Kaakkois-Suomen ammattikorkeakoulu

Kymen Laakson Liitto

Euroopan unionin osarahoittama

Prosessikuvaus
Toimittajien kartoittaminen ja arviointi, sopimusten arviointi sekä toimittajiin liittyvien riskien arviointi NIS2-vaatimusten näkökulmasta

Kaakkois-Suomen Ammattikorkeakoulu Oy

Kyberturvan tulevaisuus Kymenlaaksossa –hanke

28.11.2024

DITTMAR & INDRENIUS

JOHDANTO, TAUSTA JA KÄYTTÖOHJEET

DITTMAR & INDRENIUS

Johdanto (1/2)

- Tämä aineisto on tarkoitettu Kyberturvan tulevaisuus Kymenlaaksossa –hankkeen käyttöön hankkeen päättymiseen asti 31.12.2025. Lisäksi materiaali on tarkoitettu NIS2-opintokokonaisuuden aineistoksi 31.12.2027 asti.
- Aineistoa ei päivitetä säännöllisesti, joten aineistossa ei huomioida sen valmistumisen (28.11.2024) jälkeisiä mahdollisia muutoksia sääntelyssä ja muissa olosuhteissa.
- Materiaali on laadittu Dittmar & Indrenius Asianajotoimisto Oy:n toimesta Kaakkois-Suomen Ammattikorkeakoulu Oy:n toimeksiannosta. Materiaalin on tuottanut Kyberturvan tulevaisuus Kymenlaaksossa –hanke, jota rahoittaa Kymenlaakson Liitto Euroopan Unionin Oikeudenmukaisen siirtymän rahastosta (JTF).
- Jos aineistoa lainataan sellaisenaan, tulee tekijä ilmoittaa tekijänoikeuslainsäädännön edellyttämällä tavalla.

Johdanto (2/2)

- Tähän prosessikuvaukseen on koottu NIS2-sääntelyyn perustuvat vaatimukset ja esimerkit niiden toteuttamisesta seuraavien kokonaisuuksien osalta:
  A. NIS2-sääntelyn piiriin kuuluvan toimijan ICT-toimittajien kartoittaminen ja arviointi (mukaan lukien riskiarvioinnit);
  B. ICT-toimittajien kanssa tehtyjen tai tehtävien sopimusten arviointi; sekä
  C. muut keskeiset ICT-toimittajiin liittyvät riskienhallinnan toimenpiteet.
- NIS2-sääntelyllä tarkoitetaan tässä prosessikuvauksessa EU:n kyberturvallisuusdirektiivin (EU) 2022/2555 täytäntöönpanevaa kansallista kyberturvallisuuslakia. Tämän prosessikuvauksen valmistumisen hetkellä kansallisen lainsäädännön lainsäädäntöprosessi on vielä kesken.
  - Tämä prosessikuvaus perustuu NIS2-sääntelyä koskevaan hallituksen esitykseen (HE 57/2024 vp) ja Liikenne- ja viestintävirasto Traficomin (”Traficom”) suositusluonnokseen NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä (Traficom/18410/09.00.02/2023).
- Prosessikuvaus on tarkoitettu sääntelyn alaan kuuluvien toimijoiden tueksi NIS2-sääntelyn vaatimusten noudattamiseen ja vaatimusten toteutumisen arviointiin. Tämän prosessikuvauksen avulla ei kuitenkaan ole mahdollista varmistaa tyhjentävästi NIS2-sääntelyn vaatimusten toteutumista, sillä NIS2-sääntely edellyttää toimenpiteiden perustumista yrityksen omaan riskiarviointiin ja riskienhallinnan toimintamalliin.

