VAHTI-sihteeristö

8.10.2025

# Vinkkejä kyber- ja digiturvan kehittämiseen syksyllä 2025

*Oheiset vinkit pohjautuvat Digi- ja väestötietoviraston Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän asettamien VAHTI-työryhmien sihteeristön sekä asiantuntijoiden havaintoihin ja keskusteluihin.*

## Johdanto

Organisaation kyber- ja digiturvallisuuden kehittäminen on jatkuva prosessi, ei yksittäinen projekti. Se edellyttää suunnitelmallista toimintaa, mutta myös valmiutta reagoida nopeasti erilaisiin poikkeamiin. Kehittäminen perustuu organisaation nykytilan tuntemiseen riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvan sekä tietosuojan osalta. Näihin liittyvien kehittämistarpeiden tunnistaminen on edellytys vaikuttaville toimenpiteille.

Tähän muistioon on koottu keskeisten vuosina 2024–2025 havaittujen tietoturvatapahtumien pohjalta tunnistettuja tarkistettavia kehittämiskohteita. Muistion lopussa esitetään 26 nostoa, joiden avulla organisaatio voi arvioida omaa kyberturvallisuuden ja digiturvallisuuden tilaa. Materiaali tarjoaa tiiviin ja käytännönläheisen kokonaisuuden keskeisistä, ajankohtaisista havainnoista.

## 1. Kyber- ja digiturvallisuuden tilannekuva sekä johtaminen

Suojelupoliisi ja Traficomin Kyberturvallisuuskeskus julkaisivat tiedotteen 29.8.2025, jossa todettiin Suomen uhkatason pysyneen edelleen kohonneena. Käytännössä vakavien tapausten (tietomurtojen) määrä on jo yli kaksinkertaistunut viime vuoteen verrattuna. Lisäksi Kyberturvallisuuskeskus julkaisi 9.9.2025 vuoden 2025 ensimmäisen varoituksen koskien Microsoft M365-tilimurtoja, joiden määrä on kasvanut merkittävästi. Nämä sekä muut huolestuttavat kansainväliset uutiset osoittavat, että verkkorikollisuuden määrä ja vaikuttavuus on edelleen kasvamassa vuoden 2025 aikana ja saman trendin uskotaan jatkuvan vuonna 2026.

Jokaisen julkisen hallinnon organisaation johdon tulisi saada säännöllisesti, useamman kerran vuodessa tietoa organisaation kyber- ja digiturvallisuuden tilanteesta, myös muulloin kuin merkittävien häiriöiden, tietoturvatapahtumien tai tietomurtojen yhteydessä.

Turvallisuuden kehittäminen ja häiriöiden hallinta onnistuvat vain, jos:

- roolit ja vastuut on määritelty selkeästi ja dokumentoitu,
- muutoksista viestitään aktiivisesti kaikille osapuolille,
- tarvittavat dokumentit ovat ajan tasalla ja helposti saatavilla.

Ajantasaiset ohjeet ja dokumentaatio sekä riittävät ja osaavat saatavilla olevat resurssit voivat häiriön tai tietomurron sattuessa ratkaista sen, eteneekö selvitys nopeasti vai hidastuuko se merkittävästi.

Mikäli organisaatio ei itse tuota juurikaan sen käyttämiä palveluita vaan hankkii niitä ulkoisilta palveluntarjoajilta, tällöin hankintoihin, kilpailutuksiin, sopimuksiin, mahdollisiin auditointeihin ja säännöllisiin toimittajatapaamisiin tulee kiinnittää erityistä huomiota.

VAHTI-sihteeristö

8.10.2025

**1.1 Organisaation johdon tulee varmistaa, että organisaatiolla on toimiva ja turvallisuuden eri osa-alueet kattava riskienhallinta, jonka toiminnasta sille raportoidaan.**

Riskienhallinta on kaiken turvallisuustyön ydin ja poikkileikkaava teema, jonka perusteella organisaatio pystyy tehokkaasti tunnistamaan kehittämiskohteita ja kohdentamaan resurssit kustannustehokkaasti. Koska riskienhallinta ei voi koskaan kattaa kaikkia mahdollisia uhkia, kannattaa keskittyä merkittävimpien riskien hallintaan.

