ICT-Palvelutuotannon varautuminen

– suositukset huoltovarmuus-organisaation yrityksille

Huoltovarmuusorganisaatio
Digipooli

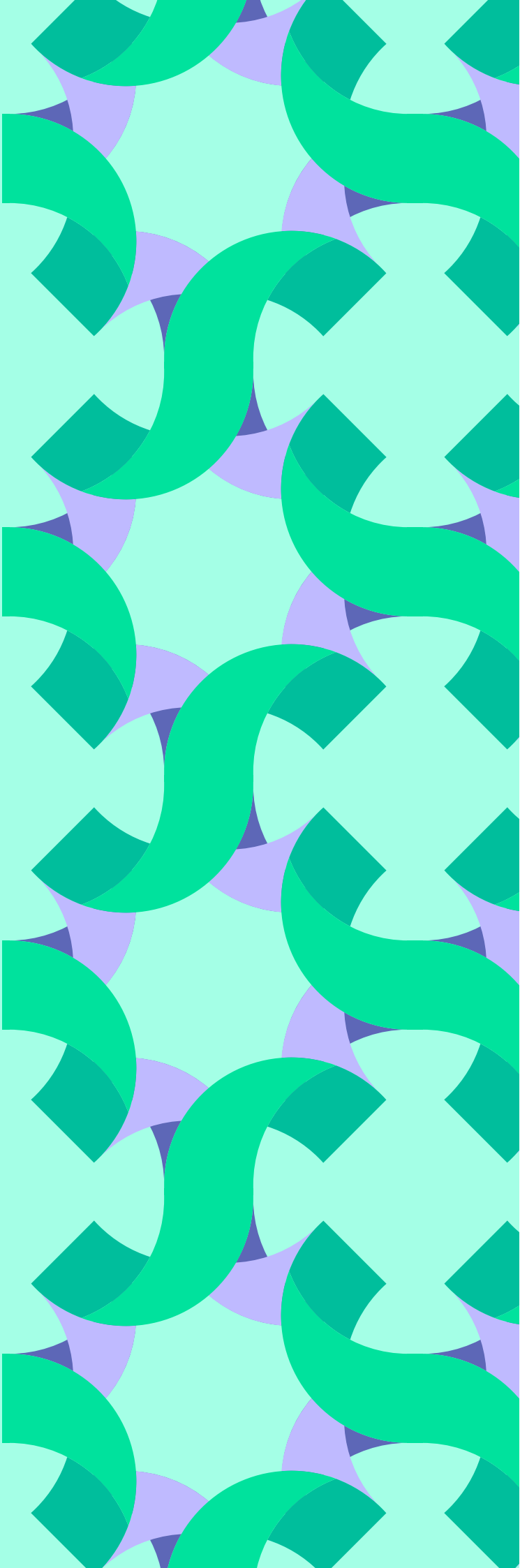
Huoltovarmuusorganisaatio
Digipooli

www.huoltovarmuuskeskus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa. Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Julkaisija:
Huoltovarmuusorganisaatio, Digipooli.
Huoltovarmuusorganisaatio on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus ja sen hallitus, Huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit.

Laatinut: Jatkuvuuskonsultointi Oy
Kansikuva: Freepik
Taitto: Entra Marketing Oy
Julkaisuvuosi: 2024
ISBN: 978-952-7470-37-4



Sisältö

1 Tiivistelmä 4

2 Ohjeen tavoite, sisältö ja kohderyhmä 5

3 Varautumisen valmistelevat tehtävät 6

3.1 ICT-palvelutuotannon varautuminen osana yrityksen varautumista 6
3.2 Varautumisen vaatimusten määrittely 9
3.3 Varautumisen suunnittelu 10
3.4 Toteutustavan valinta 11
3.5 Toimintaympäristön seuranta, uhkakuvat ja riskienhallinta 13
3.6 Päivittäiset ICT-palvelutuotannon prosessit 15
3.7 Varautumisen huomioiminen kaikissa järjestelmän elinkaaren vaiheissa 16
3.8 ICT-infrastruktuuri – suojaaminen ja käytettävyyden varmistaminen 17
3.9 Sovellukset – turvallisuus ja varautuminen 19
3.10 Tietoturvallisuus 21
3.11 Henkilöstö, henkilöstön käytettävyys ja työvoiman saatavuuden varmistaminen 22
3.12 Fyysinen turvallisuus ja kriittinen infrastruktuuri 24
3.13 Tiedon säilyvyyden ja oikeellisuuden varmistaminen 26
3.14 Palautumisen varmistaminen 27
3.15 Palveluntarjoajien ja toimitusketjun varautuminen 28

4 Toiminta vakavassa häiriötilanteessa ja jälkitoimet 31

4.1 Kriisiorganisaatio ja johtamistoiminta 31
4.2 Häiriön tapahtuma-analyysi ja jälkiarviointi 31

5 Varautumisen jatkuva kehittäminen, koulutus ja harjoittelu 32

5.1 Varautumisen organisointi ja kehittäminen 32
5.2 Koulutus ja harjoittelu 34

6 Ulkoiset vaatimukset ICT-palvelutuotannon varautumiselle 36

7 Loppusanat 38

LIITTEET

LIITE 1 Varautuminen ja varautumissuunnitelma 1
LIITE 2 Esimerkki – Liiketoiminnan vaatimusanalyysi (BIA) ja riskiarvio 4
LIITE 3 Järjestelmien ja tiedon luokittelu sekä vaatimusten johtaminen kriittisyysluokittelun kautta 8
LIITE 4 Esimerkki – OT-ympäristön toimintamalli 15
LIITE 5 Varmuuskopiointi ja tiedon muuttumattomuuden varmistaminen 17
LIITE 6 Lokitietojen kerääminen ja käsittely 19
LIITE 7 Esimerkki - Varautuminen ICT-palvelusopimuksessa 20
LIITE 8 Kriisiorganisaatio ja johtamistoiminta 22

1 Tiivistelmä

Varautuminen tarkoittaa toimenpiteitä, joilla pyritään varmistamaan kriittisten toimintojen mahdollisimman häiriötön hoitaminen kaikissa olosuhteissa, niin normaali- kuin poikkeusoloissa. Sen ***lähtökohtia ovat yrityksen tunnistamat yhteiskunnalle ja yritykselle kriittiset palvelut***. Yrityksen tulee tunnistaa ne palvelut ja prosessit, jotka ovat välttämättömiä sekä yrityksen omalle toiminnalle että laajemmin yhteiskunnalle. Näiden toimintojen jatkuvuus on turvattava kaikissa olosuhteissa ja ***ICT-palvelutuotannon varautuminen on siinä olennainen osa***.

Varautuminen on strateginen investointi ja parantaa riskienhallintaa, vähentää taloudellisen tappion riskiä sekä mahdollistaa toiminnan jatkumisen häiriötilanteissa. Lisäksi varautuminen lisää sidosryhmien luottamusta, varmistaa sääntelyvaatimusten noudattamisen ja tuo kilpailuetua toimialan häiriötilanteissa. Varautuminen on myös osa yrityksen yhteiskuntavastuuta, sillä se tukee kriittisten julkisten palveluiden jatkuvuutta ja yhteiskunnan vakautta kriisitilanteissa. (kts. liite 1)

Varautumisen toimenpiteiden on perustuttava kattavaan riskienarviointiin sekä toimintaympäristön ***tilannekuvaan ja sen seurantaan***. On olennaista tunnistaa ja arvioida mahdolliset riskit, jotka voivat vaikuttaa kriittisiin palveluihin ja prosesseihin. Arviointi muodostaa pohjan varautumissuunnitelmalle, jonka avulla voidaan varmistaa toiminnan jatkuvuus kaikissa olosuhteissa. Toimintaympäristön tilannekuvan muuttuminen käynnistää tarvittavat ennakkoon suunnitellut toimenpiteet.

Yritysten koosta riippumatta varautuminen on tärkeää ja varautumisen toimenpiteet voidaan sopeuttaa yrityksen koon sekä tunnistettujen riskien mukaan. Vaiheista tarvittaessa varautumisen suunnittelu ja toteutus:

1. Aloita kaikkein kriittisimmistä palveluista ja niiden tarvitsemista välttämättömistä järjestelmistä ja tiedosta
2. Toteuta ensin vaikutukseltaan suurimmat varotoimet
3. Tee varautumisen kehittämisestä jatkuva prosessi

Keskeiset osa-alueet ICT-palvelutuotannon varautumisessa ovat:

- ***Kriittisten palveluiden tunnistaminen ja niiden vaatimukset:*** Ensimmäinen askel varautumisessa on tunnistaa yrityksen tuottamat kriittiset palvelut ja niille asetetut vaatimukset. Näiden pohjalta johdetaan ICT-palvelutuotannon varautumisen vaatimukset.
- ***Varautumisen vaatimusten ja riskiarvioinnin perusteella toteutettavat varotoimet***
  - ***Henkilöstön ja työvoiman saatavuuden varmistaminen:*** Varmistettava, että tarvittava henkilöstö ja osaaminen ovat riittäviä ja käytettävissä kaikissa olosuhteissa.
  - ***Tiedon käytettävyyden, luottamuksellisuuden ja eheyden varmistaminen:*** Tieto on suojattava, sen käytettävyys ja eheys on taattava kaikissa tilanteissa sekä varmistettava kyky palauttaa tieto häiriötilanteen jälkeen.
  - ***Järjestelmien ja tietoliikenteen suojaaminen*** erityyppisiltä uhilta.
  - ***Tietoturva ja fyysinen turvallisuus:*** Sekä tietoturva että fyysinen turvallisuus on otettava huomioon varautumissuunnitelmissa.
  - ***Toipumisen varmistaminen:*** Nopea toipuminen vakavista häiriöistä on varmistettava varamenettelyin, varmuuskopiointikäytännöillä sekä kattavilla toipumissuunnitelmilla.
  - ***Toimitusketjun ja ulkoisten riippuvuuksien hallinta:*** Varautumisen vaatimukset on ulotettava koko toimitusketjuun ja varmistettava palveluntarjoajien kyky hallita ja toipua vakavista häiriötilanteista.
- ***Kriisiorganisaatio ja sen johtaminen sekä toiminta häiriötilanteessa:*** Kriisitilanteen hallinta edellyttää selkeästi määritellyt roolit ja vastuut sekä ennalta sovitut toimintatavat vakavien häiriötilanteiden hoitamiseksi.
- ***Varautumisen jatkuva kehittäminen:*** Varautumissuunnitelmien jatkuva päivittäminen ja parantaminen varmistaa niiden pysymisen ajantasaisina ja tehokkaina.
- ***Koulutus ja harjoittelu:*** Koulutukset ja harjoitukset varmistavat, että henkilöstö ja yhteistyökumppanit ovat hyvin valmistautuneet, tuntevat sovitut toimintatavat ja suunnitelmat sekä kykenevät vastaamaan erilaisiin häiriötilanteisiin.

2 Ohjeen tavoite, sisältö ja kohderyhmä

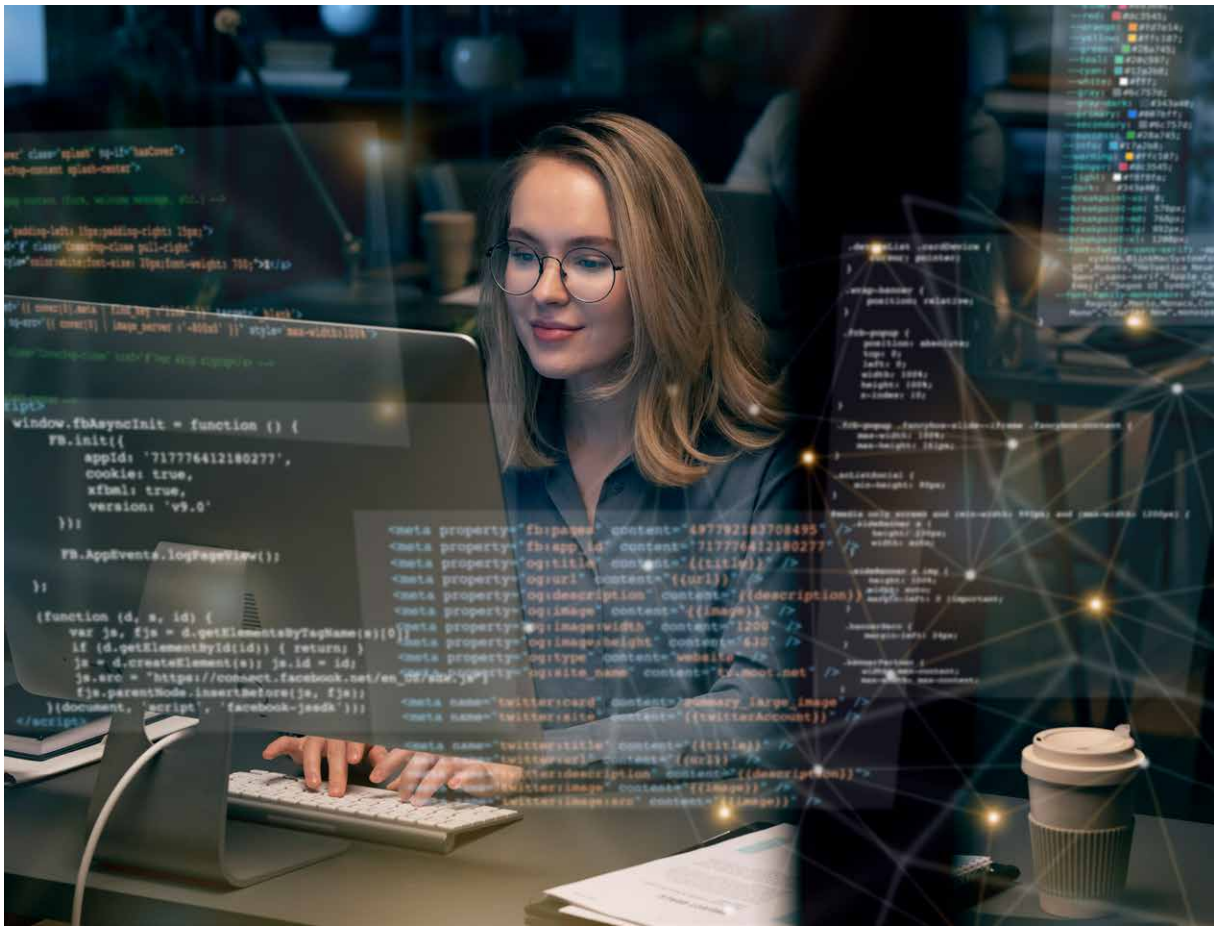
ICT-palvelutuotannon varautuminen on keskeinen osa yrityksen varautumisuunnittelua. Tässä ohjeessa esitetään huoltovarmuuden näkökulmasta ***suosituksia huoltovarmuuskriittisten yrityksen ICT-palvelutuotannon varautumisesta***. Ohjeessa huomioidaan varautuminen niin normaali- kuin poikkeusolojen vakaviin häiriötilanteisiin. Esitetyt suositukset eivät ole velvoittavia.

Varautuminen tarkoittaa toimenpiteitä, joilla pyritään varmistamaan kriittisten toimintojen mahdollisimman häiriötön hoitaminen kaikissa olosuhteissa, niin normaali- kuin poikkeusoloissa. Varautumisen käsitteet on hyvä kerrata liitteestä 1.

Tämä ohje on tehty kaikille huoltovarmuuskriittisille toimialoille ja niillä toimiville yrityksille. Ohje kuvaa varautumisen vaatimukset ja suosituksia mitkä on hyvä sisällyttää palvelutuotannon varautumissuunnitelmiin, mutta ei ota kantaa esimerkiksi teknisiin ratkaisuihin.

Lukujen alussa olevassa tietolaatikossa on aina tiivistetysti, miten huoltovarmuuskriittisten yritysten ICT palvelutuotannossa suositellaan toimittavan tai mitä huomioitavan. Ohjeessa ei ole käsitelty sektoriviranomaisten ja lainsäädännön asettamia toimialakohtaisia vaatimuksia toiminnan häiriöttömyydelle ja varautumiselle muuten kuin esimerkinomaisesti.

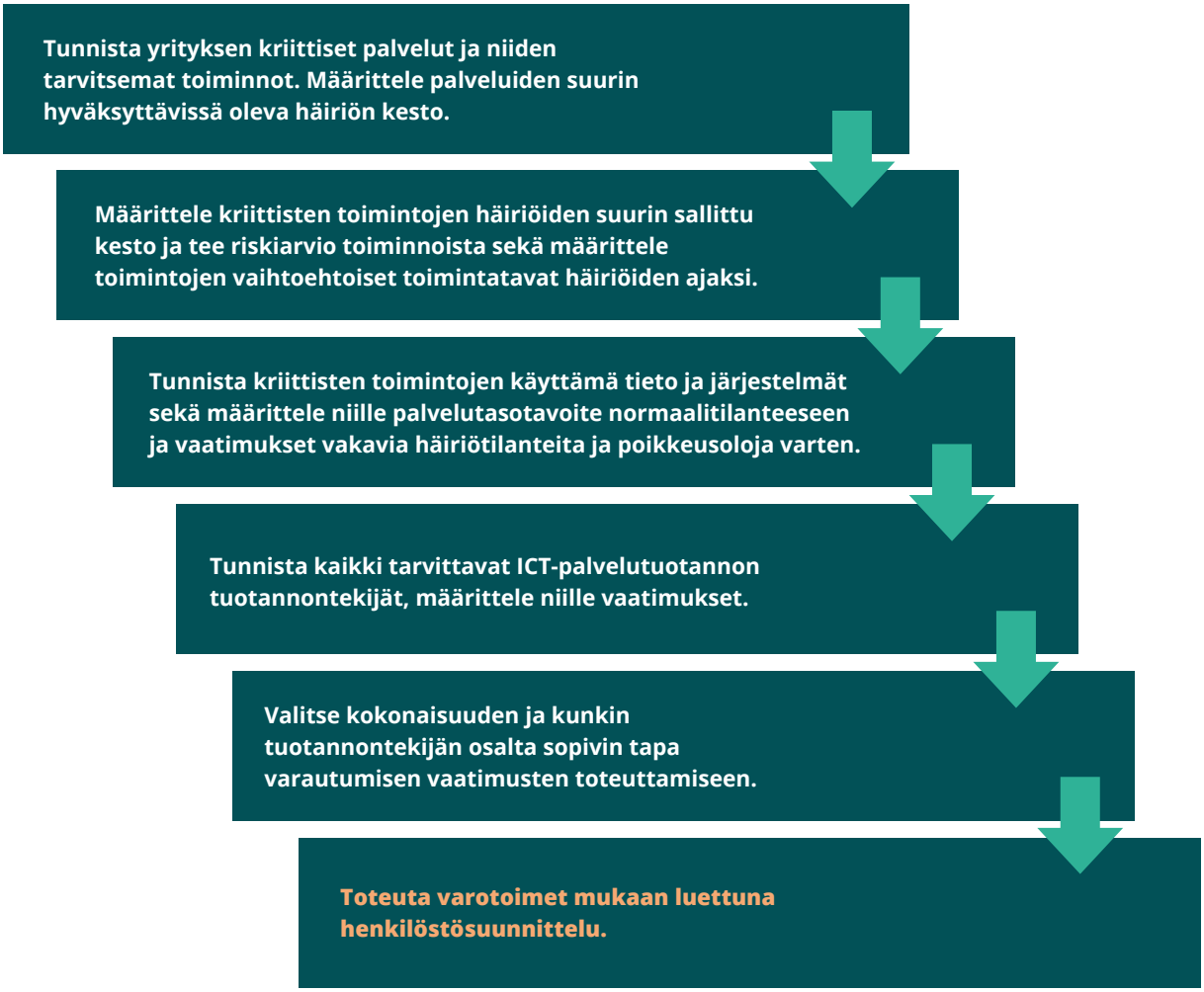
Ohje on suunnattu erityisesti huoltovarmuuskriittisten yrityksen ICT-palvelutuotantoa johtaville ja siitä vastaaville, joiden on osattava asettaa vaatimukset ja valvoa ICT-varautumista. Toinen kohderyhmä ovat palveluntarjoajat, joiden asiakkaiden on määriteltävä varautumisen vaatimukset. Palveluntarjoajien tulee tarvittaessa ottaa vaatimusten määrittely esille asiakkaiden kanssa sekä ymmärtää ja huomioida asiakkaidensa varautumisvaatimukset osana omaa palvelutuotantoaan.



3 Varautumisen valmistelevat tehtävät

3.1 ICT-palvelutuotannon varautuminen osana yrityksen varautumista

ICT-palvelutuotannon varautumisen edellytyksenä on yrityksen yhteiskunnalle tuottaminen kriittisten palveluiden tunnistaminen sekä niiden tuottamiseen tarvittavien elintärkeiden toimintojen, järjestelmien ja tiedon tunnistaminen. ICT-palvelutuotannon varautuminen on kiinteä osa yrityksen varautumista kokonaisuutena ja ICT-palvelutuotannon varautumisen vaatimukset johdetaan yrityksen kriittisistä palveluista kuvan 1 mukaisesti. ***Aloita varautumisen suunnittelu ja toteuttaminen kaikkein kriittisimmistä palveluista ja riskialttiimmista tuotannontekijöistä.*** Laajenna vähitellen suunnitelmat ja varotoimet kattamaan kaikki keskeiset palvelut.



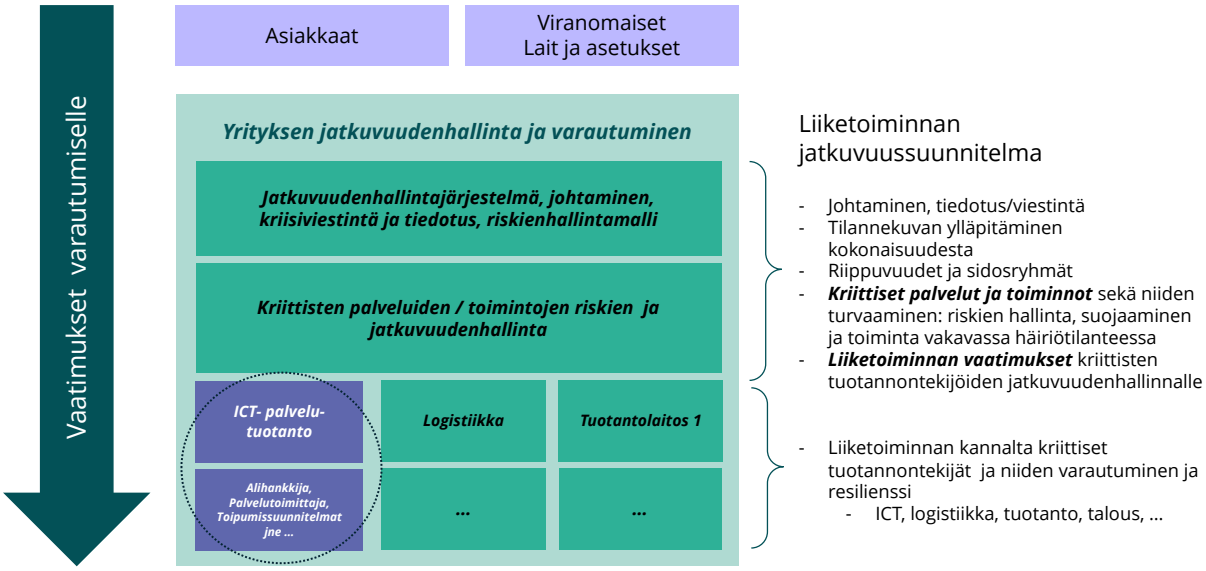
Kuva 1 ICT-palvelutuotannon vaatimusten johtaminen yritystason vaatimuksista

ICT-palvelutuotannon varautuminen:

- ***Tunnista ja kuvaa*** yritykselle ja yhteiskunnan kannalta ***kriittiset yrityksen tuottamat palvelut*** sekä niiden vaatimat kriittiset ***priorisoidut toiminnot*** ja ***tuotannontekijät***.
- ***Vaiheista tarvittaessa suunnittelu ja toteutus, aloita kaikkein kriittisimmistä palveluista ja riskialttiimmista tuotannontekijöistä.*** Laajenna vähitellen kattamaan yrityksen kaikki yhteiskunnalle tärkeät toiminnot.
- ***Varmista, että eri osapuolten varautumissuunnitelmat ovat yhdenmukaiset***, yhteensopivat ja kattavat.

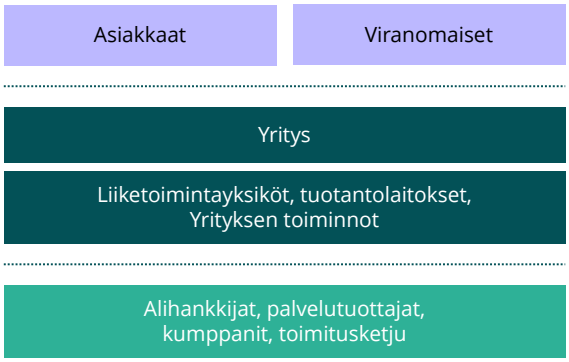
Yrityksen ylin johto määrittelee varautumisen strategiset tavoitteet, varmistaa riskienhallinnan ja varautumisen riittävät toimintamallit. Johdolle myös raportoidaan säännöllisesti varautumisen tilanne ja kehitys.

Varautumisen perustana ovat ***yrityksen ja liiketoiminnan suunnitelmat***, jotka pohjautuvat ***tunnistettuihin kriittisiin palveluihin j***a ajantasaiseen, ***uhkamallit*** huomioivaan ***riskien arviointiin*** erityisesti kriittisten palveluiden osalta. Niitä täydentää ICT-palvelutuotannon suunnitelma, joka kattaa palvelutuotannon kannalta hallinnolliset, toiminnalliset ja tekniset toimenpiteet, joilla varmistetaan tiedon saatavuus, eheys ja luottamuksellisuus sekä palveluiden mahdollisimman häiriötön toiminta ja tavoitteiden mukainen toipuminen. Lisäksi varautumisessa tulee tunnistaa asiakkaan ja oman toimialaan kohdistuvat viranomaisten vaatimukset ja velvoitteet (kts. luku 6).



Kuva 2 ICT-palvelutuotannon varautumien osana yrityksen varautumista

Yrityksen tulee tunnistaa niin oman toiminnan jatkuvuudelle kuin huoltovarmuudelle kriittiset palvelunsa sekä arvioida suurin sallittu haitta näille häiriötilanteissa. Yritystasolla määritellään koko organisaatiota koskevat varautumiskäytännöt ja toimintamallit, joilla varmistetaan kokonaisvaltainen varautuminen ja tehokas toiminta kriisien aikana. Yrityksen, palveluntuottajien (kuten ICT-palveluntuottajien), viranomaisten ja mahdollisten asiakkaiden ***varautumis- ja toipumissuunnitelmien yhteensopivuus, yhdenmukaisuus ja kattavuus on varmistettava kokonaisuutena*** (kts. liite 1).



Kuva 3 Yhteensovitettavat varautumissuunnitelmat

Kriittisten palveluiden tunnistaminen

Varautuminen perustuu kriittisten palveluiden tunnistamiseen:

- ***HVO yritykset määrittelevät liiketoiminnan jatkuvuuden ja yhteiskunnan huoltovarmuuden kannalta kriittiset palvelunsa, niiden tarvitsemat toiminnot sekä näille varautumisen vaatimukset.***
- Tunnistettujen kriittisten palveluiden ja liiketoiminnan niille asettamien vaatimusten perustella ICT-palvelutuotanto suunnittelee ja toteuttaa päivittäisen palvelutuotannon ja varautumisen niin normaaliolojen pieniin kuin vakaviin häiriöihin sekä poikkeusoloihin. Huomioi tavoitteita asetettaessa ***häiriön kesto ja sekä yksittäistä järjestelmää että laajat, useita järjestelmiä tai tietovarantoja koskevat häiriöt.***
- ICT-palvelutuotannon sopimusten tulee vastata toiminnon kriittisyyttä ja kriittisyyden vaatimat varautumisen vaatimukset on oltava vaadittavalla tasolla sopimuksia tehdessä.

Yrityksen ja liiketoimintojen on tunnistettava tuottamansa palvelut, jotka yrityksen jatkuvuuden ja erityisesti yhteiskunnan kannalta kriittisiä. Näiden palveluiden osalta on ymmärrettävä eri häiriötilanteiden vaikutukset palveluiden tuottamiseen ja sitä kautta yrityksen ja yhteiskunnan toimintaan sekä määriteltävä tavoitteet palvelujen tuottamiselle ja varautumiselle niin normaali- kuin poikkeusoloissa.

Yrityksen johto vastaa, että yhteiskunnan ja yrityksen jatkuvuuden kannalta kriittiset palvelut tunnistaan. Liiketoiminnalla on paras käsitys mitkä toiminnot, tiedot ja järjestelmät ovat toiminnan kannalta kriittisiä. Liiketoiminta vastaa siitä, että se tunnistaa ja ymmärtää tarvitsemiensa toimintojen, tietojen ja järjestelmien häiriötilanteiden vaikutukset sen kyvylle toimia ja tuottaa myös yhteiskunnalle kriittisiä palveluita. ICT-palvelutuotanto tukee ja auttaa näiden tunnistamisessa ja vaatimusten määrittelyssä. Kriittisten palveluiden ja toimintojen tunnistaminen sekä vaatimusten määrittelyprosessi on tärkeää toteuttaa tiiviissä yhteistyössä liiketoiminnan ja ICT-palvelutuotannon välillä. ICT-palvelutuotanto ymmärtää järjestelmien, tietoverkkojen ja datan keskinäisriippuvuudet sekä tekniset haasteet, jotka voivat vaikuttaa palveluiden jatkuvuuteen sekä varautumisstrategian valintaan.

Esimerkiksi ***liiketoiminnan vaikutusanalyysi*** (BIA Business Impact Analysis) auttaa arvioimaan erilaisten keskeytysten vaikutuksia (kts. liite 2).

Kyberturvallisuuslain perusteluissa todetaan, että yrityksen tulee toteuttaa turvallisuus- ja riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja ***riittäviä suhteessa riskeihin sekä viestintäverkon tai tietojärjestelmän merkitykselle*** toimijan toiminnan ja palveluntarjonnan kannalta huomioiden yhteiskunnalliset ja taloudelliset vaikutukset.

3.2 Varautumisen vaatimusten määrittely

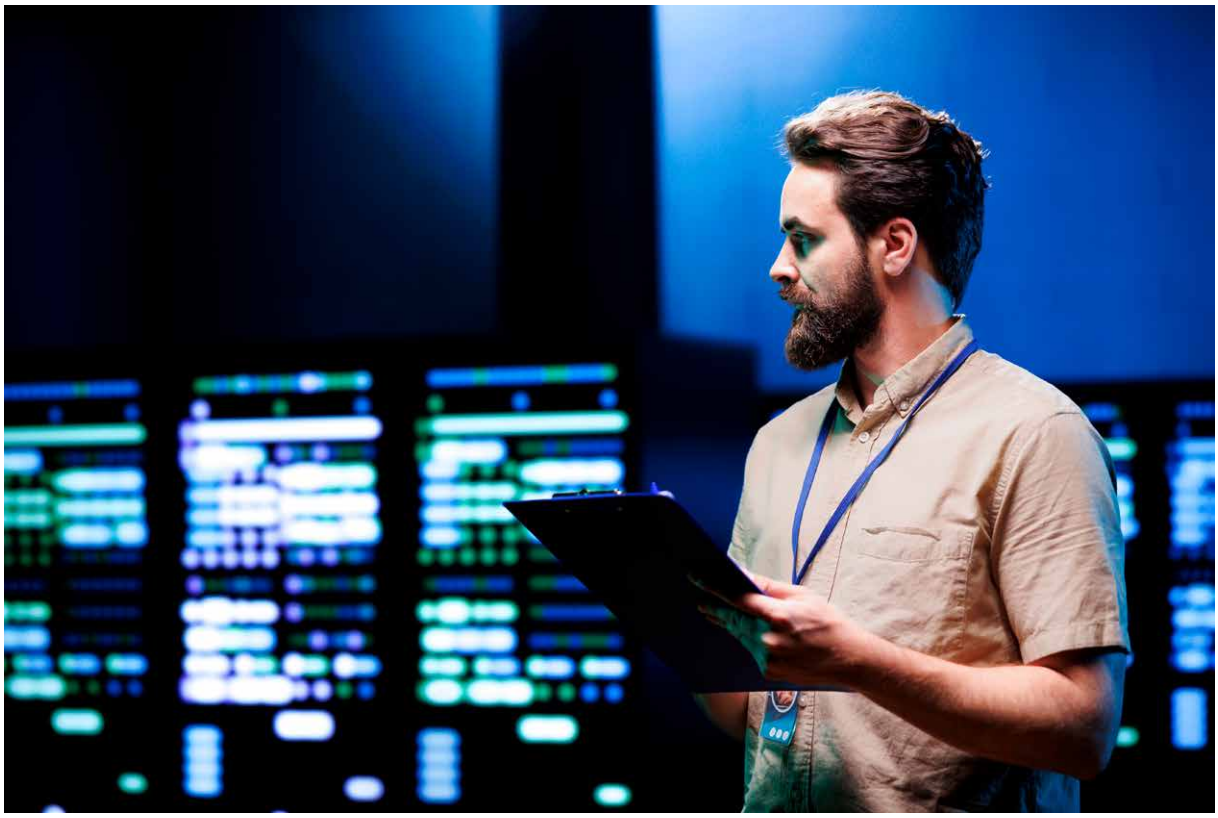
Aloita kaikkein kriittisimmistä järjestelmistä ja tiedosta!