NIS2-sääntelyn lähtökohdat

- NIS2-sääntely asettaa sen soveltamisalaan kuuluville toimijoille **vähimmäisvaatimukset kyberturvallisuuden riskienhallinnalle**. Riskienhallinnan toteuttamiseen sisältyy liikkumavaraa, jota sääntelyn piiriin kuuluvat toimijat voivat käyttää NIS2-sääntelyn asettamien raamien rajoissa.
- Riskienhallinnan toimenpiteet on suhteutettava
  i. toimijan toiminnan laatuun ja laajuuteen;
  ii. mahdollisesta poikkeamasta kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen;
  iii. poikkeamien todennäköisyyteen ja vakavuuteen;
  iv. toimenpiteistä aiheutuviin kustannuksiin; sekä
  v. ajantasainen kehitys huomioon ottaen käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.
- Tarvittavat riskienhallinnan toimenpiteet voivat siis vaihdella toimijan koon, toimialan ja toimijaan kohdistuvien uhkien perusteella.
- Valvovien viranomaisten määräykset eri toimialoilla tulee ottaa soveltuvin osin huomioon, jos tällaisia määräyksiä on annettu.

Prosessikuvauksen käyttöohje

- Tässä prosessikuvauksella ”*yrityksellä*” tarkoitetaan tätä prosessikuvausta hyödyntävää tahoa, joka kuuluu NIS2-sääntelyn piiriin.
- **Tämä prosessikuvaus on rajattu ICT-toimittajiin liittyvään riskienhallintaan** NIS2-sääntelyn näkökulmasta. Prosessikuvaus ei siis kuvaa tyhjentävästi kaikkia NIS2-sääntelyn mukaisia kyberturvallisuuden riskienhallinnan vähimmäisvaatimuksia.
- Koska yrityksen riskienhallinnan tulee perustua yrityksen omaan arvioon riskeistä ja tarpeellisista toimenpiteistä niiden hallitsemiseksi, ei ole mahdollista antaa yleistä ja tyhjentävää luetteloa tarpeellisista ja riittävistä riskienhallinnan toimenpiteistä.
- **Riskiarvioinnin, *riskienhallinnan toimintamallin* ja sen alaisten *riskienhallintatoimenpiteiden*** dokumentoiminen ja dokumentaation pitäminen ajan tasalla on tärkeää, jotta yritys voi osoittaa noudattavansa NIS2-sääntelyä.

DITTMAR & INDRENIUS

Kyberturvallisuuden riskienhallinnan lähtökohdat (1/2)

- **Riskiperustainen lähestyminen**
  - Toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen.
- **Tavoitteena on estää tai minimoida *poikkeamien* vaikutukset**
  - Kyberturvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin.
  - ***”Poikkeamalla”*** tarkoitetaan tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.
- **Kaikki vaaratekijät huomioiva lähestymistapa**
  - Yrityksen riskienhallinnassa tulee noudattaa kaikki vaaratekijät huomioivaa lähestymistapaa ja varmistaa, että yrityksen riskienhallintaprosesseissa otetaan huomioon kyberturvallisuusriskit.

