**: Häiriötilanteiden hallintaprosessi oli yrityksessä määritelty vain tavanomaisten IT-ongelmien käsittelemistä varten. Tietoturvaongelmiin ei ollut varauduttu ja kun yrityksessä sitten tapahtui laajamittainen tietoturvaongelma, ei käytössä ollut riittävästi ennalta suunniteltuja toimintatapoja, määriteltyjä rooleja tai sovittuja vastuita. Tilanteen haltuunotto vei huomattavasti aikaa ja järjestäytyminen kesti kauan. Tämä hidastutti merkittävästi tilanteeseen reagointia ja tilanteesta toipumista.*

Näin liikkeelle:

- Kehitä selkeät toimintatavat poikkeamien hallintaan, mukaan lukien toimet poikkeamien rajoittamiseksi, niiden syiden selvittämiseksi ja vaikutusten korjaamiseksi.
- Analysoi poikkeamien syyt ja ota opiksi niistä parempaa tulevaisuuden varautumista varten; pidä yllä toiminnan jatkuvuutta ja häiriötilanteista palautumisen suunnitelmia.
- Varmista kyky tunnistaa ja estää haitallista teknistä liikennettä verkossa ja sisällytä suunnitelmiin menettelyt kriittisissä tilanteissa toimimiseen.
- Määrittele varmuuskopiointi ja sen käytännöt, kuten varmuuskopioitavat järjestelmän osat, niiden säilytysajat ja palautuksen testaus sekä turvaa viestintäverkkojen ja tietojärjestelmien ylläpito sekä haavoittuvuuksien hallinta.

HUOM! Huolehdi, että vaatimusten **perustaso** toteutuu: Varmuuskopiot on eriytetty fyysisesti ja loogisesti niistä järjestelmistä, joista ne on otettu. Varmuuskopioita on suojattu vähintään vastaavan tasoisilla menettelyillä kuin alkuperäistä dataa, mukaan lukien oikea-aikainen tuhoaminen. Varmuuskopioiden palautuksen testaamista tehdään säännöllisesti.

Toimijalla on kirjalliset käytännöt, joilla määritetään vastuut ja toimenpiteet erityisesti vakavia poikkeamia varten sekä käytännöt NIS-ilmoituksen tai muun viranomaisilmoituksen tekemiseen poikkeamatilanteissa.

Lain mukaan pakollisten ilmoitusten lisäksi tietoturvaloukkauksista kannattaa ilmoittaa myös Traficomin kyberturvallisuuskeskukselle sekä poliisille.

Toimitusketjun ja ulkoisten riippuvuuksien hallinta (DEPENDENCIES/THIRD PARTIES)

Toimijan lainsäädännölliset velvoitteet:

- **Varmistettava** toimitusketjun **toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky**, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt.
- Oltava **ajantasainen tieto kaikista toimintaan vaikuttavista välittömistä toimittajista**.
- **Otettava turvallisuusnäkökohdat huomioon suhteessa toimitusketjunsa välittömiin laite- tai palvelutoimittajiin**. Riskien hallintatoimenpiteitä harkitessa otettava huomioon välittömälle toimittajalle ja palveluntarjoajalle ominaiset haavoittuvuudet, tuotteiden ja palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt. Nämä voivat sisältää erilaisia turvallisuuteen liittyviä vaatimuksia esimerkiksi saatavuuden, ylläpidettävyyden ja sopimusten osalta.
- Toimijat voivat hallita toimitusketjujen kyberturvallisuusriskiä myös **sisällyttämällä kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin**, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa.
- Laissa säädettyjen vaatimusten kannalta **toimija vastaa itse siitä, että se hankkii omaan toimintaansa sellaisia tuotteita ja palveluita, että toimijan riskienhallinnan vaatimukset täyttyvät**. Lain vaatimukset eivät siis koske alihankkijaa, ellei se itsekin ole toimija, jonka toimintaa sääntely koskee.
- **Varauduttava välttämättömien resurssien**, kuten sähkönjakelun, tietoliikenneyhteyksien ja jäähdytyksen **häiriöihin ja estää viestintäverkkojen ja tietojärjestelmien tuhoutuminen, vahingoittuminen tai toimijan kriittisten toimintojen keskeytyminen** välttämättömien resurssien puutteen tai häiriön vuoksi.

Toimitusketjut eli alihankinta- ja toimitussuhteet ovat ketjuja, ja ketju on niin vahva kuin sen heikoin lenkki. Toimitusketjujen turvallisuudesta huolehtiminen on tärkeää, sillä merkittävä osa organisaatioihin kohdistuvista tietoturvaloukkauksista toteutetaan niiden käyttämien toimittajaverkostojen, palveluiden, tuotteiden tai avoimen lähdekoodin projektien kautta. Tällöin hyväksikäytetään organisaatioiden luottamusta toimittajiinsa. Pahantahtoinen toimija tunkeutuu toimittajan järjestelmiin ja saastuttaa toimitusketjussa käytetyn osan omalla haittakoodillaan, jonka jälkeen se leviää normaalia tuotteen jakelukanavaa pitkin yhteistyö- ja asiakasorganisaatioihin. Tavoitteena riippuvuuksien tunnistaminen ja riippuvuusriskin hallinta.

Toimijan tulee ymmärtää toimitusketjunsa, luoda tilannekuva, asettaa tietoturvavaatimukset toimitusketjulle, määrittää hallintamalli, operatiivinen toimintakyky, poikkeamaraportointi sekä turvallisuuden johtaminen ja kehittäminen. Hyvä lähtökohta tämän hahmottamiselle on lähteä

tutkimaan ulkoistettavan- tai toimittajan vastuulle annettavan osakokonaisuuden vaikuttavuutta oman liiketoiminnan tai NIS2 sidonnaisen palvelun tuottamiseen. Millaisia valvonnan, kontrollin ja toimintavarmuuden seurannan toimintoja olisi tarpeen muodostaa, jos kyseisen osakokonaisuuden tuottaisi yrityksen oman henkilöstö? Samat vaatimukset pätevät tällöin toimitusketjuun ja siinä toimiviin palveluntarjoajiin.