- ***Määrittele*** kriittisille palveluille ja edelleen järjestelmille liiketoiminnan vaatimusten perustella ***vaatimukset käytettävyydelle ja toipumiselle***.
- ***Priorisoi*** järjestelmät ja tieto.
- ***Muista vaihtoehtoiset toimintatavat ja varajärjestelmät.***

Kriittisille palveluille ja niiden perusteella ICT-palvelutuotannolle määriteltävät vaatimukset ohjaavat varautumisen toimenpiteiden toteutusta. Määriteltäviä vaatimuksia ovat esimerkiksi

- ***Palvelutasotavoitteet (SLA)***, joihin päivittäisessä toiminnassa tulee päästä. Palvelutasotavoitteita ovat mm. käytettävyys, pisin sallittu katko ja palveluaika.
- Vakavia häiriöitä varten ***suurin hyväksyttävissä oleva häiriön kesto palvelussa***, mitä ei saa ylittää vaarantamatta yrityksen tai yhteiskunnan toimintaa (MTO – Maximum Tolerable Outage) eli aikaraja, johon mennessä järjestelmät on oltava toiminnassa ja data palautettu toiminnan vaatimalle tasolle.
- ***Tiedon*** luottamuksellisuuden, saatavuuden ja kriittisyyden taso sekä eheysvaatimukset.
- Kriittisen palvelun ***alhaisin hyväksyttävä palvelutaso häiriön aikana*** (MBCO – Minimum Business Continuity Objetive) sekä ja liiketoiminnan vaihtoehtoiset toimintatavat
- Mahdolliset poikkeavat ***vaatimukset poikkeusoloja varten***.

Liitteessä 3 on esimerkki kriittisten palveluiden ja niiden vaatimien toimintojen luokittelusta näiden palveluiden varautumisvaatimusten määrittelystä sekä niistä johdetuista ICT-palveluiden varautumisvaatimuksista.



3.3 Varautumisen suunnittelu

Suunnittele varautuminen liiketoiinnan priorisoinnin perusteella:

- Johda suojaustarve ja varautumistoimet liiketoiminnan tekemän kriittisyysluokittelun ja vaatimusten pohjalta.
- Määrittele kriittisten palveluiden ja toimintojen tarvitsemat ***ICT-palvelutuotannon tuotannontekijät***, luokittelee ne kriittisyyden mukaan.
- Määrittele kriittisille tuotannontekijöille vaatimukset normaalille käytettävyydelle ja vikasietoisuudelle sekä vakavista häiriöstä toipumiselle (RTO, RPO).
- Määrittele toipumissuunnitelmaa varten ***tärkeysjärjestys järjestelmille, alustoille ja ympäristöille huomioiden sekä tekniset että toiminnalliset riippuvuudet ja liiketoiminnan vaatimukset***.
- Priorisoi ICT-palvelutuotannon tehtävät: mitä voidaan jättää vakavassa häiriötilanteessa tekemättä?
- Tunnista ICT-palvelutuotantoon ja sen kriittisiin tuotannon tekijöihin liittyvät riskit sekä määrittele riskienhallintakeinot.
- Tee vaatimusten perusteella varautumissuunnittelu ja toipumissuunnittelu sekä toteuta tarvittavat toimenpiteet.

ICT-palvelutuotanto suunnittelee ja mitoittaa tarvittavat toimenpiteet tuotannontekijöilleen liiketoiminnan priorisoinnin mukaisesti. ICT-palvelutuotannon tuotannontekijöitä ovat mm.

- Järjestelmät ja niiden tarvitsemat ympäristöt (mm. tieto, ohjelmistot, tekniset alustat ja laitteet sekä pilvipalvelut, varusohjelmistot ja hallinta-ohjelmistot, tietoliikenneyhteydet ml. laitteet sekä tietoliikennekaapelit, loki-, tiedonhallinta- ja varmistusohjelmistot)
- Henkilöstö ja osaaminen
- Tilat kuten toimistotilat, konesalit ja muut laitetilat
- Pilvipalvelut
- ICT-palveluntarjoajat
- Laitetoimittajat
- Palvelutuotannon prosessit ja hallintamallit

ICT-palvelutuotannon vaikutusanalyysissä on huomioitava kaikki tarvittavat tuotannontekijät sekä näiden väliset riippuvuudet. Lisäksi arvioidaan riskit ja uhat, jotka voivat vaikuttaa tunnistettuihin tuotannontekijöihin, sekä valitaan toteutustapa kunkin järjestelmän ja tuotannontekijän varautumisen toteuttamiseksi. Vaikutusanalyysin perustella määritellään tuotannontekijöille varautumisen vaatimukset kuten

- ***Palautuspistetavoitteen*** (RPO – Recovery Point Objective), joka määrittelee maksimiajan, jonka ajalta tietoa voidaan menettää vakavissa häiriötilanteissa. Lisäksi määriteltävä tarvittava aika ja tapa mahdollisille manuaalisille tehtäville datan saamiseksi toiminnan jatkumisen vaatimalle tasolle.
- Järjestelmille ja muille tuotannontekijöille ***toipumisaikatavoitteet*** (RTO – Recovery Time Objective), jossa huomioitu MTO ja RPO sekä mahdollisen manuaalisen työn vaatima aika (MTO > RTO + käsityön vaatima aika)

Järjestelmien ja tiedon vaatimukset määräävät pitkälti varmistavien muiden tuotannontekijöiden kriittisyyden. Myös järjestelmien keskinäinen priorisointi liiketoiminnan kannalta on huomioitava: mitkä järjestelmät tulee laajoissa häiriöissä palauttaa ensimmäisenä? Arvioinnissa on huomioitava sekä yksittäisten järjestelmien että useiden järjestelmien yhtäaikaisten häiriöiden laajemmat vaikutukset. Vaatimusten oikeaan mitoittamiseen on kiinnitettävä huomioita, sillä ne vaikuttavat sekä häiriönsietokykyyn että varautumisen kustannuksiin.

Järjestelmien ja tiedon luokittelu

Järjestelmien ja tiedon luokittelu niitä käyttävien toimintojen kriittisyyden perustella helpottaa vaatimusten määrittelyä ja luo yhteisen kielen liiketoiminnan ja ICT-palvelutuotannon välille. Tiedon luokittelussa huomioitava tiedon arvo ja tiedon hyödyntäminen muussa kuin alkuperäisessä tarkoituksessa. Esimerkiksi vähäarvoisena pidettävä järjestelmän, prosessin tai toiminnon ohjaamiseen ja prosessin toiminnasta kertyvä tieto voi olla arvokasta tarkemmin analysoituna toiminnan kehittämisessä, jolloin suojaustarve kasvaa.

Luokittelun pohjalta voidaan toteuttaa tehokkaasti kunkin luokan vaatimusten mukainen varautuminen ja suojaus. Luokittelu perustuu liiketoiminnan vaikutusanalyysissä tunnistettujen elintärkeiden palveluiden ja niiden vaatimien toimintojen kriittisyyteen.

Luokittelun ***tarkoituksena on auttaa määrittämään järjestelmät ja tieto, joihin suojaustoimet on ensisijaisesti kohdistettava***. Lisää luokittelusta esimerkkeineen on liitteessä 3.

3.4 Toteutustavan valinta

Huomioi ICT-palvelutuotannon varautumisen toteutustapoja valittaessa:

- ***Tarkastele kokonaisuutta*** yhdessä liiketoiminnan kanssa ja valitse kokonaisuuden kannalta sopivin vaihtoehto huomioiden:
  - ***Liiketoiminnan vaatimukset ja vaihtoehtoiset toimintatavat***
  - ***Kustannukset***
  - ***Osaaminen ja resurssit***
  - ***Erilaiset tekniset ratkaisut***
- ***Huomioi*** kaikki eri palvelutuotannon vaihtoehtoiset keinot, liiketoiminnan kyky toimia tilapäisesti vaihtoehtoisella tavalla, varajärjestelmät, järjestelmäkehitys, arkkitehtuurimuutokset jne.
- ***Varmista*** toteutustavan vaatimien ***resurssien ja osaamisen saatavuus*** kaikissa tilanteissa.
- Varmista, että vaatimukset ovat ***oikeansuhtaisia ja ovat linjassa toiminnalle ja palvelulle asetettuihin vaatimuksiin*** sekä niiden toimintaan häiriötilanteessa.
- Varmista, että vaatimukset kattavat riittävän laajasti riskit huomioiden vakavat häiriötilanteet ja poikkeusolot.

ICT-palvelutuotanto valitsee sopivimman tavan vaatimusten täyttämiseksi. Valinta voi olla iteratiivinen prosessi, jonka onnistunut läpivienti edellyttää tiivistä yhteistyötä liiketoiminnan kanssa. Valinnan yhteydessä tulee tarkastella sekä ICT-palvelutuotannon että liiketoiminnan toimenpiteet kuten vaihtoehtoiset toimintamallit sekä mahdolliset varajärjestelmät. Valittava toteutustapa vaikuttaa riskien todennäköisyyteen ja vaikutuksiin sekä varautumisen kustannuksiin. Tavoitteena on löytää kustannustehokas ratkaisu, joka takaa yrityksen kriittisten palvelujen toiminnan hyväksytyllä riskitasolla. Sopivin ratkaisu saattaa vaatia esimerkiksi muutoksia liiketoiminnan prosesseissa, varajärjestelmien käyttöönottoa tai arkkitehtuurimuutoksia.

ICT-palvelutuotannolle asetetut vaatimukset tulee olla riittävät ja kaikki vakavat riskit huomioivia, mutta samalla suhteutettu liiketoiminnan mahdollisuuteen toimia riskien toteutuessa.

Esimerkki. Kriittinen palvelu tarvitsee toimiakseen kolme eri järjestelmää, jotka toimivat samassa omassa laitetilassa olevassa teknisessä ympäristössä. Kaikkien kolmen järjestelmän yhtäaikainen häiriö keskeyttää palvelun välittömästi ja häiriön suurin hyväksyttävissä oleva kesto on kolme tuntia. Mikäli häiriö koskee kahta järjestelmää, palvelua pystytään varamenettelyin tuottamaan niin, että häiriön suurin hyväksyttävä kesto on 2 päivää. Vastaavasti yhden järjestelmän häiriön suurin hyväksyttävissä oleva kesto on 5 päivää. Vaihtoehtoisia lähestymistapoja ovat esimerkiksi:

- Järjestelmät pidetään samalla alustalla ja ympäristössä, varmistetaan että järjestelmien ja ympäristön RTO on aina alle 3 h.
- Järjestelmä pidetään edelleen samalla alustalla, mutta nopea toipuminen ja korkea käytettävyys varmistetaan mm. kahdentamisella ja maantieteellisellä hajautuksella sekä automatiikalla. Järjestelmän käytön estävän todennäköisyys pienenee merkittävästi.
- Hajautetaan järjestelmät eri alustoille, esimerkiksi yksi edelleen on omassa laitetilassa ja kaksi muuta siirretään eri pilvialustoille. Todennäköisyys kahden tai kolmen järjestelmän samanaikaiselle häiriölle pienenee merkittävästi.
- Liiketoiminta ottaa yhdelle tai useammalle järjestelmistä varajärjestelmän tai kehittää vaihtoehtoisen toimintatavan häiriötilanteita varten, jolloin sekä yksittäisten että kaikkia kolmea järjestelmää koskevan häiriön vaikutus pienenee ja järjestelmiin kohdistuvat vaatimukset voidaan arvioida uudelleen.

Esimerkki. Yrityksellä on useita tuotantolaitoksia ja yksi toimipiste. Yritys on rakentanut arkkitehtuurin Citrix-alustalle niin tuotannon kuin toimistotyön osalta: kaikki toiminta edellyttää yhteyttä Citrix-alustaan ja yhteys sallittu ainoastaan yrityksen verkosta. Häiriö Cirtirx:in käytössä keskeyttää tuotannon alle tunnissa ja toimistotyön välittömästi. Citrix-ympäristö on rakennettu vikasietoiseksi, mutta yritysverkkoa tai muita tietoliikenneyhteyksiä ei ole varmennettu tai kahdennettu. Vaihtoehtoisia lähestymistapoja häiriön sietokyvyn lisäämiseksi ovat esimerkiksi:

- Tietoliikenne ja yhteys palveluun varmennetaan yritysverkkoa kehittämällä ja kahdentamalla komponentit sekä käyttämällä useamman operaattorin yhteyksiä, jolloin järjestelmän käytön estävän tietoliikennehäiriön todennäköisyys pienenee.
- Mahdollistetaan yhteys Citrix-palveluun yritysverkon ulkopuolelta ja otetaan käyttöön yritysverkon ulkopuoliset varayhteydet jokaiselle toimipisteelle/tuotantolaitokselle.
- Luodaan vaihtoehtoiset toimintatavat tai varajärjestelmä, joiden avulla voidaan toimia hyväksyttävissä olevalla tasolla tilapäisesti häiriön aikana.

Esimerkki. Yrityksen tuotantolaitos toimii 24/7. Tuotanto keskeytyy, mikäli sitä tuotantolaitoksella sijaitsevassa tuotantoa ohjaavassa järjestelmässä (OT-järjestelmä) on yli 30 minuutin katkos, mikä on samalla suurin sallittu katkos järjestelmän käytettävyydessä. Tuotantolaitoksen sähkönsaanti on varmistettu kahdella erillisellä voimajohdolla, jota tulevat samalta sähköasemalta. Käytettävissä oleva varavoima riittää tuotannon hallittuun alasajoon. Mikäli tuotantolaitoksen sähkönsaanti katkeaa (esim. sähköaseman vaurioituessa), niin tuotanto keskeytyy eikä myöskään OT-järjestelmää tarvita. Vaikka muuten järjestelmän käytettävyysvaatimus on korkea, niin riittää että UPS/varavoima kestää vain järjestelmän hallitun alasajon vaatiman ajan, jotta laitoksen sähköjen palauduttua järjestelmä käynnistyy ongelmitta.

3.5 Toimintaympäristön seuranta, uhkakuvat ja riskienhallinta

Toimintaympäristön ja uhkien seuranta sekä tilannekuva

Seuraa toimintaympäristöä jatkuvasti:

- Suunnittele ICT-organisaation ***tilannekuvan muodostaminen***.
- ***Määrittele*** tilannekuvan muodostamisessa ***käytettävät tietolähteet.***
- Kerää ja analysoi organisaation hiljaiset signaalit.
- ***Hyödynnä oman toimialan tiedonvaihtoryhmiä*** ja tilannetietoa jakavia organisaatioita ja välitä heille omat havaintosi.
- ***Ylläpidä tilannekuvaa jatkuvasti.***

Varautumisessa korostuu ***häiriöiden ennakointi***, joka perustuu eritasoisten signaalien tunnistamiseen. Tärkeätä on havaita toimintaympäristön näkyvät muutokset, uudet ja muuttuvat uhat sekä arvioida näistä johtuvat riskien toteutumisen todennäköisyyden ja vaikutusten muutokset. Heikkojen signaalien ja ensioireiden havaitseminen on keskeistä, sillä ne voivat ennakoida merkittäviä muutoksia tai häiriöitä. Organisaation hiljainen, kokemuksen kautta kertynyt epävirallinen tieto, auttaa heikkojen signaalien tunnistamisessa.

Toimintaympäristön seuranta ja tilannekuvan ylläpitäminen ovat osa organisaation johtamisjärjestelmää. Seurannan tulee kattaa kaikki keskeiset toiminnot ja erityyppiset uhat. Ennakointia toteutetaan organisaation eri osissa ja tiedon tehokas jakaminen sekä organisaation sisällä että yhteistyökumppaneiden välillä edistää häiriöiden ennaltaehkäisyä, madaltaa reagointikynnystä ja nopeuttaa toimintaa häiriötilanteissa. ***Selvitä, mistä tietoa kannattaa kerätä*** ja kuinka usein sekä mistä tietolähteistä kriisitilanteessa saa lisätietoa tai apua tilannekuvan muodostamiseen. ***Määrittele eri osastojen tilannekuvatietotarpeet ja määritelle miten niistä muodostetaan ICT-palvelutuotannon ja sen johdon tilannekuva sekä miten ICT-palvelutuotannon tilannekuva välitetään edelleen yrityksen johdolle yrityksen tilannekuvan muodostamista varten.***

Hyödynnä seurannassa toimialan vakiintuneita yhteistoimintarakenteita ja -ryhmiä (kuten toimialan ISAC-tiedonvaihtoryhmiä[1], jotka ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä sekä Huoltovarmuusorganisaation pooleja[2]), tilannetietoa jakavia organisaatioita (mm. Kyberturvallisuuskeskus) sekä tilaisuuksia ja arvioi mahdollisia päällekkäisyyksiä tiedon keruussa ja analysoinnissa, jotta varmistetaan tehokkuus ja tarkkuus. ***Huoltovarmuusorganisaatioon kuuluvien yritysten odotetaan hakeutuvan mainittuihin tiedonvaihtoryhmiin ja aktiivisesti kehittävän tilannekuvaansa oman varautumisen ja huoltovarmuuden takaamiseksi.***

Vastaavasti välitä matalalla kynnyksellä omat havainnot eteenpäin toimialan ja turvallisuuden yhteistyöryhmille, jotta on mahdollista ylläpitää laajempaa koko yhteiskuntaa koskevaa tilannekuvaa.

Tietoturvallisuuden hallinnassa on hyvä huomioida ***ajantasaisen kyberuhkatiedon hyödyntäminen suojautumiseen ja varautumiseen***. Kyberuhkatieto (cyber threat intelligence) auttaa organisaatioita tunnistamaan ja ymmärtämään tietoturvauhkia. Se sisältää analysoitua tietoa kyberuhista, kuten hyökkäystavoista, uhkatoimijoista ja haavoittuvuuksista ja tietoa hyödynnetään suojaustoimenpiteiden suunnittelussa ja uhkien torjunnassa. Kyberuhkatiedon perusteella ylläpidetään tietoturvallisuuden tilannekuvaa mahdollisimman ajantasaisesti ja tarvittaessa tilannekuvan muuttuessa nostetaan valmiustasoa ja varaudutaan uhkien toteutumiseen.

Nykyisin ei enää riitä yksittäisen turvajärjestelmien tietosyötteet tai listaukset mistä voi hakea uhkatietoa tarvittaessa, vaan kyberriskein hallintaan tarvitaan jatkuvaa tietoa vähintään sekä Suomeen että yrityksen toimialaan liittyen. Kyberuhka- ja haavoittuvuustietoja keräävät, tuottavat ja jakavat esimerkiksi Kyberturvallisuuskeskuksen CERT-FI[3] ja kansainväliset CERT-organisaatiot, EU:n tietoturvaorganisaatio ENISA[4] (European Union Agency for Cybersecurity) sekä tietoturvayhtiöt ja palveluntarjoajat.

1 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

2 https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/sektorit-ja-poolit

3 https://www.kyberturvallisuuskeskus.fi/fi/varoitukset-ja-ilmoitukset

4 https://www.enisa.europa.eu

Riskienhallinta

Tarkastele kriittisten palveluiden ICT:n tuotannontekijöihin liittyvät riskit kattavasti:

- ***Laadi*** korkean riskiarvion saaneille riskeille ***hallintakeinot*** todennäköisyyden ja/tai vaikutuksen pienentämiseksi.
- ***Huomioi varautumissuunnitelmassa kaikki riskit, joilla on merkittävä vaikutus kriittisiin toimintoihin***, vaikka niiden todennäköisyys olisi pieni.
- Muista kaikki vaaratekijät huomioiva lähestymistapa.
- Huomioi riippuvuudet ja mahdolliset keskittymäriskit.
- Huomioi riskit sekä ”ylä-” että ”alavirtaan” toimitusketjussa.

Varautumisen suunnittelu perustuu vaatimusten lisäksi säännöllisesti tehtävään riskiarvioon. *Riskienhallintamalli ja toimintatavat määritellään yritystasolla, ja niiden toteutumista seurataan johdonmukaisesti.* ***Varautumisen riskienhallinnassa*** keskitytään erityisesti kriittisiin toimintoihin liittyviin vakaviin uhkiin ja riskeihin, kun taas yleinen riskienhallinta kattaa laajemmin erilaisia ja eritasoisia riskejä organisaation toiminnassa. ***ICT-palvelutuotannon varautumiseen liittyvä riskiarvio*** *kohdistetaan tunnistettuihin kriittisiin tuotannontekijöihin. Riskien arvioinnissa kannattaa käyttää yrityksesi käytössä olevaa riskienarviointimenetelmää ja -kriteeristöä yhdenmukaisuuden varmistamiseksi.*

Varautumisen riskiarvioinnissa huomioidaan tavanomaisten ICT-palvelutuotantoa koskevien riskien lisäksi laajasti erilaiset mahdolliset uhkatekijät, olivat ne luonnollisia, ihmisten aiheuttamia, teknologisia tai sosiaalisia. Huomioitavia uhkia ovat mm.

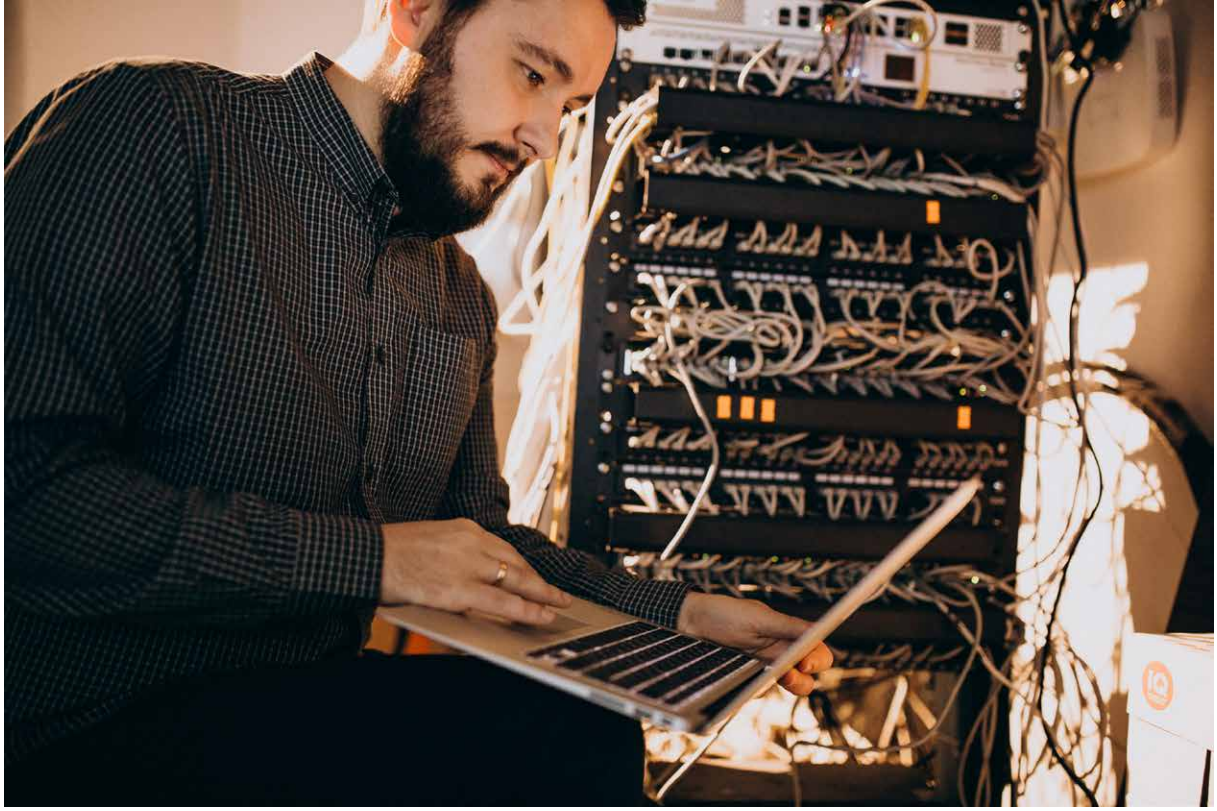
- Toimittajiin ja palvelutuottajiin liittyvät riskit
- Teknologiariskit ja tekniset häiriöt
- Inhimilliset virheet ja väärinkäytökset
- Henkilöstöön ja työvoiman saatavuuteen liittyvät uhkat
- Kriittisen infrastruktuurin vakavat ja mahdollisesti pitkäkestoiset tai toistuvat häiriöt (kuten energian ja veden jakelu, liikenne ja logistiikka, polttoaineiden saatavuus)
- Erilaiset kyberhäiriöt ml. laajat ja vakavat kyberhäiriöt
- Pandemiat ja terveysuhkat
- Suuronnettomuudet
- Toimitusketjujen katkokset, vakavat häiriöt kansainvälisessä logistiikassa
- Luonnonkatastrofit
- Sosiaaliset kriisit ja lakot sekä levottomuudet
- Sabotaasit ja fyysiseen turvallisuuteen liittyvät uhkat
- Poliittiset ja geopoliittiset uhkat

Varautumisen kannalta on huomioitava myös ne vaikutukseltaan vakavat riskit, joiden todennäköisyys on pieni. Lisää riskien hallinnasta on liitteessä 1.

Lisätietoa riskienhallinnasta mm. ISO 31000:2018 Risk Management Guidelines -standardista, joka tarjoaa ohjeita ja käytäntöjä yrityksen riskienhallintaan.

Esimerkiksi Kyberturvallisuuslaki (HE 57/2024) edellyttää, että yrityksen on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu organisaation kriittisissä toiminnoissa tai palveluntarjonnassa käytettäviin tietojärjestelmiin ja viestiverkkoihin. Riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan ja toiminnan jatkuvuuteen. Riskienhallinnassa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit kaikki vaaratekijät huomioivan lähestymistavan mukaisesti. Lain perusteluiden mukaan vaikutuksia arvioitava erityisesti yhteiskunnalle merkityksellisten toimintojen näkökulmasta ja huomioitava häiriön vaikutukset myös niille, jotka käyttävät tai ovat riippuvaisia toimijan palveluista.

Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta edellyttää, että kriittisen toimijan riskiarvioinnissa on otettava huomioon kaikki merkitykselliset riskit, jotka voivat johtaa poikkeamaan. Arviossa huomioidaan mm. toimialojen tai rajat ylittävät riskit, onnettomuudet, luonnonkatastrofit, kansanterveydelliset hätätilanteet, hybridiuhat ja muut uhat sekä muut toimivaltaisen ministeriön määrittämät uhat. Samoin on otettava huomioon, missä määrin muut toimialat ovat riippuvaisia kriittisen toimijan tarjoamasta keskeisestä palvelusta.



3.6 Päivittäiset ICT-palvelutuotannon prosessit

Varmista ICT-palvelutuotannon perusprosessien toimivuus, ohjeistus ja resursointi. Varautumisen kannalta erityisesti huomioitava:

- Tietoturvan ja altistuman hallinta.
- Kapasiteetin ja saatavuuden hallinta.
- Tapahtumien hallinta.
- Häiriönhallinta, vakavien häiriöiden hallinta.
- Ongelmien hallinta.
- Muutosten hallinta.
- Konfiguraation hallinta.
- Julkaisuiden hallinta.
- Testaus ja validointi.

Varmista, että palvelutuotannon suunnitelmat ja resurssit ovat riittäviä normaali- ja häiriötilanteisiin.

Varautuminen rakentuu olemassa olevien toimivien ICT-palvelutuotannon prosessien päälle. Oletuksena on, että yrityksen palvelutuotannon normaalit prosessit ovat toimivia ja hyvin dokumentoituja sekä johdettuja ja niitä kehitetään säännöllisesti. Varmista yhdessä palveluntarjoajien kanssa palvelutuotannon prosessien toimivuus kokonaisuutena.

Hyvin toteutetut tietoturvan, altistuman, kapasiteetin, saatavuuden, tapahtumien, häiriöiden ja vakavien häiriöiden, ongelmien, muutosten, konfiguraation ja julkaisuiden hallinta sekä testaus ja validointi turvaavat ICT-palvelutuotannon mahdollisimman häiriöttömän toiminnan. Kriisitilanteessa vakavien häiriötilanteiden hoitaminen perustuu toimivaan häiriönhallintaprosesseihin. Lisätietoa ICT-palvelutuotannon prosesseista ja toimintamalleista löytyy mm. ITIL-[5] sekä COBIT-viitekehyksistä[6].

5 https://www.axelos.com/best-practice-solutions/itil , https://itsm.tools/

6 https://www.isaca.org/resources/cobit

3.7 Varautumisen huomioiminen kaikissa järjestelmän elinkaaren vaiheissa

Suunnittele ja toteuta vaatimusten mukaiset varotoimet kokonaisuutena ja kiinnitä niihin huomiota ***kaikissa järjestelmän elinkaaren vaiheissa***.

Määrittele varautumisen vaatimukset hankintavaiheessa:

- Varmista, että hankinnan valmistelu kattaa varautumisen edellytykset (yrityksen tuottaman palvelun kriittisyys liiketoiminnalle ja yhteiskunnalle tunnistettu ja niiden perustella johdettu vaatimukset) sekä muutostilanteeseen (järjestelmän käyttöönotto) kohdistuvat vaatimukset.
- Määrittele ICT-palvelun tai järjestelmän varautumisen vaatimukset liiketoiminnan vaatimusten perusteella. Varmista järjestelmän kriittisyyden ja riskitason huomioiminen.
- Kuvaa mitä haluat saavuttaa ja mitä olet ostamassa.
- Ota palveluntarjoaja tai toimittaja mukaan, varmista yhteinen näkemys.
- Esitä tarjouspyynnössä selkeät tavoitteet ja vaatimukset, jätä tilaa palveluntarjoajan ehdotuksille. Kerro mitä pitää saavuttaa, anna palveluntarjoajan esittää vaihtoehtoisia ratkaisuita.
- Varmista, että hankittava palvelu tai järjestelmä täyttää vaatimukset ja sisällytä vaatimukset sopimukseen.

Varmista vaatimusten ja niiden toteutuksen ajantasaisuus säännöllisesti.

Muista varmistaa vaatimusten riittävyys sekä niiden toteutus järjestelmäkehityksen ja palvelun muutosten yhteydessä.

Varautumisen vaatimukset on huomioitava kaikissa ICT-palvelun elinkaaren vaiheissa. Vaatimukset on otettava huomioon palvelua tai järjestelmää määriteltäessä ja hankittaessa, käytettäessä sekä kehitettäessä esimerkiksi tietoturvavaatimusten tapaan. Varautumisen vaatimuksiin on kiinnitettävä huomiota erityisesti ***hankintavaiheessa***, jolloin vaatimukset täyttävän järjestelmän tai palvelun kehittäminen tai hankkiminen on kustannustehokkaampaa kuin korjaaminen jälkikäteen.

Varautumisen ja sen vaatimusten huomiointi on ***sisällytettävä ICT-hankintaprosessiin***. Järjestelmämuutosten ja -kehityksen yhteydessä vaatimukset on aina tarkistettava ja päivitettävä. Lisäksi olemassa olevien järjestelmien vaatimusten ajantasaisuus ja riittävyys tulee tarkistaa säännöllisesti ICT-palvelutuotannon varautumissuunnitelman päivityksen yhteydessä.

Varautumisen toimenpiteet riskien toteutumisen todennäköisyyksien pienentämiseksi, toteutumisen vaikutusten minimoimiseksi, häiriön aikaiseksi vaihtoehtoiseksi toimintatavaksi ja häiriöstä palautumiseksi ***tulee suunnitella kokonaisuutena huomioiden kattavasti sekä liiketoiminnan että ICT:n toimenpiteet***. Toimenpiteet täydentävät toisiaan ja muodostavat kokonaisuuden, jolla varautumiselle asetettavat vaatimukset voidaan täyttää koko järjestelmän elinkaaren ajan.