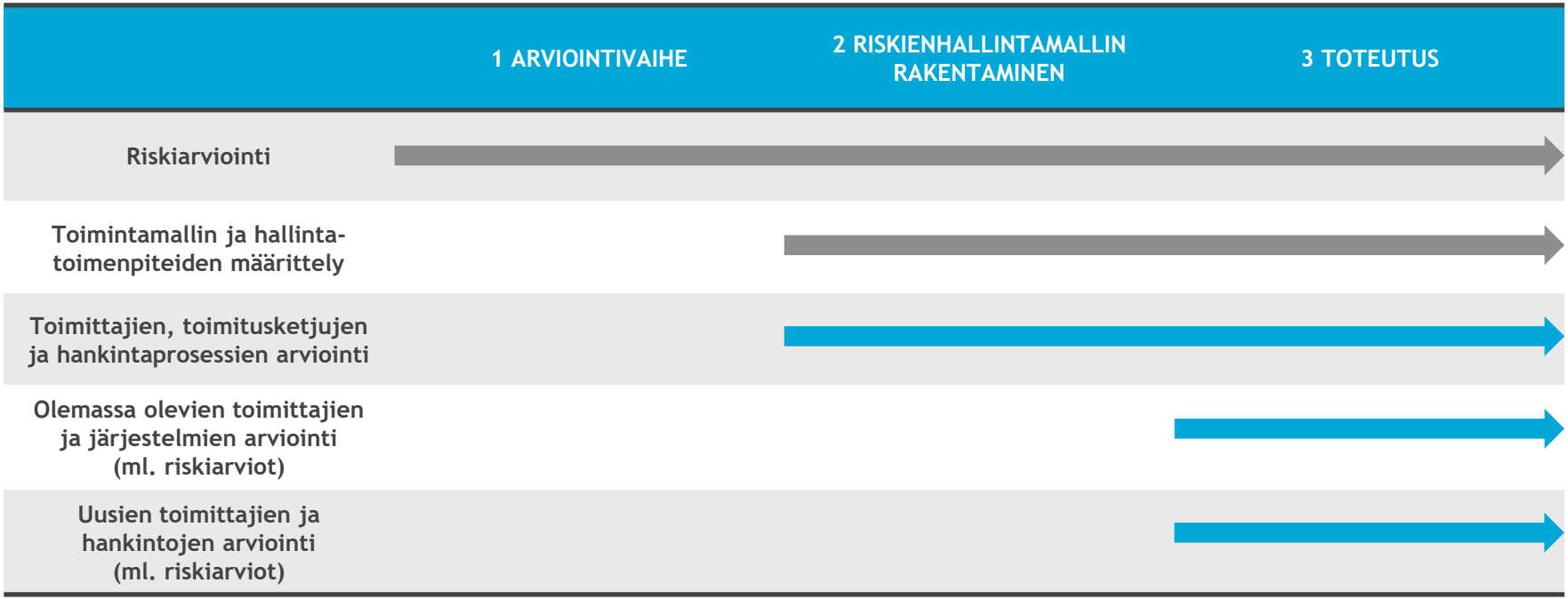
Kyberturvallisuuden riskienhallinnan lähtökohdat (2/2)

- Toimijalla on oltava käytössä ajantasainen kyberturvallisuutta koskeva ***riskienhallinnan toimintamalli*** viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta.
  - Toimintamallissa on määritettävä ja kuvattava kyberturvallisuutta koskevan **riskienhallinnan tavoitteet, menettelyt ja vastuut sekä *hallintatoimenpiteet***, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan kyberuhkilta ja poikkeamilta.
  - Toimijoiden on toteutettava kyberturvallisuutta koskevan riskienhallinnan toimintamallin mukaiset oikeasuhtaiset tekniset, operatiiviset tai organisatoriset ***hallintatoimenpiteet*** viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.
- Riskienhallinnan toimintamalli ja hallintatoimenpiteet tulee pitää ajan tasalla, eli kyberturvallisuuden riskienhallinnan tulee olla jatkuvaa.

NIS2-vaatimukset toimittajiin liittyvässä riskienhallinnassa

- Kyberturvallisuuden riskienhallinnan toimintamallissa on otettava huomioon erityisesti seuraavat NIS2-sääntelyyn perustuvat kokonaisuudet liittyen ICT-palvelujen, tuotteiden ja järjestelmien toimittajiin:
  i. ***viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus*** *sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi*;
  ii. ***toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky****, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt*; ja
  iii. ***omaisuudenhallinta*** *ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen*.
- Lisäksi seuraavat NIS2-sääntelyyn perustuvat kokonaisuudet ovat soveltuvin osin relevantteja toimittajiin liittyvässä riskienhallinnassa:
  - henkilöstöturvallisuus ja kyberturvallisuuskoulutus; pääsynhallinnan ja todentamisen menettelyt; salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt; poikkeamien havainnointi ja käsittely; varmuuskopiointi; perustason tietoturvakäytännöt; sekä toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Toimittajiin liittyvä riskienhallinta osana riskienhallinnan toimintamallia
Aikajana