Toteuttamalla organisaation jatkuvuudenhallintaa ja varautumiskykyä organisaatio voi toipua paremmin toteutuneista riskeistä ja kehittää omaa resilienssiä sekä riskinottokyvykkyyttä. Jokainen tällainen tapahtuma pitää käydä läpi erikseen ja varmistaa sen taustalla olleet syyt, jotta organisaatio ja mahdollisesti muut sidosryhmät voivat oppia tapahtumasta ja kehittää omaa toimintaansa ja kehittää samalla riskienhallinnan tarkkuutta.

**1.2 Varmistakaa, että organisaation johto ja henkilöstö tuntevat organisaation toiminnan kannalta oleellisen lainsäädännön ja vaatimukset, suojattavan omaisuuden sekä niihin liittyvät uhat ja riskit.**

Toimintaympäristön, vaatimusten ja suojattavan omaisuuden tunnistaminen toimii perustana kyber- ja digiturvan toimenpiteille, riskienhallinnalle ja ohjeistuksille. Jos edellä mainittuja teemoja ei tunneta riittävän hyvin, myöskään yksityiskohtaisempia turvallisuustoimenpiteitä ei voida kohdentaa oikein.

**2. Tekninen tietoturvallisuus**

**2.1 Varmistakaa että organisaatio on tunnistanut kaikki julkiseen verkkoon näkyvät laitteet ja palvelut, ja että ne ovat automaattisten tietoturvapäivitysten, hallinnan sekä valvonnan piirissä.**

Useat tietomurrot käynnistyvät ns. verkon reunalaitteiden, palvelimien tai päätelaitteiden kautta niissä piileviä haavoittuvuuksia hyödyntämällä. Tämän takia organisaatiolla tulee olla ajantasainen kuva sen käytössä olevasta ICT-toimintaympäristöstä, jonka avulla se on selvillä laitteiden ja palveluiden turvallisuuden tasosta ja elinkaaren tilasta. Organisaatioiden tulee seurata aktiivisesti keskeisten laitetoimittajien ja viranomaisten haavoittuvuustiedotteita ja varmistaa, että myös palveluntarjoajat toimivat näin.

Suomessa on useita esimerkkejä siitä, että tietomurto on käynnistynyt hyökkääjän havaittua haavoittuvuuden kriittisessä organisaation verkkolaitteessa, palvelimessa tai palvelussa, jonka kautta on murtauduttu organisaation palvelimille tai sisäverkkoon. Rikolliset tulevat yhä enemmän hyödyntämään tekoälyä näiden haavoittuvuuksien tunnistamisessa ja hyökkäysten toteuttamisessa. Aika, kuinka nopeasti verkkorikolliset hyödyntävät tunnistettuja haavoittuvuuksia aikaisempien viikkojen sijaan on nyt jopa enää tunteja. Tämän takia organisaatioilla tulee olla näkymä omaan hyökkäyspintaan ja kykyä havaita ja reagoida haavoittuvuuksiin entistä nopeammin tulee parantaa.

Esimerkiksi 14.10.2025 loppuu Microsoft Windows 10-käyttöjärjestelmän tietoturvapäivitysten tuki, joka edellyttää tätä käyttävien tietokoneiden päivittämistä Windows 11-käyttöjärjestelmään, poikkeustapauksissa maksullisten päivitysten hankkimista tai laitteiden turvallista eristämistä. On erittäin todennäköistä, että verkkorikolliset tulevat metsästämään pian tietoturvapäivitysten ulkopuolelle jääviä Windows 10-työasemia ja käyttämään niitä apuna hyökkäyksissä.

**2.2. Varmistakaa, että organisaation käytössä olevien ICT-laitteiden toiminta lokitetaan kattavasti riittävän pitkäaikaisesti sekä lokit suojataan mahdolliselta hyökkääjän lokien muutos- tai hävittämisyrityksiltä.**

Nämä toimenpiteet eivät välttämättä estä yhtään tietomurtoa, ellei lokitukseen ole kytketty muuta havainnointi- ja reagointikykyä, mutta lokitusta edellytetään useissa velvoitteissa ja ne helpottavat merkittävästi tapahtumien jälkikäteistä selvittämistä ja teknisen ympäristön eheydestä varmistumista. Keskitetyn lokienhallinnan hyödyntäminen on suositeltavaa niin valvonnan kuin samanaikaisten tapahtumien seurannan ja selvittämisen näkökulmasta.

