TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä

Kyberturvallisuuslaki -webinaari 12.5.2025

Erityisasiantuntija Päivi Timlin & tietoturva-asiantuntija Topi Talikka

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen tuottama suositus

Suositus **valvoville viranomaisille** NIS2-direktiivin mukaisista kyberturvallisuuden riskienhallinnan toimenpiteistä.

Suositus voi tukea myös **toimijoiden** kyberturvallisuuden **riskienhallinnan suunnittelua**.

Suositukseen on koottu **tietoa ja käytännön esimerkkejä** siitä, millaisia toimenpiteitä laissa säädettyihin **vaatimuksiin** voi kuulua.

Suosituksessa kuvataan myös erilaisia **keinoja**, joita valvova viranomainen voi harkintansa ja arvionsa mukaan käyttää **ohjaus- ja valvontatehtävissään**.

Säädöspohja

- Liikenne- ja viestintäviraston Kyberturvallisuuskeskus on laatinut tämän suosituksen osana keskitetyn yhteyspisteen viranomaisyhteistyötä ja koordinointitehtävää.
- Suosituksen taustalla on NIS 2 -direktiivi eli **kyberturvallisuusdirektiivi**.
- Suositus keskittyy kyberturvallisuuslain 9 §:ssä ja tiedonhallintalakiin lisätyssä 18 c §:ssä säädettyihin **kyberturvallisuuden riskienhallinnan toimenpiteisiin**.

Säädöspohja

- Suosituksessa ja sen **laajennetussa ohjeistuksessa** on huomioitu komission NIS 2 -direktiivin 21 artiklan 5 kohdan perusteella valmistelema **täytäntöönpanoasetus** ((EU) 2024/2690), jolla vahvistetaan hallintatoimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset.
- Kohdistettu DNS-palveluntarjoajille, aluetunnusrekistereille, pilvipalvelujen tarjoajille, datakeskuspalvelujen tarjoajille, sisällönjakeluverkkojen tarjoajille, hallintapalvelun tarjoajille, tietoturvapalveluntarjoajille, verkossa toimivien markkinapaikkojen tarjoajille, verkossa toimivien hakukoneiden tarjoajille, verkkoyhteisöalustojen tarjoajille ja luottamuspalvelun tarjoajille.
- **Laajennettu ohjeistus** on hyödyllinen myös toimijoille, joilla on korkeampi kyberturvallisuusriski. Esim. toimijat, joilla on omaa ohjelmistokehitystä.

Suosituksen soveltamisesta

- Ei sido viranomaisia eikä toimijoita. Sitovat velvoitteet säädetään:
  - Laeissa,
  - Euroopan komission antamassa tarkentavassa sääntelyssä ja
  - toimialakohtaisen viranomaisen määräyksissä.
- Toimialakohtaiset määräykset tai muu erityissääntely voi sisältää suosituksesta poikkeavia, tiukempia vaatimuksia.
  - Valvova viranomainen ratkaisee, millaiset toimenpiteet täyttävät säädetyt vaatimukset kullakin toimialalla.
  - Suosituksen mukaisten käytäntöjen toteuttaminen ei takaa sitä, että toimija täyttäisi kansallisen sääntelyn edellyttämät vaatimukset.