Täyttääkseen toimitusketjujen turvallisuutta koskevan velvoitteen toimijoiden tulisi niiden toimintaympäristö huomioiden:

- tunnistaa omaan liiketoimintaan liittyvät toimittajat ja heidän tuottamien palveluiden vaikutukset oman toiminnan toteutukseen.
- ylläpitää toimitusketjusta kuvausta, joka sisältää toimijoiden keskinäiset riippuvuudet, palveluiden sisältämät tunnistetut haavoittuvuudet ja uhat sekä tunnistettujen riskien vaikutukset. Kuvauksen tulee kattaa myös palveluntarjoajien ja toimittajien keskeiset alihankkijat.
- ottaa riskienhallinnassaan huomioon toimitusketjuhäiriön vaikutus yrityksen omaan toimintaan sekä varautua mahdolliseen toimitushäiriöön.
- määritellä roolit, vastuut ja valtuudet toimittajien kyberturvallisuuden määritelylle, valvonnalle ja tarkastajille. Toimittajien tulee määritellä vastaavat roolit ja vastuut omassa henkilöstössään.
- sisällyttää omasta toiminnasta tunnistetut tarpeelliset riskienhallinnan kontrollikeinot ja tavoitetilat toimittajan kanssa määriteltäviin palvelutasosopimuksiin ja muihin sopimusteknisiin rakenteisiin, sekä sopia niiden tilaa koskevasta valvonnasta ja viestinnästä.
- tehdä yhteistyötä sisäisten ja ulkoisten sidosryhmien kanssa jakamalla tietoa sekä parhaita käytänteitä.

Toimijan tulee siis kyetä ylläpitämään ajantasaista luetteloa välittömistä toimittajistaan, priorisoida viestintäverkkoihin ja tietojärjestelmiin liittyvien riskien kannalta olennaiset laite- ja palvelutoimittajat. Lisäksi toimijan on sovittava tai muutoin varmistettava, että toimittajan riskienhallintatoimenpiteet ovat sillä tasolla, että yrityksen omat riskienhallintavaatimukset voidaan täyttää. Tämä edellyttää käytännössä, että toimijan on itse arvioitava toimittajan riskienhallintaa sekä sisällytettävä sopimuksiin vaatimuksia riskienhallinnan tasosta. Sopimusprosessin yhteydessä toimittajalta saadut kirjalliset todisteet

riskienhallintamenettelyistään on syytä taltioida sopimusdokumenttien yhteyteen. Lisäksi toimijan tulee toteuttaa häiriöiden aiheuttamien vahinkojen vähentämiseen liittyvät järjestelyt, eli varajärjestelmät. On hyvä huomata, että vaikka alihankkija tai toimittaja olisi myös itse NIS2-direktiivin vaatimusten kohteena, alihankkija vastaa sääntelyn nojalla vain siihen itseensä kohdistuvien vaatimusten täyttämisestä ja erikseen siltä palveluita tai tuotteita hankkivan toimijan suhteen siitä, mitä alihankinnassa on sovittu.

Toimitusketjun hallinnassa olennaisia seikkoja on arvioida sitä, kuinka kriittinen alihankkija tai toimittaja on yrityksen toiminnalle. Arvioinnin kehikkona on hyvä käyttää tietoturvallisuuden perusmallia, eli toimittajan vaikutusta yrityksen omien viestintäverkkojen ja tietojärjestelmien luottamuksellisuudelle, eheydelle sekä saatavuudelle. Toimittajat ovat suositeltavaa asettaa riskitason mukaan järjestykseen ns. riksiluokan mukaan. Riskiluokka koostuu vähintään kahdesta seikasta: toimittajan tärkeydestä yrityksen omalle toiminnalle sekä saatavilla oleva tieto toimittajan omasta riskienhallinnasta (eli riskienhallintatasosta). On hyvä huomata, että paras tieto toimitusketjun riskeistä on usein toimittajien hallinnasta vastaavilta henkilöillä.

Toimijoiden tulisi arvioida ja otettava huomioon toimittajiensa tuotteiden ja palveluntarjoajiensa palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet ja toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt. Kyberturvallisuusriskien hallintatoimenpiteitä tulee sisällyttää sopimusjärjestelyihin, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa. Toimijan omat kyberturvallisuuden hallintavaatimukset ja niihin liittyvät toimenpiteet tuleekin sisällyttää toimitussopimuksiin ja toimittajaan kohdistuviin valvontakeinoihin. Lainsäädännön vaatimuksia ei ole syytä sellaisenaan siirtää toimittajalle ns. ”sateenvarjolauseella” tyyliin: ”toimittajan tulee täyttää NIS2-direktiivin vaatimukset”. Toimijat voivat käsitellä myös ensisijaisten toimittajien alihankkijoiden eli arvoketjun seuraavista tasoista johtuvia riskejä. On kuitenkin hyvä muistaa, että jokainen toimittaja vastaa omista riskeistään itsenäisesti ja tarvittaessa riskitietoa arvoketjussa jakaen.

Toimijan hankkiessa ulkoistettuja palveluita, on tärkeää ymmärtää omien palveluiden edellyttämä tietoturvallisuuden taso ja palveluntarjoajan kyvykkyys toimittaa riittävän turvallista palvelua näiden vaatimusten mukaisesti.