**2.3. Varmistakaa, että organisaation varmuuskopiojärjestelmä on suojattu kattavasti, se toimii suunnitellusti ja kykenette tarvittaessa palauttamaan laajempia tietojärjestelmäkokonaisuuksia.**

Erityisen tärkeää on varmistaa, että mahdollinen hyökkääjä ei pysty hävittämään tai muokkaamaan organisaation varmuuskopioita. Tunnetuimpien lunnashaittaohjelmarikollisjärjestöjen hyökkäyssuunnitelmista löytyy kattavat ohjeet sekä lokien että varmuuskopioinnin toiminnan halvaannuttamiseksi tai tuhoamiseksi. Tämän takia varmuuskopiojärjestelmän pitää olla suojattu, irrotettu tai muuten eristetty turvallisesti muusta ICT-palveluympäristöstä. Suositeltavaa on myös ottaa talteen ns. pitkäaikaissäilytettäviä turvakopioita, joita voidaan tarvittaessa fyysisesti säilyttää toisessa tilassa. Varmuuskopiointia ei voida pitää luotettavana ja toimivana, ellei sitä säännöllisesti testata, myös hieman haastavampien palautusten osalta.

**2.4. Varmistakaa organisaationne kyky ennakolta havaita, tunnistaa ja reagoida tietomurtoyrityksiin.**

Organisaation toiminnan kriittisyys vaikuttaa siihen, tuleeko sillä tai sille ICT-palveluita tuottavalla organisaatiolla olla 24/7 kyvykkyys seurata, havainnoida, tunnistaa ja reagoida sen ICT-ympäristössä tapahtuvaan tietomurtoepäilyyn. Tämän ohella organisaatiolla tulee olla ohjeistus ja tiedotus, miten sille voidaan ilmoittaa tällaisista tai näiden epäilystä, ja miten prosessi tällaisen ilmoituksen jälkeen lähtee organisaatiossa liikkeelle.

Erityisenä haasteena useassa organisaatiossa on se, että heillä ei ole omaa henkilöstöä käytettävissä virka-ajan ulkopuolella. Esimerkiksi perjantai-illalla tehty ilmoitus tai epäilys saattaa jäädä reagoimatta viikonlopun yli 60 tunniksi, jona aikana epäilyksen sijaan maanantaina organisaatiolla saattaa olla vastassa ja käynnissä jo tietomurto.

Tämä ei automaattisesti edellytä 24/7-tietoturvavalvomon hankkimista, myös virka-aikana toimivasta aktiivisesta valvonnasta on hyötyä. Tärkeää on kuitenkin varmistaa, että organisaation käytössä olevat haittaohjelmien torjuntaohjelmat on konfiguroitu oikein hälyttämään erilaisista poikkeamista ja yrityksistä, sekä näitä ilmoituksia seurataan ja niihin reagoidaan edes virka-aikaisin.

On myös tärkeää, että organisaation koko henkilöstö on ohjeistettu ja koulutettu ilmoittamaan organisaation prosessien mukaisesti, mikäli he havaitsevat jotain tavallisesta poikkeavaa. Tämä vaatimus koskee myös toimitusketjun organisaatioiden henkilöstöjä.

**3. Jatkuvuudenhallinta ja varautuminen sekä häiriö- ja kriisitilanteiden hallinta**

**3.1 Organisaatio on tunnistanut sen palveluiden ja toiminnan kriittisyyden.**

Kaikki palvelut eivät ole yhtä tärkeitä. Tämän takia on tärkeää varmistaa, että organisaation voimavarat suunnataan sen kriittisimpien palveluiden turvallisuuden kehittämiseen, ylläpitämiseen ja valvontaan.

**3.2. Organisaatiolla tulee olla selkeät suunnitelmat ja ohjeet erilaisia häiriöitä, hyökkäyksiä ja tietomurtoja varten, lisäksi vastuut eri henkilöiden ja eri toimijoiden välillä tulisi olla selkeät tällaisen tapahtuessa.**

Suunnitelmat tulee olla vastuuhenkilöiden osalta myös etukäteen harjoiteltu. Suunnitelmissa pitää olla selkeät ohjeet viranomaisille tehtäviä ilmoituksia varten sekä kriisiviestintään omaan organisaatioon, sidosryhmille, julkisuuteen sekä mahdollisille tietomurron uhreille.