Kyberturvallisuuden riskienhallinnan toimenpiteet

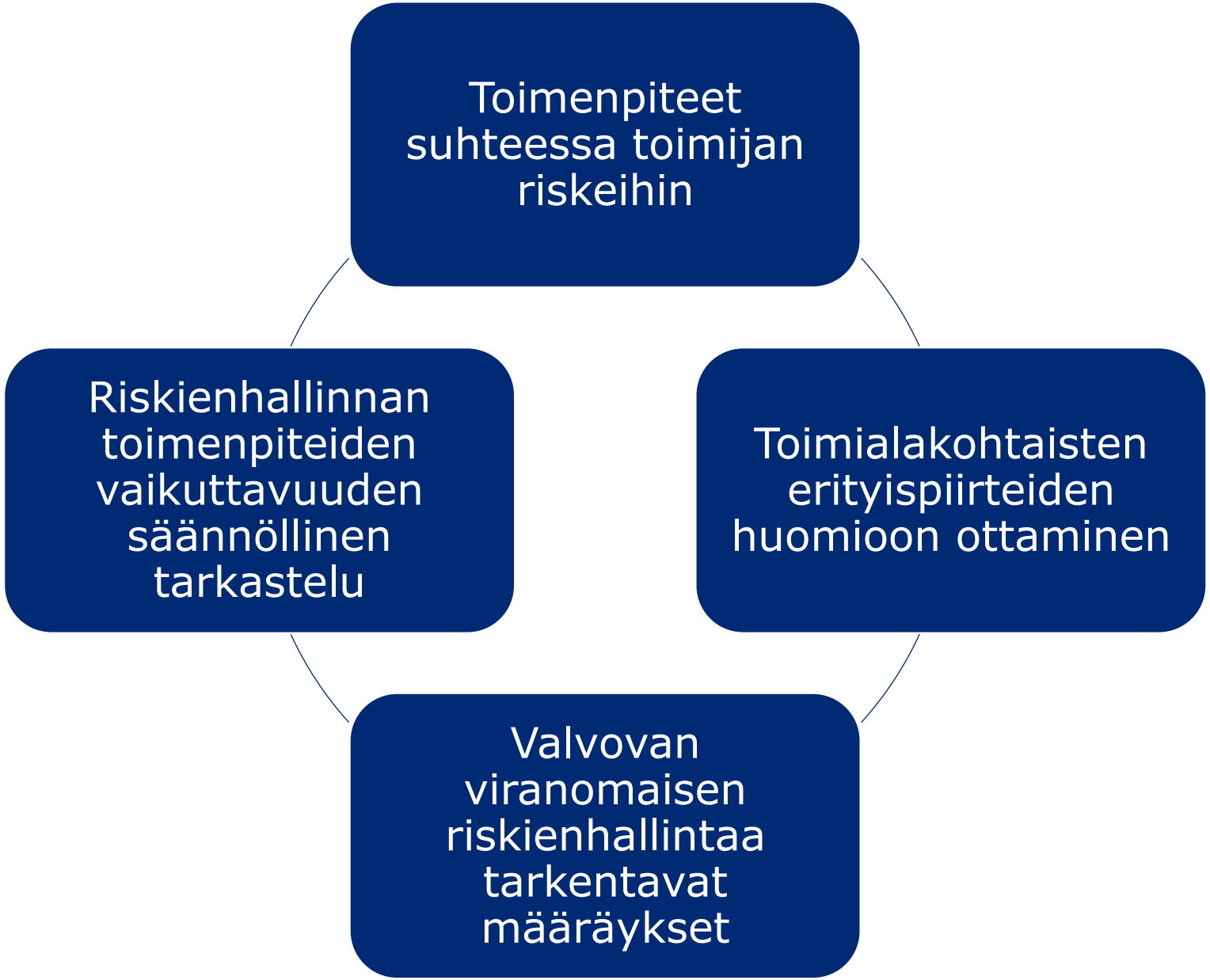
Suosituksen sisällöstä

- Toimijalle asetetaan **riskienhallintavelvoite** kyberturvallisuuslain 2 luvussa 7-10 §:ssä ja tiedonhallintalain 4 a luvussa 18 b-c §:ssä.
- Suositukseen on koottu yleisimmin käytetyt kyberturvallisuuden **riskienhallintakeinot**.
  - Esimerkkejä toteutuksista, joita valvova viranomainen saattaa kohdata valvonnan yhteydessä.
  - Esimerkkejä todennusmenetelmistä ja viittaukset yleisimpiin kansallisiin ja kansainvälisiin viitekehyksiin.

Riskiperustainen lähestymistapa

Toimijan on toteutettava riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.

Kyberturvallisuuslaki 7 § 2 mom.