Palveluntarjoajan on helpompi vastata tarjouspyyntöön, kun toimija osaa kertoa tietoturvallisuuden tarpeistaan riittävän kattavasti ja selkeästi. Mitä ns. tietoturvallinen palvelu tarkoittaa toimijalle itselleen:

- Mitä tietoja käsitellään ja kuka niitä käsittelee?
- Millaisia luottamuksellisuusvaatimuksia tiedoille on?
- Mitä ovat tärkeimmät toiminnot/palvelut?
- Mitä riskejä organisaatiolle voisi aiheutua palvelun tietoturvaongelmien tai toimimattomuuden takia?
- Kuinka kauan tulette toimeen ilman palvelua eli mikä on vaadittava palvelutaso?

Palveluntarjoajan tietoturvalupaukset ja tietoturvallisuuden kyvykkyys on tarpeen arvioida, kuten yllä on todettu. Arvioinnin taso voi vaihdella dokumentaation arvioinnista aina ulkoiseen auditointiin riippuen hankittavan palvelun kriittisyydestä. Palveluntarjoajalta on hyvä selvittää ainakin seuraavat:

- Millaiset tietoturvallisuuden periaatteet ja toimintamallit toimittajalla on sekä miten tietoturvallisuuden hallinnan vastuut on organisoitu?
- Mikä tai millainen tietoturvalupaus hankittavalle palvelulle on (onko olemassa dokumentoitua tietoturvallisuuden kuvausta)?
- Onko saatavilla palveluun liittyviä tietoturvallisuuden sertifikaatteja tai auditointiraportteja?
- Keitä kumppaneita palveluntarjoaja käyttää ja onko myös näiden tietoturvallisuuden taso arvioitu?

Tietoturvavaatimuksiin liittyvät ehdot on perusteltua kirjata sopimuksiin mahdollisimman selkeästi. Hankittaessa vakioituja palveluita, esim. pilvipalvelut, asiakaskohtaiset sopimukset eivät useinkaan ole mahdollisia, joten silloin vaatimusten täyttyminen on varmistettava palveluntarjoajan toimitus- ja käyttöehdoista.

On suositeltavaa harkita ainakin seuraavien tietoturva-asioiden kirjaamista sopimuksiin. Hankittavan palvelun luonne ja vaatimukset lopulta määrittelevät, mitä tietoturvallisuudesta on syytä kirjallisesti sopia:

- Palvelulta vaadittavat tietoturvaratkaisut ja riskienhallintakeinot
- Palveluntarjoajan sitoutuminen hankkijan tietoturvallisuuden tavoitteisiin

- Palveluntarjoajan henkilöstön taustatarkistukset (esim. turvallisuusselvitykset) ja vaitiolositoumukset
- Luottamuksellisten tietojen suojaamisen (ml. periaatteet ja keinot)
- Palveluntarjoajan kanssa sovitut tietoturvastandardit ja käytännöt
- Palvelun riittävän ja sovitun tietoturvatason osoittaminen
- Palveluun liittyvien henkilöiden tietoturvallisuusosaamisen varmistaminen
- Palvelun ja käytettävän tietojen eriyttäminen muista asiakkaista
- Toimintatavat palveluntarjoajan henkilöstön työskennellessä toimijan tiloissa
- Mahdollisuus palvelun tietoturvallisuuden ”tason” tarkastukseen (auditointiin)
- Palvelun jatkuvuussuunnittelu ja suunnitelmien testaaminen
- Tietojen turvallinen tuhoaminen esim. laitteiden vaihdon yhteydessä
- Palvelun tietoturvatason mittaaminen ja seuranta
- Poikkeamien ilmoittaminen ja ripeä käsittely – myös läheltä piti tilanteissa
- Tietoturvayhteistyö ja palvelun tietoturvan jatkuva kehittäminen
- Tietoturvallisuuden huomiointi sovelluksissa ja sovelluskehityksessä
- Mahdolliset sanktiot vakavista tietoturvapoikkeamista

Esimerkki: *Organisaatio voi myös laatia toimitusketjun kartan tai luettelon, joka näyttää sen keskeiset toimittajat, alihankkijat ja palveluntarjoajat sekä niiden kyberturvallisuuden riskit. Organisaatio sopii kyberturvallisuuteen liittyvien vastuiden jakautumisesta mahdollisimman tarkasti, kattaen koko arvoketjun ja palveluun liittyvät osa-alueet.*

Tapaus*: Lauantaina 29.10.2022, jolloin pahantahoinen toimija tunkeutui maan raideliikenteestä vastaavan Dänische Staatsbahnen (DSB) ICT-palveluntoimittajan Supeon-ohjelmistojen testausympäristöön ja aiheutti Tanskan junaliikenteen pysähtymisen maanlaajuisesti.*

Tapaus*: Organisaation erään tietojärjestelmän toimittajan kanssa oli hankinnan yhteydessä kyllä tehty tukisopimus, mutta vain minimitasolla, koska järjestelmän merkitystä liiketoiminnan jatkuvuudelle ei ollut ymmärretty. Kun tuossa liiketoimintakriittisessä järjestelmässä sitten tapahtui häiriö, ei järjestelmän toimittajalta saatu hankittua tukea riittävän nopeasti, koska tukisopimuksen palvelutaso oli sovittu liian alhaiseksi mikä ei vastannut liiketoiminnan tarpeita. Yrityksen hankintaosastolla oli tapana luokitella toimittajat lähinnä toimittajien*

vuosittaisen laskutuksen perusteella eikä toimittajan liiketoimintakriittisyyttä arvioitu. Toimittajan merkitys yrityksen liiketoiminnan jatkuvuudelle ei mitenkään noussut esiin ennen tuota häiriötä.