Vastuut tulee olla selkeästi kuvattuna, tässä on mahdollista käyttää erilaisia malleja, yksi sellainen on tunnettu RACI-vastuunjakomatriisi.

Etenkin uhreihin liittyvään viestintään vaikuttaa merkittävästi se, mitä tietoja on vuotanut, tunnistetaanko uhrit sekä uhreihin liittyvät muut (demografiset) taustatiedot. Nämä suunnitelmat voivat olla osana laajempaa jatkuvuudenhallintaa, varautumista ja valmiutta sisältävää ohjekokonaisuutta.

Osana suunnitelmia tulisi toteuttaa säännöllistä harjoitustoimintaa erilaisia tilanteita varten. Suosittelemme, että jokainen organisaatio osallistuu Digi- ja väestötietoviraston yhdessä muiden viranomaisten kanssa toteuttamaan Taisto25-kyber- ja digiturvaharjoitukseen marraskuussa 2025.

**4. Henkilöstön kyber- ja digiturvaosaamisen kehittäminen**

**4.1 Organisaation johdon tulee varmistaa, että henkilöstö saa säännöllistä, ajantasaista koulutusta siihen kohdistuvien uhkien tunnistamiseksi ja turvalliseen toimintaan.**

Tämä koskee organisaation koko henkilöstöä, niin IT-henkilöstöä kuin esihenkilöitä, päälliköitä ja ylintä johtoa. Annettuja ohjeita ja muita tunnettuja IT-palvelutuotannon hyviä käytäntöjä pitää noudattaa. Nämä pitää olla sovittuna myös organisaatiolle palveluita tuottavien alihankkijoiden ja muiden toimijoiden osalta.

Erityisesti verkkorikollisuus, kansalaisiin kohdistuneet digihuijaukset ja organisaation henkilöstöön kohdistuvat kalasteluviestit ovat sekä määrällisesti kasvaneet että kehittyneet laadullisesti parin viimeisen vuoden aikana. Näistä ajantasainen tiedottaminen on tärkeää, jotta henkilöstö ei haksahda klikkaamaan tällaisia erittäin hyvin valmisteltuja hyökkäyskampanjoita ja sitä kautta vaaranna omia ja organisaation tietoja.

Yhä useampi työntekijä on siirtynyt 2020-luvulla etätöihin, joka on saattanut aiheuttaa pysyviä, merkittäviä muutoksia toimintatavoissa. Nyt loppuvuoden 2025 aikana kannattaisi tehdä päivitys ja muistutus henkilöstölle siitä, mitkä ovat ne keskeiset uhat ja riskit, jotka jokaisen tulisi muistaa erityisesti etätöissä.

**4.2 Varmistakaa, että henkilöstö osaa hallita käyttäjätunnuksia ja salasanoja turvallisesti.**

Useissa tietomurroissa on pystytty hyödyntämään eri keinoilla haltuun saatuja käyttäjien, myös pääkäyttäjien (administrator) salasanoja. Erityisesti pääkäyttäjien turvallinen toiminta on kriittistä, mutta myös jokaisen käyttäjän tulee huolehtia, että jokaisessa palvelussa käytetään laadukkaita ja ainutkertaisia salasanoja.

Pääkäyttäjien, mutta myös henkilöstön tulee käyttää kaksivaiheista tunnistautumista kaikissa niissä palveluissa, joissa se on mahdollista. Tämän ohella pääkäyttäjille on suositeltavaa hankkia muita pelkästään laitteiden ja palveluiden hallintaan tarkoitettuja turvapalveluita tai -laitteita. Erityisesti pääkäyttäjäoikeuksiin liittyvää tietoturvaa on myös mahdollista tehostaa hallinnollisten käytäntöjen, kuten vähimpien oikeuksien periaatteen, tehtävien eriyttämisen ja pääsyn valvonnan ja rajoittamisen avulla. Mikäli organisaationne tarjoaa palveluita asiakkaille, myös asiakkaille on syytä tarjota kaksivaiheinen tunnistautuminen sekä viestiä turvallisesta palveluiden käytöstä.