Kaikki vaaratekijät huomioiden

- Riskien tunnistamisessa huomioidaan internet-välitteisen uhkan lisäksi fyysinen uhka. Tahallinen tai tahaton tapahtuma. Ulkoisen uhkan lisäksi sisäinen uhka.
- Toimijan on huomioitava riskienhallinnassaan teknisen tietoturvallisuuden lisäksi myös verkko- ja tietojärjestelmiensä fyysisen ympäristönsä suojaus.

Kyberturvallisuuden riskienhallinnan toimenpiteet

1. Kyberturvallisuuden **riskienhallinnan toimintaperiaatteet** ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi

2. Viestintäverkkojen ja tietojärjestelmien **turvallisuutta koskevat toimintaperiaatteet**

3. Viestintäverkkojen ja tietojärjestelmien **hankinnan, kehittämisen ja ylläpidon turvallisuus** sekä tarvittavat menettelyt **haavoittuvuuksien** käsittelyyn ja julkistamiseen

4. **Toimitusketjun** välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja **häiriönsietokyky**, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien **kyberturvallisuuskäytännöt**

5. **Omaisuudenhallinta** ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen

6. **Henkilöstöturvallisuus ja kyberturvallisuuskoulutus**

7. **Pääsynhallinnan ja todentamisen** menettelyt

8. **Salausmenetelmien** käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön

9. **Poikkeamien havainnointi ja käsittely** turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi

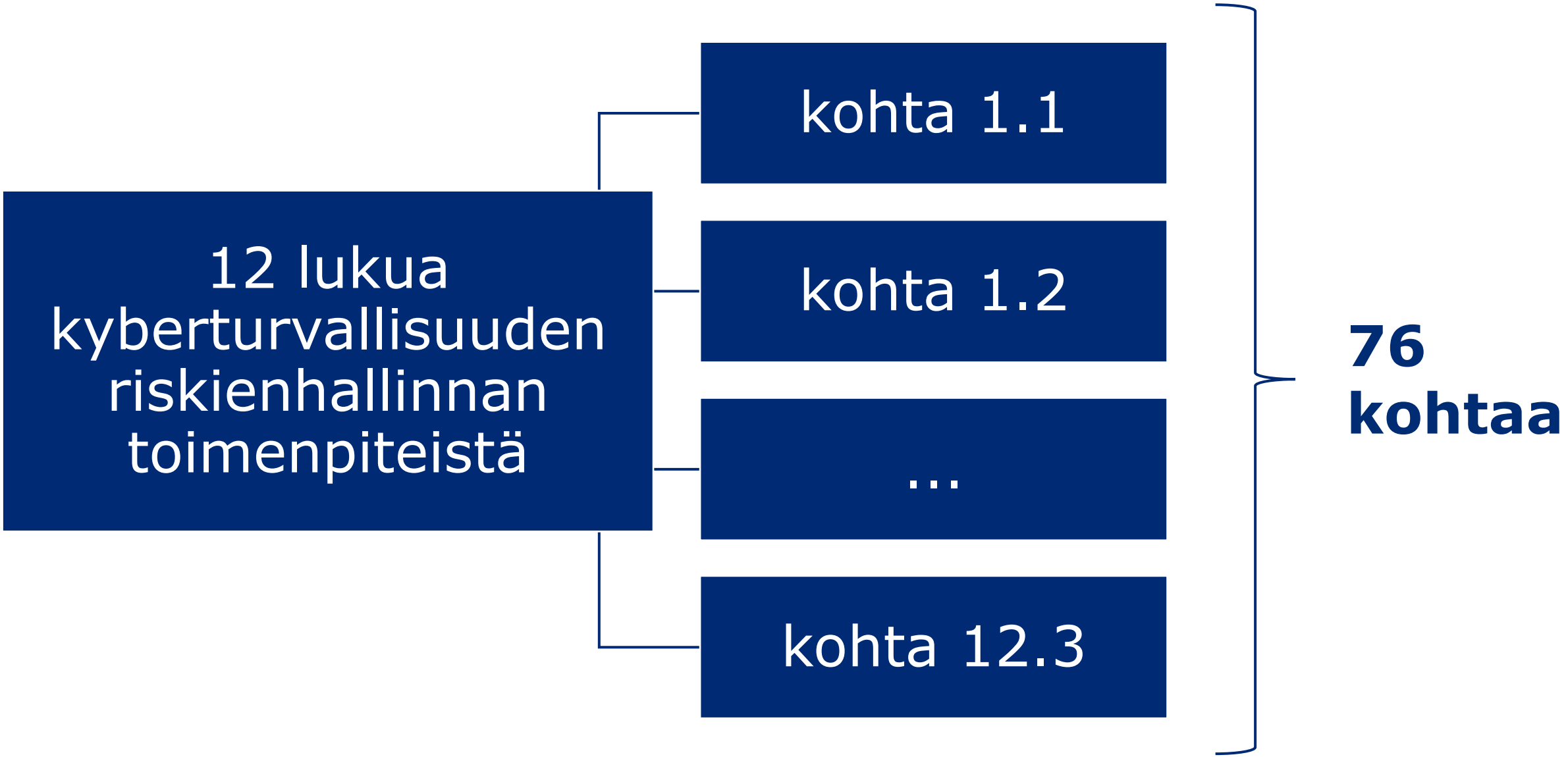
10. Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan **jatkuvuuden hallinta** ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö

11. **Perustason tietoturvakäytännöt** toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi

12. Toimenpiteet viestintäverkkojen ja tietojärjestelmien **fyysisen ympäristön** ja tilaturvallisuuden sekä **välttämättömien resurssien** varmistamiseksi

Kyberturvallisuuslaki 9 §
Tiedonhallintalaki 18 c §

Suosituksen rakenne


12 lukua kyberturvallisuuden riskienhallinnan toimenpiteistä
kohta 1.1
kohta 1.2
...
kohta 12.3
76 kohtaa

Esimerkki suosituksen kohdasta

10.3 Palautustestaus ja varmuuskopioiden suojaaminen

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.11.

- Varmuuskopioiden palautusta ja varajärjestelmien toimivuutta tulisi testata säännöllisesti, ensisijaisesti automaattisesti. Testauksessa pitäisi tarkastaa myös varmuuskopioiden eheys. Varmuuskopioiden palautustestaus on tehtävä turvallisesti niin, ettei se vaaranna tuotantojärjestelmää.
- Varmuuskopioita on säilytettävä turvallisessa tilassa, joka on toimijan riskienhallinnan perusteella riittävän eriytettynä varmuuskopioitavasta järjestelmästä. Tämä voi tarkoittaa esimerkiksi muuta toimitilaa tai erillistä palotilaa. Varmuuskopioita voi säilyttää tarvittaessa useassa muodossa, joiden palautusnopeuksissa voi olla eroa, kuten levylle otetut varmistukset sekä erilliset pitkäaikaisarkistot.
- Varmuuskopioiden suojaamisessa voidaan ottaa huomioon niiden eheyden, saatavuuden ja luottamuksellisuuden tarpeet. Tämä tarkoittaa esimerkiksi riittävää fyysistä suojausta ja muita kontrolleja, kuten salausta.