***Tapaus**: Tietoturvan nykytilan kartoituksessa kävi ilmi, että tietojärjestelmien operointia toteuttava toimittaja oli ottanut käyttöön alihankkijoita oman resurssipulansa tukemiseksi, tiedottamatta tästä omille asiakkailleen. Alihankintana konkreettista operointia tekevät toimittajat eivät haastattelussa tienneet ollenkaan nykytilakartoitusta tekevät toimijan korkean turvallisuuden vaatimuksista, eivätkä heidän toimintatapansa olleet tunnistettujen riskien, uhkien ja sopimusteknisten vaatimusten mukaisia. Syyksi aliurakoinnin käyttöönotolle selvisi kiire, resurssipula ja palveluntarjoajasopimuksiin liitetyt uhkasakot. Palveluntuottajat ja toimittajat on syytä priorisoida niiden liiketoimintakriittisyyden perusteella ja tukipalvelut yms. pitää sovittaa vastaamaan liiketoiminnan palvelutasoa ja kriittisyyttä.*

Näin liikkeelle:

- Pidä yllä tietoa kaikista suorista toimittajista, jotka vaikuttavat liiketoimintaasi, ja arvioi heidän haavoittuvuutensa, tuotteidensa laadun, häiriönsietokyvyn sekä kyberturvallisuusriskien hallintaan liittyvät käytännöt.
- Vastaa omasta riskienhallinnastasi hankkiessasi tuotteita ja palveluja suorilta toimittajilta ja sisällytä kyberturvallisuusriskien hallinta osaksi sopimuksia.
- Varautu kriittisten resurssien, kuten sähkön ja tietoliikenneyhteyksien, häiriöihin ja suojele viestintäverkkojasi ja tietojärjestelmiäsi vahingoilta.

HUOM! Huolehdi, että vaatimusten **perustaso** toteutuu: varmista, että keskeisten ja toimintaan suoraan vaikuttavien toimittajien riskitaso sekä riskienhallinnan käytänteet ovat tiedossasi ja sopimuksella hallittuja.

Toimijan on hankittava vain sellaisia tuotteita ja palveluita, että toimijan omat riskienhallinnan vaatimukset täyttyvät. Tämä edellyttää omien riskienhallintakeinojen huomioimista hankintaprosessissa.

Henkilöstön hallinta (WORKFORCE)

Toimijan lainsäädännölliset velvoitteet:

- Oltava **henkilöstöön liittyvät menettelytavat**, joissa huomioidaan myös ulkoiset toimijat, kuten alihankkijat. Menettelytapojen tulisi huomioida myös työsuhteen päättymisen ja työtehtävien muutoksien jälkeiset vastuut ja velvollisuudet.
- **Henkilöstöä ja ulkoisia toimijoita on tiedotettava** heidän työtehtäviensä ja tarjoamiensa palveluiden turvallisuuteen liittyvistä vastuista ja velvoitteista, esimerkiksi salassapitoon liittyen.
- **Henkilöstön tulee tuntea käytössä olevat turvallisuusmenettelyt ja sitoutua** niiden noudattamiseen.
- Huolehdittava siitä, että **henkilöstöllä on kyvykkyys toimia** tavalla, joka vastaa kyberturvallisuuden hallintamallia ja hallintatoimenpiteitä. Tämän saavuttamiseksi henkilöstölle **tulee järjestää koulutusta**, jolla pyritään tietoisuuden parantamiseen yleisesti kyberturvallisuudesta, ajantasaisten menettelyiden ja käytäntöjen tuntemuksesta sekä tunnetuista kyberturvallisuusriskeistä.
- Koulutuksella tai muulla vastaavalla tavalla **tulee varmistua, että henkilöstöllä on** työtehtäviinsä nähden **riittävä osaaminen** viestintäverkon ja tietojärjestelmän suojaamisesta, kyberturvallisuusriskien tunnistamisesta, riskienhallintakäytännöistä ja niiden vaikutusten arvioinnista toimijan tarjoamiin palveluihin liittyen, ja että tätä osaamista myös ylläpidetään riittävällä tasolla.
- Vaikka toimijan johtoa ei luettaisi toimijan henkilöstön osaksi, **johdolla on oltava riittävä perehtyneisyys kyberturvallisuuden riskienhallintaan**.

  HUOM! Henkilöstöturvallisuudella tarkoitetaan menettelyjä, joilla varmistetaan henkilöiden tietoturvavastuut ja velvollisuudet, tietoturvaosaaminen ja taustatarkastukset (taustantarkistukset käsitelty kohdassa 1.3 ACCESS – Identiteetin- ja pääsynhallinta) sekä avainhenkilöriskien hallinta.

Merkittävä osa tietoturvapoikkeamista juontaa juurensa ihmisiin, koska he toimivat viestintäverkkojen ja tietojärjestelmien käyttäjinä eri rooleissa ja tarkoituksissa. Henkilöstöturvallisuudella tarkoitetaan tässä yhteydessä menettelyjä, joilla varmistetaan käytössä olevan työvoiman kyberturvallisuusosaaminen riittävällä tasolla.

Toimijalla on oltava kyky kehittää ja ylläpitää henkilöstön kyberturvallisuusosaamista ja -valmiutta. Toimijan tulee määritellä ja ylläpitää suunnitelmia, prosesseja, teknologiaa ja kontrolleja organisaation kyberturvallisuuskulttuurin luomiseksi ja sopivan ja osaavan henkilöstön takaamiseksi, suhteessa sekä suojattaviin kohteisiin kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin. Tavoitteena kyberturvallisuuden vastuiden jakaminen, kyberhenkilöstön kehittäminen, henkilöstön hallintatoimet ja kybertietoisuuden lisääminen.

Erilaisia selvityksiä ja tarkastuksia (esimerkiksi taustojen tarkistuksia, turvallisuusselvityksiä ja huumetestejä) on syytä teettää suhteessa tehtävän riskeihin tarvittaessa uusia työntekijöitä palkatessa sekä ulkoisia toimijoita valittaessa.

Työntekijöiden palkkaukseen ja sisäisiin siirtoihin liittyvissä menettelyissä on syytä huomioida kyberturvallisuus. Menettelyissä kannattaa huomioida mm. kriittiset työyhdistelmät, pääsyoikeudet sekä tarve mahdollisille taustatarkistuksille tai turvallisuusselvityksille. Myös työsuhteen päättymiseen liittyvissä menettelyissä huolehditaan kyberturvallisuuden toteutumisesta varmistamalla käyttöoikeuksien poisto ja yrityksen laitteiden ja materiaalin palauttaminen.