**5. Tiedonhallinnan toteuttaminen ja ohjeistaminen**

**5.1 Organisaatiolla tulee olla selkeät ohjeet tiedonhallintaan, jotka on koulutettu henkilöstölle ja henkilöstön osaamista seurataan.**

Jokaisen organisaation yksi tärkeimpiä tehtäviä on huolehtia sen henkilöstön, asiakkaiden ja muiden sidosryhmien tuottamien tietojen ja datan turvallisesta hallinnasta. Henkilöstöllä tulee olla selkeät ohjeet siihen, miten erilaisia tietoja käsitellään, minne niitä tallennetaan ja miten toimitaan etenkin erityisiin henkilötietoryhmiin liittyvien ns. ”arkaluonteisten” sekä turvakiellon alaisten henkilötietojen käsittelyn osalta. Käytännössä henkilöstön tulee osata, miten tietoja luokitellaan, tunnistaa missä fyysisissä tiloissa niitä voidaan käsitellä, tietää, mitä laitteita ja digipalveluita pitää käyttää erilaisten tietojen käsittelyyn sekä mitä tiedoille tehdään, kun niitä ei enää tarvita.

Henkilöstö tulee ohjeistaa ja kouluttaa tiedon elinkaaren kaikkiin vaiheisiin työtehtävien ja vastuiden mukaisesti. Tämä alkaa siitä, mitä tietoja voidaan tuottaa ja käsitellä, ja päättyy siihen, mitä tiedolle tulee tehdä, kun tietoa ei enää tarvita operatiivisessa toiminnassa.

Tietoja ei saa noin vain hävittää, vaan sen tulee pohjautua organisaation asian- ja tiedonhallinnasta johdettuihin ohjeisiin ja neuvottuihin turvallisiin käytäntöihin. Asian- ja tiedonhallinnasta vastaavien tulee varmistaa, että tiedonhallinnan elinkaarenhallinta toimii ohjeistetusti ja tiedot poistetaan tai arkistoidaan vaatimusten mukaisesti. Vastaavasti jokainen käyttäjä voi itse huolehtia siitä, että tarpeettomat väliaikaiset työtiedostot eivät jää roikkumaan omalle työasemalle, saati yhteiskäyttöisille tiedostopalvelimille.

Organisaation tulee pyrkiä minimoimaan rakenteeton henkilötieto. Tällaisia henkilötietoja voi löytyä esim. sähköposteista, verkkolevyiltä ja yhteistoimintatyökaluista, kuten Teams. Rakenteettoman henkilötiedon sijainnit tulee tunnistaa ja dokumentoida sekä valvoa niiden ylläpitoa.

**6. Alihankkijat, sidosryhmät ja toimitusketjut**

**6.1 Organisaation pitää tunnistaa sen oma ja sille palveluita tuottavien toimijoiden rooli osana usein kompleksista toimitusketjukokonaisuutta.**

VAHTI-sihteeristö 8.10.2025

Jokainen organisaatio on entistä riippuvaisempi sen alihankkijoista ja toimitusketjuista. Helpointa tämä on havaita esimerkiksi sähkönjakelu- ja tietoliikenneyhteyksien riippuvuuksien osalta.

Organisaatio voi omasta näkökulmastaan pitää joitain palveluitaan “ei niin kriittisinä”. Mutta jos nämä palvelut toimitetaan asiakasorganisaatiolle, joka tuottaa yhteiskunnan kannalta kriittisiä toimintoja, ne voivat olla asiakkaalle elintärkeitä.

Jokaisen organisaation tulee siksi tunnistaa roolinsa erilaisissa toimintaverkostoissa ja alihankintaketjuissa sekä priorisoida turvallisuuden kehittäminen näiden riippuvuuksien ja kriittisyyksien mukaisesti.

Organisaation pitää dokumentoida kaikki edellä mainitut asiat ja katselmoida ja tarvittaessa päivittää dokumentit säännöllisesti. Samalla tulee varmistaa, että dokumentaatio on käytettävissä myös tilanteissa, joissa sähköä ja/tai tietoliikenneverkkoja ei ole käytettävissä.