3.8 ICT-infrastruktuuri – suojaaminen ja käytettävyyden varmistaminen

Suunnittele ICT-arkkitehtuuri varautumisen vaatimusten perustella:

- Määrittele ICT-infrastruktuurille arkkitehtuuri, joka perustuu tehtyyn luokitukseen ja riskiarvioon.
- Suunnittele ja toteuta toimialuejako kriittisyysluokittelun ja toiminnallisuuden perusteella.
- Varmista arkkitehtuurin mukainen toteutus, kuten toimialuejako ja segmentointi.
- Huomioi konesali-, pilvi- tai hybridiratkaisun valinnassa myös varautumisen vaatimukset ja tehty riskiarvio.
- Varmista tietoliikenneratkaisu ja/tai suunnittele ja toteuta varajärjestelyt.
- Huomioi arkkitehtuurissa ulkoiset vaatimukset sekä mahdolliset auditoinnit.

Hyvin suunniteltu arkkitehtuuri luo pohjan ICT-palvelutuotannon varautumiselle, järjestelmien hankinnalle, ylläpidolle ja kehittämiselle. Arkkitehtuuriratkaisuilla parannetaan häiriönsietokykyä nostamalla ympäristön turvallisuuden tasoa, parantamalla käytettävyyttä ja toipumiskykyä.

Arkkitehtuurin suunnittelun avulla luodaan ICT-toimintaympäristön tavoitetila joka nostaa varautumisen ja turvallisuuden tasoa sekä parantaa kustannustehokkuutta ja laatua. Toimenpiteet kohdistetaan suunnitelmallisesti tärkeimpiin osa-alueisiin. Arkkitehtuurin pitää kehittyä jatkuvasti ja sen jatkokehittämiseen ja ajan tasalla pitämiseen on luotava toimintamalli vastamaan toimintaympäristön muutoksia.

ICT:n tekniseen arkkitehtuuriin kuuluvat esimerkiksi tietoliikenneverkot ja -laitteet, tietoturvallisuus ja turvaratkaisut, palvelimet, järjestelmät sekä tieto ja sen tallennusratkaisut. Tiedon, järjestelmien ja yleisesti ICT omaisuuden sekä käyttäjien luokittelu sekä luokittelun mukaiset vaatimukset muodostavat pohjan suunnittelulle ja arkkitehtuurivalinnoille. Huomioi valintaa tehdessä mm. seuraavat uhat:

- Eri pituiset ja eri syistä johtuvat paikalliset ja kansainväliset tietoliikennehäiriöt
  - Tietoliikennearkkitehtuurilla ja -ratkaisuilla voidaan vaikuttaa operaattoreiden häiriöiden vaikuttavuuteen.
- Laitetiloihin ja tietoverkkoihin kohdistuvat fyysiset uhat, alueelliset vakavat häiriöt (suuronnettomuudet, epidemiat tai pandemiat, levottomuudet jne.)
  - Esimerkiksi palvelutuotannon hajauttaminen sekä pilvipalveluiden hyödyntäminen ovat keinoja vähentää fyysisten vahinkojen vaikutusta.
- Teknologia- ja toimittajariskit (myös maariskit), logistiikkariskit
  - Arkkitehtuurivalinnat vaikuttavat käytettävään teknologiaan ja sen myötä myös toimittajiin liittyviin riskeihin.
- Ohjelmistoriskit sekä yksittäisten komponenttien tai sovellusten kriittisyyden muodostamat keskittymäriskit.

Luokittelun ja vaatimusten huomioiminen on varmistettava myös silloin, kun arkkitehtuurisuunnittelun tekee ulkopuolinen kumppani. Tehtävät valinnat kattavat niin omassa tai palveluntoimittajan laitetilassa toimivat järjestelmät, pilviympäristöt kuin palveluna ostettavat järjestelmät. Arkkitehtuurisuunnittelulla on tärkeä rooli erityisesti silloin, kun tietohallintopalvelut ja ICT-toiminnot ovat kumppanien toimittamia, sillä arkkitehtuuri osaltaan kuvaa liiketoiminnan asettamat vaatimukset ICT-toteutukseksi.

Palveluiden ja teknisen ympäristön ryhmittely

Palveluiden ja teknisen ympäristön jakaminen eri alueisiin mahdollistaa vaatimusten mukaisen ympäristön toteuttamisen yhdenmukaisesti, mahdollisimman kustannustehokkaasti ja vakavassa häiriötilanteessa tai sellaisen uhatessa mahdollistaa eri luokkaan kuuluvien palveluiden eristämisen, saarekekäytön sekä erilaiset toipumiskäytännöt. Liikennettä voidaan haluttaessa varmistaa ja kontrolloida eri alueiden välillä. Kriittiset tuotantoympäristöjen (OT-ympäristöt, Operaation Technology) jatkuvuuden turvaaminen edellyttää OT-ympäristön erottamista omaksi kokonaisuudekseen. Liitteessä 4 on esimerkki OT-ympäristön toteutuksesta ja siihen kohdistuvista vaatimuksista.

Esimerkki (1) asioista, joilla toimialuejako voidaan toteuttaa:

- ***Palvelua käyttävät ja ylläpitävät käyttäjäorganisaatiot/ryhmät.*** Pyritään sijoittamaan saman käyttäjäryhmän käyttämät palvelut samaan toimialueeseen ja estää muilta käyttäjäryhmiltä ylipäätään pääsy toimialueeseen. Tämä mm. parantaa tietoturvaa, yksinkertaistaa ongelmien selvittämistä ja kustannusten kohdistamista.
- ***Tietojärjestelmien ja työasemien saavutettavuusluokitus (kriittisyys).*** Pyritään sijoittamaan saman kriittisyysluokan palvelut ja työasemat samaan toimialueeseen. Tämä mm. mahdollistaa tarkoituksenmukaiset rakenteet kriittisten palvelujen kahdentamiselle (kaikkien palvelujen kahdentaminen ei ole tarkoituksenmukaista) ja helpottaa kustannusten/resurssien kohdistamista kriittisiin palveluihin.
- ***Tietojärjestelmien riskiluokitus.*** Pyritään sijoittamaan saman riskiluokan omaavat tietojärjestelmät samaan toimialueeseen. Tämä mahdollistaa tarkoituksenmukaiset rakenteet riskialttiiden palvelujen suojaamiselle (kuten palomuurien, tunnistautumisen yms. suojausjärjestelmien määrän minimointi) ja helpottaa kustannusten/resurssien kohdistamista riskialttiisiin palveluihin
- ***Tiedon luotettavuus-, eheys- ja tietosuojaluokitukset.*** Toimialueita suunnitellessa otetaan huomioon tiedon luokitukset siten, että tietojärjestelmät ja työasemat, joiden avulla käsitellään saman luokituksen omaavaa tietoa, pyritään sijoittamaan samaan toimialueeseen.
- ***Tekniset seikat ja lisenssinäkökohdat.*** Pyritään yhtenäistämään erilaiset tekniset ratkaisut ja tehostamaan lisensointeja. Tämä alentaa kustannuksia monella tapaa esim. lisensointikulujen vähenemisellä ja epäsuorasti osaamistarpeiden/resursoinnin järkeistämisellä.
- ***Organisaatiomallit ja toimintaprosessit.*** Pyritään yhdistämään organisaation ja toimintaprosessien mukaan eri palvelut samalle alueelle, Kuitenkin otetaan huomioon organisaatioiden eläminen. Tämä helpottaa mm. käyttäjäryhmiin pohjautuvia määrityksiä ja mahdollistaa myös kulujen allokoinnin tietylle organisaatiolle suoraviivaisesti.

Esimerkki (2) hyvinvointialueen toimialuemäärityksestä – toimialue x, joka sisältää arkaluonteista tietoa sisältävät palvelut ja järjestelmät:

- ***SoTe,*** johon kuuluvat sekä terveydenhuoltoon että sosiaalitoimeen liittyvät järjestelmät ja palvelut. Toimialue on jaettu kahtia terveydenhuollon ja sosiaalitoimen kesken.
- ***Integraatiopalvelut,*** johon kuuluvat kaikki järjestelmien väliseen tiedonsiirtoon ja integrointiin tarkoitetut järjestelmät, käyttäjillä ei pääsääntöisesti suoraa pääsyä.
- ***Testi,*** johon kuuluvat kaikki testaukseen, kehitykseen ja koulutukseen liittyvät järjestelmät. Käyttäjinä koko yhtymä.
- ***Huoltovarmuus,*** johon kuuluvat kaikki ne järjestelmät, jotka mahdollistavat kriittisten SoTe-järjestelmien toiminnan myös poikkeusoloissa. Näitä järjestelmiä ovat mm. varavoima-, ovi-, videojärjestelmät ja vastaavat. Kyseiset järjestelmät eivät itsessään sisällä arkaluonteista tietoa

Pilvipalvelu vai konesali?

Oma tai palveluntarjoajan konesali sekä pilvipalvelut tarjoavat erilaisia tapoja hallita riskejä ja turvata jatkuvuus. Arkkitehtuuriratkaisu oman konesalin, yhden tai useamman pilvipalvelun yhtäaikaisen hyödyntämisen tai hybridiratkaisun välillä on perustuttava toiminnallisiin ja varautumisen vaatimuksiin sekä riskiarvioon. Luokittelusta saadaan pohja vaatimuksille ja niiden asianmukaisille toteutusvaihtoehdoille.

Oikein suunniteltuna ratkaisut täydentävät toisiaan varautumisessa ja muodostavat yhdessä toimintavarman arkkitehtuurin. Tätä aihetta on käsitelty tarkemmin Digipoolin ohjeessa Huoltovarmuutta pilvipalveluilla.[7]

7 https://www.digipooli.fi/digipoolin-uusi-opas-auttaa-pilvipalveluista-paattamisessa/

Tietoliikenteen varmistaminen

Varaudu kriittisten palveluiden tietoliikenteen osalta useiden operaattorien yhteyksin. Mikäli yhteyksien kriittisyys on toiminnalle äärettömän tärkeä, hyödynnä esimerkiksi satelliittiyhteyksiä varayhteytenä signaloinnin varmistamiseksi.

Kriittisten järjestelmien tietoliikenteen toimivuuden varmistamiseen ja vaihtoehtoisiin yhteyksiin on kiinnitettävä erityistä huomiota. ***Varaudu*** oman verkon ja vuokrattujen kuitujen häiriöiden lisäksi ***yhden tai useamman teleoperaattorin palvelun yhtäaikaiseen paikalliseen tai valtakunnalliseen häiriöön***. Huomioi myös kansainvälisten yhteyksien häiriöiden vaikutus järjestelmien toimintaan.

Kriittisyysluokittelun ja riskiarvion mukaisesti ulkoisten yhteyksien varmentamisessa voidaan käyttää saman tietoliikenneoperaattorin kahdennettuja yhteyksiä, useamman operaattorin yhteyksiä, ***jotka eivät todennetusti käytä samoja kaapelireittejä ja laitetiloja*** tai käyttää vaihtoehtoisia teknologioita tai reittejä (mm. mobiiliverkko, tai joissain tapauksissa varmentaminen radio- tai satelliittiyhteyksillä).

Vastaavasti yrityksen kommunikointi- ja tiedotuskanavien osalta on suunniteltava vaihtoehtoiset kanavat, mikäli ensisijainen ei ole käytettävissä.

Esimerkki. Valtionhallinnon yhteydet (2021): kaivinkone vaurioitti tietoliikennekaapeleita, minkä seurauksena valtionhallinnon työntekijöiden sähköposti- ja videoneuvottelujärjestelmät lakkasivat laajalti toimimasta. Samalla myös esimerkiksi kansalaisille suunnattu Suomi.fi palvelu ei ollut käytettävissä. Pääyhteys ja varayhteys kulkivat samassa kaivannossa, joten molemmat yhteydet katkesivat yhtä aikaa.

3.9 Sovellukset – turvallisuus ja varautuminen

Varmista sovellusten turvallisuus osana varautumista:

- Määrittele sovellusten kriittisyys sekä turvallisuuden ja varautumisen vaatimukset luokittelun avulla.
- Tarkasta vaatimukset ja mitä ne edellyttävät hankinnalta.
- Muista turvallinen ohjelmistokehitys.
- Tarkasta ja varmista hankittavan ohjelmiston turvallisuus.
- Varmista kolmannen osapuolen komponenttien turvallisuus.
- Huomioi mahdolliset keskittymäriskit ja tee tarvittavat varasuunnitelmat.

Teknisen ympäristön suojaamisen lisäksi huolehdi sovellusten turvallisuudesta. Varmistamalla sovellusten turvallisuus elinkaaren jokaisessa vaiheessa ja huomioimalla mahdolliset keskittymäriskit voidaan merkittävästi vähentää vakavien häiriöiden vaaraa.

Huomioi järjestelmäkehityksessä turvallinen ohjelmistokehitys ja ylläpito: missä ja miten ohjelmistoa kehitetään, ketkä sitä kehittävät, miten ohjelmisto liittyy olemassa oleviin tietoihin ja järjestelmiin sekä missä ohjelmisto tulee sijaitsemaan ja miksi. Näille asetettavat vaatimukset ja tehtävät varautumistoimet tulee perustua riskiarvioon järjestelmän kriittisyyden lisäksi. Huomioi ainakin ***vakavat ohjelmisto- tai konfiguraatiovirheet*** (vaikuttavat mm. järjestelmän käytettävyyteen tai tiedon eheyteen), ***kyberuhat ja tietoturva, teknologiariskit, toimittajaan liittyvät riskit*** (mm. maariski, taloudellinen tilanne, osaaminen), ***sopimukselliset riskit sekä erilaiset keskittymäriskit***. Ota huomioon kattavasti riskit ja varautuminen erityisesti tietoturvan ja infraan hallintaan liittyvien sovellusten hankinnassa.

Valmisjärjestelmän tai SaaS-palvelun käyttöönotossa ohjelmiston ja alustan sekä käyttöympäristön turvallisuus on arvioitava vaatimuksia vasten mahdollisuuksien mukaan tarkastamalla arkkitehtuuri, ohjelmistokehityksen periaatteet, tekninen ympäristö sekä teknisellä testaamisella.

Kun ***sovellukset käyttävät kolmansien osapuolien kirjastoja tai palveluita***, varmista niiden turvallisuus. ***Laadi myös varasuunnitelma*** siltä varalta, että nämä komponentit tai palvelut eivät toimi tai ole käytettävissä. Kolmannen osapuolen kirjastoihin ja riippuvuuksiin sekä näiden haavoittuvuuksiin liittyvien päivitysten hallintaan on myös kiinnitettävä huomiota. Esimerkiksi toimitusketjuhyökkäyksissä on päästy vaikuttamaan ohjelmistokomponentteihin. Lisäksi ne voivat muodostaa keskittymäriskin, mikäli sovellukset ovat liian riippuvaisia yksittäisistä komponenteista.

Log4j (2021). Log4j-haavoittuvuus paljasti keskittymäriskin, joka johtui siitä, että Log4j-kirjastoa käytettiin laajasti eri ohjelmistoissa ja palveluissa maailmanlaajuisesti. Haavoittuvuus levisi nopeasti, mikä johti maailmanlaajuisiin kyberhyökkäyksiin, teki siitä suuren turvallisuusriskin sekä aiheutti merkittävää vahinkoa. Keskittymäriski syntyi, koska:

- Monilla yrityksillä ja palveluntarjoajilla oli kriittisiä järjestelmiä, jotka riippuivat samasta komponentista.
- Monet eivät olleet tietoisia siitä, että heidän käyttämänsä sovellukset tai palvelut perustuivat Log4j-kirjastoon, mikä teki korjausten toteuttamisesta haastavaa.

Facebookin palvelukatko (2021). Facebook, WhatsApp ja Instagram olivat poissa käytöstä useita tunteja katkoksen aikana. Facebook Login on suosittu tapa käyttää yhtä tunnusta ja salasanaa kirjautuessa kolmannen osapuolen sovelluksiin, joten häiriö esti myös kirjautumisen useisiin palveluihin Facebookin, WhatsAppin ja Instagramin lisäksi.

Heinäkuussa 2024 kyberturvallisuusyrityksen ***CrowdStriken Falcon Sensor*** -ohjelmiston virheellinen päivitys aiheutti laajoja häiriöitä maailmanlaajuisesti. Päivityksessä oli ytimen konfiguraatiovirhe, joka johti Windows-järjestelmien kaatumiseen ja laitteiden toimintahäiriöihin. Yli 8,5 miljoonaa laitetta kärsi ongelmasta, ja vaikutukset tuntuivat erityisesti kriittisillä aloilla, kuten pankeissa ja lentoyhtiöissä. Korjausprosessi vaati manuaalisia toimenpiteitä, taloudelliset menetykset olivat merkittäviä.

SolarWindsin 2020 IT-hallintaohjelmistoon kohdistunut hyökkäys vaikutti useisiin organisaatioihin, mukaan lukien suuret yritykset ja valtion laitokset. SolarWindsin laaja käyttö IT-infrastruktuurien hallinnassa teki hyökkäyksestä erityisen laajalle levinneen ja vakavan.

Ohjelmistokomponenttien ja -kirjastojen turvallisuuden tarkistamiseen lähteitä ovat mm:

- ***National Vulnerability Database (NVD)*** on Yhdysvaltojen kansallinen tietoturva-aukkojen tietokanta, jota hallinnoi NIST (National Institute of Standards and Technology): nvd.nist.gov
- ***CVE Details*** on riippumaton tietokanta, joka tarjoaa tietoa CVE-haavoittuvuuksista: cvedetails.com
- ***Open Web Application Security Project (OWASP)*** tarjoaa Dependency-Check-työkalun, joka analysoi ohjelmiston kirjastot ja komponentit ja tunnistaa tunnetut haavoittuvuudet CVE-tietokannan avulla: owasp.org
- ***Snyk*** tarjoaa sekä maksullisen että ilmaisen haavoittuvuustarkastuksen, jolla voi skannata projekteja tunnettuja kirjastohaavoittuvuuksia vastaan: snyk.io
- ***GitHub*** ylläpitää tietokantaa avoimen lähdekoodin kirjastojen haavoittuvuuksista: github.com/advisories

3.10 Tietoturvallisuus

Huoltovarmuusorganisaatioon kuuluvien yritysten odotetaan hoitavan tietoturvan asianmukaisesti esimerkiksi ISO27001-vaatimusten mukaisesti:

- Huolehdi tietoturvasta kattavasti ja toteuta vähintään perustason tietoturvakäytännöt.
- Toteuta suojaustoimet tehtyjen luokitusten mukaisesti (järjestelmät ja ICT-infrastruktuuri sekä niiden kriittisyys- ja tietoturvallisuuden riskitasoluokitukset).
- Ylläpidä tietoturvan tilannekuvaa osana ICT:n ja yrityksen toimintaympäristön tilannekuvaa.
- Suunnittele valmiiksi tarvittavat suojaustoimenpiteiden korotukset, uhkiin varatutuminen ja valmiuden tason nostot tilannekuvan muutoksia varten.
- Toteuta suunnitellut toimenpiteet tilannekuvan muuttuessa.

Tietoturvan hallinta perustuu yrityksen toimintojen kriittisyyden ymmärtämiseen, osana ICT-palvelutuotannon varautumista. Huoltovarmuuskriittisten yritysten oletetaan huolehtivan tietoturvasta ja yrityksellä oletetaan olevan kirjalliset tietoturvallisuutta koskevat toimintaperiaatteet ja menettelytavat, kuten tietoturvapolitiikka, kyberriskien hallintamalli ja poikkeamien käsittelyprosessi sekä tietoturvaohjeistus. Samoin tietoturvan hallintaa toteutettavien toimenpiteiden ja suojaamiseen käytettävien ratkaisujen odotetaan olevan ajantasaisia ja oikeansuhtaisia.

Varaudu tunnistettuihin tietoturvauhkiin oikeansuhtaisella suojaus- ja valvontaratkaisulla sekä suunnitelmalla ja harjoittelemalla toimenpiteet uhkien toteutumisen varalle. Järjestelmien ja ICT-infrastruktuurin luokittelun tulee ohjata sekä teknisiä ratkaisuja että muita suojaustoimenpiteitä. Kyberturvallisuuskeskuksen[8] ja Digipoolin[9] sivuilta löytyy runsaasti ohjeistusta tietoturvasta ja varautumisesta tietomurtoihin.

Kyberturvallisuuslaki edellyttää yritykseltä ajantasaisia ja oikeansuhtaisia toimenpiteitä huomioiden riskitaso ja mahdollisen häiriön vaikutukset. Laissa edellytetään myös vähintään perustason tietoturvakäytäntöjä. Tietoturvakäytännöt liittyvät laajasti tässä ohjeessa esitettyihin ICT-palvelutuotannon varautumisen vaatimuksiin ja niitä on käsitelty tämän ohjeen eri kappaleissa.

Kyberturvakeskuksen julkaisema Kybermittari[10] ja tietoturvallisuuden standardisarja 27000 tarjoavat työkaluja tietoturvan hallintaan. Kyberturvallisuuskeskus on myös tehnyt luonnoksen ***perustason tietoturvakäytännöistä***[11].

8 https://www.kyberturvallisuuskeskus.fi

9 https://www.digipooli.fi/varautuminen-tietomurtoon/

10 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari

11 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mita-nis2-direktiivissa-esitetyt-kyberhygieniakaytannot-ovat

3.11 Henkilöstö, henkilöstön käytettävyys ja työvoiman saatavuuden varmistaminen

Varmista henkilöstön ja työvoiman käytettävyys:

- ***Määrittele minimiorganisaatio ja osaaminen***, jolla varautumisen vaatimukset pystytään täyttämään sekä tee suunnitelma sen täyttämiseksi kaikissa eri tilanteissa. Huomioi tehtävien priorisointi ja mitä voidaan jättää tekemättä.
- Tee vähintään ***kriittisten toimintojen henkilöstösuunnittelu***, joka huomioi myös poikkeusolot.
- Tunnista ***kriittiset osaamisalueet ja avainhenkilöt.***
- Huolehdi seuraajasuunnittelusta ja sijaisten määrittämisestä.
- Laadi ja toteuta suunnitelma riittävän laaja-alaisen osaamisen varmistamiseksi.
- ***Varaudu sekä avainhenkilöiden menetykseen että laajempaan henkilöstöpulaan.***
- Selvitä ***hätätyön*** käyttömahdollisuus.
- Selvitä henkilöstövajauksen korvaaminen alihankinnalla, tee tarvittavat sopimukset.
- Tee ***turvallisuusselvitykset.***
- Tee ***poikkeusolojen henkilövaraukset*** ja tarkista ne säännöllisesti sekä organisaatio-, tehtävä- tai henkilömuutosten yhteydessä. Varaudu poikkeusolojen organisaation suunnittelussa siihen, etteivät kaikki henkilöt olekaan käytettävissä.
- Varmista toimintakyky myös silloin, jos ulkomaiset työntekijät eivät ole käytettävissä esimerkiksi poikkeusoloissa.

Häiriötilanteita varten asetettujen tavoitteiden saavuttamiseksi ICT-palvelutuotannon on ***määriteltävä organisaatio, joka vähintään tarvitaan palveluiden jatkuvuuden varmistamiseksi sekä suunniteltava tarvittavan osaamisen ja työvoiman saatavuuden turvaaminen***. Suunnittelussa huomioitava lainsäädännön, kuten työaikalain, asettamat rajoitukset, joita on noudatettava myös kriisitilanteissa. Lisäksi on huomioitava riski avainhenkilöiden ja muiden kriittisten resurssien menettämisestä sekä laajamittaiset poissaolot (esim. työvoimapula), jotka voivat vaikuttaa tehtävien hoitamiseen myös organisaation kriittisten osaamisalueiden ulkopuolella.

Työvoiman saatavuutta voidaan parantaa mm.

- Avainhenkilöiden ***seuraajasuunnittelulla***
- ***Kouluttamalla*** henkilöstöä monipuolisesti, käyttämällä tehtäväkiertoa ja varmistamalla sijaisjärjestelyt.
- Varautumalla ***alihankinnan käyttöön*** henkilöstövajauksen yhteydessä
- ***Priorisoimalla ICT-palvelutuotannon tehtävät:*** mitä tehtäviä voidaan jättää tekemättä ja mihin keskitytään vakavissa häiriö- tai poikkeustilanteessa tai työvoimapulan yhteydssä.
- ***Tarvittaessa poikkeusolojen henkilövarauksilla*** (VAP, vapautettu aseellisesta palvelusta sodan aikana)

Avainhenkilöt ja kriittiset osaamisalueet

ICT-palvelutuotannon kriittisyysluokittelun perusteella määritellään osaamisalueet, jotka ovat välttämättömiä varautumisen vaatimusten täyttämiseksi. Nämä osaamisalueet on huomioitava henkilöstön osaamisvaatimuksissa, koulutuksessa, palveluhankinnoissa ja resursoinnissa.

Kriittisimpien toimintojen (kuten esimerkiksi häiriönselvitys ja palautuminen) tulee tehdä henkilöstösuunnittelua, joka huomioi osaamistarpeet ja suunnittelee sekä ennakoi kehitystä. Osana henkilöstösuunnittelua tulee miettiä varamiesmenettelyt. Mikäli kriittisen toiminnon henkilöstösuunnittelun myötä selviää, että kriittinen henkilö voi joutua asepalvelukseen, tulee käynnistää poikkeusolojen henkilövarauksen (VAP varaus) hakeminen ja varata henkilö tekemään yrityksen yhteiskunnan kannalta elintärkeää tehtävää. Toisaalta jos varaus ei onnistu joko henkilön oman tahdon tai puolustusvoimien tärkeän tehtävän takia, tulee suunnitella toimittavan varamiesjärjestelyn mukaisesti.

Hätätyö

Hätätyö tarkoittaa työtä, jota tehdään ennakoimattoman ja poikkeuksellisen tapahtuman seurauksena, kun on tarpeen suojella ihmisten henkeä, terveyttä tai omaisuutta tai varmistaa yhteiskunnan toiminnan jatkuvuus. Hätätyötä voidaan teettää äkillisen kriisin sattuessa, jos normaalein työjärjestelyin ei kyetä vastaamaan

tilanteeseen. Hätätyön käyttömahdollisuus ja toimintatapa tulee selvittää etukäteen ja tiedottaa henkilöstöä asiasta.

Työsuojeluhallinnon sivuilta (työsuojelu.fi) ja työaikalaista löytyy lisätietoa hätätyöstä ja siihen liittyvistä määräyksistä (mm. hätätyön teettämisen edellytykset, mistä ja miten voidaan poiketa, työajan tasoittuminen hätätyön jälkeen, hätätyöilmoitus).

Ulkomaiset työntekijät

Poikkeusolot Suomessa tai ulkomailla, kiristyvä poliittinen tai geopoliittinen tilanne, ympäristökatastrofit tai vakavat onnettomuudet voivat estää ulkomaalaisten työntekijöiden saapumisen Suomeen tai heidän työskentelynsä Suomessa. Samoin etätyöskentely joistakin maista tai maanosista voi estyä teknisten tai poliittisten syiden vuoksi. Tämä riski on huomioitava varautumisessa sekä oman henkilöstön, että ICT-palveluntarjoajien osalta.

Henkilöstön väärinkäytökset ja turvallisuusselvitys

Yrityksen on ehkäistävä tahallisia tai tahattomia väärinkäytöksiä oman ja palveluntarjoajien henkilöstön osalta sekä varauduttava niiden toteutumiseen esimerkiksi:

- Estämällä vaaralliset tehtäväyhdistelmät
- Pääsynhallinnan ja käyttöoikeuksien hallinnalla (ns. pienimmän oikeuden periaate)
- Vähentämällä henkilöihin kohdistuvan painostuksen riskiä mm. estämällä vaaralliset tehtäväkokonaisuudet, salaamalla tarvittaessa yhteystiedot tai henkilön rooli, antamalla suositukset sosiaalisen median käytöstä yksityisyyden suojaamiseksi, valmiit suunnitelmat ja toimintatavat fyysiseen suojaamiseen, ilmoituskanavat ja valmiit toimintamallit fyysisiä uhkia varten.
- Huolehtimalla tietoturvaosaamisesta ja -tietoisuudesta sekä tietoturvavalvonnalla
- Tekemällä selkeät eettiset ja toiminnalliset ohjeet ja politiikat sekä väärinkäytösten raportointikanava ja valmis toimintamalli väärinkäytösten varalle.
- Rakentamalla kontrollit väärinkäytösten havaitsemiseksi nopeasti mm. poikkeamien seurannalla ja riittävien lokitietojen keräämisellä erityisesti kriittisten toimintojen ja laajojen käyttöoikeuksien osalta.
- Mahdollisuuksien mukaan referenssien tarkistukset rekrytoinnin yhteydessä.
- Huoltovarmuuden ja turvallisuuden kannalta kriittisissä tehtävissä työskentelevien osalta tulee tehdä mahdollisuuksien mukaan turvallisuusselvitys.

Poikkeusolot

Turvallisuusselvityslakiin on esitetty muutosta, jonka jälkeen perusmuotoinen henkilöturvallisuusselvitys voidaan laatia sellaiseen palvelussuhteeseen tai toimeksiantotehtävää suorittamaan valittavasta taikka palvelussuhdetta tai toimeksiantotehtävää hoitavasta, joka toimii tehtävissä, joissa voi vahingoittaa yhteiskunnan toimivuuden kannalta välttämättömän infrastruktuurin toimivuutta tai kriittisen tuotannon jatkumista taikka voi näissä tehtävissään saamiensa salassa pidettävien tietojen oikeudettomalla käytöllä merkittävällä tavalla vaarantaa valtion turvallisuutta tai muuta merkittävää yleistä etua. Muutosesitys on osa hallituksen esitystä laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja joidenkin muiden lakien muutoksiksi.

Organisaatiot voivat hakea keskeisille henkilöille vapautusta asepalveluksesta (VAP-varaus) poikkeusoloja varten. Yksiköiden tulee tarkastella säännöllisesti poikkeusoloissa tarvitsemansa avainhenkilöstön tarve ja tehdä tarvittavat VAP-varaukset.

3.12 Fyysinen turvallisuus ja kriittinen infrastruktuuri

Suojaa järjestelmät, tietoliikenneyhteydet ja tarvittavat tilat fyysisesti:

- ***Suunnittele varotoimet*** riskiarvion perustella.
- ***Suojaa*** toimitilat, laitetilat, tietoverkon laitteet ja fyysiset yhteydet.
- Muista myös kannettavat ja siirrettävät laitteet.
- Tarvittaessa ***hajauta toimintaa maantieteellisesti*** tai varaa tarvittavat ***väistötilat***. Huolehdi väistötilan toimintavalmiudesta ja harjoittele niihin siirtymistä.
- Huolehdi sähkön saannin, lämmityksen ja jäädytyksen varmistamisesta.
- Rajaa pääsy kriittisiin tiloihin vain sitä tarvitseville ja huolehdi valvonnasta.

Tietoverkon ja tietojärjestelmien fyysinen ympäristö sekä ICT-palvelutuotannon työympäristö on suojattava uhilta, vahingoilta ja häirinnältä, jotka saattaisivat vaarantaa tiedon tai palveluiden saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Suojaamisessa on huomioitava toimitilat, laitetilat, tietoverkon laitteet ja fyysiset yhteydet. Lisäksi on muistettava suojata kannettavat tai liikuteltavat laitteet ja ohjeistaa niihin liittyvät käytännöt varkauksien ja väärinkäytösten ehkäisemiseksi.

Suojaus fyysisiltä vahingoilta ja niiden vaikutuksilta voi tapahtua sekä pienentämällä vahingon todennäköisyyttä erilaisilla suojaustavoilla että pienentämällä mahdollisen häiriön vaikutusta rakentamalla ympäristö ja järjestelmät vikasietoisemmiksi arkkitehtuurin sekä järjestelmien suunnittelun ja toteutuksen yhteydessä. Sopivat varotoimet suunnitellaan riskiarvion sekä kriittisyysluokituksen pohjalta. Arvioinnissa ja suojaamistoimenpiteissä on otettava huomioon myös ICT-palveluntarjoajien ja kumppaneiden fyysinen turvallisuus ja vaadittava heiltä vastaavat toimenpiteet.

Fyysiseen suojaamiseen ja varautumiseen sisältyvät esimerkiksi

- Laitteiden ja tietoliikennekaapeleiden sijoittaminen suojattuihin tiloihin
- Kulunvalvonta ja kulkuoikeuksien hallinta, valvontakamerat ja tallentimet sekä hälytysjärjestelmät
- Palohälytys ja automaattiset sammutusjärjestelmät, fyysisten laitteiden turvaaminen palo- tai vesivahingoissa
- Fyysisten tilojen ja laitteiden sekä tietoliikenneyhteyksien kahdentaminen tai monistaminen sekä laitteiden ja toimintojen hajauttaminen maantieteellisesti
- Sähkön ja lämmön saannin turvaaminen
- Mahdolliset väistötilat
- Vartiointipalvelut ja henkilösuojaus tarvittaessa

Osana toimintaympäristön tilannekuvaa on seurattava fyysiseen turvallisuuteen liittyvien riskien ja niiden todennäköisyyksien muutoksia. Fyysisen suojauksen ja valvonnan tasoa tulee nostaa tarvittaessa uhkatason noustessa tai riskien kasvaessa.