DITTMAR & INDRENIUS

TYÖKALUT

DITTMAR & INDRENIUS

Prosessikuvaukseen liittyy kaksi työkalua

Toimittajien arviointilomake (Liite 1)

- Arviointilomake on tarkoitettu toimittajien ja järjestelmien turvallisuutta koskevien vaatimusten toteutumisen arvioimiseksi.
- Lomake on suunniteltu käytettäväksi suorien toimittajien arvioimiseksi
  1) osana hankintaprosessia; ja
  2) olemassa olevien toimittajien ja järjestelmien arviointiin.

Toimittajien auditointilomake (Liite 2)

- Auditointilomake on tarkoitettu
  1) yrityksen jo olemassa olevien toimittajien auditoimiseen; sekä
  2) toimittajien kanssa solmittujen tai solmittavien sopimusten auditoimiseen.
- Auditointilomake toimii parina arviointilomakkeen kanssa.

➢ Huom. On suositeltavaa päivittää nämä työkalut yrityksen oman riskienhallinnan toimintamallin mukaiseksi.

DITTMAR & INDRENIUS

TOIMITTAJIEN JA NIIDEN TARJOAMIEN JÄRJESTELMIEN ARVIOINTI JA AUDITOINTI

DITTMAR & INDRENIUS

A. Toimittajien kartoittaminen ja arviointi

DITTMAR & INDRENIUS

A. Toimittajien ja palveluntarjoajien kartoittaminen ja arviointi

- Yrityksen tulee varmistaa, että sillä on käytössään menettelyt, joilla varmistetaan ICT-hankintojen riittävä turvallisuus.
  - Yritys vastaa siitä, että se käyttää toiminnassaan sellaisia tuotteita ja palveluita, jotka vastaavat yrityksen riskienhallinnan vaatimuksia. Nämä vaatimukset määritellään NIS2-vaatimusten mukaisesti yrityksen kyberturvallisuuden ***riskienhallinnan toimintamallissa*** ja sen mukaisissa ***hallintatoimenpiteissä***.
- Toimittajien ja palveluntarjoajien kartoittamiseen ja arviointiin tulee sisältyä ainakin seuraavat kokonaisuudet:

1. Toimintaan ja palveluntarjontaan vaikuttavien välittömien toimittajien kartoittaminen
2. Toimittajiin ja heidän tuotteisiin ja palveluihin liittyvien riskien tunnistaminen, arvioiminen ja hallinta
3. Toimittajien palveluiden, järjestelmien ja tuotteiden riittävän turvallisuuden varmistaminen
4. Kriittisten järjestelmien, tuotteiden ja palvelujen tunnistaminen

A1. Toimintaan ja palveluntarjontaan vaikuttavien välittömien toimittajien kartoittaminen

- Yrityksellä tulee olla ajantasainen tieto kaikista toimintaan ja palveluntarjoajaan vaikuttavista välittömistä toimittajista.
- Yrityksellä tulee olla **listaus tai hakemisto**, joka kattaa ainakin:
  - kaikki välittömät laite- ja palvelutoimittajat sekä tarvittaessa muut yrityksen kyberturvallisuuteen vaikuttavat toimittajat;
  - toimittajien yhteystiedot; ja
  - palvelut, järjestelmät ja tuotteet, joita toimittaja tuottaa ja/tai toimittaa.
  - Lisäksi on suositeltavaa, että toimittajien kanssa tehtyjen sopimusten perustiedot ilmenee listauksesta tai hakemistosta (sopimuskauden tiedot ja sopimuksen kohteen elinkaareen liittyvät keskeiset tiedot).
- Lisäksi on hyvä huomioida, että tällä listauksella on yhteys yrityksen omaisuusluetteloon.
  - NIS2-sääntelyn mukaan riskienhallinnan toimintamallin hallintatoimenpiteisiin tulee sisältyä omaisuudenhallinnan kokonaisuus ja turvallisuuden kannalta tärkeiden toimintojen tunnistaminen (omaisuudenhallinnan kokonaisuutta ei eritellä tarkemmin tässä prosessikuvauksessa).