Todennus

1. Valvova viranomainen todentaa, että toimija on mahdollisuuksien ja tarpeen mukaan määrittänyt toimenpiteet, joilla varmuuskopioiden ja varajärjestelmien toimivuutta testataan säännöllisesti, esimerkiksi kerran viikossa. Tämä voi olla automatisoitua tai manuaalista. Keskeistä on, että mekaanisen palautuksen lisäksi tarkastetaan myös se, että tieto saadaan palautettua eheänä ja käyttökelpoisena, sekä mahdollinen varajärjestelmä pystytettyä oikealla tiedolla. Valvovan viranomainen todentaa, että varmuuskopiot on suojattu riittävästi. Esimerkiksi arkkitehtuurikuvauksissa, järjestelmädokumentaatiossa tai vastaavassa pitäisi olla kuvattuna se, miten varmuuskopiojärjestelmä tai sen osa on eriytetty muusta järjestelmästä. Tämän pitäisi varmistaa se, että jos esimerkiksi viestintäverkkoon ja tietojärjestelmään pääsee hyökkääjä, ei tämä voi päästä käsiksi kaikkiin varmistuksiin.
2. Valvova viranomainen todentaa katselmoinneilla ja haastatteluilla, miten toimija testaa varmuuskopioiden toimivuutta mahdollisuuksien ja tarpeen mukaan. Tästä tulisi käydä ilmi esimerkiksi suoritetut toimenpiteet varmuuskopioiden eheyden varmistamiseksi sekä testauksen säännöllisyys. Valvova viranomainen voi tarvittaessa hyödyntää myös fyysisiä katselmointeja sen varmistamiseksi, että varmuuskopioita on eriytetty muusta järjestelmästä riittävästi. Katselmoinnissa tulisi varmistua esimerkiksi siitä, että uhkat kuten tulipalo, tulvat ja henkilöuhka, eivät koske sekä varmistettavaa järjestelmää että varmuuskopioita.
3. Jos kyseessä on fyysisen erottelun sijaan perusteltu looginen erottelu, voi valvova viranomainen hyödyntää esimerkiksi toimijan tekemiä skannauksia ja yhteydenottoyrityksiä sen varmistamiseksi, että eriytettyyn varmuuskopiointijärjestelmään ei pääse käsiksi varmistettavan viestintäverkon ja tietojärjestelmän puolelta.

Perustelut

Poikkeamatilanteista palautumisen yhteydessä tapahtuu liian usein niin, että palautus ei onnistu tai hyökkääjä onnistuu tuhoamaan sekä tietojärjestelmän että varmuuskopiot. Tämän vuoksi palautuksen kattava ja säännöllinen testaaminen sekä palautusjärjestelmän suojaaminen voivat olla toiminnan kannalta elintärkeitä.

Viitteet

ISO/IEC 27002:2022 (5.33, 8.13, 8.14, 8.24)

IEC 62443-2-1:2010 (4.3.4.3.9)

IEC 62443-2-1:2024 (DATA 1.1, DATA 1.2, DATA 1.5, DATA 1.6, DATA 1.7, AVAIL 1.2, AVAIL 2.3)

IEC 62443-2-4:2024 (SP.12.01, SP.12.02, SP.12.03, SP.12.04, SP.12.05, SP.12.06, SP.12.07)

NIST CSF 1.1 (PR.IP-4, RC.RP-1, RC.IM-1, RC.IM-2)

NIST CSF 2.0 (PR.DS-11, RC.RP-01, RC.RP-05, ID.IM-03)

NIS CG Reference document (3.12.2 Backup and redundancy management)

Työkalut

Julkri (TEK-20, VAR-09)

Kybermittari (RESPONSE-4, ARCHITECTURE-1, ARCHITECTURE-5)

1. Kyberturvallisuuden **riskienhallinnan toimintaperiaatteet** ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi

- Riskienhallinnan toimintamalli ja riskien arviointiin liittyvät käytännöt
- Tarpeiden ja uhkien tunnistaminen
- Riskien käsittely ja hallintatoimenpiteiden ajantasaisuus

2. Viestintäverkkojen ja tietojärjestelmien **turvallisuutta koskevat toimintaperiaatteet**

- Turvallisuutta koskevat toimintaperiaatteet ja menettelyt (tietoturvapolitiikka)
- Turvallisuuden jalkauttaminen
- Turvallisuusmenettelyiden valinta

3. Viestintäverkkojen ja tietojärjestelmien **hankinnan, kehittämisen ja ylläpidon turvallisuus** sekä tarvittavat menettelyt **haavoittuvuuksien** käsittelyyn ja julkistamiseen

- Elinkaaren, muutosten ja päivitysten hallinta
- Turvallisuuden huomiointi hankinnoissa
- Järjestelmäkovennukset
- Verkkosegmentointi
- Haavoittuvuuksien käsittely

4. **Toimitusketjun** välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja **häiriönsietokyky**, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien **kyberturvallisuuskäytännöt**

- Välittömien toimittajien ja palveluntarjoajien listaus
- Toimitusketjut ja niiden riskienhallinta