Kyberturvallisuuslaki edellyttää toimijalta ajantasaisia sekä riskiin ja häiriönvaikutus huomioiden oikeansuhtaisia toimienpiteitä viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden varmistamiseksi. Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten turvatoimien toteuttamisesta siten, että järjestelmiä, tiloja, verkkoja ja muita resursseja suojataan luvattomalta pääsyltä sekä muilta vahingoilta ja häiriöiltä. Toimijan tulisi tunnistaa fyysisen ympäristön tekijät, joiden turvallisuus on viestintäverkkojen ja tietojärjestelmien toiminnan kannalta tärkeää ja suojata näitä toimintaan vaikuttavien uhkien vaikutukselta ja häiriöiltä. Toimijan tulisi huomioida myös viestintäverkkoihin ja tietojärjestelmiin vaikuttavat fyysiset ympäristöt, jotka voivat olla hyvin erilaisia ja esimerkiksi maantieteellisesti laajoja tai suppeita. Fyysisiä uhkia ovat ympäristötekijät ja pahantahtoiset toimijat. Viestintäverkkoja ja tietojärjestelmiä tulisi valvoa ja niitä tulisi suojata luvattomalta fyysiseltä pääsyltä, vahingoilta ja häiriöiltä. Lisäksi on suojauduttava luonnollisilta ja yhteiskunnallisilta tapahtumilta, kuten tulipaloilta, tulvilta ja levottomuuksilta. Toimijan tulisi varautua 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.

Kriittisten tilojen kahdentaminen ja väistötilat

Kriittisten tilat voidaan kahdentaa tai suunnitella toiminnan jatkaminen mahdollisissa erillisissä väistötilaoissa. Väistötilojen käyttö on harjoiteltava ja varmistettava riittävät varmistetut tietoliikenneyhteydet ja kulkuoikeudet tiloihin. Väistötilan työvälineet ja yhteydet tulee pitää ajantasaisina ja toimivina.

Tilojen kahdentaminen ja maantieteellinen hajauttaminen voidaan tehdä eri tasoisesti kriittisyyden ja asetettujen vaatimusten mukaisesti kuten esimerkiksi:

- Varmuuskopiot ja tarvittava ohjeistus sekä mediat järjestelmien ja ICT-infrastruktuurin pystyttämiseen uuteen ympäristöön on sijoitettu fyysisesti eri kohteeseen.
- Väistötila, johon toiminta siirtyy tarvittaessa. Väistötila voi olla toimitilan korvaava tai teknisen ympäristön ja järjestelmien toipumiseen käytetty laitetila (ns. disaster recovery site).
- Osana arkkitehtuurisuunnittelua tilojen ja järjestelmien kahdentaminen tai monistaminen sekä pilvipalveluiden hyödyntäminen osana ympäristöjen monistamista tai kahdentamista eri tasoisesti.
- Arkkitehtuurin suunnittelun yhteydessä käsitellyn segmentoinnin mahdollistama eristäminen ja itsenäinen käyttö saarekkeina

Maantieteelliselle hajautukselle ja vaadittaville etäisyyksille ei ole yksiselitteistä suositusta. Toteutustapa riippuu järjestelmän kriittisyydestä, käytettyjen tilojen turvallisuudesta, järjestelmiä tarvitsevan toiminnan luonteesta ja tunnistetuista uhkista. Vaihtoehtoja uhkatason mukaan ovat esimerkiksi:

- Hajautus samassa toimintaympäristössä esim. tehdasalueella: järjestelmät sidoksissa alueeseen ja alueen laajempien häiriöiden tai vaurioitumisen yhteydessä järjestelmille ei ole tarvetta.
- Sijoittaminen eri tiloihin lähialueella toiminnan ollessa sidoksissa ko. paikkakuntaan. Ratkaisu suojaa kiinteistöön tai aivan sen lähialueelle rajoittuvilta vahingoilta.
- Hajauttamien eri puolille Suomea mahdollistaa toiminnan jatkumisen laajojen alueellisten häiriöidenkin yhteydessä. Esimerkiksi laajan sähkönjakelu- tai tietoliikennehäiriön vaikutusalue voi vaihdella kymmenistä kilometreistä satoihin kilometreihin.
- Kansainvälisten pilvipalveluiden tai ulkomaisten laitetilojen hyödyntäminen, joka mahdollistaa toiminnan jatkamisen tarvittaessa myös Suomen rajojen ulkopuolelta.

Sähkön saannin turvaaminen

Sähkönsaannin varmistaminen tehdään UPS- ja varavoimajärjestelmillä. Varavoima mitoitetaan siten, että kriittiset järjestelmät pystytään pitämään käytössä pidempienkin tai usein toistuvien sähkökatkojen aikana. Järjestelmien ja ICT-infrastruktuurin sähkön saanti on hyvä varmistaa vähintään niin pitkäksi aikaa kuin niitä tarvitsevat toiminnot pystyvät toimimaan ilman sähköä. Varavoiman osalta varmistettava polttoaineen saanti sähkökatkojen ja muiden häiriöiden aikana ja huomioitava myös poikkeusolot polttoaineen toimitussopimuksissa.

Ympäristöolosuhteiden huomiointi ja varmistaminen

Fyysiseen varautumiseen kuuluvat myös ICT-palvelutuotannon toiminnan varmistaminen ympäristöolosuhteissa tapahtuvien muutosten ja vahinkojen yhteydessä (kuten myrskyt, tulvat, tulipalot ja vesivahingot) sekä näiden aiheuttamien vahinkojen estäminen tai rajoittaminen. Esimerkiksi laitetilojen osalta huolehdittava jatkuvasta valvonnasta lämpötilan ja kosteuden osalta sekä varmistettava palohälytys- ja sammutusjärjestelmien toiminta.

Pääsynhallinta ja luvattoman tunkeutumisen estäminen

Fyysisten rakenteiden on järjestelmien kriittisyys ja riskitaso huomioiden estettävä tunkeutumisen kriittisiin kohteisiin tai tietoliikenneyhteyksiin. Tarvittavien rakenteiden ja ratkaisuiden osalta on hyvänä lähtökohtana Katakrin[12] fyysisen turvallisuuden osion määrittelemän Perustason (IV) vaatimukset. Korkeamman turvatason vaatimuksissa mukaan tulee myös luvattoman kuuntelun esto ja hajasäteilyn vaatimukset.

Pääsynhallinnalla rajataan pääsy tiloihin vain sitä tehtävissään tarvitseville henkilöille ja estetään ei-toivottujen henkilöiden pääsy palvelutuotannon tiloihin. Kulunvalvonnassa käytetään tarvittaessa tallentavaa kulunvalvontajärjestelmää, jolla voidaan todentaa tilassa toimineet henkilöt.

12 https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

3.13 Tiedon luottamuksellisuuden ja oikeellisuuden varmistaminen

Varmista tiedon luottamuksellisuus, eheys, saatavuus ja oikeellisuus:

- ***Tieto on keskeinen resurssi, suojaa se kriittisyyden mukaisesti.***
- Suunnittele suojaus- ja varotoimenpiteet tiedon kriittisyys-, eheys- ja saatavuusvaatimusten mukaisesti.
- Huolehdi ***varmuuskopioinnista ja lokikäytännöistä.***
- Rakenna tarvittavat kontrollit ja valvonta tiedon eheyden ja muuttumattomuuden varmistamiseksi sekä väärinkäytösten havaitsemiseksi.
- ***Varmista kyky tiedon palauttamiseen testaamalla ja harjoittelemalla.***

Tieto tukee päätöksentekoa ja operatiivisia toimintoja ja sen avulla yritykset voivat analysoida suoritustaan, mukautua markkinoiden muutoksiin ja reagoida tehokkaasti muutoksiin. Kun kriittinen tieto on saatavilla, eheää ja oikein varmistettua, organisaatio pystyy jatkamaan toimintaansa häiriöiden aikana ja toipumaan niistä nopeammin.

Huomioi riskien käsittelyssä kattavasti tietovuoto tai -varkaus, tiedon manipulointi sekä tuhoaminen tai tuhoutuminen tahallisesti tai vahingossa.

Kiinnitä kriittiseen tietoon erityistä huomiota varmuuskopioinnissa ja toipumisen suunnittelussa. Järjestelmät ja tekninen ympäristö voidaan yleensä rakentaa uudelleen, mutta tuhoutunut tai korruptoitunut tieto on usein palautettavissa vain varmuuskopioilta. Varmuuskopiointi toteutetaan tiedon luokituksen ja liiketoiminnan asettaman palautuspistevaatimuksen (RPO) mukaisesti. Rakenna kriittisyyden mukaisesti tarvittavat kontrollit tiedon eheyden ja muuttumattomuuden varmistamiseksi. Varmuuskopioinnista ja palautumisesta sekä tiedon muuttumattomuuden varmistamisesta on tarkemmin liitteessä 5 sekä luvussa 3.14 Palautumisen varmistaminen.

Harkitse tietosuojaan, tietoturvaan ja tiedonhallintaan liittyen tietotilinpäätöksen ottamista osaksi yrityksen raportointikäytäntöjä.[13]

13 https://www.fordione.fi/

3.14 Palautumisen varmistaminen

Panosta toipumiseen:

- Laadi varmuuskopiointipolitiikka, tee ***varmuuskopiointi tiedon ja järjestelmineen kriittisyyden vaatimusten mukaisesti.***
- Laadi lokipolitiikka ja toteuta sen mukaiset ***lokikäytännöt*** sekä tarkista lokitietojen saatavuus säännöllisesti.
- ***Harjoittele ja testaa palautumista*** sekä järjestelmittäin että laajempien kokonaisuuksien osalta. Muista todentaa tiedon palautus toiminnan vaatimalle tasolle.
- Varmista myös palveluntuottajien kyky toipua.
- Varmista toipumissuunnitelmien taso ja harjoittele niiden mukaista toimintaa. ***Sovita omat ja palveluntarjoajien suunnitelmat saumattomaksi kokonaisuudeksi.***

Järjestelmien ja tiedon suojaaminen pienentää vakavien häiriöiden riskiä, mutta ei poista sitä kokonaan. Täydellinen suojautuminen vahingoilta ei ole mahdollista, joten toipumisen varmistaminen on tarpeen. Kyky toipua riittävän nopeasti rajaa häiriöiden vaikutusta. Vakava häiriö voi koskea myös järjestelmiä, joiden käytettävyyteen on panostettu esimerkiksi kahdentamalla. Järjestelmien kriittisyyden ja asetettujen palautumisvaatimusten (RPO, RTO) mukaisesti valitaan sopivin varmuuskopiointi- ja toipumisstrategia yhdessä muiden varotoimenpiteiden kanssa.

Laadi ***varmuuskopiointipolitiikka*** ja käytännöt riskiluokituksen mukaisesti. Varmista politiikan ja valittujen käytäntöjen mukainen toteutus. Varmuuskopioinnista on tarkemmin liitteessä 5.

Huolehdi varmuuskopioinnin lisäksi ***lokikäytännöistä***. Lokit tarjoavat yksityiskohtaista tietoa järjestelmien ja sovellusten tapahtumista, virheistä sekä käyttäjien toiminnoista. Niiden avulla voidaan jäljittää häiriöiden ja tietoturvaloukkausten syitä, selvittää niiden vaikutuksia ja estää vastaavia tilanteita toistumasta. Toipumistilanteissa lokit auttavat palauttamaan järjestelmät edeltävään tilaan. Varautumisen näkökulmasta säännöllinen lokien seuranta ja analysointi auttavat tunnistamaan epäilyttäviä poikkeamia ja mahdollisia haavoittuvuuksia ennen kuin ne ehtivät eskaloitua vakaviksi ongelmiksi. Lisäksi lokit ovat kriittisiä mahdollisten väärinkäytösten ja rikosten selvittämiseksi. Lokikäytännöistä tarkemmin liitteessä 6 sekä esimerkiksi Kyberturvakeskuksen sivuilla.[14]

Liiketoiminta vastaa toipumissuunnittelusta oman toimintansa osalta ja ICT-palvelutuotanto ICT-infran, järjestelmien, tiedon ja oman toimintansa osalta. Niin ICT-palvelutuotannolla kuin kriittisellä ICT-palveluntarjoajalla on oltava auditoitavissa olevat ***toipumissuunnitelmat (Disaster Recovery Plan, DRP) vähintään kriittisten järjestelmien (ml. tietoliikenne ja siihen liittyvät laitteet ja järjestelmä) osalta***. Tee toipumissuunnitelma sekä ICT-infralle kokonaisuutena että yksittäisille järjestelmille. Kokonaissuunnitelma huomioi laajan häiriön vaatiman järjestelmien priorisoinnin ja keskinäiset riippuvuudet sekä ICT-infrastruktuurin toipumisen vaatimat toimenpiteet. Yksittäisen järjestelmän toipumissuunnitelma kuvaa kyseiseen järjestelmään liittyvät yksityiskohtaiset toimenpiteet normaalitilaan palaamiseksi.

ICT-palveluntarjoajilta on edellytettävä vastaavia toipumissuunnitelmia, niiden säännöllistä ylläpitoa ja suunnitelmallista testausta sekä harjoittelua.

Toipumissuunnitelmien tulee sisältää vähintään seuraavat asiat.

- Varmuuskopiointi- ja lokikäytännöt
- Häiriönhallintaprosessi
- Toipumisessa tarvittavat resurssit
- Riippuvuudet ja priorisointi (muut järjestelmät, ympäristöt, alustat)
- Toimintatapa toipumiseksi (Recovery Procedure), sekä kokonaisuutena että järjestelmittäin (ml. tarvittavat lisenssit, mediat, laitteet, yhteydet).
- Tunnistetut järjestelmäkohtaiset riskit ja niiden huomioiminen
- Käytännöt vahingon tai häiriön rajaamiseksi ja eristämiseksi
- Toipumissuunnitelman testauskäytännöt ja -suunnitelma

Kyberturvallisuuslaki edellyttää, että toimijalla on riskienhallinnataan perustuvat ajantasaiset menettelyt varmuuskopioinnista ja palautumisen suunnittelusta. Lain perusteluissa todetaan mm., että jatkuvuus olisi varmistettava ja sen voisi tehdä esimerkiksi riskienhallinnan perusteella luodulla jatkuvuussuunnitelmalla sekä ***toipumissuunnitelmalla***.

14 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

3.15 Palveluntarjoajien ja toimitusketjun varautuminen

Huolehdi koko toimitusketjun varautumisesta:

- ***Tunnista kriittiset palveluntarjoajat*** ja alihankintaketju.
- ***Varmista varautumisen vaatimusten välittyminen*** ketjussa esimerkiksi sopimuksellisesti. Huomioi palvelun tuottaminen force majeure -tilanteissa.
- Edellytä ***varautumis- ja toipumissuunnitelmat***, varmista suunnitelmien yhteensopivuus omien suunnitelmiesi kanssa.
- Huomioi mahdollinen ***maariski*** ja riippuvuus kansainvälisestä logistiikasta.
- ***Hajauta*** toimittajariskiä mahdollisuuksien mukaan.
- Tarvittaessa varmista ja auditoi varautumisen vaatimusten toteutuminen.
- Hyödynnä SOPIVA-suosituksia sopimuksissa, muista myös palautumisen testaamisen ja harjoittelun sisällyttäminen sopimuksiin.

Kyverturvallisuuslaki edellyttää, että toimijalla on ***ajantasainen tieto kaikista toimintaan vaikuttavista välittömistä toimittajista***. Toimijan on huomioitava turvallisuusnäkökohdat toimitusketjunsa välittömien laite- tai palveluntoimittajien osalta. Riskien hallintatoimenpiteissä on huomioitava ***välittömälle toimittajalle ja palveluntarjoajalle ominaiset*** haavoittuvuudet, tuotteiden ja palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt. ***Hallintaa voidaan tehdä myös sisällyttämällä vaatimukset sopimuksiin.***

Toimittajien valinta ja toimittajariskit

Yrityksen on tunnettava kriittisiin palveluihin liittyvät ICT-kumppanit ja palveluntuottajat osana ICT-palvelutuotannon kriittisten resurssien määrittelyä. ***Tunnista kriittiset toimittajat*** ja selvitä mahdolliset vaihtoehtoiset kumppanit ongelmatilanteiden varalle. Mikäli mahdollista, käytä useampaa toimittajaa hajauttamaan ja pienentämään toimittajariskiä. Arvio toimittajiin liittyvä mahdollinen ***maariski*** ja hajauta hankintoja tarvittaessa eri maihin tai maanosiin. Palvelun ***riippuvuus kansainvälisen logistiikan toimivuudesta*** ja geopolitiikan aiheuttamista uhista on huomioitava. Varmista asetettujen varautumisen kriteerien toteutuminen koko toimitusketjun osalta.

Sopimukset ja palveluntarjoajan velvollisuudet sekä varautuminen

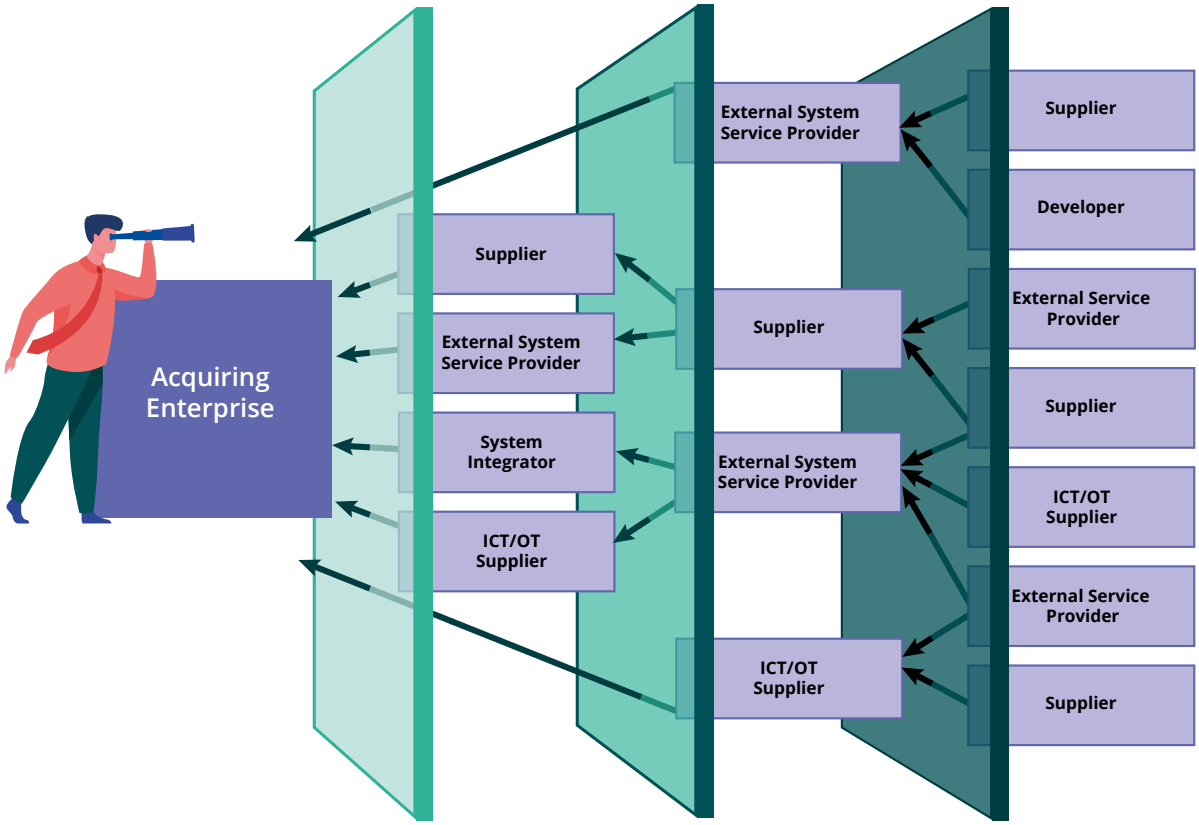
Varautumisen vaatimukset on mahdollista siirtää ICT-palveluntuottajille sopimuksellisesti. ***Palveluntuottajien varautuminen ja toiminnan jatkuvuus häiriötilanteissa on varmistettava kirjaamalla varautumiseen liittyvä velvoitteet ja tavoitteet sopimukseen velvoittaviksi.*** Samalla on varmistettava velvoitteiden täyttämisen seurattavuus sekä varautumisen vaatimusten välittyminen kaikille alihankintaketjun kriittisille toimijoille.

Palvelutaso on varmistettava ulottamalla palvelutaso-, varautumis- ja toipumisvaatimukset koko palveluketjuun ja varmistamalla niiden vastaavan järjestelmien, tiedon ja ICT-infran kriittisyysluokitusta. Mitä pidempi palveluiden toimitusketju on, sitä vähemmän on näkyvyyttä osapuolten varautumisen tasoon. Varmista, että omat palvelutarjoajat vaativat sopimuksellisesti omilta alihankkijoiltaan saman tasoiset varotoimet ja suunnitelmat kuin mitä heiltä edellytetään. Mahdollisuuksien mukaan käy läpi toimitusketjun resilienssi ja varmista ketä palveluiden toimitusketjussa on osallisena. ***Sisällytä myös eri tasoinen harjoittelu ja testaaminen sopimuksiin.***

Kriittisten ICT-palveluiden tarjouspyynnössä ja palvelusopimusten valmistelussa on huomioitava varautumisvaatimukset ja ***erityistarve toiminnalle "Force Majeure" -tilanteissa***. Tarvittaessa on edellytettävä palvelun toimittaminen vaatimustason mukaisesti myös poikkeustilanteissa.

Vastuumatriisi on yksinkertainen ja tehokas työkalu roolien ja vastuiden dokumentointiin sekä näiden viestintään kaikille osapuolille. Vastuumatriisi auttaa varmistamaan, että kaikki tietävät sekä omat että muiden vastuut, mitä tehtäviä kenellekin kuuluu ja kenen kanssa tehtävät tehdään. Vastuumatriisiin hyödyntämisestä sopimuksissa on tarkemmin Digipoolin julkaisemassa ohjeessa Kyberturva ICT-sopimuksissa – Vältä yleiset karikot.[15]

Huoltovarmuuskeskus on julkaissut ***SOPIVA-suositukset***[16] kumppaniverkoston varautumisen varmistamiseksi sopimuspohjaisesti. Liitteessä 7 on esimerkki sopimusrakenteesta ja varautumisen vaatimuksista.



Kuva 7 Alihankintaketjun läpinäkyvyyden heikkeneminen, lähde: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

15 https://www.huoltovarmuuskeskus.fi/files/b9169115999d78c4a4b16101ddafb60b26e994c5/kyberturva-ict-sopimuksissa.pdf

16 https://www.huoltovarmuuskeskus.fi/sopiva/

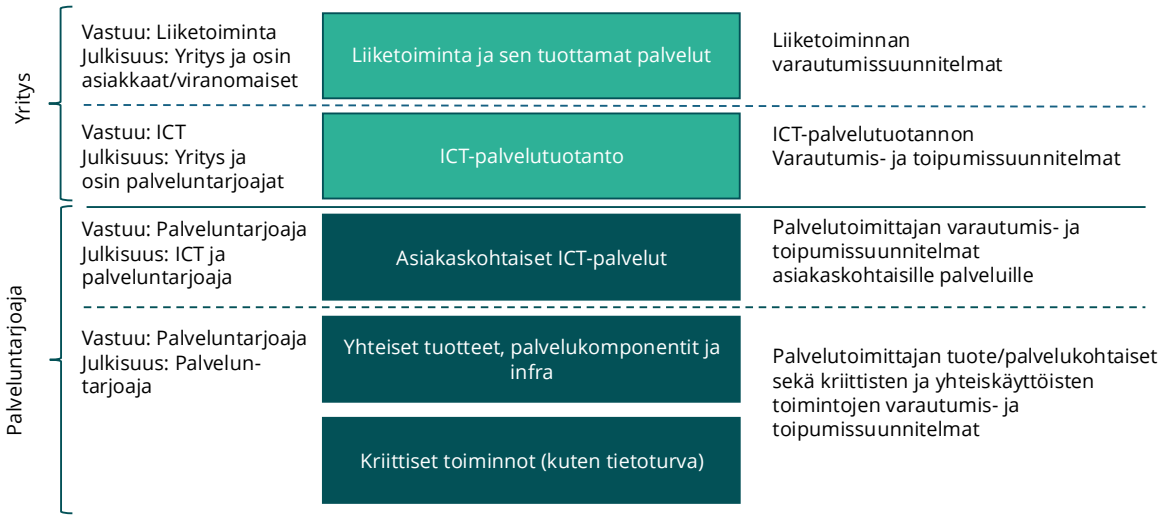
Yhteistyökumppaneiden ja palveluntuottajien varautumisen varmistaminen

Varautumisen vaatimusten välittyminen kriittisille palveluntarjoajille ja koko alihankintaketjulle on varmistettava tarkastamalla, että palveluntuottajien ja yhteistyökumppanien jatkuvuus- varautumis- ja toipumissuunnitelmat ovat yhteensopivia ja vastaavat varautumiselle asetettuja vaatimuksia. Varautumisen vaatimusten täyttyminen on varmistettava myös ulkoistettujen SaaS- ja pilvipalveluiden osalta.

Priorisoitujen toimintojen palvelutoimittajien on kuvattava palveluun tai toimintoon liittyvät toimintamallit ja vastuut häiriötilanteissa. Palvelutuottajalla tulee olla oma jatkuvuuden hallintamallinsa ja varautumissuunnitelma sekä toipumissuunnitelmat (kts. luku 3.14 Palautumisen varmistaminen).

Palveluntarjoajan kanssa on sovitttava ***asiakkaan käyttämiin järjestelmiin ja palveluihin liittyvistä varautumis- ja toipumissuunnitelmista***. Asiakaskohtaiset suunnitelmat ovat lähtökohtaisesti asiakkaan saatavilla (katso kuva 8).

Palveluntarjoajan varautumissuunnitelma ja palvelun tuottamisessa käytettävän infran sekä kriittisten sisäisten toimintojen varautumis- ja toipumissuunnitelmat ovat palveluntarjoajan sisäisiä dokumentteja, jotka kuvaavat miten palveluntarjoaja varmistaa oman toiminnan jatkumisen. Suunnitelmia ei yleensä anneta asiakkaille, mutta varmista suunnitelman olemassaolo ja keskeinen sisältö. Elintärkeiden järjestelmien osalta edellytä mahdollisuutta auditoida suunnitelmat yritystäsi koskevilta osuuksilta esimerkiksi puolueettoman kolmannen osapuolen toimesta. Varmista toipumissuunnitelmien kattavuus ja kaikkien suunnitelmien yhteensopivuus omien suunnitelmien kassa.



Kuva 8 Yrityksen ja ICT-palvelutarjoajan varautumis- ja toipumissuunnitelmat

Kaikkein kriittisimpien järjestelmien osalta tarvittaessa tarkista ja hyväksy menettelytavat ja tekniset ratkaisut hankintavaiheessa, joilla palvelulle määritellyt vakavan häiriötilanteen ja poikkeusolojen varautumisen vaatimukset toteutetaan sekä todenna niiden toteutuminen. Palvelujen toimittaja- ja teknologiavalinnoissa on huomioitava ylläpitopalvelujen ja resurssien sekä varaosien saatavuus häiriötilanteissa ja poikkeusoloissa palvelujen luonteen edellyttämässä laajuudessa.

4 Toiminta vakavassa häiriötilanteessa ja jälkitoimet

Varautumisessa vakaviin häiriötilanteisiin on olennaista luoda ***dokumentoidut ja harjoitellut menettelyt, jotka ohjaavat organisaatioita vastaamaan häiriöön, palautumaan ja jatkamaan toimintaa vaatimusten mukaisella tasolla***:

- Määrittele selkeät vastuut ja organisaatio palvelutuotannossa ja kumppanien kesken. Hyödynnä normaaleja päivittäisiä toimintamalleja mahdollisimman pitkälle.
- Määrittele ja vastuuta keskeiset roolit ja huomioi myös sijaisuudet (kriisin johtaja ja johtoryhmä, tilannekuvasta vastaava, viestinnästä vastaava, häiriönkorjausta ohjaava).
- Määrittele toimintatapa rikosepäilyissä ja selvitä viranomaisten yhteystiedot etukäteen.
- Sovi kriisiorganisaation käynnistymistapa, kokoontumispaikka ja käytettävät viestivälineet.
- Päätä erikseen paluusta normaaliorganisaatioon ja muista häiriön jälkitoimien johtaminen.
- Muista tapahtuma-analyysi tilanteen palauduttua normaaliksi.

4.1 Kriisiorganisaatio ja johtamistoiminta

Palvelutoiminnan varautuminen ja jatkuvuudenhallinta ***sisällytetään osaksi organisaation normaalia johtamista ja toimintaa***. ICT-organisaation ja palvelutoimittajien suunnitelmiin on vähintään kuvattava toiminta vakavissa häiriötilanteissa sisältäen mm. kriisiorganisaation, roolit ja vastuut. Vakavien häiriötilanteiden toimintatavat on oltava dokumentoitu, koulutettu ja harjoiteltu.

Kriisiorganisaatiosta, sen rooleista ja toiminnasta on esimerkki liitteessä 8.

Kyberturvallisuuslain perusteluissa todetaan, että toimijalla tulisi olla dokumentoidut menettelyt toiminnan jatkuvuuden ja häiriötilanteista palautumisen osalta. Jatkuvuus olisi varmistettava ja sen voisi tehdä esimerkiksi ***riskienhallinnan perusteella luodulla jatkuvuussuunnitelmalla sekä toipumissuunnitelmalla***. Suunnitelmat voisivat sisältää esimerkiksi ***olosuhteet***, joissa niiden käyttö aktivoidaan sekä tarvittavia ***rooleja, resursseja, toimenpiteitä ja viestintäkanavia*** koskevat suunnitelmat sekä tarvittavat suojatut varaviestintäjärjestelmät. Suunnitelmien tulisi sisältää ***vähintään kriisinhallintamenettelyt*** erittäin vakavien poikkeamien varalta.

4.2 Häiriön tapahtuma-analyysi ja jälkiarviointi

Tilanteen normalisoiduttua tehdään tapahtuma-analyysi ja jälkiarviointi, jolle on hyvä määritellä aikaraja ja vastuullinen henkilö. Läpikäytäviä asioita ovat ainakin:

- ***Tapahtuman kulku, häiriö ja sen juurisyyt*** (tai juurisyyn selvityksen eteneminen) sekä mahdollisuus tapahtumien ennakointiin jatkossa
- ***Häiriönaikainen toiminta***, onnistumiset ja kehityskohteet, mm.
  - toiminnan käynnistyminen
  - johtaminen ja yhteistyö
  - toimittajien toiminta ja yhteistyö
  - häiriön eristäminen, vahingon minimointi ja toipuminen
  - viestintä
  - teknisen lokitiedon keräys ja kattavuuden varmistaminen
- Mahdolliset ***reklamaatiot*** tai ***sanktiot*** ja ***juridiset seuraukset***
- Tunnistetut ***kehitystehtävät ja toimenpide-ehdotukset***

Läpikäynnistä laaditaan raportti, johon kirjataan kehityskohteet riskin tunnistamisen, todennäköisyyden ja vaikutuksen pienentämiseksi sekä häiriönaikaisen toiminnan kehittämiseksi. Raportti esitellään esimerkiksi ICT-palvelutuotannosta vastaaville sekä yrityksen johtoryhmälle, jotka käsittelevät esitetyt kehityskohteet ja hyväksyvät tarvittavat kehitystoimet sekä suunnitelmien päivitykset.

5 Varautumisen jatkuva kehittäminen, koulutus ja harjoittelu

5.1 Varautumisen organisointi ja kehittäminen

Sisällytä varautuminen osaksi normaalia johtamistoimintaa:

- Liitä varautumisen kehittämisen tehtävät osaksi ICT-palvelutuotannon vuosikelloa.
- Määrittele ja vastuuta varautumisen kehittämisen kannalta keskeiset roolit.
- Laadi varautumiselle mittarit ja seuraa niiden kehitystä säännöllisesti.