Henkilöstön kyberturvallisuustietoisuutta kohotetaan säännöllisesti, jotta varmistutaan siitä, että henkilöstö tuntee tehtävään liittyvät ja käytössä olevat turvallisuusmenettelyt. Henkilöstön tietoturvakoulutus on hyvä miettiä roolipohjaisesti. Pelkkä yleinen, kaikille yhteinen koulutus ei riitä vastaamaan tilanteisiin, jossa eri rooleissa kohdataan erilaisia kyberuhkia. Taloushallinnon prosesseja varten on syytä määritellä varmennus- ja hyväksyntäkäytännöt, ja henkilöstöä on syytä rohkaista varmistamaan asiat matalalla kynnyksellä.

***Tapaus**: Tietoturvakoulutus hoidettiin organisaatiossa siten, että taloon tuleville uusille työntekijöille annettiin omatoimisesti opiskeltavaksi yleinen, lähinnä yrityksen tietoturvapolitiikkaan pohjautuva tietoturvakoulutusmateriaali. Työntekijöille ei erikseen koulutettu heidän työtehtävänsä kannalta relevantteja kyberuhkia.*
Eräänä päivänä taloushallinnon työntekijä sai sähköpostilla huijausviestin, jossa häntä ohjeistettiin maksamaan lasku. Työntekijä ei osannut kyseenalaistaa viestiä, joten hän ei myöskään varmistanut viestin oikeellisuutta ja tämän seurauksena yhtiö menetti merkittävän summan rahaa maksettuaan huijareiden lähettämän laskun.

Näin liikkeelle:

- Varmista, että turvallisuustoimenpiteet ja velvollisuudet ulottuvat työsuhteen päättymiseen ja tehtävien muutoksiin asti, mukaan lukien alihankkijoiden rooli ja vastuut.
- Kouluta henkilöstöä ja ulkoisia toimijoita heidän turvallisuusvastuistaan ja -velvoitteistaan, korostaen salassapidon tärkeyttä ja kyberturvallisuuden periaatteita.
- Huolehdi, että sekä henkilöstö että johto ovat koulutettuja ja osaavat suojata viestintäverkkoja ja tietojärjestelmiä, tunnistamaan riskejä ja noudattamaan riskienhallintakäytäntöjä.

HUOM! Huolehdi, että vaatimusten **perustaso** toteutuu: kirjalliset tietoturvakäytännöt on laadittu ja henkilöstö, alihankkijat ja muut kumppanit ovat tietoisia ohjeiden sisällöstä ja sijainnista, mukaan lukien luottamuksellisen tiedon käsittely. Käytäntöjä tarkastellaan ja tarvittaessa päivitetään säännöllisesti, esimerkiksi vuosittain tai muutosten yhteydessä.

Varmista perehtyneisyys, järjestä koulutusta ja huolehdi alihankkijoiden hallinnasta myös tietoturvallisuuden näkökulmasta.

Kyberturvallisuusarkkitehtuuri (ARCHITECTURE)

Toimijan lainsäädännölliset velvoitteet:

- Toiminnoille **kriittiset kohteet tulee tunnistaa ja tarvittaessa suojata** ajantasaisin teknisin keinoin, esimerkiksi eristämällä eli ”vyöhykkeistämällä” (segmentointi).
- **Luotava salausmenetelmien** käyttämistä koskevat **toimintaperiaatteet ja menettelyt** sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön, joilla suojataan tarvittaessa tiedon luottamuksellisuutta, aitoutta ja eheyttä sen säilyttämisen tai tietoverkossa siirtämisen aikana. Valittava salaustekniikka, joka on suojaukseltaan riittävä salattavan tiedon laatuun, salausluokitukseen, suojausaikaan ja suorituskykyvaatimuksiin nähden.
- Salaustekniikan osalta on **huomioitava salausalgoritmien, käyttötapojen ja avainvahvuuksien** lisäksi **myös avaimen saatavuus sekä turvallinen säilytys, luonti ja hallinta**.
- Käytetyn **salausmenetelmän vaatimusten tulee olla ajantasaisia koko järjestelmän elinkaaren ajan**, jolloin esimerkiksi salausalgoritmin tulee olla vaihdettavissa (kryptoketteryys).
- Todettava **perustason kyberhygieniakäytännöt** toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi. Varmistettava, että perustason **kyberhygieniakäytännöt on toteutettu ja että työntekijät noudattavat niitä**. Käytäntöjen taso tulee mitoittaa toimintojen kriittisyyteen perustuen. Valittujen toimenpiteiden tulee perustua yleisiin hyviin käytäntöihin sekä riskienarviointiin.

  HUOM! Kyberhygieniakäytännöt eli perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi viittaavat pääosin muissa kohdissa (1.1-10.10.) kuvattuja vaatimuksia, kuten viestintäverkon rakenteellista turvallisuutta, haitallisen liikenteen havainnointia ja estämistä, toimintojen jäljitettävyyttä ja monitorointia, luottamattomuuden periaatetta (zero-trust), ajantasaisia ohjelmistopäivityksiä, laitteiden ja ohjelmistojen turvallista konfigurointia, verkon segmentointia, identiteetin- ja pääsynhallintaa sekä käyttäjien osaamisen parantamista ja tarvittaessa viestintäverkkojen sekä tietojärjestelmien turvallisuutta parantavien teknologioiden käyttöönottoa. Katso myös tämän oppaan sivu 9.