5. **Omaisuudenhallinta** ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen

- Omaisuuden luettelointi ja sen luokittelu
- Omaisuudenhallinnan menettelyt ja ohjeet koko elinkaaren ajalle
- Omaisuusluettelon ajantasaisena pitäminen

6. **Henkilöstöturvallisuus ja kyberturvallisuuskoulutus**

- Henkilöstöturvallisuuden menettelyt ja toimintatavat
- Salassapito ja velvollisuudet
- Taustatarkistukset
- Henkilöstökoulutus
- Johdon perehtyneisyys

7. **Pääsynhallinnan ja todentamisen** menettelyt

- Pääsynhallinnan menettelyt
- Käyttöoikeuksien jatkuva ylläpito
- Vähimpien oikeuksien periaate
- Pääsynhallintaan liittyvä kirjanpito
- Pääkäyttäjätunnukset
- Turvalliset todennusmenetelmät

8. **Salausmenetelmien** käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön

- Kryptografian toimintaperiaatteet ja menettelyt
- Tiedon salaustekniikat
- Salauksen elinkaari

9. **Poikkeamien havainnointi ja käsittely** turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi

- Poikkeamanhallinnan menettelyt
- Poikkeamien raportointi
- Tapahtumakirjaukset
- Poikkeamanhallintaprosessi
- Juurisyyanalyysi ja kokemuksista oppiminen
- Merkittävät poikkeamat

10. Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan **jatkuvuuden hallinta** ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö

- Jatkuvuus- ja toipumissuunnittelu
- Varmuuskopiot ja varajärjestelmät
- Palautustestaus ja varmuuskopioiden suojaaminen
- Varaviestintäjärjestelmät

11. **Perustason tietoturvakäytännöt** toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi

- Asettavat perustason käytännöt, joiden avulla toimija pystyy torjumaan suurimman osan yleisimmistä tietoturvauhkista
- Parantavat yksinään organisaation kypsyystasoa ja kyberturvallisuuden tilaa

12. Toimenpiteet viestintäverkkojen ja tietojärjestelmien **fyysisen ympäristön** ja tilaturvallisuuden sekä **välttämättömien resurssien** varmistamiseksi

- Tilaturvallisuus ja fyysinen pääsynvalvonta
- Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan
- Toiminnalle välttämättömien resurssien jatkuvuuden varmistaminen

Perustason tietoturvakäytännöt

1. Toimija on ohjeistanut perustason tietoturvakäytännöt henkilöstölle, alihankkijoille ja muille kumppaneille

2. Toimija on tunnistanut kriittisimmän omaisuutensa

3. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä

4. Toimija on erottanut kriittiset ja haavoittuvat viestintäverkot ja tietojärjestelmät muista ympäristöistä

5. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä haitallisia ja luvattomia ohjelmistoja vastaan

6. Toimija on järjestänyt tunnistautumisen sisäisiin ja ulkoisiin palveluihinsa ja laitteisiinsa turvallisesti

7. Toimija on erottanut järjestelmiensä pääkäyttäjätunnukset ja korotettujen oikeuksien tunnukset muista tunnuksista

8. Toimija on varmistanut, että sen luottamuksellista tietoa käsitellään turvallisesti

9. Toimija on huolehtinut, että sen järjestelmiä päivitetään säännöllisesti ja kriittiset päivitykset asennetaan viivytyksettä