Hyvä käytäntö on katselmoida dokumentaatio vuosikellon mukaisesti ja merkitä dokumentaatioon, milloin katselmointi on viimeksi toteutettu, vaikka itse sisältöön ei tulisikaan muutoksia. Näin organisaatio ja henkilöstö tunnistavat voimassa olevan ja uusimman version dokumentaatiosta.

## 7. Digi- ja väestötietoviraston lisämateriaaleja ja maksuttomia palveluita

### Henkilöstön osaamisen kehittäminen ja tiedonvaihto

Digi- ja väestötietoviraston digiturvatunti henkilöstölle sekä VAHTI-ajankohtaiskatsaus johdolle ja asiantuntijoille
https://dvv.fi/digiturvatilaisuudet

Digiturvan tietopankki
https://kehittajille.suomi.fi/palvelut/digiturva

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän asettamat kolme VAHTI-työryhmää – näitä asioita ei kannata miettiä ja kehittää yksin, vaan yhdessä – tule mukaan toimintaan:
https://dvv.fi/vahti

### Organisaation kyber- ja digitaalisen turvallisuuden tilannekuva sekä harjoittelu

Digi- ja väestötietoviraston tilannekuvapalvelu
Digiturvan kokonaiskuvapalvelu - Digi- ja väestötietovirasto - Suomi.fi

Ilmoittautukaa Taisto-harjoitukseen marraskuussa 2025
TAISTO-harjoitus | Digi- ja väestötietovirasto | Digi- ja väestötietovirasto

Tutustukaa harjoituksen ennakko-ohjeistukseen
- ohje harjoitukseen valmistuvalle organisaatiolle

Voitte hyödyntää myös harjoituksen ennakkotehtävää kyber- ja digiturvan kehittämisessä
- Taisto-harjoituksen ennakkotehtävä

VAHTI-sihteeristö

8.10.2025

**Liite 1. Kysymyksiä, joiden avulla organisaatio voi tarkistaa oman toiminnan turvallisuutta**

**1. Kyber- ja digiturvallisuuden tilannekuva sekä johtaminen**

*Kysymys 1:*
*Milloin organisaation johdolle on viimeksi raportoitu organisaation uhkatilanteesta tai merkittävästä tietoturvatapahtumasta?*

*Kysymys 2:*
*Milloin organisaatio on viimeksi käynyt perusteellisesti läpi tällaisen tapahtumaketjun, joka on johtanut myös kyseisen tapahtuman osalta riskienhallinnan kehittämiseen ja onko sovitut toimenpiteet toteutettu?*

*Kysymys 3:*
*Miten tunnette organisaatiotanne koskevat vaatimukset ja lainsäädännön kyber- ja digiturvaan liittyen?*

*Kysymys 4:*
*Miten varmistatte, että kyber- ja digiturvallisuus tukee organisaation strategiaa?*

*Kysymys 5:*
*Miten tunnistatte organisaationne suojattavan omaisuuden sekä niihin kohdistuvat riskit ja uhat?*

**2. Tekninen tietoturvallisuus**

*Kysymys 6:*
*Milloin organisaationne on suorittanut verkko- tai haavoittuvuusskannauksen internet-verkosta tai organisaation sisäverkosta etsien haavoittuvuuksia?*

*Kysymys 7:*
*Miten tarkistatte, että käytössänne olevien ICT-laitteiden ja ohjelmistojen tietoturvapäivitykset menevät perille ja ovat ajantasaiset?*

*Kysymys 8:*
*Miten olette varmistaneet, että teillä ei jää käyttöön turvattomia, kattavan suojauksen ulkopuolella olevia Windows 10-työasemia tai muita päätelaitteita?*

*Kysymys 9:*
*Miten olette varmistaneet, että verkkolaitteiden, palvelinten ja päätelaitteiden lokitukset on vakioitu ja määritetty keräämään tietoja tarkoituksenmukaisesti?*

*Kysymys 10:*
*Miten olette harjoitelleet lokitietojen hyödyntämistä?*

*Kysymys 11:*
*Miten olette varmistaneet, että mahdollinen hyökkääjä ei pysty hävittämään tai muuttamaan lokitietoja?*