ICT-palveluiden varautuminen tulee sisällyttää osaksi normaalia johtamista ja toimintaa sekä kumppaniverkoston hallintaa. Sille on varattava riittävästi resursseja, kuten henkilöstöä ja rahaa, jotta varautumisen vaatimukset voidaan täyttää. Varautumisen hallinnan toimenpiteet (kts. kuva 9) sisällytetään ICT-palvelutuotannon vuosikelloon ja sovitetaan yhteen yrityksen riskien- ja jatkuvuudenhallintajärjestelmän kanssa.

Kuva 9 Esimerkki ICT-palvelutuotannon varautumisen vuosikellosta

Tietohallinnon ja palvelutuotannon johto vastaa oman vastuualueensa varautumisen suunnittelusta ja toteutuksesta asetettujen vaatimusten mukaisesti. Jatkuvuudenhallinta toteutetaan yhteistyössä liiketoiminnan kanssa ja osana yrityksen varautumista. Varautumisen ja jatkuvuudenhallinnan kehittämiseen ja johtamiseen on hyvä nimetä vastuuhenkilö, jolle varataan riittävästi aikaa asioiden edistämiseen. Lisäksi riskienhallinta ja varautuminen tulee sisällyttää kaikkien osa-alueiden vastuuhenkilöiden tehtäviin. Huomioi resurssoinnissa ainakin seuraavat ***ICT-palvelutuotannon varautumisen roolit*** (joita yhdellä henkilöllä voi olla useita):

- ***Varautumisesta ja jatkuvuudenhallinnasta vastaava***, jonka tehtävänä on varmistaa varotoimien eteneminen sekä varmistaa vuosikellon mukaisten tehtävien hoitaminen. Lisäksi henkilö vastaa varautumiseen liittyvästä raportoinnista ICT-palvelutuotannon johdolle ja kokonaisuutena eri suunnitelmien yhteensovittamisesta.

- ***Toimintaympäristön ja tilannekuvan seurannasta vastaava.***
- ***Uhkien tunnistamisesta ja riskienhallinnasta vastaava.***
- ***ICT-palveluntuottajien yhteyshenkilö*** varautumiseen ja sen kehittämiseen liittyvissä asioissa, jonka tehtäviin kuuluu myös palveluntuottajien varautumisen tason ja suunnitelmien yhteensopivuuden varmistaminen.
- ***Eri osa-alueiden vastuuhenkilöiden*** (tietoturva, alustat ja arkkitehtuuri, tietoliikenne, järjestelmien vastuuhenkilöt, tilat, toiminnot) tehtäviin ja vastuisiin sisällytetty ***oman osa-alueen varautumisen*** suunnittelu ja toimenpiteiden toteutus.
- ***Yhteyshenkilöt liiketoiminnoille***, jotka varmistavat liiketoiminnan kriittisten palveluiden varautumisen vaatimusten välittymisen ICT-palvelutuotannolle ja tekevät varautumiseen liittyvää suunnittelua yhdessä liiketoimintojen edustajien kanssa.

ICT-palvelutuotannon varautumiselle ***laaditaan mittarit*** ja niiden toteutumista seurataan ja raportoidaan säännöllisesti yrityksen johdolle. Mittareita voivat olla mm.

- ***Suunnitelmien kattavuus:*** kuinka suuren osan suunnitelmat kattavat yrityksen kriittisistä palveluista ja toiminnoista, ICT-palvelutuotannon prosesseista, järjestelmistä ja infrastruktuurista.
- ***Harjoitusten ja testien kattavuus:*** kuinka suuren osan toteutetut harjoitukset kattavat kriittisistä palveluista ja toiminnoista, henkilöstöstä, prosesseista, järjestelmistä, tunnistetuista uhkaskenaarioista jne. sekä harjoitusten ja testien määrä.
- ***Testien onnistumisprosentti*** ja taso (esim. palautusten testaukset ja niiden onnistumisprosentti).
- ***Henkilöstön perehdytyksen ja koulutuksen kattavuus.***
- Varautumisen toimenpiteiden ***vaikuttavuusarvio.***

Huoltovarmuuskeskus on tehnyt yrityksen varautumisen tilanteen arviointiin työkaluja (mm. Huoltovarmuuskeskuksen Extranetistä löytyvä Kypsyysanalyysi). Lisäksi jatkuvuudenhallinnan standardin ISO 22301 vaatimukset ja sertifikaatti voivat toimia varautumisen mittareina.

Vuosikellon mukainen kehittäminen pohjautuu PDCA-malliin. ***ISO 22301:n jatkuvuudenhallintaan sovitettu PDCA-malli*** (Plan, Do, Check, Act) luo raamin jatkuvuuden hallinnalle.

PLAN / ESTABLISH (Luodaan): Luodaan liiketoiminnan jatkuvuutta koskevat toimintaperiaatteet, tavoitteet, päämäärät, valvontatoimet, prosessit ja menettelyt liiketoiminnan jatkuvuuden parantamiseen (jotta saavutetaan organisaation yleisten toimintaperiaatteiden ja tavoitteiden mukaisia tuloksia).

DO (Toteuta): Toteutetaan määriteltyjä politiikkoja, toimintamalleja/prosesseja ja valvontakäytäntöjä.

CHECK (seuraa ja varmista): Seurataan ja tarkastellaan toteumaa liiketoiminnan jatkuvuuden tavoitteisiin ja toimintamalleihin nähden, raportoidaan tulokset johdolle sekä määritetään ja hyväksytään korjaus- ja kehitystoimet. Harjoitellaan suunnitelmien mukaista toimintaa ja kootaan harjoituksessa havaitut kehitystarpeet toimenpiteitä varten.

ACT (Ylläpito ja kehittäminen): Ylläpidetään ja kehitetään toteuttamalla korjaavia toimia havaintojen perusteella ja arvioimalla uudelleen kehystä, suunnitelmia ja jatkuvuuden tavoitteita.

5.2 Koulutus ja harjoittelu

Kouluta varautumissuunnitelman mukaiset toimintamallit ja harjoittele säännöllisesti:

- Varmista henkilökohtainen osaaminen ja toiminta.
- Harjoittele organisaation toimintaa häiriötilanteessa ja kriisinjohtamista.
- Harjoittele yhteistyötä yrityksen sisällä ja palveluntarjoajien sekä sidosryhmien kanssa.
- Tee harjoitussuunnitelma ja varmista sen kattavuus henkilöstön, organisaation, kriittisten toimintojen ja niihin liittyvien järjestelmien sekä palveluntarjoajien ja yhteistyötahojen osalta.
- Osallistu toimialatasoisiin, alueellisiin tai valtakunnallisiin harjoituksiin.
- Huomioi harjoitukset ICT-palvelutuottajien kanssa tehtävissä sopimuksissa.

ICT-palvelutuotannon organisaatiolle, johdolle ja muille toimijoille on ***koulutettava*** yrityksen ja palvelutuotannon toimintojen ***varautumisen toiminnot sekä harjoiteltava niitä säännöllisesti***. Koulutus on osa henkilöiden perehdytystä ja tehdään aina tehtävien vaihtuessa sekä suunnitelmien tai ohjeistusten päivittyessä. Koulutuksen sisältö ja tavoitteet on määritettävä vastuualueiden mukaisesti. Koulutuksella ja harjoituksilla varmistetaan yksilöiden kyvykkyys, organisaation toimintakyky ja yhteistoiminta kumppaneiden ja yhteistyötahojen kanssa vakavassa häiriötilanteessa.

Johdon osalta koulutuksen ja harjoitusten pääpaino on riskienhallinnassa ja johtamisessa sekä viestinnässä. Lisäksi palvelutuotannon johdon on oltava perehtynyt yritystason varautumissuunnitelman mukaiseen toimintaan.

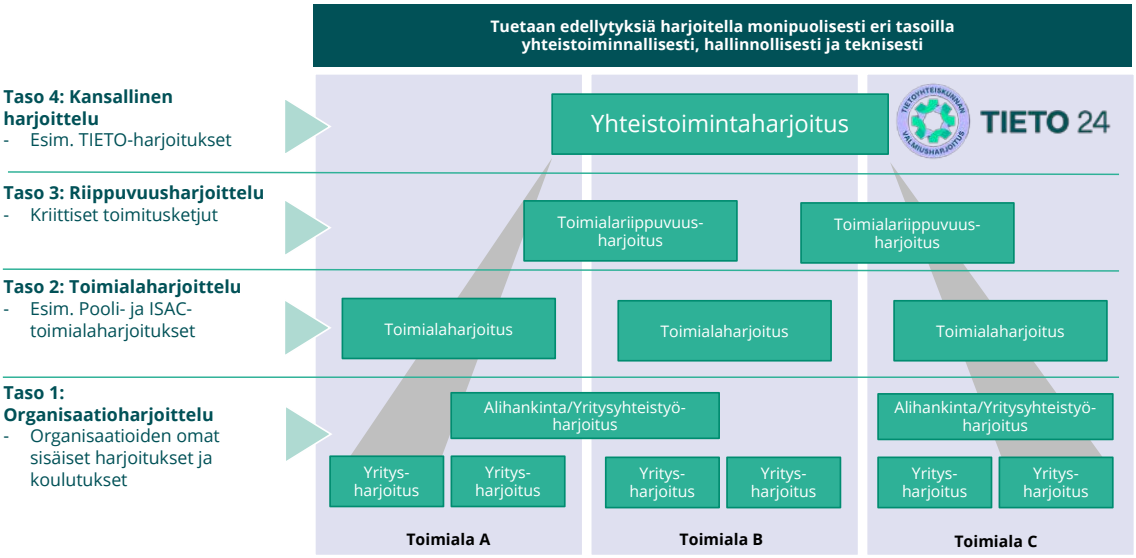
Palvelutuotannon organisaatioon kuuluvilla ja toipumissuunnitelmista vastaavilla yksityiskohtaisempi koulutus määräytyy tehtävien perusteella ja perustuu ohjeistuksen sekä suunnitelmien läpikäyntiin. Suunnitelmien toimivuus testataan määrävälein erilaisissa harjoituksissa.

Harjoitukset ovat osa henkilöstön koulutusta ja ne parantavat organisaation toimintakykyä poikkeustilanteissa. Harjoitussuunnitelma laaditaan usealle vuodelle ja siinä huomioidaan erityyppiset harjoitukset ja testit sekä varmistetaan niiden kattavuus ainakin uhkaskenaarioiden, kriittisten palveluiden, toimintojen, järjestelmien ja henkilöstön osalta. Erityyppisiä harjoituksia ovat mm.

- ***Työpöytäharjoitukset*** roolien ja toimintatapojen läpikäyntiin tai esimerkiksi valmistautumisena toiminnallisiin kriisinjohtamisharjoituksiin.
- ***Toiminnalliset kriisinjohtamisharjoitukset (CME Crisis Management Exercise)*** kriisin johtamisen ja häiriötilanteen hallitsemisen sekä viestinnän harjoittelemiseen
- ***Tekniset testit***, kuten varmuuskopioiden palauttamiset ja kattavammat toipumissuunnitelmien testaukset.

Harjoituksia tulee toteuttaa eri tasoisina ja laajuisina kuten yksittäisten henkilöiden harjoittamisena, teknisinä palautumis- ja toipumistoimenpiteiden testaamisena sekä organisaation eri yksiköiden sisäisinä ja yhteisinä harjoituksina. Lisäksi huoltovarmuuskriittisten organisaatioiden tulee osallistua toimialatasoisiin, riippuvuus- ja toimitusketjujen sekä kansallisiin harjoituksiin harjoitustoiminnan tavoitekehyksen mukaisesti (kts. kuva 10)

HARJOITUSTOIMINNAN TAVOITEKEHYS



Kuva 10 Harjoitustoiminnan tavoitekehys, Digipooli

Harjoitukset dokumentoidaan ja keskeiset havainnot ja parannusehdotukset kirjataan jatkosuunnittelua ja toteutusta varten. Jatkotoimenpiteiden valmistelu vastuutetaan ja hyväksytyt uudet toimintamallit liitetään osaksi varautumissuunnitelmaa vuosikellon tehtävien mukaisesti.

Harjoitusten ja testausten tulokset ovat perustana varautumisen arvioinnille ja ylläpidolle. Kriittisimpien palvelutoimittajien varautumisen taso ja todellinen kyvykkyys toimia poikkeustilanteissa todennetaan säännöllisesti palvelutoimittajien kanssa toteutettavilla yhteisillä harjoituksilla.

Harjoittelussa on hyvä hyödyntää yrityskohtaisten harjoituksen lisäksi olemassa olevia harjoituskehyksiä (kuten ***TIETO-harjoituksia***) sekä olemassa olevia teknisiä harjoitusympäristöjä (mm. Jyväskylän ammattikorkeakoulun kyberturvallisuuden ja tekoälyn tutkimuskeskuksen ***JYVSECTEC***:in ylläpitämä harjoitusympäristö, jossa myös tehdään tutkimusta).

6 Ulkoiset vaatimukset ICT-palvelutuotannon varautumiselle

Tunnista mitkä lait, asetukset tai toimialaa koskevat erityisvaatimukset koskevat yrityksesi kriittisiä toimintoja:

- Huomioi asiakkaita ja omaa toimintaa ohjaavat lait, asetukset ja määräykset.
- Huomioi myös poikkeusolojen vaatimukset ja muuttuva ympäristö.

Tämä kappale erittelee ulkoisia asioita, joita tulee huomioida ICT-palvelutuotannon varautumisessa. Huoltovarmuusorganisaatiossa oletetaan, että yritykset ovat käsitelleet ja huomioineet sekä dokumentoineet ulkoiset vaatimukset ICT-palvelutuotannon varautumisessa.

Suomessa varautuminen huoltovarmuuden osalta perustuu pitkälti yritysten vapaaehtoisuuteen. Lainsäädäntö asettaa joillekin kriittisille toimialoille, kuten energia- ja terveydenhuoltoalalle, tarkempia vaatimuksia, mutta useimmissa tapauksissa yritysten oma-aloitteinen suunnittelu on avainasemassa. Oletuksena on, että yritysten johto määrittelee tarvittavan varautumisen ja varmistaa sen toteutumisen.

Tunnista mitkä lait, asetukset tai toimialaa koskevat erityisvaatimukset koskevat yrityksesi kriittisiä toimintoja. Huomaa, että lainsäädäntö, viranomaisohjeistukset ja toimialan standardit voivat asettaa vaatimuksia tietojen käsittelylle ja toipumiselle häiriötilanteista.

Asiakkaiden varautumisen vaatimukset

Asiakkaita ohjaava lainsäädäntö vaikuttaa myös oleellisesti yrityksen toimintaan kohdistuviin vaatimuksiin. Asiakkaiden vaatimukset on huomioitava sopimuksissa ja edelleen vaatimuksina palvelutuotannolle. Tunnistetut vaatimukset tulee huomioida jo palvelukehityksessä. ICT-palvelutuotannon on varmistettava, että se pystyy vastaamaan yrityksen asiakkaiden tarpeisiin suunnittelemalla ja toteuttamalla vaatimukset täyttävät tekniset ja toiminnalliset ratkaisut. Esimerkiksi tieto- ja viestintätekniikan, finanssi-, energia- ja terveydenhuoltosektoreilla on häiriönsietokykyyn liittyviä vaatimuksia, jotka on myös palveluntarjoajien täytettävä.

Lait, asetukset ja viranomaismääräykset

Kaikkia toimialoja koskevia suoraan ICT-palvelutuotantoon liittyviä viranomaismääräyksiä ja asetuksia on vähän. NIS2-direktiivin toteuttava Laki kyberturvallisuuden riskienhallinnasta[17] koskettaa valtaosaa huoltovarmuuskriittisiä yrityksiä ja edellyttää ICT-toimintojen kattavaa riskien hallintaa ja jatkuvuuden varmistamista. Toimenpiteet on suhteutettava mm. poikkeamasta johtuviin ennakoitavissa oleviin välittömiin vaikutuksiin, järjestelmien riskialttiuteen, riskien todennäköisyyteen ja vakavauuteen sekä teknisiin mahdollisuuksiin torjua uhka.

Useimmat ICT-palvelutuotannon ulkoiset varautumisvaatimukset tulevat yrityksen tai yrityksen asiakkaiden kriittisten palveluiden häiriönsietokykyyn kohdistuvien lakien ja asetusten kautta (esimerkiksi Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta[18]). Osa määräyksistä on toimialakohtaisia säädöksiä ja kohdistuvat myös ICT-palveluihin. Vaikka vaatimukset ovat vain tietylle sektorille, niin ne toimivat hyvinä suosituksina kaikille toimialoille. Toimialan suositukset eivät ole sitovia määräyksiä, mutta tietyillä toimialoilla tehtävä valvonta edellyttää, että yritysten on läpäistävä valvovan viranomaisen tarkastukset. Mikäli suosituksia ei ole noudatettu, yritys joutuu hyväksytysti perustelemaan valintansa.

Esimerkkejä toimialakohtaisista, toimialan yrityksiä koskevista ja niiden ICT:hen kohdistuvista vaatimuksista:

- Laki sähköisen viestinnän palveluista ja Traficomin määräykset asettavat vaatimuksia mm. teleyrityksille viestintäverkkoihin liittyen.[19]
- DORA-asetus (Digital Operational Resilience Act) velvoittaa finanssialan yrityksiä varmistamaan digitaalisen toiminnan häiriönsietokyvyn.[20]

17 Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_57+2024.aspx?TSPD_101_R0=0814c91602ab200043d68f1fd8170b7fc20b1b8e234d01384872176ebe95900ae4af299b2dcbbd4308ca7457811430005c6b2efd4b5e38317f37d06a3acfdb19a5cbb88f19be87e1c0247bff8f6f1abe0e4d4ec8ba412321593b0edeb31b72e4

18 https://valtioneuvosto.fi/hanke?tunnus=SM047:00/2022

19 https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

20 https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

- Sähkö- ja maakaasuverkonhaltijoiden on laadittava varautumissuunnitelma, ja lisäksi toimijoiden on huolehdittava viestintäverkkojensa ja tietojärjestelmiensä riskien hallinnasta.[21]

Laki huoltovarmuuden turvaamisesta

Huoltovarmuuden turvaamisesta annetun lain (1390/1992)[22] 1 §:n mukaan huoltovarmuudella tarkoitetaan kykyä turvata poikkeusolojen ja niihin verrattavissa olevien vakavien häiriöiden varalta väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömät taloudelliset toiminnot ja niihin liittyvät tekniset järjestelmät.

Lain 2 §:n mukaan Valtioneuvosto asettaa huoltovarmuudelle yleiset tavoitteet, joissa määritellään valmiuden taso ottaen huomioon väestön ja välttämättömän talouselämän sekä maanpuolustuksen vähimmäistarpeet.

Lain 5 §:n 1 momentin mukaan huoltovarmuuden kehittämistä ja ylläpitoa varten on Huoltovarmuuskeskus (HVK), jonka yhteydessä toimii Huoltovarmuusorganisaatio, jonka pysyvinä yhteistoimintaeliminä komitean tapaan toimivia sektoreita ja pooleja. Poolit ovat viranomaisten ja yrityksen vapaaehtoinen yhteistyöelin, jonka roolina on varmistaa valtakunnan eri toimintojen toimintavalmius normaalioloissa, normaaliolojen vakavissa häiriöissä ja poikkeusoloissa.

Edelleen lain 8 e §:ssä todetaan, että HVK:lla, sektoreilla ja pooleilla on oikeus saada elinkeinonharjoittajilta ja elinkeinoelämän järjestöiltä tietoja tuotantokapasiteetista, toimitiloista, henkilöstöresursseista sekä muista seikoista, jotka ovat välttämättömiä laissa säädettyjen tehtävien hoitamiseksi. Lain nojalla saatuihin tietoihin sovelletaan mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään asiakirjasalaisuudesta sekä vaitiolovelvollisuudesta ja hyväksikäyttökiellosta. Poolien tehtävistä ja organisaatiosta sekä toiminnan suunnittelusta ja rahoituksesta on määrätty yleisesti HVK:n työjärjestyksessä ja taloussäännössä.

Valtioneuvoston päätös huoltovarmuuden tavoitteista 2024

Valtioneuvoston päätös huoltovarmuuden tavoitteista käsittelee Suomen muuttunutta turvallisuusympäristöä ja sen vaikutuksia huoltovarmuuteen. Huoltovarmuuden tavoitepäätöksen lähtökohtana on Suomen muuttunut turvallisuusympäristö, joka heijastuu myös huoltovarmuustoimintaan. Uudet ja vahvistuneet uhat edellyttävät, että huoltovarmuuden turvaamisen ja varautumisen tasoa vahvistetaan

Päätöksessä korostetaan kansallista ja kansainvälistä yhteistyötä, kriittisen infrastruktuurin suojaamista sekä eri toimijoiden välistä yhteistyötä huoltovarmuuden turvaamiseksi. Digitaalisen infrastruktuurin ja tietovarantojen turvaaminen sekä kyberturvallisuuden kehittäminen ovat tärkeitä huoltovarmuuden tavoitteita.

Huoltovarmuuskeskus vastaa huoltovarmuusrahaston kantokyvyn arvioinnista ja varmistamisesta sekä tukee kriittisiä yrityksiä varautumissuunnittelussa ja toiminnan turvaamisessa.

Valmiuslaki ja Puolustustilalaki

Valmiuslaki[23] antaa viranomaisille oikeuden asettaa kriittisille yrityksille lisävelvollisuuksia, kuten lisäraportointivaatimuksia tai toiminnan rajoituksia. *Puolustustilalaki*[24] puolestaan laajentaa viranomaisten toimivaltuuksia poikkeusolojen aikana.

Normaaliolojen lainsäädäntö on voimassa ja ohjaa toimintaa myös poikkeusolojen aikana. Valmius- ja Puolustustilalakien voimaantulo kuitenkin vaikuttaa yrityksen toimintaympäristöön. Erityisesti huoltovarmuuden turvaamiseksi ja poikkeusolojen aikaisen toiminnan varmistamiseksi yrityksen on varautumisessa huomioitava Valmius- ja Puolustustilalain perusteella muuttuva toimintaympäristö, kasvava riskitaso sekä kyettävä nostamaan omaa valmiustasoaan tilanteen mukaisesti.

21 https://energiavirasto.fi/varautuminen-ja-tietoturva

22 https://www.finlex.fi/fi/laki/ajantasa/1992/19921390

23 https://www.finlex.fi/fi/laki/ajantasa/2011/20111552

24 https://www.finlex.fi/fi/laki/ajantasa/1991/19911083?search%5Btype%5D=pika&search%5Bpika%5D=puolustustilalaki

7 Loppusanat

Erityisesti Huoltovarmuusorganisaatioon kuuluvan yrityksen on tärkeät panostaa ICT-palvelutuotantonsa varautumiseen ja kehittää siihen liittyviä suunnitelmia ja käytäntöjä. Varautumiseen liittyviä keskeisiä asioita ovat tietoturva ja tietosuoja, toiminnan jatkuvuus, varajärjestelmät ja -menettelyt, henkilöstön osaaminen sekä yhteistyöverkostot. Näiden avulla yritys voi varmistaa, että sen toiminta on resilienttiä ja kykenee vastaamaan sekä normaaliolojen että poikkeusolojen haasteisiin, turvaten yhteiskunnan ja yrityksen kriittiset palvelut. On tärkeää, että yritykset jatkuvasti arvioivat ja päivittävät varautumissuunnitelmiaan, jotta ne pysyvät ajan tasalla muuttuvien uhkakuvien ja toimintaympäristön vaatimusten kanssa. Varautuminen ei ole kertaluonteinen projekti, vaan jatkuva prosessi, joka vaatii sitoutumista ja resursseja yrityksen kaikilta tasoilta. ***Kehitä varautumista pitkäjänteisesti, aloita kaikkein kriittisimmistä palveluista ja niihin liittyvistä kriittisimmistä järjestelmistä ja tiedosta.*** Laajenna varautumissuunnitelmaa ja varotoimenpiteitä kattamaan kaikki kriittiset palvelut ja niihin liittyvät kriittiset tuotannontekijät.

Varautuminen ei myöskään ole vain tekninen prosessi, vaan se on myös kulttuurin ja asenteiden muokkaamista niin, että koko organisaatio sekä sidosryhmät ymmärtävät toimintavarmuuden ja jatkuvuuden merkityksen. Hyvin suunnitellut ja harjoitellut varautumistoimenpiteet voivat olla ratkaisevia, kun häiriötilanne iskee. Ne voivat säästää aikaa, resursseja ja ennen kaikkea turvata liiketoiminnan jatkuvuuden ja maineen sekä yhteiskunnalle kriittisten palveluiden toiminnan.

Yritysten koosta riippumatta varautuminen on tärkeää ja varautumisen toimenpiteet voidaan sopeuttaa yrityksen koon sekä tunnistettujen riskien mukaan. Hyvin järjestettynä varautuminen on osa päivittäisiä toimintoja ja auttaa tehokkaasti varmistamaan toiminnan jatkuvuuden kaikissa tilanteissa.

Mahdolliset kysymykset ohjeen sisältämiin tai ohjeesta puuttuviin aiheisiin voi lähettää sähköpostilla osoitteeseen digipooli@teknologiateollisuus.fi

LIITE 1

Varautuminen ja varautumissuunnitelma

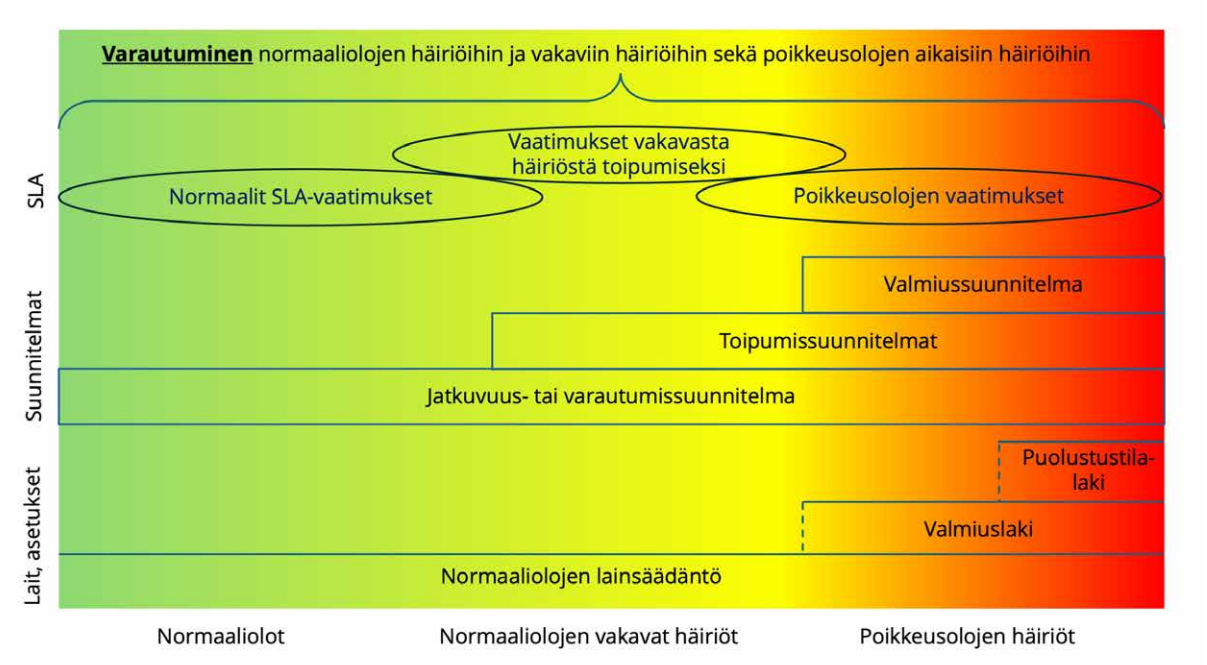
Varautuminen tarkoittaa toimenpiteitä, joilla pyritään varmistamaan kriittisten toimintojen mahdollisimman häiriötön hoitaminen kaikissa olosuhteissa, niin normaali- kuin poikkeusoloissa. Varautumisen ja jatkuvuussuunnittelun tärkeimmät tavoitteet ovat vakavien häiriötilanteiden vaikutusten minimoiminen, kriittisten palveluiden tuottaminen vaaditulla vähimmäistasolla sekä palveluiden palauttaminen normaalitasolle mahdollisimman nopeasti. Laajempi huoltovarmuuteen liittyvä sanasto on nähtävillä Huoltovarmuusorganisaation sivuilla (https://www.huoltovarmuuskeskus.fi/sanasto#v).

Varautumistoimenpiteitä ovat muun muassa riskienarviointi, jatkuvuus- ja valmiussuunnittelu, tekniset ja rakenteelliset ennakkovalmistelut ja ratkaisut, koulutus, harjoitukset sekä tilojen ja kriittisten resurssien varaukset. Varautuminen käsittää kokonaisvaltaisesti suunnittelun, käytännön toimenpiteiden toteutuksen ja kehittämisen, sekä koulutuksen ja harjoittelun.

Tyypilliset varautumiseen liittyvät suunnitelmat ovat:

- Varautumis- tai jatkuvuussuunnitelma, joka sisältää toimenpiteet, joilla varmistetaan yrityksen toiminnan jatkuvuus normaali- ja poikkeusoloissa
- Erilaisten häiriötilanteiden toipumissuunnitelmat tarkentavat varautumissuunnitelmaa yksityiskohtaisilla toimenpiteillä toiminnan palauttamiseksi normaaliksi.
- Mahdolliset valmiuslain asettamat vaatimukset ja tehtävät on kuvattu valmiussuunnitelmassa.

Varautumis- ja jatkuvuussuunnitelmat, samoin kuin toipumissuunnitelmat, ovat vähintään kaikkien häiriötilanteiden hoitoon osallistuvien käytettävissä, mutta valmiussuunnitelman jakelu on rajattu. Kuvassa 1 on esitetty varautumisen kattavuus, eri suunnitelmat sekä niiden suhde toimintaympäristöön vaikuttavaan voimassa olevaan lainsäädäntöön ja eritasoisiin häiriötilanteisiin.



Kuva 1 Varautuminen, palveltutasot, suunnitelmat ja toimintaympäristö eri tilanteissa

Varautumisen ja jatkuvuussuunnittelun hyödyt

Varautuminen ja liiketoiminnan jatkuvuussuunnittelun ensisijainen hyöty on riskienhallinta: suunnittelu tunnistaa ja analysoi keskeiset liiketoimintariskit, kuten teknologiset häiriöt ja toimitusketjuongelmat, ja tarjoaa keinoja niiden ehkäisemiseksi ja vaikutusten minimoimiseksi. Tämä vähentää merkittävästi keskeytyksistä aiheutuvia taloudellisia tappioita ja mahdollisuuden toiminnan jatkamiselle niin normaalioljen kuin poikkeusolojen häiriötilanteissa. Jatkuvuussuunnittelu lisää myös sidosryhmien, kuten asiakkaiden ja sijoittajien, luottamusta yritykseen, sillä se osoittaa yrityksen varautuneen uhkiin ja kyvyn reagoida niihin tehokkaasti *. Lisäksi suunnittelu auttaa varmistamaan, että yritys noudattaa alan sääntelyvaatimuksia ja standardeja, mikä vähentää juridisia riskejä ja voi tuoda kilpailuetua muihin markkinatoimijoihin verrattuna. Taloudellisten tappioiden minimoinnin lisäksi yritys suojelee mainettaan, sillä nopea ja hallittu reagointi kriiseihin vahvistaa sen asemaa luotettavana toimijana. Varautumisen ja jatkuvuussuunnittelun avulla yritys voi parantaa kykyään selviytyä ja jopa hyötyä kilpailijoiden heikkouksista kriisitilanteissa, jolloin se vahvistaa asemaansa markkinoilla. **

Varautuminen on keskeinen osa *yrityksen yhteiskuntavastuuta*. Yritys, joka panostaa varautumiseen, ei ainoastaan suojaa omaa toimintaansa ja sidosryhmiään, vaan tukee samalla kriittisten julkisten palveluiden jatkuvuutta. Huoltovarmuuskriittisillä yrityksillä on keskeinen rooli näiden palveluiden ylläpidossa ja varautumisessa, ja ne tukevat näin yhteiskunnan vakauden ja toimintakyvyn säilymistä kriisitilanteissa.