10. Toimija on huolehtinut, että sen palvelut ja laitteet on turvallisesti konfiguroitu

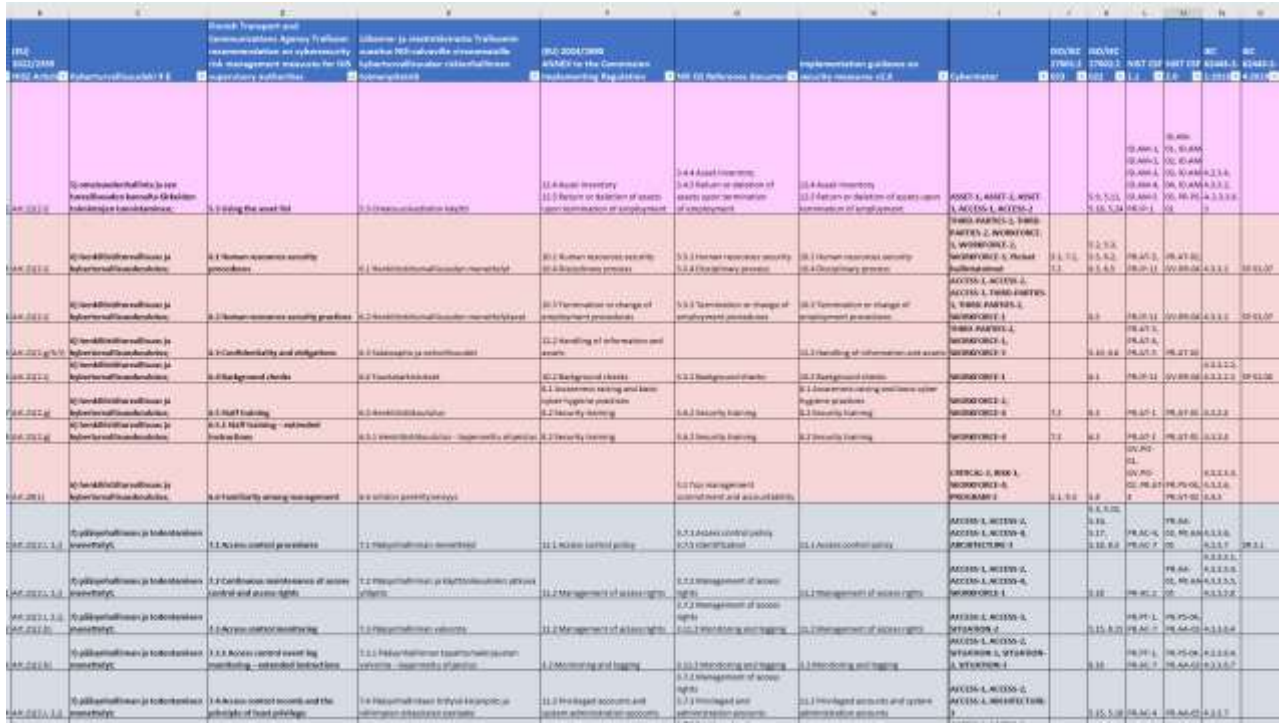
11. Toimija on huolehtinut, että sen kriittiset palvelut ja tieto-omaisuus on varmuuskopioitu

12. Toimija on varautunut, miten sen toiminta voidaan ylläpitää vakavissa poikkeamissa

13. Toimijalla on käytössään kriittisten toimintojen tapahtumakirjaus (loki)

Ristiinviittaustaulukko

- Suosituksen liitteenä on julkaistu ristiinviittaustaulukko, josta kaikki suosituksessa käytetyt standardiviittaukset löytyvät taulukkomuodossa.
- Muista riskiperustainen lähestymistapa!
- Laki ei velvoita minkään standardin käyttöä, mutta ne voivat antaa lisätukea riskienhallinnan suunnitteluun.
- Standardit voivat sisältää laista poikkeavia vaatimuksia.



Yhteenveto

- Suositus tarjoaa katalogin erilaisista kyberturvallisuuden riskienhallintatoimenpiteisiin liittyvistä menetelmistä
- Riskien hallinta on jatkuvaa! Riskien tunnistaminen, arviointi ja käsittely sekä hallintatoimenpiteiden ajantasaisuuden varmistaminen ovat riskienhallinnan keskiössä
- Jos kyberturvallisuus ja sen riskienhallinta on organisaatiolle uusi asia, alkuun pääsee parhaiten perustason tietoturvakäytäntöjä soveltamalla
- Ole matalalla kynnyksellä yhteydessä omaan valvovaan viranomaiseesi, heiltä saa ohjausta ja tukea kyberturvallisuuslain soveltamiseen

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos!

Tutustu myös Kyberturvallisuuskeskuksen NIS2-teemasivuihin