A2. Toimittajiin ja heidän tuotteisiin ja palveluihin liittyvien riskien tunnistaminen, arvioiminen ja hallinta

- Yrityksen tulee
  - tunnistaa mahdollisten toimitusketjuhäiriöiden vaikutus omaan toimintaansa ja palveluihinsa;
  - määritellä tarpeelliset varautumistoimet mahdollisissa toimitushäiriöissä;
  - arvioida ja käsitellä välittömiin toimittajiin kohdistuvat riskit;
  - valita ja toteuttaa oikeasuhtaiset riskienhallinnan toimenpiteet toimitusketjuihin liittyen ja toteuttaa toimenpiteet sellaisiin toimittajiin, joihin kohdistuvilla riskienhallinnan toimenpiteillä on kyberturvallisuutta edistävä vaikutus.
- Riskienhallinnan toimenpiteitä harkitessa yrityksen tulee ottaa huomioon välittömälle toimittajalle ja palveluntarjoajalle ominaiset
  - haavoittuvuudet, kuten sijainnista, tuotevalikoimasta tai toimialan luonteesta johtuvat haavoittuvuudet;
  - tuotteiden ja palveluiden yleinen laatu ja häiriönsietokyky;
  - tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet; sekä
  - toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt.

A3. Toimittajien palveluiden, järjestelmien ja tuotteiden riittävän turvallisuuden varmistaminen (1/2)

- **Yrityksen tulee pyrkiä ylläpitämään viestintäverkkojen ja tietojärjestelmien riittävää turvallisuuden tasoa koko niiden elinkaaren ajan.**
  - Tämä voi tarkoittaa esimerkiksi päivityksiä sopimukseen, päivityksiä ylläpitoon ja säännöllisiä turvallisuustarkastuksia.
  - Mahdollisiin muutoksiin palveluntoimittajan osalta tulee varautua siten, että palvelu tai resurssi voidaan tarvittaessa siirtää tai palauttaa omaan hallintaan. Tarvittaessa on varauduttava myös omistussuhteiden muutoksiin.
  - Tuote tai palvelu tulee olla turvallisesti konfiguroitavissa ja sille tulee olla saatavilla tietoturvapäivityksiä koko suunnitellun elinkaaren ajan silloin, kun konfiguroitavuus ja päivitettävyys on kohteelle olennaista.
- Toimijalla tulisi olla menettelyt ja toimintatavat palveluiden, järjestelmien ja tuotteiden testaamiseen, siinä laajuudessa kuin sille on toimintaan, tarpeisiin ja riskeihin perustuva tarve.
  - Turvallisuuden testaamisen tulee olla organisoitua, määriteltyä, suunnitelmallista ja säännöllistä.
  - Hankinnan kohteesta voidaan varmistua lisäksi hyväksyntätesteillä (acceptance test).
- Jos palveluissa, järjestelmissä tai tuotteissa käsitellään luottamuksellisia tietoja, yrityksen tulee varmistaa, että toimittajat noudattavat yrityksen määrittelemiä turvallisen tietojenkäsittelyn käytäntöjä ja ohjeita.

A3. Toimittajien palveluiden, järjestelmien ja tuotteiden riittävän turvallisuuden varmistaminen (2/2)