* 2023 tehdyn kyselyn perusltella jatkuvuussuunnittelu on yrityksille enemmän strateginen investointi kuin vaatimuksenmukaisuuden takia tehtävä panostus. (https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html)

** Aikanaan Nokian ja Ericssonin puhelimiin komponentteja valmistavalla Philipsin puolijohdekomponenttitehtaalla oli tulipalo, joka saatiin nopeasti hallintaan ja Philips arvioi toimintaan tulevan kuuden päivän katkos. Nokialla oli ennalta luotu prosessi ja suunnitelmat komponenttivirtojen tarkkailemiseen ja Nokia havaitsi nopeasti, ettei Philipsin komponenttien toimittaminen tule normalisoitumaan kuudessa päivässä. Philipsin tavarantoimitus normalisoitui kuudessa viikossa. Ericssonilla ei ollut ennalta luotuja valvontaprosesseja eikä varasuunnitelmaa. Nopean reagoinnin takia Nokia ehti saamaan Philipsin resurssit itselleen komponenttien toimituksen varmistamiseksi. Ericsson puolestaan vähätteli pienen tulipalon vaikutuksia tuotantoon. Tapauksen jälkeen Nokian tuotto kasvoi vuosineljänneksellä 42 % ja Ericsson lopulta lopetti itsenäisen matkapuhelinvalmistuksen.

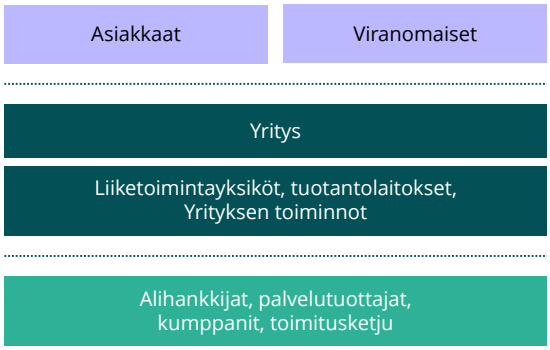
Esimerkiksi ***Kyberturvallisuuslain*** perusteluissa todetaan, että yrityksellä on oltava dokumentoidut menettelytavat toiminnan jatkuvuuden varmistamiseksi ja häiriötilanteista palautumiseksi. Jatkuvuus tulee varmistaa esim. riskienhallinnan perusteella luodulla ***jatkuvuussuunnitelmalla sekä toipumissuunnitelmilla***. Suunnitelmien tulee sisältää vähintään kriisinhallintamenettelytavat erittäin vakavien poikkeamien varalta. Riskienhallinnan mukaisesti suunnitelmia tulee ylläpitää ja kehittää säännöllisesti sekä niiden mukaista toimintaa harjoitella.

Samoin ***Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta*** edellyttää, että yhteiskunnan kannalta kriittisen toimijan on laadittava asianmukaisia ja oikeasuhtaisia teknisiä, turvallisuuteen liittyviä ja organisatorisia toimenpiteitä sisältävä ***suunnitelma häiriönsietokyvyn varmistamiseksi.***

Varautumissuunnitelma

Yrityksen varautumissuunnitelma kattaa kaikki kriittiset toiminnot ja voi muodostua yritystasolla määritellyistä toimenpiteistä ja eri yksiköiden omista jatkuvuussuunnitelmista. ***Yritystasolla määritellään koko organisaatiota koskevat varautumiskäytännöt ja toimintamallit, joilla varmistetaan kokonaisvaltainen varautuminen ja tehokas toiminta kriisien aikana.*** Yritystasolla määritellään vähintään:

- Varautumisen tavoitteet ja toimintamallit
- Yrityksen kriisiorganisaatio ja sen johtaminen ml. roolit ja vastuut
- Yritystason tilannekuvan ylläpitäminen ja raportointi
- Kriisiviestintä
- Jatkuvuudenhallinnan ja varautumisen hallintamalli sekä kehittäminen
- Riskienhallintamalli ja -käytännöt
- Eri osapuolten ja sidosryhmien suunnitelmat, niiden yhteensopivuus ja kattavuus kokonaisuutena sekä eri tasoisten suunnitelmien yhteensovittaminen (esimerkiksi ICT-palveluntuottajat, asiakkaat ja viranomaiset).
- Yleiset ja toimialakohtaiset määräykset sekä asiakkaiden asettamat vaatimukset



Kuva 2 Yhteensovitettavat varautumisen vaatimukset ja suunnitelmat

Yrityksen, palveluntuottajien (kuten ICT-palveluntuottajien), viranomaisten ja mahdollisten asiakkaiden ***varautumis- ja toipumissuunnitelmien yhteensopivuus, yhdenmukaisuus ja kattavuus on varmistettava kokonaisuutena*** esimerkiksi seuraavilla tavoilla:

1. ***Varmista varautumissuunnitelman suunnittelun ja ylläpidon kokonaisvaltainen prosessi:*** Kartoita huomioitavat lait ja asetukset sekä sidosryhmät, joiden suunnitelmat ja vaatimukset on huomioitava.
2. ***Sopimukset ja velvoitteet:*** Varmista asiakkaiden varautumisen vaatimukset ja niiden sisällyttäminen sopimuksiin ja palvelukuvauksiin. Varmista vaatimusten välittyminen ICT-palvelutuottajien sopimuksiin.
3. ***Roolien ja vastuiden läpikäynti:*** Varmista yhteinen ymmärrys vaatimuksista, sopimusten sisällöstä, rooleista ja vastuista esimerkiksi RACI- tai RAS-CI-matriisien avulla.
4. ***Yhteistyö ja kommunikaatio:*** Sisällytä vaatimusten ja suunnitelmien läpikäynti säännöllisiin sidosryhmätapaamisiin. Tapaamiset varmistavat, että kaikki osapuolet ovat tietoisia suunnitelmien päivityksistä, toimintatavoista ja riskienhallinnasta. Kommunikointikanavien ja roolitusten tarkistaminen etukäteen parantaa reagointikykyä.
5. ***Yhdenmukaistaminen ja standardit:*** Käytä jatkuvuudenhallinnan standardia ISO 22301 tai muita vastaavia viitekehyksiä luomaan yhtenäisyyttä eri suunnitelmien välillä.
6. ***Testaaminen ja arviointi:*** Yhteiset harjoitukset eri sidosryhmien kanssa antavat realistisen käsityksen suunnitelmien kattavuudesta ja havainnollistavat mahdollisia kehityskohteita.

LIITE 2

Esimerkki – Liiketoiminnan vaatimusanalyysi (BIA) ja riskiarvio

Liiketoiminnan vaikutusanalyysi (BIA Business Impact Analysis) auttaa arvioimaan erilaisten keskeytysten vaikutuksia. Analyysi on ajallisesti jaksotettu ja arvioinnissa huomioidaan häiriön pituus. BIAn avulla tunnistetaan toiminnan jatkuvuutta uhkaavat riskit, priorisoidaan eri toiminnot sekä selvitetään niiden väliset riippuvuudet. Analyysin perusteella toiminnot luokitellaan kriittisyysluokkiin. Kriittisten toimintojen luokitteluun on myös olemassa työkaluja kuten *VAHTI-ohje Kriittisten kohteiden luokittelu*[1].

Vaikutusanalyysin päätavoitteena on selvittää kriittisten palveluiden kannalta mitkä toiminnot ovat tärkeitä, mikä palvelutaso on välttämätöntä säilyttää häiriöiden aikana ja millä aikavälillä häiriön vaikutukset on poistettava. Toimintoihin liitetään tieto, järjestelmät, laitteet ja käyttäjät. Näiden perusteella määritellään vaatimukset prosessien, toimintojen ja järjestelmien varautumiselle sekä suojaustarve.

Lisätietoa liiketoiminnan vaatimusanalyysistä mm.:

ISO 22301:2019 – Security and resilience – Business continuity management systems standardi tarjoaa yksityiskohtaisia ohjeita liiketoiminnan jatkuvuuden hallinnasta, mukaan lukien parhaita käytäntöjä ja vaatimuksia BIA:n toteutukseen yrityksissä.

NIST SP 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems sisältää myös yksityiskohtaisia tietoja siitä, kuinka suorittaa liiketoiminnan vaikutusanalyysi (BIA) erityisesti ICT-palveluiden ja tietojärjestelmien varautumisessa.

Vaatimusanalyysi voidaan suorittaa eri tavoin. Yksi helppo tapa on lähteä liikkeelle yrityksen palveluiden kriittisyyden analysoinnilla ja porautua asteittain mm. järjestelmä- ja tietotasolle.

Ennen arvioinnin aloittamista on tehtävä kriittisyysluokittelu. Mahdollisuuksien mukaan kannattaa käyttää samaa luokittelua kuin yrityksen riskiarvioinneissa. Arvioi palveluiden kriittisyys sekä yhteiskunnan että yrityksen kannalta. Käytä tarvittaessa apuna eri näkökulmia kriittisyysarvioinnin tukena.

Arvioinnin vaiheet:

1. ***Määrittele kriteerit*** häiriöiden vaikutusten vakavuuden arvioimiseksi. Määrittele myös mikä on suurin hyväksyttävissä oleva vaikutus normaalioloissa, vakavan häiriön sattuessa ja poikkeusoloissa. Määrittele tarvittaessa eri näkökulmat auttamaan arvioinnissa.
2. ***Arvioi palveluiden*** häiriöiden vaikutus ajan funktiona ja ***tunnista kriittiseksi osoittautuvat palvelut*** tarkempaa tarkastelua varten.
3. ***Arvioi eri toimintojen*** häiriöiden vaikutus *kriittisiin palveluihin* ja ***tunnista kriittiset toiminnot*** tarkempaa tarkastelua varten,
4. ***Arvioi eri tuotannontekijöiden*** (järjestelmät, tietoliikenne, ICT-infra, tieto, tilat, henkilöt, palveluntarjoajat jne.) häiriöiden vaikutus *kriittisiin toimintoihin* ja ***tunnista kriittiset tuotannontekijät sekä määrittele niiden suurin hyväksyttävissä oleva häiriön kesto***.
5. ***Arvioi kriittisiin tuotannontekijöihin liittyvät uhat ja tee riskiarvio***

Analyysin lopputuloksena tiedetään, mitkä palvelut ovat kriittisiä, mitä toimintoja ja tuotannontekijöitä tarvitaan ehdottomasti palveluiden tuottamiseksi sekä mikä on pisin hyväksyttävissä oleva häiriön kesto näille. Tiedon perustella määritellään mm. varautumisen vaatimukset ja tarvittavat varotoimet.

Esimerkki arvioinnista:

1. ***Määrittele kriteerit häiriöiden vakavuuden arvioimiseksi.*** Esimerkiksi asteikko 1-5: normaalisti toiminnassa häiriön vaikutus saa olla korkeintaan 2, normaaliolojen vakavissa häiriötilanteissa 3 ja koskaan häiriön vaikutus ei saa ylittää vakavuusluokka 4. Esimerkkejä kriteereistä:

1 https://dvv.fi/documents/16079645/110183105/Kriittisten+kohteiden+luokittelun+menetelm%C3%A4kuvaus.pdf/2e6a64a6-4ad6-8e0c-e7bb-74b999b467f5/Kriittisten+kohteiden+luokittelun+menetelm%C3%A4kuvaus.pdf?t=1661257252575

ESIMERKKI: HÄIRIÖN KRIITTISYYSLUOKITTELU, HÄIRIÖN VAIKUTUS YRITYKSELLE TAI YHTEISKUNNALLE

	1 Vähäinen	2 Pieni	3 Kohtalainen	4 Suuri	5 Kriittinen/Erittäin suuri
Yritys	Vähäinen vaikutus yrityksen toimintaan, haitta on lyhytaikainen ja helposti hallittavissa.	Aiheuttaa jonkin verran haittaa, mutta se on kohtuullisesti hallittavissa.	Aiheuttaa merkittäviä mutta hallittavissa olevia ongelmia.	Aiheuttaa vakavia ongelmia liiketoiminnassa, mikä voi johtaa merkittäviin taloudellisiin menetyksiin ja vaikuttaa pitkään yrityksen toimintamahdollisuuksiin	Toteutuminen johtaa yrityksen toiminnan laajamittaiseen häiriintymiseen tai päättymiseen
Yhteiskunta	Vähäinen vaikutus yksittäiseen yhteiskunnan palveluihin	Yhteiskunnallisesti pieniä, paikallisia vaikutuksia, jotka eivät juuri vaikuta laajempiin toimintoihin tai sidosryhmiin. Paikallisia tai pieniä haittoja (lähinnä "kiusaa") yhteiskunnan kriittisiin toimintoihin.	Tuntuvat vaikutukset lyhytaikaisesti useampaan yhteiskunnalle tuotettavaan palveluun.	Vaikutukset merkittäviä tietyn palvelun osalta tai kohtuullisia vaikutuksia laajalti eri yhteiskunnan kriittisiin palveluihin. Merkittäviä yhteiskunnallisia seurauksia, joista toipuminen vie kohtuullisen kauan.	Vaikutukset suuria tietyn keskeisen palvelun tai useamman palvelun osalta. Vakavia yhteiskunnallisia seurauksia, jotka voivat aiheuttaa laajamittaista häiriötä tai uhkaa yhteiskunnan toiminnoille.
ARVIOINNISSA APUNA KÄYTETTYJÄ ERI NÄKÖKULMIA HELPOTTAMAAN VAIKUTUKSEN ARVIOINTIA					
Talous	Vähäinen menetys, vaikutus on helposti hallittavissa, eikä se aiheuta merkittäviä sopeutustoimia. Esimerkiksi <1% liikevaihdosta tai liikevoitosta vuositasolla	Pieni taloudellinen menetys, joka johtaa vähäisiin sopeutustoimiin, mutta ei vaikuta merkittävästi yrityksen taloudelliseen vakauteen. Esim. 1–5 % liikevaihdosta tai <10% liikevoitosta vuositasolla	Merkittävä taloudellinen menetys, joka vaatii huomattavia toimenpiteitä, kuten kustannussäästöjä, mutta ei vielä uhkaa yrityksen jatkuvuutta. Esim. 5–10 % liikevaihdosta tai 10-50% liikevoitosta vuositasolla	Suuri taloudellinen menetys, joka merkittävästi yrityksen taloudelliseen suorituskykyyn ja edellyttää laajamittaisia sopeutustoimia ja siirtää investointeja. Esim. 10–25 % liikevaihdosta tai 50-100% liikevoitosta vuositasolla.	vakava taloudellinen vahinko, joka uhkaa yrityksen taloudellista jatkuvuutta ja voi johtaa toiminnan merkittävään supistamiseen tai lopettamiseen. Esim. >25% liikevaihdosta tai > 100% liikevoitosta vuositasolla.
Omaisuus	Vähäinen vaikutus toiminnon toimintaan. Omaisuus helposti korvattavissa tai ei vaikuta merkittävästi omaisuuden käytettävyyteen tai arvoon,	Vähäistä vahinkoa omaisuudelle, mutta vahinko on helposti korjattavissa ja kustannukset ovat matalat. Omaisuuden käyttö ei ole merkittävästi vaarantunut. Vähäistä vahinkoa omaisuudelle, mutta vahinko on helposti korjattavissa ja kustannukset ovat matalat. Omaisuuden käyttö ei ole merkittävästi vaarantunut. eikä merkittävästi vaikuta toimintaan.	Huomatta omaisuusvahinko, joka voi vaatia merkittäviä korjaustoimenpiteitä ja aiheuttaa kustannuksia. Omaisuuden arvo tai käyttö on tilapäisesti vaarantunut eikä omaisuus ole välittömästi korvattavissa. Vaikuttaa lyhytaikaisesti useampaan toimintoon.	Vaikuttaa yhtiön toimintaan. Vakavaa vahinkoa omaisuudelle, mikä voi vaikuttaa toiminnan jatkamiseen. Korjauskustannukset ovat korkeat, ja vaikutukset omaisuuden arvoon ovat merkittäviä, omaisuuden korvaaminen vie kohtuullisen kauan..	Vaikuttaa merkittävästi yhtiön toimintaan. Omaisuuden täydellinen tuhoutumiseen tai pitkäaikaiseen käyttökelvottomuuteen. Kustannukset ovat erittäin suuret, ja vaikutukset ovat pysyviä tai korjaamattomia.
Prosessit	Sisäinen virhe. Vaikutukset toiminnon sisäisiä, ei merkittävää vaikutusta toimintaan.	Laajemmat vaikutukset yhtiön toiminnassa. Pieniä viivästyksiä tai häiriöitä, mutta toiminta pysyy vakaana.	Tuntuvia viivästyksiä tai ongelmia, jotka vaikuttavat tuotantoon tai toimituksiin, mutta ongelmat voidaan ratkaista kohtuullisessa ajassa.	Vaikutukset ulottuvat yhtiön ulkopuolelle, kuten asiakkaille ja sidosryhmille. Vakavia häiriöitä toiminnassa, mikä johtaa tuotannon viivästymiseen tai toimitusten keskeytymiseen. Toipuminen vaatii laajoja toimia.	Vakavia ja pitkäaikaisia vaikutuksia, uhkaa yrityksen kykyä toimittaa tuotteita tai palveluita ja voi johtaa laajoihin liiketoiminnallisiin ongelmiin tai toiminnan päättymiseen.
Maine	Vähäinen negatiivinen huomio, ei juuri vaikutusta.	Negatiivinen julkisuus, joka vaikuttaa sidosryhmien suhteisiin mutta jää väliaikaiseksi	Huomattavaa negatiivista huomiota, joka vaikuttaa väliaikaisesti asiakkaisiin tai muihin sidosryhmiin. Maine saadaan palautettua kohtuullisessa ajassa.	Vakavia vaikutuksia sidosryhmien suhteisiin, voi johtaa asiakassuhteiden menettämiseen ja vaikeuttaa uusien asiakkaiden hankintaa. Palautuminen vaatii merkittäviä toimenpiteitä.	Vakava mainehaitta, joka voi aiheuttaa laajaa luottamuksen menettämistä ja jopa johtaa liiketoiminnan loppumiseen.
Henkilöstö	Ei merkittävää vaikutusta henkilöstöön. Työolosuhteet ja työhyvinvointi pysyvät ennallaan, eikä tarvetta toimenpiteisiin synny. Lyhyt sairasloma, vähäinen osaamisen menetys	Aiheuttaa vähäistä haittaa, mutta vaikutukset ovat palautuvia ja helposti hallittavissa ja työntekijöiden hyvinvointi palautuu nopeasti normaaliksi. Pidempiaikainen yksittäinen sairasloma, avainhenkilön menetys.	Väliaikainen henkilöstövaje useamman henkilön tai kriittisen osaamisen menetyksen johdosta, joka johtaa työtaakan kasvuun väliaikaiseti. Aiheuttaa merkittäviä häiriöitä työssä, kuten huomattavaa stressiä, kuormitusta tai tyytymättömyyttä ja voi johtaa esimerkiksi sairauspoissaoloihin, mutta ongelmat ovat kuitenkin hallittavissa.	Merkittävä osaamisvaje avaintoiminnoissa, vakavia vaikutuksia henkilöstön hyvinvointiin, kuten työuupumusta tai vakavia stressitiloja. Työkyky heikkenee ja tilanne vaatii merkittäviä toimenpiteitä, kuten työolosuhteiden muutoksia tai kuntoutusta.	Toiminnan kannalta merkittävän osaamisen pysyvä menetys joka vaikuttaa kriittisten palveluiden toimittamiseen. Aiheuttaa erittäin vakavia ja mahdollisesti pysyviä vaikutuksia henkilöstön hyvinvointiin, kuten vakavia työperäisiä sairauksia tai onnettomuuksia sekä johtaa irtisanoutumisiin ja mahdollisesti työvoimapulaan.
Asiakkaat	Vähäinen vaikutus yksittäiseen palveluun, ei juuri vaikutusta asiakaskokemukseen tai asiakkaiden luottamukseen.	Pieniä häiriöitä tai haittoja, mutta asiakassuhteet säilyvät ennallaan.	Tuntuvat vaiktukset lyhytaikaisesti useampaan asiakkaille. Yritys pystyy palauttamaan luottamuksen ja asiakassuhteet, mutta vie kohtuullisen ajan.	Vaikutukset merkittäviä tietyn kriittisen palvelun osalta. Palvelun tuottaminen keskeytynyt lyhyellä aikavälillä. Johtaa asiakkaiden tyytymättömyyteen ja mahdollisesti asiakaskatoon.	Vaikutukset suuria tietyn keskeisen palvelun tai useamman palvelun osalta. Palvelun tuottaminen keskeytynyt pitkällä aikavälillä. Vakavia seurauksia, jotka voivat johtaa laajamittaiseen asiakaskatoon ja pysyviin mainehaittoihin.
Toimitusketju ja verkosto	Ei juurikaan vaikutusta yhteistyökumppaneiden tai alihankkijoiden toimintaan. Toiminta jatkuu normaalisti ilman merkittäviä häiriöitä.	Pieniä häiriöitä tai viivästyksiä, mutta nämä ovat helposti hallittavissa, eikä niillä ole pitkäaikaisia vaikutuksia yhteistyösuhteisiin.	Huomattavia vaikutuksia, jotka voivat aiheuttaa väliaikaisia häiriöitä alihankkijoiden tai kumppaneiden toimintaan, mutta näistä voidaan toipua suhteellisen nopeasti ilman merkittäviä pitkäaikaisia haittoja. Kohtalainen vaikutus yhteiskunnassa, tuntuvia vaikutuksia tietyillä alueilla tai yhteisöissä, mutta rajoittuvat tiettyihin ryhmiin tai alueisiin	Merkittäviä häiriöitä alihankkijoiden tai yhteistyökumppaneiden toiminnassa, jotka voivat vaikuttaa heidän kykyynsä toimittaa palveluita tai tuotteita. Tämä voi johtaa toimitusten viivästymiseen tai lisäkustannuksiin ja vaarantaa pitkän aikavälin yhteistyön. Laajempia yhteiskunnallisia vaikutuksia, jotka voivat herättää huolta tai vaatia merkittäviä yhteiskunnallisia toimenpiteitä.	Vakavia häiriöitä, jotka voivat johtaa alihankkijoiden tai yhteistyökumppaneiden toiminnan keskeytymiseen tai loppumiseen. Tämä voi katkaista yhteistyösuhteet ja aiheuttaa laajoja toiminnallisia tai taloudellisia vaikutuksia kaikille osapuolille.
Terveys / turvallisuus	Ei ole juuri vaikutusta ihmisten fyysiseen tai henkiseen terveyteen. Mahdolliset vaikutukset ovat lieviä ja lyhytaikaisia	Vaikutus useille henkilöille, ei kuitenkaan kriittisiä vaikutuksia kenellekkään. Aiheuttaa lieviä haittoja, kuten tilapäistä stressiä tai fyysistä kuormitusta, mutta vaikutukset ovat palautuvia ilman pitkäaikaista terveyden tai hyvinvoinnin heikentymistä	Johtaa useille merkittäviin mutta hoidettavissa oleviin terveys- tai hyvinvointiongelmiin, kuten huomattavaa stressiä, työuupumusta tai fyysisiä vaivoja tai aiheuttaa yksitäiselle henkilöille vakavia terveys- tai hyvinvointiongelmia.	Vakavia terveys- tai hyvinvointiongelmia useille henkilöille, kuten pitkäaikaista työkyvyn heikkenemistä, vakavaa stressiä tai fyysistä haittaa	Aiheuttaa erittäin vakavia ja pysyviä terveysvaikutuksia tai voi johtaa henkilömenetyksiin

Esimerkki häiriön kriittisyyden kriteereistä

2. ***Arvioi palveluiden eri pituisten häiriöiden vaikutus valitun asteikon mukaisesti (kts. kuva 1. Palvelun häiriön vaikutus)***

a. Valitse tarvittaessa palvelun kannalta sopivat näkökulmat helpottamaan kriittisyyden arviointi.

b. Arvioi eri pituisten häiriöiden vaikutus

c. Arvio myös alin taso, jolla palvelua on pystyttävä tuottamaan häiriön aikana (MBCO)

d. Tunnista kriittiset palvelut eli palvelut, joissa häiriön vaikutus on suuri joko yritykselle tai yhteiskunnalle.

e. Määrittele kriittisille palveluille suurin hyväksyttävissä oleva häiriön kesto normaalioloissa, vakavissa häiriötilanteissa ja poikkeusoloissa

f. Luokittelun lisäksi kuvaa vaikutus sanallisesti, jolloin uudelleen arviointi on myöhemmin helpompaa

3. ***Analysoi tunnistetut kriittiset palvelut (kts. kuva 2. Eri toimintojen häiriöiden vaikutus palveluun)***

a. Tunnista yrityksen toiminnot, joista kriittinen palvelu on riippuvainen

b. Arvioi toimintojen eri pituisten häiriöiden vaikutus palvelun toimittamiseen eli tunnista kriittiset toiminnot

c. Arvioi kriittisen toiminnon alin taso, jolla sen on kyettävä toimimaan häiriön myös aikana

4. ***Analysoi kriittiset toiminnot (kts. kuva 3. Järjestelmähäiriöiden vaikutus kriittisiin toimintoihin)***

a. Tunnista toiminnon tarvitsemat tuotannontekijät: järjestelmät, tieto sekä muut resurssit

b. Arvioi tuotannontekijöiden häiriöiden vaikutus toimintoon (tunnista kriittiset tuotannon tekijät kuten järjestelmät ja tieto)

1. Palvelun häiriön vaikutus

PALVELU	Näkökulma	Häiriön kesto				
		< 3 h	< 8 h	< 1 vrk	< 3 vrk	< 35vrk
Palvelu 1	Yritys	1	2	3	4	5
	Yhteiskunta	1	1	2	2	3
	Maine, luottamus	1	2	2	3	4
	Asiakkaat	1	2	3	4	5
	Henkilöstö	1	1	1	2	2
	MBCO	0 %	0 %	20 %	50 %	100 %

Normaalioloissa sallittu

Vakavassa häiriötilanteessa sallittu

Ei saa koskaan ylittää

2. Eri toimintojen häiriöiden vaikutus palveluun

Toiminto	Näkökulma	Häiriön kesto				
		< 3 h	< 8 h	< 1 vrk	< 3 vrk	< 3 vrk
Toiminto 1	Taloudellinen	1	2	3	4	5
	Juridinen, viranomaiset	1	1	2	2	3
	Maine, luottamus	1	2	2	3	4
	Asiakkaat	1	2	3	4	5
	Henkilöstö	1	1	1	2	2
	MBCO	0 %	0 %	20 %	50 %	100 %
Toiminto 2	Taloudellinen	1	1	2	2	3
	Juridinen, viranomaiset	1	1	2	2	3
	Maine, luottamus	1	1	2	2	3
	Asiakkaat	1	1	2	2	3
	Henkilöstö	1	1	2	2	3
	MBCO	0 %	0 %	0 %	20 %	50 %
Toiminto 3	Taloudellinen	1	2	3	4	5
	Juridinen, viranomaiset	1	1	2	2	3
	Maine, luottamus	1	1	2	2	4
	Asiakkaat	1	2	3	3	4
	Henkilöstö	1	1	1	2	2
	MBCO	0 %	0 %	20 %	50 %	100 %

3. Järjestelmähäiriöiden vaikutus kriittisiin toimintoihin

Kriittinen resurssi	Toiminto	Häiriön kesto				
		< 3 h	< 8 h	< 1 vrk	< 3 vrk	< 3 vrk
Järjestelmä A	Toiminto 1	1	2	3	4	5
Järjestelmä B	Toiminto 1	1	1	1	2	2
Järjestelmä C	Toiminto 1	1	1	2	2	4
Järjestelmä D	Toiminto 2	1	1	2	2	3
Järjestelmä E	Toiminto 2	1	1	2	2	3

Arvioinnin vaiheet

Riskienhallinta

Varautumisen suunnittelu perustuu vaatimusten lisäksi säännöllisesti tehtävään uhka-analyysiin ja riskiarvioon. Liiketoiminnan vaikutusanalyysissä tunnistetuille kriittisille järjestelmille, tiedolle ja muille ICT-tuotannontekijöille tehdään varautumisen kannalta kattava riskien arviointi.

Riskienhallintamalli ja toimintatavat määritellään yritystasolla, ja niiden toteutumista seurataan johdonmukaisesti. Varautumisen riskienhallinnassa keskitytään erityisesti kriittisiin toimintoihin liittyviin vakaviin uhkiin ja riskeihin, kun taas yleinen riskienhallinta kattaa laajemmin erilaisia ja eritasoisia riskejä organisaation toiminnassa. ICT-palvelutuotannon varautumiseen liittyvä riskiarvio kohdistetaan tunnistettuihin kriittisiin ICT:n tuotannontekijöihin. Riskien arvioinnissa kannattaa käyttää yrityksesi käytössä olevaa riskienarviointimenetelmää ja -kriteeristöä yhdenmukaisuuden varmistamiseksi.

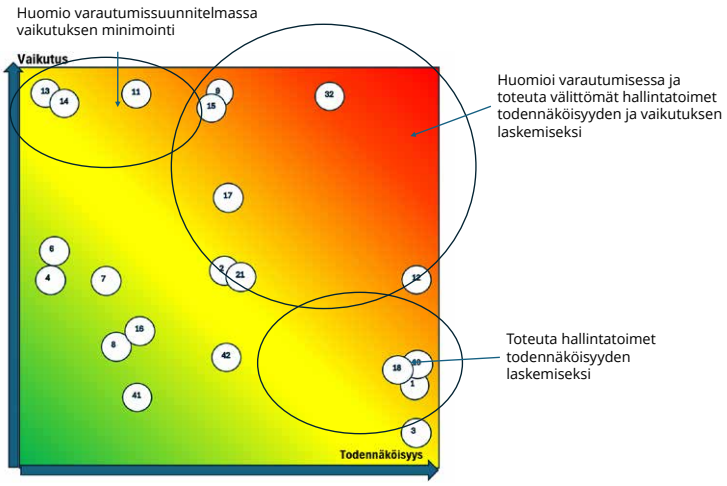
Varautumisen riskiarvioinnissa huomioidaan tavanomaisten ICT-palvelutuotantoa koskevien uhkien ja riskien lisäksi laajasti erilaiset mahdolliset uhkatekijät, olivat ne luonnollisia, ihmisten aiheuttamia, teknologisia tai sosiaalisia. Huomioitavia uhkia ja riskejä ovat mm.

- Toimittajiin ja palvelutuottajiin liittyvät riskit
- Teknologiariskit ja tekniset häiriöt
- Inhimilliset virheet ja väärinkäytökset
- Henkilöstöön ja työvoiman saatavuuteen liittyvät uhkat
- Kriittisen infrastruktuurin vakavat ja mahdollisesti pitkäkestoiset tai toistuvat häiriöt (kuten energian ja veden jakelu, liikenne ja logistiikka, polttoaineiden saatavuus)
- Kyberuhat ml. laajat ja vakavat kyberhäiriöt
- Pandemiat ja terveysuhat
- Suuronnettomuudet
- Toimitusketjujen katkokset, vakavat häiriöt kansainvälisessä logistiikassa
- Luonnonkatastrofit
- Sosiaaliset kriisit ja lakot sekä levottomuudet
- Sabotaasit ja fyysiseen turvallisuuteen liittyvät uhkat
- Poliittiset ja geopoliittiset uhat

Tunnistettujen riskien todennäköisyys ja vaikutus arvioidaan tyypillisesti asteikolla 1–5, ja niiden tulo määrittää riskin arvon. Asteikot ja niiden kriteerit on hyvä määritellä yrityskohtaisesti. Riskien vaikutusarvioissa ja liiketoiminnan vaikutusanalyysissä kannattaa käyttää samoja kriteereitä. Riskien arvioinnissa käytettävien todennäköisyysluokista on esimerkki alla olevassa kuvassa. Korkean arvon saavat riskit vaativat konkreettisia hallintatoimia kuten seurantakäytännöt, riskien todennäköisyyden pienentäminen, ennakoivat toimenpiteet uhan kasvaessa sekä toimenpiteet riskin toteutuessa, kuten vaikutuksen rajoittaminen, torjuminen, toipuminen ja jälkitoimenpiteet. Varautumisen kannalta on huomioitava myös ne vaikutukseltaan vakavat riskit, joiden todennäköisyys on pieni.

	1 Hyvin epätodennäköinen	2 Epätodennäköinen	3 Mahdollinen	4 Todennäköinen	5 Hyvin todennäköinen
Kuvaus ja ARO (Annualized Rate of Occurrence, tapahtuman todennäköisyys vuodessa)	Uhkan toteutuminen erittäin epätodennäköistä (mutta mahdollista), ARO 1% tai alle	Uhkan toteutuminen on epätodennäköistä, mutta mahdollista. ARO alle 10%	Uhka voi toteutua, mutta ei kovin usein, ARO 10-20%	Uhka voi toteutua säännöllisesti tai useita kertoja, ARO 20-50%	Uhka toteutuu lähes varmasti ja hyvin usein, ARO 50%-100%

Esimerkki, riskien todennäköisyyksien luokittelu



Riskiarvion huomioiminen varautumissuunnitelmassa

LIITE 3

Järjestelmien ja tiedon luokittelu sekä vaatimusten johtaminen kriittisyysluokittelun kautta

Järjestelmien ja tiedon luokittelu

Järjestelmien ja tiedon luokittelu niitä käyttävien toimintojen kriittisyyden perustella helpottaa vaatimusten määrittelyä ja luo yhteisen kielen liiketoiminnan ja ICT-palvelutuotannon välille. Tiedon luokittelussa huomioitava myös tiedon arvo ja tiedon hyödyntäminen muussa kuin alkuperäisessä tarkoituksessa. Esimerkiksi vähäarvoisena pidettävä järjestelmän, prosessin tai toiminnon ohjaamiseen ja prosessin toiminnasta kertyvä tieto voi olla arvokasta tarkemmin analysoituna toiminnan kehittämisessä, jolloin suojaustarve kasvaa.