*Kysymys 12:*
*Miten olette varmistaneet, että mahdollinen hyökkääjä ei pysty lamauttamaan varmuuskopiojärjestelmäänne?*

*Kysymys 13:*
*Miten organisaationne on varmistanut, että sen käytössä olevat haittaohjelmien torjuntaratkaisut sekä muut tietoturvatuotteet ovat konfiguroitu oikein ja että niiden tuottamiin hälytyksiin reagoidaan?*

*Kysymys 14:*
*Mistä löytyy ohje organisaation henkilöstölle ilmoittaa havaitsemistaan uhkista tai riskeistä, entä organisaation ulkopuolisille henkilöille tai toimijoille?*

**3. Jatkuvuudenhallinta ja varautuminen sekä häiriö- ja kriisitilanteiden hallinta**

*Kysymys 15:*
*Mistä löytyy ajantasainen lista organisaation toiminnalle kriittisistä palveluista sisältäen kaikki keskeiset, esimerkiksi tietoturvatapahtuman hallinnassa tarvittavat tiedot?*

*Kysymys 16:*
*Milloin organisaation jatkuvuus- ja varautumissuunnitelmat on viimeksi katselmoitu ja päivitetty?*

*Kysymys 17:*
*Milloin organisaatio on harjoitellut sen prosessien ja ohjeiden mukaista toimintaa siihen kohdistuvan vakavan häiriön tai tietomurron osalta? Miten harjoituksessa tunnistettuja kehittämistoimenpiteitä on edistetty?*

*Kysymys 18:*
*Miten organisaation sisäiset toimintavastuut, entä kriittisten alihankkijoiden ja muiden toimittajien ja sidosryhmien kesken on kuvattu?*

*Kysymys 19:*
*Milloin organisaation johdolle ja muille vastuuhenkilöille on järjestetty viestintäkoulutusta koskien häiriö- tai tietomurron yhteydessä tarvittavaa kriisiviestintää? Onko harjoituksissa huomioitu myös vastuuhenkilöiden varahenkilöt?*

**4. Henkilöstön kyber- ja digiturvaosaamisen kehittäminen**

*Kysymys 20:*
*Miten hyvin organisaatiossa toimii viestintä koskien organisaatioon kohdistuvaa kalasteluviestikampanjaa? Milloin tällainen on viimeksi havaittu?*

*Kysymys 21:*
*Milloin organisaatio on viimeksi päivittänyt etätyöhön liittyvää tietoturvaan ja tietosuojaan liittyvää riskienhallintaa ja ohjeistusta?*

*Kysymys 22:*
*Mistä organisaatiosta löytyy ajantasaiset ohjeet henkilöstölle turvalliseen työskentelyyn digilaitteiden ja -palveluiden osalta?*

*Kysymys 23:*
*Mistä organisaatiosta löytyy ajantasaiset ohjeet järjestelmien pääkäyttäjille turvalliseen ICT-laitteiden ja -palveluiden hallinnointiin?*

**5. Tiedonhallinnan toteuttaminen ja ohjeistaminen**

*Kysymys 24:*
*Milloin organisaatiossa on viimeksi katselmoitu, miten tiedonhallinnan ohjeiden mukainen toiminta on toteutunut ja varmistettu, että tiedot päätyvät niihin palveluihin tai sijainteihin, jonne ne on tarkoitettu?*

*Kysymys 25:*
*Miten henkilöstö osaa hallita tuottamiaan tietoja oikein, jotta sellaiset tiedot, joita ei tarvita, hävitetään turvallisesti ja vastaavasti sellaiset tiedot, jotka edellyttävät tietojen säilyttämistä, säilytetään oikeissa tietojärjestelmissä määräaikojen mukaisesti?*

**6. Alihankkijat, sidosryhmät ja toimitusketjut**

*Kysymys 26:*
*Miten organisaatio on tunnistanut kriittisten palveluiden tuottamiseen liittyvät toimijat ja varmistanut näiden turvallisuuden tason?*

**Lisätietoa ja kysymyksiä?**

Sähköpostitse
digiturva@dvv.fi

Kimmo Rousku
Johtava erityisasiantuntija, VAHTI-pääsihteeri
etunimi.sukunimi@dvv.fi