- Hankittavien järjestelmien tulee olla yrityksen toiminnan ja tarpeiden perusteella riittävän turvallisia muun muassa eheyden, saatavuuden ja luottamuksellisuuden suhteen.
  - Arvioitaessa riittävän turvallisuustason täyttymistä voidaan kiinnittää huomiota esimerkiksi kykyyn suojautua tavallisimpia kyberhyökkäyksiä vastaan.
  - Jo hankinnan alkuvaiheessa yrityksen tulee määritellä vaadittavat turvallisuusvaatimukset ja toimittaa ne toimittajille. Vaatimukset liitetään osaksi toimittajan kanssa tehtävää sopimusta soveltuvin osin.
- Hankinnan kohteen tai olemassa olevan tuotteen turvallisuudesta voi yrittää varmistua esimerkiksi
  - sopimuksellisin keinoin;
  - tutkimalla tuotteen tai palvelun ominaisuuksia;
  - edellyttämällä ja tarkastelemalla esimerkiksi relevantteja sertifiointeja;
  - varmistumalla toimittajan luotettavuudesta; ja
  - varautumalla riskeihin (ks. edellä kohta A2).
- On suositeltavaa varmistaa, että hankitusta palvelusta, järjestelmästä tai tuotteesta on olemassa dokumentaatio, joka kattaa sen sisällön sekä turvallisen konfiguraation ja käytön.
- **Työkalu**: Arvioinnissa voidaan käyttää **Toimittajien arviointilomaketta** (Liite 1).

A4. Kriittisten kohteiden tunnistaminen (1/2)

- Riskienhallinnassa tulee **tunnistaa luottamuksellisuuteen, eheyteen, saatavuuteen ja aitouteen liittyvät tarpeet sekä sen kohteena toimintojen kannalta keskeiset palvelut, järjestelmät, prosessit ja henkilöt**.
  - Riskiperustaisen lähestymisen mukaisesti, mitä merkittävämpi viestintäverkko tai tietojärjestelmä on toimijalle, sitä kattavammin siihen kohdistuvia uhkia tulee arvioida.
- Riskiarvion perusteella yrityksen tulee **tunnistaa kriittiset tietojärjestelmät, viestintäverkot, laitteet ja palvelut**
  - joita ilman yritys ei voi toimia;
  - joihin kohdistuu toimialakohtaisia lakisääteisiä velvoitteita; tai
  - joihin kohdistuva tietoturvaloukkaus voi aiheuttaa suurta vahinkoa.
- Kriittiset kohteet tulee huomioida ja luokitella yrityksen omaisuusluettelossa.

A4. Kriittisten kohteiden tunnistaminen (2/2)

- Kriittisiin kohteisiin tulee soveltaa yrityksen riskienhallintamallin mukaisia riskeihin mitoitettuja korkeatasoisia riskienhallintatoimia, esim.:
  - Kriittisiä kohteista koskeviin sopimuksiin voidaan vaatia korkeatasoisempia kyberturvallisuusvaatimuksia.
  - Turvallisuuden kannalta kriittisimpien kohteiden turvallisuudesta voidaan huolehtia esimerkiksi tarkastelemalla säännöllisesti prosesseja tai teknisillä testauksilla.
  - Voidaan varmistaa, että kriittisten viestintäverkkojen ja tietojärjestelmien turvallinen konfiguraatio ylipäätään on mahdollista ja että niille tuotetaan asianmukaisia turvallisuuspäivityksiä.
  - Yritys voi tarvittaessa pyytää kriittisistä tuotteista ja palveluista komponenttilistaa (esim. software bill of materials, hardware bill of materials), jotta riippuvaisuudet ja näihin kohdistuvat haavoittuvuudet voidaan tunnistaa ja hallita.
- Soveltuvin osin voidaan hyödyntää EU:n tasolla NIS-yhteistyöryhmän, Euroopan komission ja ENISA:n koordinoituja turvallisuusarviointeja tietyistä kriittisistä toimitusketjuista, jos tällaisia arviointeja on tehty.