Luokittelun pohjalta voidaan toteuttaa tehokkaasti kunkin luokan vaatimusten mukainen varautuminen ja suojaus. Luokittelu perustuu liiketoiminnan vaikutusanalyysissä tunnistettujen elintärkeiden palveluiden ja niiden vaatimien toimintojen kriittisyyteen.

Luokittelun ***tarkoituksena on auttaa määrittämään järjestelmät ja tieto, joihin suojaustoimet on ensisijaisesti kohdistettava***. Kullekin luokalle määritellään mm. varautumisen vaatimukset ja toteutustapa sekä tiedon käsittelysäännöt. Luokiteltaessa järjestelmiä ja tietoa on huomioitava ja kirjattava mahdolliset järjestelmäkohtaiset poikkeavat vaatimukset.

Luokitukset tarkastetaan säännöllisin väliajoin.

Luokitteluperusteina voidaan käyttää mm.

- ***Vaatimus järjestelmän ja tiedon käytettävyydelle***, käytettävyys normaalioloissa ja suurin sallittu katko vakavissa häiriötilanteissa toiminnalle kriittisimpien järjestelmien tunnistamiseksi.
- ***Järjestelmän riskitaso*** eli millainen uhka voi kohdistua järjestelmään aiheuttamatta merkittäviä ongelmia. Tämä auttaa määrittämään suojaamisen kannalta kriittisimmät järjestelmät.
- ***Tiedon luottamuksellisuus*** eli minkä tasoisia menetyksiä tiedon päätyminen vääriin käsiin aiheuttaa. Tämä määrittää tietoturvariskeiltään kriittisimmät tiedon.
- ***Tiedon eheys*** eli millainen vaikutus tiedon oikeellisuudella on liiketoimintaan tai minkä tasoisia menetyksiä tiedon muuttuminen tai katoaminen aiheuttaa. Luokituksen tarkoituksena on määrittää tietojen katoamisen näkökulmasta kriittisimmät järjestelmät

Järjestelmien luokitteluun on olemassa myös esimerkiksi toimialakohtaisia ohjeita kuten sote-tietojärjestelmien luokitteluun neliportainen malli.[2]

Esimerkki: Kaupunki vastasi kaupunkilaistensa useista elintärkeistä toiminnoista, kuten terveyspalvelut, vesi- ja ympäristöhuolto. Kaupunki käytti useita alan todistetusti hyvämaineisia palveluntarjoajia, joilla on ajanmukaiset ja ajantasaiset järjestelmät palveluiden tuottamiseen sekä turvaamiseen. Kaupungin parhaiten turvattu järjestelmä oli Museojärjestelmä, ei sen kriittisyyden vuoksi vaan järjestelmän omistajan ansiosta. Järjestelmän saatavuuteen ja turvallisuuteen oli panostettu erityisen paljon. Toisaalta kaupunkilaisten kannalta huomattavasti kriittisempien toimintojen käyttämien järjestelmien turvallisuus ei ollut samalla tasolla. Turvaamisessa ja tietoturvan hallinnassa on vain osaltaan kysymys tekniikasta ja hyödyntämisestä. Tärkeämpää on toimintojen kriittisyydestä johdetut toimenpiteet, joilla mitoitetaan varautuminen oikein.

2 https://www.kuntaliitto.fi/sites/default/files/media/file/Sote-tietojarjestelmat-pilvipalveluina_0.pdf

Esimerkkiyrityksen toteuttama järjestelmien ja tiedon luokittelu

Esimerkkiyrityksen toteuttama luokittelu toimintojen kriittisyydelle, järjestelmien käyttävyydelle, järjestelmien ja tiedon väärinkäytösten riskille sekä tiedon eheydelle ja luottamuksellisuudelle ja näiden perusteella johdetut vaatimukset ja käsittelysäännöt järjestelmille ja tiedolle.

1) ESIMERKKI: Toimintojen kriittisyysluokat ja niiden kriteerit

	Vähäinen	Kohtalainen	Merkittävä	Kriittinen
Omaisuus	Vähäinen vaikutus toiminnon toimintaan. Omaisuus helposti korvattavissa.	Vaikuttaa lyhytaikaisesti useampaan toimintoon. Omaisuus ei välittömästi korvattavissa.	Vaikuttaa yhtiön toimintaan. Omaisuuden korvaaminen vaikeaa ja vie pitkän ajan.	Vaikuttaa merkittävästi yhtiön toimintaan. Omaisuus pysyvästi menetetty.
Prosessit	Sisäinen virhe. Vaikutukset toiminnon sisäisiä.	Laajemmat vaikutukset yhtiön toiminnassa.	Vaikutukset ulottuvat yhtiön ulkopuolelle, kuten asiakkaille ja sidosryhmille.	Vakavia ja pitkäaikaisia vaikutuksia.
Talous	Alle 100K€	100-300K€	300K-1M€	yli 1M€
Maine	Vähäinen negatiivinen huomio	Negatiivinen julkisuus, joka vaikuttaa sidosryhmien suhteisiin.	Vakavia vaikutuksia sidosryhmien suhteisiin	Maineen menetys tai vaarantuminen
Henkilöstö	Lyhyt sairasloma, vähäinen osaamisen menetys	Pidempiaikainen sairasloma, avainhenkilön menetys	Merkittävä osaamisvaje avaintoiminnoissa	Toiminnan kannalta merkittävän osaamisen pysyvä menetys
Asiakkaat / Yhteiskunta	Vähäinen vaikutus yksittäiseen palveluun	Kohtalaiset vaikutukset lyhytaikaisesti useampaan asiakkaille / yhteiskunnalle tuotettavaan palveluun.	Vaikutukset merkittäviä tietyn palvelun osalta. Palvelun tuottaminen keskeytynyt lyhyellä aikavälillä	Vaikutukset suuria tietyn keskeisen palvelun tai useamman palvelun osalta. Palvelun tuottaminen keskeytynyt pitkällä aikavälillä.
Terveys / henkilöturvallisuus	Ei vaikutusta tai vähäinen vaikutus yksittäisille henkilöille	Vaikutus useille henkilöille, ei kuitenkaan kriittisiä vaikutuksia kenellekkään	Vakavia vaikutuksia useille henkilöille	Henkilömenetyksiä

2) ESIMERKKI: Kriittisyysluokat järjestelmien pisimmille hyväksyttäville katkoille (järjestelmän saatavuus)

Arvo	Sanallinen kuvaus	Määritelmä
S1	Kriittinen	Alle 1h, pidempi käyttökatkos aiheuttaa merkittäviä ongelmia
S2	Tärkeä	Alle 4h, pidempi käyttökatkos aiheuttaa merkittäviä ongelmia
S3	Normaali	Alle 24h, pidempi käyttökatkos aiheuttaa kohtalaisia ongelmia
S4	Vähäinen	Yli 24h, pidempi käyttökatkos aiheuttaa kohtalaisia ongelmia

3) ESIMERKKI: Järjestelmään tai tietoon liittyvän väärinkäytöksen riskin suuruus

Arvo	Sanallinen kuvaus	Määritelmä
R1	Korkea riski	Järjestelmän/tiedon väärinkäyttö on helppoa tai väärinkäytön vaikutus on korkea
R2	Merkittävä riski	Järjestelmän/tiedon väärinkäyttö on suhteellisen helppoa tai väärinkäytön vaikutus on merkittävä
R3	Alhainen riski	Järjestelmän/tiedon väärinkäyttö on vaikeaa tai väärinkäytön vaikutus on alhainen

4) ESIMERKKI: Tiedon eheyden kriittisyysluokkien määritelmät

Arvo	Sanallinen kuvaus	Määritelmä
E1	Kriittinen	Tiedon menettämisestä tai muuttumisesta käyttökelvottomaksi seuraa kriittinen menetys
E2	Huomattava	Tiedon menettämisestä tai muuttumisesta käyttökelvottomaksi seuraa merkittävä menetys
E3	Kohtalainenb	Tiedon menettämisestä tai muuttumisesta käyttökelvottomaksi seuraa kohtalainen menetys
E4	Vähäinen	Tiedon menettämisestä tai muuttumisesta käyttökelvottomaksi seuraa vähäinen menetys

5) ESIMERKKI: Tiedon luottamuksellisuuden luokittelusäännöt

Arvo	Sanallinen kuvaus	Määritelmä
L1	Salainen	Tiedon joutumisesta vääriin käsiin seuraa kriittinen vahinko
L2	Luottamuksellinen	Tiedon joutumisesta vääriin käsiin seuraa merkittävä vahinko
L3	Sisäinen	Tiedon joutuminen vääriin käsiin aiheuttaa maksimissaan kohtalaisen vahingon. Kaikki tieto jota ei ole erikseen luokiteltu on sisäistä tietoa
L4	Julkinen	Tieto on julkinen

6) ESIMERKKI: Järjestelmän saatavuuteen liittyvät käsittelysäännöt ja vaatimukset järjestelmän luokituksen mukaisesti

	S1	S2	S3	S4
Laitetilat	Varalaitteistot erillisessä laitetilassa riittävän etäisyyden päässä toisistaan, laitetiloissa varmistettu sähkönsyöttö(UPS), automaattinen palonsuojausjärjestelmä, kahdennettu ilmastointi	Varalaitteistot erillisessä laitetilassa, laitetiloissa varmistettu sähkönsyöttö(UPS), automaattinen palonsuojausjärjestelmä, kahdennettu ilmastointi	Varalaitteistot erillisessä tilassa, päälaitetilassa varmistettu sähkönsyöttö(UPS), palosuojatut tilat	Ei vaatimuksia
Laitteiden varajärjestelyt	Kahdennettu kaikilta osin kahteen eri laitetilaan, automaattinen vikasietoisuus (hot-hot)	Kahdennettu varajärjestelmä (hot-standbly)	”Lämmin” varalaitteisto toisessa laitetilassa	Ei erityisjärjestelyjä, vikatilanteessa hankitaan uusi laitteisto (tai siirto virtuaalialustalle)
Sovellustason varajärjestelyt	Ohjelmistot asennettu kahdentaville laitteille. Ohjelmistoista olemassa vähintään viimeiset kolme versiota	Ohjelmistot asennettu kahdentaville laitteille. Ohjelmistoista olemassa vähintään viimeiset kaksi versiota	Ohjelmistot valmiiksi asennettu varalaitteistolle tai virtuaalipalvelimelle. Ohjelmistoista olemassa vähintään viimeiset kaksi versiota	Ei vaatimuksia
Testijärjestelmät	Pysyvä testijärjestelmä oltava, jossa voidaan koestaa tuotannossa mahdollisesti esiintyvät ongelmat ja testata muutokset ennen uuden version tuotantoon siirtoa Myös infrastruktuuri-järjestelmien muutosten vaikutukset on testattava ennen muutosten toteuttamista (verkon konfiguraatiomuutokset jne.)	Järjestelmäkohtainen testijärjestelmä (voidaan käyttää järjestelmän kahdentamiseen käytettävää järjestelmää)	Versiomuutokset on testattava testijärjestelmässä ennen tuotantoon siirtoa Testijärjestelmä on oltava käytettävissä tarvittaessa, pysyvää testijärjestelmää ei kuitenkaan vaadita	Ei vaadita
Palautuminen vikatilanteesta	Automaattinen	Mahdollisimman automaattinen	Manuaalinen, ohjeistettu	Manuaalinen
Huoltotoimet (päivitykset, konfiguraatiomuutokset jne.)	Erikseen määriteltävä järjestelmäkohtainen huoltoikkuna	Erikseen määriteltävä järjestelmäkohtainen huoltoikkuna	Erikseen määriteltävä järjestelmäkohtainen huoltoikkuna	Voidaan tehdä milloin vain, mielellään palveluajan ulkopuolella
Käytettävyystasot prosentteina (%)	99,95 %	99,90 %	99,50 %	95 %
Maksimikatko palveluaikana	15 min	30 min	2 tuntia	24 tuntia
Palveluaika	Palveluaika on 24/7	Palveluaika on 24/7	Arkisin 7-21, la ja su 9-18	Arkisin 8-16
Palautumisaikatavoite palveluajan ulkopuolella	x	x	Yksi (1) työpäivä.	Kaksi (2) työpäivää.
Päälläolon valvonta	24x7x365 pois lukien järjestelmäkohtainen huoltoikkuna. Automaattiset hälytykset valvomoon	24x7x365 pois lukien järjestelmäkohtainen huoltoikkuna. Automaattiset hälytykset valvomoon	Palvelusaikoina pois lukien järjestelmäkohtainen huoltoikkuna. Automaattiset hälytykset valvomoon	Palvelusaikoina pois lukien järjestelmäkohtainen huoltoikkuna.
Lokitiedot	Kaikki käytettävyyteen vaikuttava lokitieto reaaliaikaisesti valvontajärjestelmään, automaattiset hälyytykset valvomoon. Reagointi max 15min	Kaikki käytettävyyteen vaikuttava lokitieto reaaliaikaisesti valvontajärjestelmään, automaattiset hälyytykset valvomoon. Reagointi max 30min	Kaikki käytettävyyteen vaikuttava lokitieto reaaliaikaisesti valvontajärjestelmään, automaattiset hälyytykset valvomoon.	Ei vaatimuksia
Järjestelmän dokumentointi	Järjestelmän dokumentointi tulee olla sillä tasolla, että järjestelmän palauttaminen toimintakuntoon on mahdollista määritellyssä aikaikkunassa	Järjestelmän dokumentointi tulee olla sillä tasolla, että järjestelmän palauttaminen toimintakuntoon on mahdollista määritellyssä aikaikkunassa	Järjestelmän dokumentointi tulee olla sillä tasolla, että järjestelmän palauttaminen toimintakuntoon on mahdollista määritellyssä aikaikkunassa	Järjestelmän dokumentointi tulee olla sillä tasolla, että järjestelmän palauttaminen toimintakuntoon on mahdollista

7) ESIMERKKI: Järjestelmien ja tiedon riskiluokan mukaiset käsittelysäännöt

	R1	R2	R3
Esimerkkejä	Kannettava, jolla kytkeydytään yhtymän tietoverkkoon Erittäin arkaluontoista dataa sisältävä työasema	Järjestelmien hallintaan tarkoitettu työasema Lääkinnällisessä käytössä oleva työasema, jolla on mahdollisuus vaikuttaa suoranaisesti potilaan hoitoon Työasema, josta erityisiä yhteyksiä yhtymän tietoverkon ulkopuolelle (esim. toimittajan hallinnassa oleva työasema) Työasema, josta tarjotaan joitain palveluja rajatulle käyttäjäjoukolle (suuremmalle käyttäjäjoukolle palveluja tarjoavaa työasemaa käsitellään palvelimena)	Perustyöasema Pelkkä työasemakäyttö, ei tarjoa mitään palveluja ulospäin
Tiedon suojaus	Kaikki tiedot salatussa muodossa (esim. koko kiintolevyn salaus)	Tietojen luokittelun mukaan	Tietojen luokittelun mukaan
Palomuurisuojaus	Työasemalla oleva keskitetysti hallittava palomuuriohjelmisto pakollinen	Voidaan käyttää myös segmentti-kohtaista eli segmentin reunalla olevaa verkkopalomuuria	Ei pakollinen sisäverkossa Palomuuri oltava julkisten verkkojen sekä ko työaseman välillä
Virussuojaus/EDR	Pakollinen, laitetta ei saa kytkeä verkkoon ilman ajantasaista virustietokantaa/EDR-yhteyttä, EDR-kannan päivitys vähintään kerran tunnissa	Pakollinen, EDR-päivitys vähintään kerran tunnissa	Pakollinen, EDR- päivitys vähintään kerran päivässä
Verkkotason suojaus	Salattu VPN-yhteys tai dedikoitu palomuurilla suojattu segmentti, samassa segmentissä saa olla vain samantasoisia laitteita Yhteydet dokumentoitu ja sallittu vain määritellyt yhteydet Edistyneiden haittaohjelmien havainnointi/NDR Suojaus vähintään langattomissa (Wifi) yhteyksissä:WPA2-AES Kaikkien laitteelta muodostettavien yhteyksien pitää olla salattuja	Dedikoitu segmentti, samassa segmentissä saa vain olla samantasoisia laitteita Yhteydet dokumentoitu ja sallittu vain määritellyt yhteydet Suojaus vähintään langattomissa (Wifi) yhteyksissä:WPA2-AES Kaikkien laitteelta muodostettavien yhteyksien pitää olla salattuja	Yhteydet dokumentoitu
Varmistukset (haittaohjelmista palautuminen)	Varmistus päivittäin sisältäen myös sovellusdatat	Varmistetaan image-tasolla muutosten yhteydessä (ei käyttäjän vastuulla jatkuvaa datan varmistusta), muuttuvan datan varmistus käyttäjän vastuulla.	Käyttäjän vastuulla
Ylläpitotunnukset	Paikalliset tunnukset (root/admin-tason oikeudet vain paikallisesti) mahdollisuuksien mukaan	Erilliset ylläpitotunnukset	Erilliset ylläpitotunnukset
Autentikointi käyttäjä	2-vaiheinen/vahva tunnistautuminen	Käyttäjätunnus ja salasana, mutta suositeltavaa 2-vaiheinen/vahva tunnistautuminen	Käyttäjätunnus ja salasana
Ohjelmistojen asennus ja testaus	Ohjelmistot testattava ennen käyttöönottoa. Vain tietojärjestelmäpalvelut itse, käyttäjillä tai laitetoimittajilla ei lupaa/mahdollisuutta asentaa ohjelmia itse	Ohjelmistot testattava ennen käyttöönottoa. Vain tietojärjestelmäpalveluiden luvalla, käyttäjillä/laitetoimiittajilla ei lupaa asentaa ohjelmia ilman tietojärjestelmäpalvelujen lupaa	Vain tietojärjestelmäpalveluiden luvalla, käyttäjillä/laitetoimittajilla ei lupaa asentaa ohjelmia ilman tietojärjestelmäpalvelujen lupaa
Lisälaitteet ja massamuistit, kuten USB-muistitikku	Lisälaitteiden liittäminen ilman lupaa kielletty	Lisälaitteiden liittäminen ilman lupaa kielletty	Käyttäjillä mahdollisuus liittää lisälaitteita/muistitkkuja, mutta ohjelmien käynnistäminen / asentaminen kielletty ilman lupaa
Lokitiedot, minimitaso	Onnistuneet ja epäonnistuneet kirjautumiset, käyttöoikeusmuutokset, yhteyslokit, konfiguraatiomuutokset, ylläpitotunnuksillä tehdyt toimet	Onnistuneet ja epäonnistuneet kirjautumiset, käyttöoikeusmuutokset, yhteyslokit, ylläpitotunnuksella tehdyt toimet	Onnistuneet ja epäonnistuneet kirjautumiset, käyttöoikeusmuutokset,ylläpitotunnuksella tehdyt toimet
Kriittiset tietoturvapäivitykset (patchit)	Tavoiteasennusaika 72h patchin ilmestymisestä, patch-taso tarkistettava yhtymän verkkoon kytkeydyttäessä ja pääsy sallitaan vain ajantasaisilla patcheilla (asennetaan automaattisesti jos ei ole määritellyssä patch-tasossa)	Tavoiteasennusaika 1 vko, patch-tason raportointi buutin/sisäänkirjauksen yhteydessä	Tavoiteasennusaika 1 kk, patch-tason raportointi buutin/sisäänkirjauksen yhteydessä

8) ESIMERKKI: Käsittelysäännöt tiedon eheysluokitukselle

	E1	E2	E3	E4
Varmistusten sijainti	Tiedoista tulee olla ajantasainen varmistus fyysisesti toisessa sijainnissa (tiedot ajantasaisesti replikoitu) sekä lisäksi päivittäinen varmistus vuorokausitasolla	Tiedoista tulee olla päivittäinen varmistus olemassa vuorokausitasolla fyysisesti toisessa sijainnissa	Tiedoista tulee olla varmistus olemassa viikkotasolla fyysisesti toisessa sijainnissa	Tiedoista tulee olla varmistus olemassa kuukausitasolla eri medialla
Tiedon siirto muihin järjestelmiin	Lähetettyjen tietojen muuttumattomuus siirrossa varmistettava automaattisesti. Lähetettävästä tiedosta oltava kopio ja virhetilanteessa siirto kyetään tekemään automaattisesti uudelleen	Siirretyn tiedon sisällön muuttumattomuuden varmistaminen suositeltavaa. Lähetettävästä tiedosta oltava olemassa kopio, joka voidaan tarvittaessa lähettää uudelleen	Ei vaatimuksia	Ei vaatimuksia
Tiedon siirto muista järjestelmistä	Vastaanotettujen tietojen muuttumattomuus siirrossa varmistettava automaattisesti	Vastaanotettujen tietojen muuttumattomuus siirrossa on suositeltavaa varmistaa	Ei vaatimuksia	Ei vaatimuksia
Muuttumattomuuden varmistaminen tallennuspaikassa	Tietojen muuttuminen pitää kyetä havainnoimaan	Tietojen muuttuminen pitää kyetä havainnoimaan	Ei vaatimuksia	Ei vaatimuksia
Tietoja käsittelevien järjestelmien muutokset	Testijärjestelmä oltava, jossa voidaan testata muutoksien vaikutukset tiedon eheyteen ennen uuden version tuotantoon siirtoa	Testijärjestelmä oltava käytettävissä tarvittaessa, jossa voidaan testata muutoksien vaikutukset tiedon eheyteen ennen uuden version tuotantoon siirtoa	Tiedot varmistettava ennen järjestelmämuutoksia	Tiedot varmistettava ennen järjestelmämuutoksia
Tietoja käsittelevien järjestelmien versiopäivitykset	Testattava. Edellinen ohjelmistoversio oltava otettavissa käyttöön saatavuusluokituksen mukaisesti	Testattava. Edellinen ohjelmistoversio oltava otettavissa käyttöön saatavuusluokituksen mukaisesti	Edellinen ohjelmistoversio oltava otettavissa käyttöön saatavuusluokituksen mukaisesti	Edellinen ohjelmistoversio oltava otettavissa käyttöön saatavuusluokituksen mukaisesti
Varmistukset	Palautuspiste (RPO) määritelty ja varmistukset seuraavat RPO:ta Varmistus ja palautus määritelty, ohjeistettu ja harjoiteltu viimeisen 12kk aikana Palautus tulee olla tehtävissä saatavuusluokituksen mukaisessa aikaikkunassa	Palautuspiste (RPO) määritelty ja varmistukset seuraavat RPO:ta Varmistus ja palautus määritelty ja ohjeistettu Palautus tulee olla tehtävissä saatavuusluokituksen mukaisessa aikaikkunassa	Muuttuneen datan varmistaminen kerran päivässä, lisäksi viikoittainen full backup Data palautettavissa viimeisen 30 pv:n ajalta päiväkohtaisesti ja vuoden ajalta viikkokohtaisesti Palautus tulee olla tehtävissä saatavuusluokituksen mukaisessa aikaikkunassa	Muuttuneen datan varmistaminen kerran viikossa, lisäksi kuukausittainen full backup Palautettavissa viimeisen kuukauden ajalta viikkokohtaisesti ja vuoden ajalta kuukausikohtaisesti Palautus tulee olla tehtävissä saatavuusluokituksen mukaisessa aikaikkunassa

9) ESIMERKKI: Käsittelysäännöt tiedon luottamuksellisuuden luokitukselle

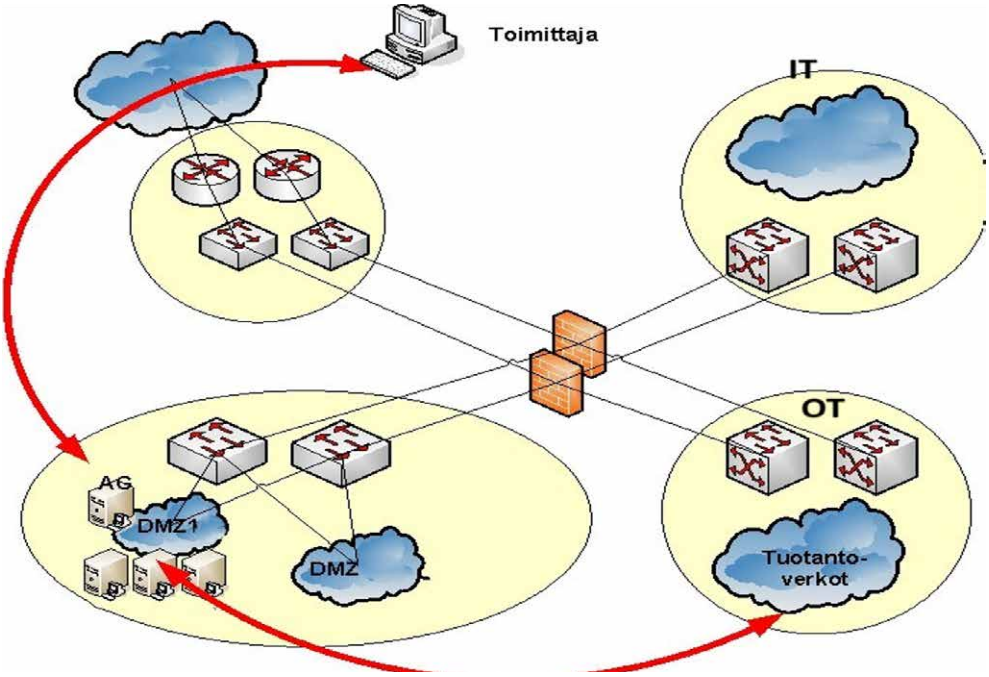
	L1	L2	L3	L4
Sisältö	Esim. Patentoimattomat (IPR) tiedot sekä sisäpiiritieto, yrityksen taloudellista tilaa kuvaavat ennusteet, salasanat ja tunnukset	Yrityssalaisuudet ja muut luottamuksellisiksi sovitut tiedot. esim. strategiset tiedot, tutkimus- ja kehitystiedot, tuotantomenetelmiä koskevat tiedot	Kaikki luokittelematon tieto, organisaatiokaaviot, sisäiset tiedotteet	Tieto joka voidaan luovuttaa vapaasti ulkopuolelle, esim. julkaistut vuosikertomukset, tilinpäätöstiedot, käyttöohjeet, yleisesitteet, mainos- ja markkinointi-materiaali
Merkintä asia-kirjaan	Suositus: Merkintä "Salainen" (engl. "Secret") joka sivulle silloin kun mahdollista, muuten esim. kanteen	Suositus: Merkintä "Luottamuk-sellinen" (engl. "Confidential") joka sivulle silloin kun mahdollista, muuten esim. kanteen	Suositus: Merkintä "Sisäinen" (engl. "Internal")	Ellei julkisuus ilmene ulko-asusta, hyvä merkitä julkiseksi (engl. "Public")
Jakelu yrityksen sisällä	Tiedon omistajan luvalla erikseen nimetyille henkilöille. Vastaan-ottaja ei saa toimittaa eteenpäin ilman lupaa	Tiedon omistajan luvalla, jakelu tehtävien mukaan. Vastaanottaja ei saa toimittaa eteenpäin ilman lupaa	Yhtymän sisällä	Vapaa
Käsittelyoikeuk-sien myöntämi-nen ja todenta-minen	Ylläpito- ja selausoikeudet annetaan nimetylle henkilölle salaiseen aineistoon ja salaisille asiakirjoille Käyttäjän todentaminen vahvalla autentikoinnilla	Ylläpito- ja selausoikeudet annetaan tehtävien mukaan luottamukselliseen aineistoon ja luottamuksellisille asiakirjoille Käyttäjän todentaminen henkilö-kohtaisella käyttäjätunnuksella ja salasanalla	Omalla henkilöstöllä oikeudet tietoon. Aineiston laatija / luokituksen tekijä myöntää oikeudet Käyttäjän todentaminen varmistaen käyttäjän olevan sisäinen, esim. verkkokirjau-tuminen Yhtymän sisäiseen tietoverkkoon	Vapaa. Ei todentamisvaadetta
Luovutus ulko-puolisille	Tiedon omistajan luvalla valvotusti, tehtävä kirjallinen vaitiolositoumus	Tiedon omistajan luvalla tai lakiin perustuen, tehtävä kirjallinen vaitiolositoumus	Harkinnan mukaan	Vapaa
Monistus ja tulostus	Kopioita voi tehdä vain tiedon omistajan luvalla. Vain virallisia kopioita. Kopioita käsiteltävä kuin alkuperäisiä. Ei tulostusta verkkotulostimille	Kopioita voi tehdä vain tiedon omistajan luvalla. Kopioita käsiteltävä kuten alkuperäisiä. Verkkotulostimille valvottuna vuotoriski minimoiden	Sisäisesti vapaa	Vapaa
Kuljetus ja siirto	Suljetussa kuoressa kirjattuna, vastaanottaja nimettävä henkilötasolla, kuittaus luovutuksesta Sisäisessä sähköpostissa salattuna määritellyille henkilöille Tietoverkoissa tieto aina salattuna Matkoilla vain tiedon omistajan kirjallisella luvalla, kuljetettava käsimatkatavarana. Ei käsitellä näkyvillä	Suljetussa kuoressa kirjattuna, vastaanottaja nimettävä henkilötasolla Sisäisessä sähköpostissa vain määritellyille henkilöille Ulkoisessa sähköpostissa ja ulkoisissa tietoverkoissa salattuna Matkoilla kuljetettava vain erityi-sesti tarvittaessa ja käsimatkatava-rana. Ei käsitellä näkyvillä	Sisäisesti vapaa Konsernin ulkopuolelle suljetussa kuoressa, vastaanottaja nimettävä henkilötasolla Ulkoiset sähköpostiyhteydet ja tietoverkot harkinnan mukaan Matkoilla kuljetettava käsimatkatavarana. Ei käsitellä näkyvillä	Vapaa
Säilytys	Ei-sähköinen: Aina murtosuoja-tuissa tiloissa, kassakaapissa jos mahdollista. Työtilojen ulkopuolella vain erityistapauksissa Sähköinen: Henkilökohtaisella käyttäjätunnistuksella suojattu sisäisissä tietojärjestelmissä. Sähköinen säilytys aina salattuna	Ei-sähköinen: Murtosuojatut tilat tai arkisto Sähköinen: Henkilökohtaisella käyttäjätunnistuksella suojattu sisäisissä tietojärjestelmissä. Työtilojen ulkopuolella säilytys aina salattuna	Ei-sähköinen Työtilat, arkisto Sähköinen: sisäiset tietojärjes-telmät, työtilojen ulkopuolella käyttäjätunnistuksella suojattuna	Ei rajoituksia
Säilytys yhtymän ulkopuolella	Vain erityistapauksissa tiedon omistajan luvalla. Salattu vahvalla salauksella, vähintään AES256. Salausavaimet hyvinvointikuntayh-tymän hallussa, muilla ei pääsyä tietoon. Vahva (monivaiheinen) autentikointi tietoon pääsyyn (2FA)	Vain erityistapauksissa tiedon omistajan luvalla. Salattu vahvalla salauksella, vähintään AES256. Suositeltavaa on, että salausavai-met ovat hyvinvointikuntayhtymän hallussa, muilla ei pääsyä tietoon. Vahva (monivaiheinen) autenti-kointi tietoon pääsyyn (2FA)	Salaus vahvalla salauksella suositeltava, vähintään AES256. Henkilökohtaiset pääsyoikeudet tietoon (käyttäjätunnus & salasana)	Henkilökohtaiset pääsyoi-keudet tietoon muutoksien tekemiseksi (käyttäjätunnus & salasana)
Poisto ja hävitys ***Service Desk avustaa tarvit-taessa fyysisessä tuhoamisessa/ päällekirjoittami-sessa**	Alkuperäinen kappale vain tiedon omistajan luvalla Ei-sähköinen media: silppurissa Sähköinen media: Tuhoamalla huolellisesti fyysisesti tai verkkole-vyillä päällekirjoittamalla* Poisto tietojärjestelmistä mahdollisimman nopeasti tiedon vanhennuttua	Alkuperäinen kappale vain tiedon omistajan luvalla Ei-sähköinen media: silppurissa tai laittamalla lukittuun tietosuoja-as-tiaan Sähköinen media: Laittamalla lukittuun tietosuoja-astiaan tai tuhoamalla fyysisesti tai päällekirjoittamalla* Poisto tietojärjestelmistä mahdollisimman nopeasti tiedon vanhennuttua	Alkuperäinen kappale vain tiedon omistajan luvalla Ei-sähköinen media: silppurissa tai laittamalla lukittuun tietosuoja-astiaan Sähköinen media: Laittamalla lukittuun tietosuoja-astiaan tai tuhoamalla fyysisesti tai päällekirjoittamalla*	Alkuperäinen kappale vain tiedon omistajan luvalla. Ei-sähköinen media: ei rajoituksia Sähköinen media: Laittamalla lukittuun tietosuoja-astiaan tai tuhoamalla fyysisesti tai päällekirjoittamalla*
Luokitusmuutos	Tiedon omistajan luvalla. Muutos merkittävä asiakirjaan	Tiedon omistajan luvalla. Muutos merkittävä asiakirjaan	Tiedon omistajan luvalla. Muutos merkittävä asiakirjaan	Vapaa
Tietoaineistosta luodut metatie-dot	Metatiedot ovat salaisia ja käsitellään samaan tapaan kuin salaisia tietoja	Metatiedot ovat sisäisiä tietoja, jotka ovat kaikkien hyvinvointikun-tayhtymän työntekijöiden saatavilla pyydettäessä	Metatiedot ovat sisäisiä tietoja, jotka ovat kaikkien hyvinvoin-tikuntayhtymän työntekijöiden saatavilla pyydettäessä	Metatiedot ovat sisäisiä tietoja, jotka ovat kaikkien hyvinvoin-tikuntayhtymän työntekijöiden saatavilla pyydettäessä

LIITE 4

Esimerkki – OT-ympäristön toimintamalli

Operatiivisten ympäristöjen (OT-ympäristöt) eristäminen IT-verkoista on merkittävä keino suojata tuotannon toimintaa. OT-ympäristöjen kaikelta eristäminen, ns Air Gapping, on usein haastavaa, sillä OT-ympäristöä ei voida täysin eristää vaan tarvitaan yhteyksiä ulkopuolelle esimerkiksi huollon tai ylläpidon vaatimuksesta. Tähän tulee suunnitella ja ottaa käyttöön turvallinen toimintamalli kaikkien kumppanien kanssa.