Kyberturvallisuusarkkitehtuuri on suunniteltu järjestelmä, joka keskittyy ja tietojärjestelmien suojaamiseen. Se kattaa laajan kirjon toimenpiteitä, kuten tietoturvallisuusohjeita, turvallisuusmalleja, verkkosuunnittelua ja riskienhallintaa. Kyberturvallisuusarkkitehtuurin tavoitteena on varmistaa, että organisaation tietojärjestelmät ovat kestäviä, luotettavia ja suojattuja kyberuhilta. Tämä on erityisen tärkeää nykypäivän digitaalisessa ympäristössä, jossa tietoturvaongelmat ovat yleisiä ja monimuotoisia.

Kyberturvallisuusarkkitehtuuri eroaa vanhakantaisesta tietoturvallisuustoiminnasta monin tavoin. Se ottaa huomioon kokonaisvaltaisen lähestymistavan, riskiperusteisen suunnittelun,

joustavuuden ja skaalautuvuuden, yhteistyön ja viestinnän sekä pitkäjänteisen suunnittelun. Perinteinen tietoturvallisuus saattaa keskittyä enemmän teknisiin ratkaisuihin ja olla toimintaperiaatteiltaan reaktiivisempaa eli lähinnä tietoturvapoikkeamiin reagoimista.

Lainsäädäntö edellyttää organisaatioilta riskilähtöistä mallia oman kyberturvallisuutensa hallintaan. Tämä saattaa olla helpompaa toteuttaa, mikäli yksittäisiä sääntelystä tai yrityksen omasta riskienhallinnasta tunnistettuja kohteita ei yritetä ratkoa yksittäisinä, erillisinä toimina vaan ne nähdään kokonaisuutena, osana laajempaa yrityksen toiminnan ohjaamiseen liittyvää riskienhallinnan rakennetta. Alla osakokonaisuuksia, joita edellä mainitusta arkkitehtuurisuunnitelmasta olisi perusteltua käsitellä:

Salausmenetelmillä tarkoitetaan kryptografisia menetelmiä, joilla tieto muutetaan sellaiseen muotoon, ettei ulkopuolinen voi saada sen sisältöä selville. Organisaatiolla on oltava kyky hallita ja ylläpitää kyberturvallisuustoimintaansa. Organisaation tulee luoda ja ylläpitää rakenteita, joilla se hallinnoi ja ohjaa organisaation kyberturvallisuuden riskienhallintakeinoja, -prosesseja ja muuta kyberturvallisuuden toimintaa suhteessa sekä organisaation omaisuuteen kohdistuviin riskeihin, että organisaation asettamiin tavoitteisiin. Tavoitteena tulisi olla kyberturvallisuusarkkitehtuurin luominen mukaan lukien verkkojen segmentointi, sovellusturvallisuus ja tietojensuojelu.

Salausmenetelmien ja muiden riskienhallintakeinojen yhteydessä viitataan usein tietojen luottamuksellisuuteen, saatavuuteen sekä eheyteen. Käsitteet eheys ja aitous ovat läheisiä toisilleen. Esimerkiksi viestinvälityksessä eheys viittaa siihen, että viesti ei muutu kulkiessaan lähettäjältä vastaanottajalle. Eheydellä voidaan viitata myös siihen, että viestin rakenne täyttää tietyt sovitut vaatimukset, esimerkiksi sisältää tietyt tietokentät määrätyssä järjestyksessä. Eheys ei kuitenkaan automaattisesti takaa aitoutta. Viesti voi olla eheä mutta väärennetty. Aitous (authenticity) viittaakin todellisuuden, alkuperän ja luotettavuuden varmistamiseen. Pyritään siis varmistumaan siitä, että digitaalinen viesti ja tiedot tulevat oikeasta, luotettavasta lähteestä.

Aitouden varmistamiseen voidaan käyttää mm. salaukseen ja varmenteisiin pohjautuvia ratkaisuja kuten sähköistä allekirjoitusta. Aitouden varmistamisella on suuri merkitys mm. erilaisten käskyjen ja ohjausviestien käsittelyssä. Ennen vastaanotetun komennon

hyväksyntää ja toteuttamista vastaanottajan tulisi pyrkiä aina varmistamaan, että viestin on lähettänyt oikeutettu, todennettu lähettäjä. Myös lokienhallinnassa on tärkeää pystyä varmistumaan kerätyn tiedon aitoudesta. Tietomurtojen yhteydessä tunkeutuja voi pyrkiä tuhoamaan tai muuttamaan lokitietoja peitelläkseen tapahtunutta. Lokit tuleekin kerätä ja säilyttää niin, että niiden aitoudesta ja eheydestä voidaan varmistua.

Haavoittuvuuksien hallintamenettelyn yhteydessä tulee määritellä, miten erilaisia haavoittuvuuksia tunnistetaan sekä käsitellään niiden havaitsemisen jälkeen. Haavoittuvuuksien hallinnan kyvykkyys pitää sisällään tavat, tekniikat ja työkalut, joilla haavoittuvuuksia etsittäisiin aktiivisesti ympäristöstä, sekä toimintatavat miten havaitut haavoittuvuudet arvioidaan, käsitellään ja korjataan.

Haavoittuvuuksien hallinnan vaatimukset tulee myös ottaa huomioon tietojärjestelmien koko elinkaaren ajan. Käytännössä tämä tarkoittaa, että kaikkien teknologioiden tulee tukea määriteltyjä vähimmäistavoiteaikoja korjauspakettien jakelulle, niissä tulisi olla voimassa oleva valmistajan tuki haavoittuvuuksien korjaamiselle ja niiden tietoturvapäivitysten tilaa tulee aktiivisesti seurata.

Hyökkäyspinnan vähentämisen osana tulee olla määritelty ohjeistus siitä, miten järjestelmät asennetaan (toisin sanoen mitkä palvelut ja ohjelmistot ovat sallittuja, miten rajoitukset määritetään, minkä palveluiden sallitaan kommunikoida internet-verkon yli jne.).

Haittaohjelmien havaitsemisen tulee tapahtua useilla kerroksilla, esimerkiksi verkon reunalla, sähköpostipalvelimella sekä työasemalla. Sen tulisi hyödyntää edistyneitä havaitsemismekanismeja (ei vain sormenjälkien tunnistamista) ja sen tulee kattaa kaikki käyttöjärjestelmät, joiden tunnistetaan olevan luonteeltaan haittaohjelmille tai hyökkäystyökaluille alttiita.

***Esimerkki**: Digitaalisessa palvelussa oli mahdollista maksua vastaan ladata käytettäväksi palvelun sisäistä valuuttaa eli saldoa. Maksut suoritettiin luottokortilla ja onnistuneen luottokorttiveloituksen jälkeen järjestelmä teki saldopäivityksen palvelun käyttämään taustajärjestelmään. Jossain vaiheessa palvelun ylläpitäjä alkoi epäillä, että palveluun oli talletettu saldoa enemmän kuin mitä oli saatu rahaa luottokorttiveloituksina. Tarkemmassa selvityksessä kävi ilmi, että puutteellisesti suunnitellun järjestelmäarkkitehtuurin vuoksi*

taustajärjestelmään olikin mahdollista ladata saldoa ilman luottokorttiveloitusta. Tämän mahdollisti kaksi erillistä puutetta arkkitehtuurissa: Ensinnäkin, taustajärjestelmää ei ollut riittävästi eristetty ulkoisesta ympäristöstä, jolloin luottokorttimaksut oli mahdollista ohittaa lähettämällä tiettyjä ohjausviestejä suoraan taustajärjestelmään. Toiseksi taustajärjestelmä ei tarkastanut vastaanottamiensa ohjausviestien aitoutta tarkemmin vaan hyväksyi lähettäjästä riippumatta kaikki vastaanottamansa viestit, jotka rakenteellisesti olivat oikeita.

***Tapaus**: Ohjelmistoalan yritys oli siirtymässä itse hallinnoiduista palvelinympäristöstä puhtaaseen pilviympäristöön. Uudessa toimintamallissa operatiivinen infrastruktuurin hallinta tapahtuu ohjelmistokehittäjien toimesta (niin sanottu DevSecOps toimintatapa), jonka tukemiseksi hankittiin taloon DevSecOps osaajia. Samalla kehityksen ja ylläpidon fokus siirtyi voimakkaasti pilviympäristöön, ja vanhojen palvelimien ylläpito lopetetiin ”pian poistuvana teknologiana”. Ohjelmistotalolla ei ollut vahvaa muutoshallintaa ja ympäristöjen dokumentointi oli vajavaista. Pilvisiirtymässä tapahtuikin yllättäviä viiveitä ja ”pian poistuvat” palvelimet pysyivätkin käytössä useamman vuoden, tosin niin että ne käytännössä unohdettiin oman onnensa nojaan. Vasta tietoturvatarkastuksessa tiedostettiin, että sillä hetkellä työtä tekevien henkilöiden ymmärryksen vastaisesti, ”pian poistuvat” palvelimet edelleen toimivat asiakkaille myytävän SaaS palvelun alustana. Toista vuotta kestänyt laiminlyönti asiakasdatan suojaamiseen käytettävien palvelimien ylläpidossa johtivat vaatimustenmukaisuuden ja laillisten vaatimusten mukaisiin sanktioihin. Juurisyynä tapahtuneelle oli kokonaiskuvan ja kommunikaation puute, joka johti tilanteeseen, jossa yritys ei itsekään enää tiennyt miten heidän ICT-palvelunsa asiakkaille tuotetaan.*

Näin liikkeelle:

- Määritä ja suojaa liiketoiminnan kriittiset alueet, esimerkiksi vyöhykkeistämällä, ja kehitä periaatteet ja käytännöt, jotka turvaavat tiedon luottamuksellisuuden, aitouden ja eheyden, mukaan lukien tehokkaat salaustekniikat.
- Varmista salauksen avainten asianmukainen saatavuus, turvallinen säilytys sekä niiden luonti ja hallinta, ja pidä käytetyt salausteknologiat ajan tasalla.
- Sovella perustason kyberturvallisuuden hygieniakäytäntöjä, kuten säännöllisiä ohjelmistopäivityksiä, verkon segmentointia ja käyttäjien kyberturvallisuustietoisuuden jatkuvaa kehittämistä.

HUOM! Huolehdi, että vaatimusten **perustaso** toteutuu: järjestelmät, jotka ovat hyvin haavoittuvia tai kriittisiä tai joiden vaarantuminen saattaa johtaa koko verkon tai järjestelmän vaarantumiseen on eriytetty vähintään loogisella tasolla muusta ympäristöstä. Tällaisia järjestelmiä ovat esimerkiksi hallintaverkot ja hallintatyöasemat. Erottelu voidaan toteuttaa käyttäen esimerkiksi seuraavia tekniikoita tai niiden yhdistelmiä: virtuaalilähiverkko, palomuuri, network access control, tunkeilijan havaitsemisjärjestelmä / murron estämisjärjestelmä (IDS/IPS), virtuaalinen erillisverkko (VPN). Myös langattomat verkot on suojattu niin, etteivät ne vaaranna muita järjestelmiä, esimerkiksi vahvan salauksen ja pääsynhallinnan avulla.

Toimijalla on käytössä haittaohjelmasuojaus, kuten päätelaitteiden virustentorjuntaohjelmisto (Anti-Virus, EDR tai XDR). Haittaohjelmasuojausta voi olla myös esimerkiksi keskitetysti sähköpostipalvelussa, kuten kalasteluviestien esto, haittaohjelmien esto, DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) jne.

Luottamuksellinen tieto siirretään lähtökohtaisesti salattuna. Toimijan käyttämillä päätelaitteilla sijaitseva luottamuksellinen tieto (tietokoneet, puhelimet, ulkoiset tallennusvälineet) on tarvittaessa salattu, esimerkiksi levysalauksella.