Viitekehyksenä OT-ympäristöjen eristämiseen voi käyttää esimerkiksi Purdue-mallia[3].



Periaatteet

Määritele periaatteet, joiden mukaan tarkemmat ympäristökohtaiset määritykset suunnitellaan ja toteutetaan. Valittava arkkitehtuuri voi olla esimerkiksi:

- Yhteydet
  - Suorat yhteydet kielletty, siirtymävaiheessa yhteydet minimiin
  - Tuotannossa olevien työasemien yhteydet ulospäin kielletty
  - Kaikki mahdolliset yhteydet ns. Access Gateway:n tms. kautta
  - Tapauskohtaiset poikkeukset edelliseen
- Käyttöoikeudet hallinnassa
  - Yksilölliset käyttäjätunnukset
  - Mikäli yhteiskäyttöisiä tunnuksia joudutaan käyttämään, varmistuttava että käyttäjä on vahvasti tunnistettu muulla tavoin
- Lokien hallinta ja valvonta
- Varmistus ja varajärjestelyt

3 https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf

Yhteydet tarkemmin

- Yhteyksien minimointi riskiluokituksen mukaan
- Käyttäjälle ainoastaan tarvittavat yhteydet ja sovellukset
- Levyjakojen korvaaminen suojatuilla tiedostonsiirto-sovelluksilla
- Oma tulostuspalvelin ja DNS-palvelin, mikäli niitä tarvitaan
- Varmistus ja varajärjestelyt kriittisyysluokan ja suojausmääritysten perusteisesti (kahdennukset, varatyöasemat jne.) huomioiden tuotantoympäristön erityispiirteet
- Teknisten ratkaisujen suunnittelu edellä mainittujen asioiden perusteella

Käyttöoikeudet

- Tuotantoverkkoon tunnistautuminen eri tunnuksilla kuin toimistoverkkoon (jolloin suora haittaohjelmien siirtyminen toimistoverkosta tuotantoverkkoon vaikeutuu)
- Oma AD tai vastaava helpottamaan käyttöoikeuksien ylläpitoa
- Käyttöoikeudet tuotannon järjestelmiin eri prosessin kautta (käyttöoikeusprosessin määritys)
  - Oikeuksia haettava erikseen
  - Oikeudet tarkistettava säännöllisesti
  - Oikeudet poistettava nopeasti (työpaikan vaihdokset, työn kuvan muutokset jne.)
  - Oikeudet dokumentoituna (kenellä on oikeudet tiettyyn järjestelmään, mitkä oikeudet milläkin käyttäjällä on)

Lokien hallinta ja valvonta

Toteutetaan lokienhallintapolitiikan tai -periaatteiden mukaisesti huomioiden edellä mainitut periaatteet ja tuotantoympäristöjen erityispiirteet kuten herkkyys häiriöille esim. agenttiohjelmistojen, EDR-järjestelmien tai lokien keräämisen osalta.

Suurin huomio lokien keräämisessä ja valvonnassa kiinnitetään IT-OT-verkkojen välisiin yhteyksiin ja niitä käyttäviin käyttäjätunnuksiin.

Kriittisten ympäristöjen valvontaa voidaan tehostaa erityisillä ns. OT-security-järjestelmillä, joilla voidaan passiivisesti tarkkailla ympäristöä, tuotantoa häiritsemättä.

Varmistus ja varajärjestelyt

Toteutetaan kriittisyysluokituksien mukaisesti huomioiden tuotantojärjestelmien erityispiirteet.

LIITE 5

Varmuuskopiointi ja tiedon muuttumattomuuden varmistaminen

Varmuuskopiointi

Varmuuskopioiden avulla suojataan arvokkaat tiedot ja tiedostot mahdollisilta tietojen menetyksiltä tai vahingoilta, joita voi aiheuttaa mm. laiteviat, haittaohjelmat, tahallinen tiedon tuhoaminen (kyberhyökkäykset, sisäiset väärinkäytökset) tai tahaton tiedostojen vahingoittaminen. Varmuuskopioiden avulla varmistetaan palautuminen nopeasti ja tehokkaasti normaaliin toimintaan varautumissuunnitelman mukaisesti. Lisäksi varmuuskopiot auttavat väärinkäytösten ja kyberhäiriöiden selvittelyssä ja tutkinnassa (kuten rikostutkinta).

Varmuuskopiointi otetaan vähintäänkin kaikista niistä järjestelmistä, joissa säilytetään toiminnan tai palveluiden kannalta kriittistä tietoa sekä järjestelmistä, joita voidaan voivat olla väärinkäytösten väline tai joiden sisältämät tiedot voivat auttaa väärinkäytösten selvittelyssä (kuten sähköposti). Yhdessä lokitietojen kanssa varmuuskopiot mahdollistavat vaativienkin tapahtumien selvittämisen.

Varmuuskopioinnin tiheys, lukumäärä ja säilytys riippuu järjestelmän kriittisyydestä, tietosisällöstä ja järjestelmälle asetetusta palautumispistetavoitteesta (RPO) ja palautumisaikatavoitteesta (RTO).

Varmuuskopiointikäytännöt kuvataan kokonaisuutena ja järjestelmittäin.

Mahdollisuuksien mukaan varmuuskopioinnissa noudatetaan seuraavia käytäntöjä:

- ***Säännöllisyys:*** Tiedon kriittisyyden ja palautumispistetavoitteen mukainen aikataulu (päivittäin, viikoittain, kuukausittain).
- ***Monikerroksinen varmuuskopiointi:*** Mahdollisuuksien mukaan käytetään monikerroksista varmuuskopiointia. Täydellisten varmuuskopioiden ja lisäksi erilliset varmuuskopiot tiedostojen muutoksista tai tapahtumat talletetaan niin, että ne voidaan ajaa järjestelmään uudelleen esim. tapahtumalokilta.
- ***3-2-1:*** Kriittisistä tiedosta säilytetään vähintään kolme erillistä varmuuskopiota, kahdessa eri mediassa, joista yksi ei ole verkossa. Muiden kopioiden säilyttämisessä voidaan hyödyntää eri pilvipalveluita. Varmuuskopioista vähintään yksi tulee sijaita fyysisesti eri paikassa kuin varmistettu järjestelmä.
- ***Riittävä säilytysaika:*** Varmuuskopioille määritellään riittävän pitkä säilytysaika (vähintään 6-12 kk mahdollisuuksien mukaan). Säilytysajassa huomioidaan mahdollisuus palata tarkasti tiettyyn ajankohtaan menneisyydessä. Esimerkiksi viimeisen 6 kuukauden ajalta päivittäiset varmuuskopiot, 6-12 kk vanhoista viikoittaiset kopiot, 1-3 v vanhoista kuukausitason kopiot jne.
- ***Tarkistus ja testaus:*** varmuuskopioiden eheys ja toimivuus testataan säännöllisesti.
- ***Salauksen käyttö:*** Kriittisten tietojen varmuuskopiot salataan.

Tiedon eheyden ja muuttumattomuuden varmistaminen

Rakenna kriittisyyden mukaisesti tarvittavat kontrollit tiedon eheyden ja muuttumattomuuden varmistamiseksi. Mahdollisia kontrolleja ovat mm.

1. ***Checksum- ja Hash-funktiot:*** Algoritmeilla, kuten MD5 tai SHA, voidaan luoda tarkistussummia, jotka auttavat havaitsemaan datan muutoksia. Ennen ja jälkeen käsittelyn luodut hash-arvot mahdollistavat datan muutosten seurannan ja havaitsemisen.
2. ***Digitaaliset allekirjoitukset ja salaus:*** Digitaalisilla allekirjoituksilla varmistetaan erityisesti arkaluontoisen tiedon osalta, ettei tietoa ole muokattu siirron aikana, ja salauksella estetään luvaton pääsy.
3. ***Auditointilokit:*** Järjestelmien ja tiedostojen käyttöön liittyvien tapahtumien tallentaminen auttaa seuraamaan, milloin dataan on tehty muutoksia ja kuka on ollut niistä vastuussa. Lokit tukevat sekä muutosten jäljittämistä että poikkeamien selvittämistä
4. ***Versiohallinta:*** Varmuuskopioinnin lisäksi erityisesti uusien päivityttävän tiedon versiohallinnan avulla voidaan tallentaa ja palauttaa tietoa, mikä mahdollistaa muutosten seurannan ja virheellisten muutosten korjaamisen.
5. ***Kaksivaiheinen tietojen muutoshyväksyntä:*** Kriittisen tiedon osalta voidaan edellyttää muutoksen hyväksymistä esimerkiksi kahden eri tahon toimesta.
6. ***Eheystarkastukset ja automaattiset hälytykset:*** Säännöllisesti suoritetut eheystarkastukset, esimer-

kiksi tietokannoille ja tiedostojärjestelmille, voivat varmistaa tiedon muuttumattomuuden.

7. ***Käyttöoikeuksien hallinta:*** Pääsynhallinta ja tarkat käyttöoikeuksien määrittelyt vähentävät luvattoman muokkaamisen riskiä. Vähimmän oikeuden periaatteen mukaisesti käyttäjille ja järjestelmille myönnetään vain ne käyttöoikeudet, jotka ovat välttämättömiä tehtävien suorittamiseksi.

LIITE 6

Lokitietojen kerääminen ja käsittely

Lokia kerätään kaikista niistä järjestelmistä, laitteista ja tapahtumista, jotka ovat tietoturvatapahtumien, väärinkäytösten tai teknisten ongelmien selvittämisen sekä kriittisten järjestelmien toipumisen kannalta merkityksellisiä. Järjestelmittäin määritellään kerättävät lokitiedot sekä niiden säilytystapa ja -aika. Keräämisessä, säilyttämisessä ja käsittelyssä huomioitava aina lainsäädäntö (mm. toimialakohtainen lainsäädäntö ja määräykset, Henkilötietolaki, Tietoyhteiskuntakaari, Laki yksityisyydensuojasta työelämässä)

Lokien käyttötarkoitus ja käytön valvonta kuvataan asianmukaisesti (mm. mihin lokitietoja saa käyttää ja kuka sekä miten). Huomioi, että loki on henkilörekisteri, mikäli se sisältää henkilötietoja. Lokitietoihin vältetään tallettamasta seuraavia tietoja, ellei sille ole erityistä tarvetta:

- henkilötunnuksia ja henkilötietolain määrittelemiä muita arkaluonteisia henkilötietoja
- luottokorttinumeroita, pankkiyhteystietoja tai vastaavia
- salasanoja (henkilöiden tai järjestelmien välisiä)
- henkilöiden välisen viestinnän sisältöä

Lokitiedot talletetaan ja ne suojataan siten, että

- lokien käsittely ja lukeminen on rajoitettu vain sitä tarvitseville henkilöille
- tietojen talletuksessa, käsittelyssä ja poistamisessa huomioidaan lokitietojen mahdollisesti sisältämät henkilötiedot tai muut salaiset tai salassa pidettävät tiedot
- lokitietojen lukemisesta ja käsittelystä kerätään lokia
- tiedot säilyvät eheinä ja muuttumattomina, lokitietoja ei pääse muuttamaan, poistamaan tai lisäämään jälkikäteen
- lokitietojen tallennusvälineet ovat riittävän hyvin suojattuja ja tieto salattu
- lokitiedot varmuuskopioidaan säännöllisesti ja yksi kopio säilytetään erillisellä, verkkoon kytkemättömällä tallennusvälineellä
- säilytysajan jälkeen lokitiedot poistetaan turvallisesti ja pysyvästi

Lokitiedot auditoidaan ja tarkastetaan esimerkiksi puolivuosittain niiden eheyden ja oikeellisuuden varmistamiseksi. Lokien tietojen tallentuminen varmistetaan.

Tietoturvatapahtumien ja väärinkäytösten selvittämistä varten lokien säilytysaika on vähintään 6 kuukautta, mahdollisuuksien mukaan 24 kuukautta tai enemmän (huomioitava myös mahdolliset lain vaatimat pidemmät säilytysajat tai vastaavasti rajoitukset säilytysaikoihin)

Lokitietoa kerätään mahdollisuuksien mukaan seuraavista tapahtumista, jotta voidaan seurata ja tarkkailla järjestelmän toimintaa, havaita poikkeamat normaalista toiminnasta ja tunnistaa tietoturvaongelmat sekä väärinkäytökset:

- ***Käyttäjätoiminnot:*** Kirjautumiset, kirjautumisyritykset, käyttäjätapahtumat ja -toiminnot, kuten salaista tai salassa pidettävää tietoa sisältävien tiedostojen avaaminen, muokkaaminen ja poistaminen.
- ***Järjestelmätapahtumat:*** Järjestelmän käynnistys- ja sammutustapahtumat, prosessien käynnistämiset ja lopettamiset, palvelintapahtumat ja järjestelmähäiriöt.
- ***Verkkoliikenne:*** Verkkoliikenteen lokitiedot, kuten IP-osoitteet, protokollat, käyttäjäagentit ja siirretyn datan määrä.
- ***Sovellustapahtumat:*** Sovellusten käyttöön liittyvät tapahtumat, kuten tietokantakyselyt, API-kutsut, virheet ja poikkeamat.
- ***Tietoturvatapahtumat:*** Kaikki tietoturvaan liittyvät tapahtumat, kuten epäonnistuneet kirjautumisyritykset, havaittu epäilyttävä tai haitallinen toiminta ja hyökkäykset sekä järjestelmien luvaton käyttö.
- ***Järjestelmän resurssien käyttö:*** Järjestelmän resurssien, kuten CPU:n, muistin ja levytilan, käyttöön liittyvät tapahtumat ja tilastot.
- ***Järjestelmämuutokset:*** Lokitiedot tietokoneiden ja käyttöjärjestelmien hallinnasta, kuten päivitykset ja konfiguraatiomuutokset.
- ***Varmuuskopiot ja palautukset:*** Lokitiedot varmuuskopioiden luomisesta ja palautuksista.
- ***Tietojen käsittely:*** Lokitiedot salaista tai salassa pidettävää tietoa sisältävien tiedostojen luomisesta, muokkauksista, poistamisista ja tietojen eheyden tarkistuksista.
- ***Käyttöoikeudet ja roolit:*** Lokitiedot käyttäjien ja ryhmien käyttöoikeuksista, rooleista ja niihin tehdyistä muutoksista.
- ***Lokien käsittely:*** Lokitiedot lokien lukemisesta, käsittelystä tai muokkausyrityksistä.
- ***Viestintä:*** Tiedot viestinnästä ja viestinvaihdosta.

LIITE 7

Esimerkki – Varautuminen ICT-palvelusopimuksessa

ICT-palvelusopimukset määrittelevät palveluntarjoajan ja asiakkaan väliset vastuut ja velvollisuudet. Sopimusten rakenne ja sisältö on suunniteltava huolellisesti, jotta ne kattavat kaikki olennaiset osa-alueet ja varmistavat palveluiden jatkuvuuden häiriötilanteissa. Varautuminen on olennainen osa ICT-palvelusopimuksia. Varautumistoimenpiteitä ovat muun muassa riskienarviointi, jatkuvuus- ja valmiussuunnittelu, tekniset ja rakenteelliset ennakkovalmistelut ja ratkaisut, koulutus, harjoitukset sekä tilojen ja kriittisten resurssien varaukset.

Palvelusopimuskokonaisuus muodostuu yleensä useista eritasoisista sopimuksista, joihin sisällytetään myös eritasoiset varautumisen vaatimukset. Sopimuskokonaisuus voi muodostua esimerkiksi raami- tai puitesopimuksesta, asiakaskohtaisista palvelusopimuksista, tuotteistetuista palvelusopimuksista ja lisenssisopimuksista. Näiden lisäksi on yleisiä sopimuksia kuten tietojenkäsittely-, tietosuoja-, tietoturva ja salassapitosopimukset.

Yleiset sopimukset
- Tietojenkäsittelysopimus
- Tietoturva- ja tietosuoja
- Salassapitosopimus
- ...

Raami- tai puitesopimus liitteineen
- Yleiset varautumisen periaatteet
- Kaikkia ostettuja palveluita koskevat varautumistoimet
- Varautumissuunnitelma

Palvelun asiakaskohtaiset sopimukset liitteineen
- Palvelukohtaiset varautumisen vaatimukset ja palvelutasot
- Palvelukohtaiset toipumissuunnitelmat

Palveluun käyttämiin tuotteisiin liittyvät sopimukset ja ehdot
- Mm. lisenssisopimukset ja -ehdot

Sopimuksiin sisällytettäviä varautumisen vaatimuksia ovat esimerkiksi

Sopimus	Sopimuksessa sovittavia varautumisen vaatimuksia (esimerkiksi)
Raami- tai puitesopimus ja liitteet	Yleiset varautumisen periaatteet ja vaatimukset ja vaatimus palveluntarjoajan ajantasaisille varautumis- ja toipumissuunnitelmille Varautumisen vaatimusten edellyttäminen alihankkijoilta. Vaatimus säännölliselle testaamiselle ja harjoittelulle sekä suunnitelmien ylläpitämiselle. Tiedottamisvelvollisuus, kommunikointi ja viestintäkäytännöt Palvelutuotannon mahdollisimman häiriöttömän toiminnan varmistaminen myös ”Force Majeure” -tilanteissa. Yhteiset ja palveluntarjoajan käytännöt uhkien ja riskien hallitsemiseksi. Poikkeaminen käsittely ja raportointi. Yleisen varautumissuunnitelman sisältö esim. ● Häiriönhallintaprosessi, vakavien häiriöiden hallintaprosessi ja toiminta kriisitilanteessa sekä yhteyshenkilöt ● Viestintä häiriötilanteessa ● Vakavan häiriötilanteen organisaatio, vastuut, yhteystiedot ● Vastuunjako häiriöiden ja palautumisen osalta: asiakas/palveluntarjoaja ● Loki- ja varmuuskopiointivaatimukset ● Henkilöstön ja työvoiman saatavuuden varmistaminen ● Fyysinen turvallisuus ● Varautumiseen liittyvä koulutus ja harjoitukset sekä jatkuva kehittäminen ● Järjestelmien ja tietovarastojen palautuksen priorisointi laajoissa häiriöissä
Palvelun asiakaskohtainen sopimus ja liitteet	Palvelukohtaiset vaatimukset normaaliolojen, vakavien häiriöiden ja poikkeusolojen osalta, kuten ● Palvelutasot (SLA) ja palautumisen vaatimukset (RTO, RPO) ● Palvelukohtaiset loki- ja varmuuskopiointivaatimukset ● Mahdolliset tekniset ja arkkitehtuurivaatimukset ● Tiedon ja järjestelmien luokittelu sekä niiden mukaiset vaatimukset sekä varotoimet Palvelukohtaiset toipumissuunnitelmat ● Toipumisessa tarvittavat resurssit ● Riippuvuudet ja priorisointi (muut järjestelmät, ympäristöt, alustat) ● Toimintatapa toipumiseksi (Recovery Procedure), ml. tarvittavat lisenssit, mediat, laitteet, yhteydet ● Tunnistetut järjestelmäkohtaiset riskit ja niiden huomioiminen ● Käytännöt vahingon tai häiriön rajaamiseksi ja eristämiseksi ● Toipumissuunnitelman testauskäytännöt ja -suunnitelma
Tuotteiden yleiset sopimus- ja lisenssiehdot	Palveluntarjoajan vakiopalvelutasot ja käytännöt Käyttöoikeuksien turvaaminen häiriöiden ja poikkeusolojen aikana Mahdolliset escrow-järjestelyt tms.
Tietoturvasopimus	Tietoturvaan liittyvät vaatimukset ja käytännöt

LIITE 8

Kriisiorganisaatio ja johtamistoiminta

Varautuminen ja jatkuvuudenhallinta ***sisällytetään osaksi organisaation normaalia johtamista ja toimintaa.***

Varautumissuunnitelmissa on määriteltävä missä tilanteessa ja miten kriisiorganisaation toiminta käynnistetään. Tyypillisesti vakavasta häiriötilanteesta ensimmäisenä kuuleva kriisinjohtoryhmään nimetty henkilö ottaa johtovastuun ja käynnistää kriisinjohtoryhmän toiminnan. Kriisiorganisaatiolle on hyvä määritellä kokoontumistapa ja -paikka ennakkoon, jota kaikki automaattisesti noudattavat. Samoin etukäteen sovitaan yhteydenpitotavat ja viestivälineet mukaan lukien vaihtoehtoiset kanavat.

Tavanomaisten häiriöiden hoitaminen tapahtuu palvelutuotannon normaalien prosessien mukaisesti. Poikkeusoloissa ja kriisitilanteessa lähtökohtaisesti toimintaa jatketaan samoilla periaatteilla, mutta johtaminen ja viestintä toteutetaan kriisiorganisaation mukaisesti sekä tarpeen mukaan lisätään resursseja ja intensiteettiä häiriön selvittämiseen ja toipumiseen.

Vakavan häiriötilanteen aikaisen ***tilannekuvan muodostaminen***, sen ylläpito, dokumentointi ja raportointi tarvitseville tahoille on vastuutettava ja resursoitava. Tiedon kerääminen, tarkistaminen ja tilannekuvan muodostaminen vaatii kriisitilanteessa vähintään yhden henkilön, usein useamman. Tilannekuvatoiminto ja sen käyttämät työvälineet, tietolähteet ja menetelmät on suunniteltava. Tilannekuvan muodostamiseen oleelliset lähteet on määriteltävä etukäteen, jotta kriisissä osataan etsiä tietoa oikeista lähteistä kattavasti. Mediaseuranta edellyttää resursseja ja myös siinä käytettävät lähteet tulee olla etukäteen määriteltyjä.

Kriisinjohtoryhmä ***päättää erikseen paluusta normaaliin, mahdolliset jälkitoimenpiteet ja niiden seurannan*** sekä mahdollisen päivystystarpeen tai korotetun valmiuden. Häiriön aikainen loki, pöytäkirjat, tilanneselostukset sekä laadittu raportti arkistoidaan.

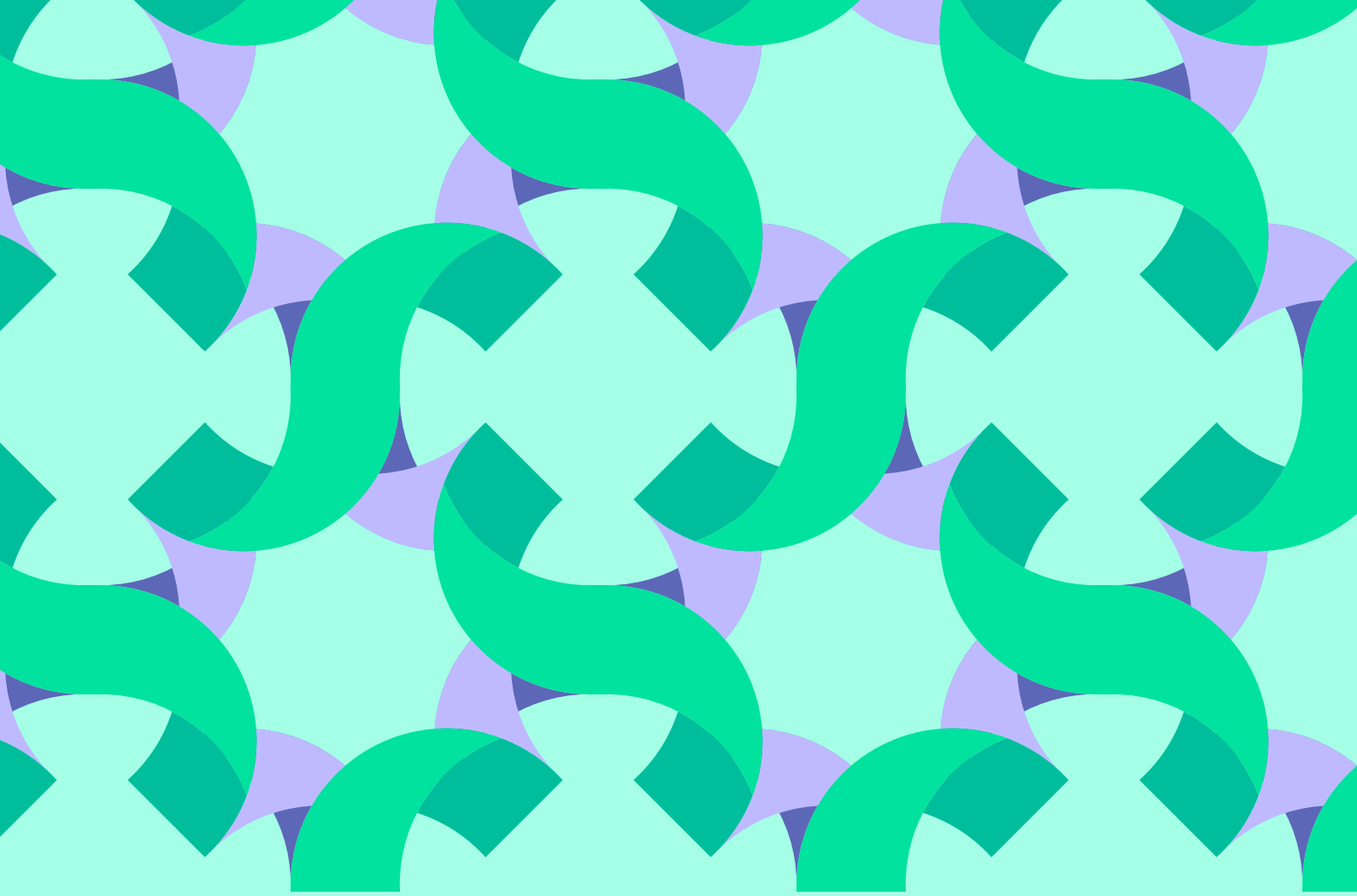
Määrittele etukäteen toimintatapa rikosepäilyjä varten (mm. kuka on yhteydessä viranomaisiin ja kenen päätöksellä) ja selvitä viranomaisten kontaktit sekä ilmoituskanavat mm. kyberhäiriöiden ilmoittamista varten. Esimerkiksi viranomaiset, poliisiammattikorkeakoulu ja kyberturvallisuuskeskus ovat julkaisseet tarkempia ohjeita rikosepäilyitä varten.[4]

Kriisitilanteen hoitaminen edellyttää selkeästi määriteltyjä vastuita, jotka ovat kaikkien osapuolten tiedossa. Vastuut ja sijaisuudet noudattavat ensisijaisesti tavanomaisia rooleja ja tehtäviä, jolloin roolit ja toimintatavat ovat tuttuja. Vakavassa häiriötilanteessa voidaan joutua toimimaan vajaalla henkilöstöllä, joten on erityisen tärkeää kuvata roolit, vastuut, valtuudet ja sijaiset – kriittisiin rooleihin on aina löydyttävä henkilö. Sijaiset ja varahenkilöt on koulutettava ja harjoitettava rooliin mukaiseen toimintaan. Varautumissuunnitelmassa pitää olla vähintään roolit, vastuut, yhteystiedot ja häiriönaikaiseen toimintaan liittyvät osuudet oltava kaikkien kriisintilanteen hoitamiseen osallistuvien saatavilla kaikissa häiriötilanteissa (suunnitelma talletettu työasemien levylle tai muistitikulle, paperikopiot tms.). Roolit ja vastuut perehdytetään henkilöille koulutuksen ja säännöllisen harjoittelun avulla harjoitussuunnitelman mukaisesti. Roolit ja vastuut, niiden säännöllinen kertaus sekä niissä tapahtuvat muutokset tiedotetaan koko organisaatiolle osana päivittäistä johtamista (esimerkiksi kuukausi tai viikkopalavereissa). Vastaavasti roolit ja vastuut sekä niiden muutokset käsitellään keskeisten sidosryhmien kanssa säännöllisissä sidosryhmäpalavereissa sekä yhteisissä harjoituksissa.

4 https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisiasia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212/Opas_Kyberrikos+on+poliisiasia.pdf
https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/asioi-kanssamme
https://poliisi.fi/kyberrikosten-tutkinta

Keskeisiä rooleja ICT-palvelutuotannon kriisiorganisaatiossa ovat yleensä:

Rooli	Roolin vastuut ja tehtävät (esimerkkejä)
Kriisin johtaja	Kriisin johtaja käyttää erikseen määriteltyjä valtuuksia kriisin / vakavan häiriötilanteen hoidon vaatimassa laajuudessa. Kriisin johtaja delegoi valtuuksia tarpeen mukaan muille kriisiorganisaation jäsenille. Kriisin johtajan tärkeimpiä tehtävät ovat: ● johtaa tilannetta kokonaisuutena ja tehdä strategiset päätökset ● seurata kokonaistilannetta, varmistaa välittömien ja häiriön kehitystä ennakoivien toimenpiteiden suunnittelu ja toteutus ● varmistaa tehtävien koordinointi ja priorisointi ● päättää ICT-organisaation vastuulla olevan viestinnän taktiikasta, sisällöstä ja menetelmistä (sisäinen viestintä, kumppaniviestintä) ● päättää paluusta normaalitilanteeseen ja häiriön jälkitoimista ● osallistua yrityksen kriisinjohtoryhmän toimintaan
Tilannekuvasta vastaava	Tilannekuvasta vastaavan tehtäviä ovat ● ylläpitää lokikirjaa ja ajantasaista ICT:n tilannekuvaa (käsitys kokonaisuudesta, vallitsevista olosuhteista ja tilanteen kehityksestä, arvio tilanteen kehittymistä, eri toimijoiden valmiuksista jne.) ja välittää tilannekuvaa kriisijohtoryhmälle ● varmistaa tiedonkulku yhteistyökumppaneille ● kerätä oman organisaation, viranomaisten, muiden yhteistoimintaosapuolien tapahtumia, päätöksiä, viestejä, määräyksiä sekä mahdollisesti muuta informaatiota. ● toimia kontaktipisteenä ulospäin
Häiriön korjaamisesta vastaava	Häiriön korjaamisesta vastaava johtaa häiriön poistoon liittyviä käytännön toimenpiteitä ja ohjaa palvelutoimittajia. Henkilö voi olla vaihdella riippuen siitä, millaisesta häiriöstä on kyse.
Viestinnästä vastaava	Vastaa ICT-palvelutuotannon vastuulla olevasta viestinnästä ICT-kriisinjohtoryhmän päätösten ja linjausten mukaisesti mm. yrityksen johdolle, yhteistyötahoille ja henkilökunnalle (huomioiden yritystasoiset linjaukset ja käytännöt)



Huoltovarmuusorganisaatio
Digipooli