Sanasto

Viestintäverkko

Sähköisen viestintäverkon siirtojärjestelmät, jotka voivat perustua pysyvään infrastruktuuriin vai keskitettyyn hallintokapasiteettiin, sekä soveltuvin osin kytkentä- tai reitityslaitteistot ja muut välineet ml. ei-aktiiviset verkkoelementit, joilla voidaan siirtää signaaleja johtojen välityksellä, radioteitse, optisesti tai muulla sähkömagneettisella tavalla6. Näiden verkkojen avulla tietojärjestelmät kommunikoivat toistensa ja tietojärjestelmien käyttäjien kanssa.

Tietojärjestelmä

Laitteita tai laitteiden ryhmiä, jotka suorittavat ohjelman avulla digitaalisten tietojen automaattista käsittelyä, sekä digitaaliset tiedot, joita viestintäverkoissa ja tietojärjestelmissä säilytetään, käsitellään, haetaan, tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai ylläpitoa varten. Tietojärjestelmä voi koostua useammasta komponentista, usein muodostaen palvelun tai toiminnon. Esimerkiksi sähköpostipalvelin voi koostua tietokannasta, verkkopalvelimesta, käyttöoikeuksien hallinnan palvelimesta, mutta näyttäytyy käyttäjille "sähköpostina".

Pahantahtoinen toimija

Pahantahtoisella toimijalla tarkoitetaan laittomin tai luvattomin keinoin toimivien, kohteelleen vahingollisia seurauksia tavoittelevia tai sallivia yksilöitä ja ryhmiä. Usein näihin toimijoihin viitataan myös termeillä kyberrikolliset, uhkatoimijat, pahantahtoiset hakkerit jne.

Palveluntarjoaja

Toimija tai yritys, joka tuottaa muille toimijoilla tarpeellista palvelua tai toimintoa. Palveluntarjoajan asiakkaat rakentavat oman toimintansa tukeutumaan, tai olemaan jopa riippuvaisia palveluntarjoajan tuottamasta palvelusta. Palvelu voi olla mitä vaan, siivouspalvelusta logistiikkapalveluiden kautta tietotekniikan ylläpitoon ja konesalipalveluihin. Käytetään myös nimityksiä toimittaja tai kumppaniyritys. Palveluntarjoaja voi olla myös ohjelmistoja tuottava taho, jonka ohjelmistokehitykseen ja sen turvallisuuteen muut toimijat luottavat.

---

[6] Mukaan lukien satelliittiverkot, kiinteät (piiri- ja pakettikytkentäiset, mukaan luettuna internet) ja matkaviestintäverkot, sähkökaapelijärjestelmät siinä määrin kuin niitä käytetään signaalinsiirtoon, radio- ja televisiolähetyksiin käytetyt verkot sekä kaapelitelevisioverkot riippumatta siitä, minkä tyyppistä informaatiota niissä siirretään.

Toimitusketju

Useammasta palveluntarjoajasta koostuva, yrityksen tai organisaation toiminnalle tärkeä palveluiden tai tuotteiden ketju, joka muodostaa toisistaan riippuvaisen kokonaisuuden. Toimitusketjun luonteeseen kuuluu toimijoiden keskinäisriippuvuus, eli ilmiö, jossa yhdenkin ketjussa toimivan palveluntarjoajan häiriöt heijastuvat koko toimitusketjun kykyyn tuottaa haluttua lopputulosta. Käytetään myös termejä alihankintaketju tai palveluntarjoajaketju.

Kyberriski

Yhteiskunnallisesti merkittävään toimintoon liittyvät riskit, jotka pohjaavat näiden toimintojen riippuvuuteen niitä tuottavista tietojärjestelmistä. Mikäli liikennevaloja ohjaava tietokone saadaan pahantahtoisen toimijan toimilla sammutettua, liikennevalot eivät toimi. Liikennevalojen toimintaan liittyy näin kyberriski.

Lisäksi laissa kyberturvallisuuden riskienhallinnasta (KRHL) on määritelty useita käsitteitä, joista alla tämän oppaan kannalta keskeisimpiä:

Kyberuhka

Potentiaalinen tilanne, tapahtuma tai toiminta, joka voi vahingoittaa tai häiritä viestintäverkkoja ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti.

Haavoittuvuus

Tieto- ja viestintätekniikan tuotteiden tai -palvelujen heikkous, alttius tai vika, jota kyberuhka voi hyödyntää.

Poikkeama

Tapahtuma, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.

Riski

Poikkeaman aiheuttamien menetysten tai häiriön mahdollisuus, joka ilmaistaan tällaisten menetysten tai häiriön suuruuden ja kyseisen poikkeaman toteutumisen todennäköisyyden yhdistelmänä.

Hallintapalvelun tarjoaja

Toimija, joka tarjoaa tieto-ja viestintätekniikan tuotteiden (verkko- ja tietojärjestelmien elementti tai elementtien ryhmä), verkkojen, infrastruktuurin, sovellusten tai muiden viestintäverkkojen ja tietojärjestelmien asentamiseen, hallintaan, käyttöön tai ylläpitoon liittyviä palveluja joko asiakkaan tiloissa tai etäyhteyden välityksellä toteutettavan tuen tai aktiivisen ylläpidon muodossa.

Tietoturvapalveluntarjoaja

Hallintapalvelun tarjoaja, joka toteuttaa kyberturvallisuusriskien hallintatoimia tai antaa tukea niitä varten, esimerkiksi tietoturvallisuuden suunnittelun, ylläpidon ja/tai valvonnan palvelut.

Oppaan laadinnassa mukana olleet asiantuntijaorganisaatiot monipuolisesti kyberturvallisuusalan eri sektoreilta.

Finnish Information
Security Cluster
Kyberala