B. Sopimusten arviointi

DITTMAR & INDRENIUS

B. Sopimusten arviointi

- Yrityksen tulee arvioida, millaisia vaatimuksia toimittajille on tarpeen asettaa yrityksen toimitusketjujen turvallisuuteen liittyen.
- Jotta sopimusehtoja ja niiden riittävyyttä voidaan arvioida, yrityksen tulee tunnistaa sopimuksen kohteen kannalta tärkeät, kyberturvallisuuteen liittyvät ominaisuudet sekä asettaa tarpeelliset ja oikeasuhtaiset vaatimukset niiden osalta.
  - Nämä vaatimukset voivat liittyä esimerkiksi palvelutasoihin, saatavuuteen ja ylläpidettävyyteen.
- Yrityksen tulee sisällyttää sen riskienhallinnan toimintamallin mukaisia hallintatoimenpiteitä sopimusjärjestelyihin, joita toimija tekee välittömien toimittajiensa ja palveluntarjoajiensa kanssa.
  - Näitä voivat olla esimerkiksi kyberturvallisuusominaisuuksien arviointi sopimuskauden aikana, vaatimukset henkilöstön koulutuksesta ja sertifioinnista, ilmoittamiskäytännöt haavoittuvuuksista sekä sopimuksen kohteen ylläpitokäytäntöjen tarkastelu.
- Huom. Yritys ei voi siirtää vastuutaan NIS2-vaatimusten noudattamisesta toimittajille, mutta yritys voi asettaa toimittajille vaatimuksia, joiden avulla yritys huolehtii riskienhallinnastaan ja velvoitteidensa noudattamisesta.
- Sopimusten arvioinnissa työkaluna voidaan käyttää **Toimittajien auditointilomaketta** (Liite 2).

C. Muut keskeiset toimittajiin liittyvät riskienhallinnan toimenpiteet

DITTMAR & INDRENIUS

C1. Perustason tietoturvakäytäntöjen noudattaminen

- Yrityksen tulee ohjeistaa sen riskienhallinnan toimintamallin mukaiset perustason tietoturvakäytännöt myös toimittajille ja muille kumppaneille.
- Yrityksellä on suositeltavaa olla kirjallinen ja päivitetty kuvaus perustason tietoturvakäytännöistä, joka on saatavilla toimittajille ja muille kumppaneille.
- Tarpeelliset perustason tietoturvakäytännöt muuttuvat ja päivittyvät riskiympäristön ja teknologian kehityksen myötä. Tämän vuoksi yrityksen on suositeltavaa seurata Traficomin ja oman toimialan valvontaviranomaisen viimeisimpiä suosituksia ja määräyksiä (siltä osin kuin niitä on annettu) perustason tietoturva- ja kyberhygieniakäytännöistä.

C2. Muutosten ja päivitysten hallinta

- Konfiguraatio- ja ohjelmistopäivitysten osalta yritys voi esimerkiksi pyrkiä siihen, että ne olisivat
  - dokumentoituja;
  - muutoshallintaprosessien mukaisesti suunniteltuja;
  - kattavia; sekä
  - kohteen ominaispiirteiden ja päivitysten kriittisyyden kannalta oikea-aikaisia.
- Yritys voi lisäksi harkita keinoja estää luvattomien tai haitallisten muutosten tekeminen.

C3. Haavoittuvuuksien hallinta

- Haavoittuvuuksien käsittelyä ja julkaisua koskevat vaatimukset kohdistuvat sellaisiin yrityksiin, jotka tuottavat sovelluksia, palveluita, laitteita tai tämän kaltaisia tuotteita.
- Löydettyjä haavoittuvuuksia varten olisi oltava olemassa raportointikanava sekä menettelytavat ja käytännöt ilmoitusten käsittelyä varten. Toimittajien arvioinnissa tulee kiinnittää huomioita siihen, onko järjestelmien haavoittuvuuksien hallinta toteutettu asianmukaisesti.
- Haavoittuvuudet voidaan ilmoittaa CVD-menettelytapojen (coordinated vulnerability disclosure) mukaisesti.

C4. Muut toimenpiteet

- Yrityksen tulee arvioida oman riskienhallinnan toimintamallin perusteella tarvittavat muut toimenpiteet liittyen erityisesti seuraaviin aihe-alueisiin:
  - Varmuuskopiointikäytännöt ja -vaatimukset;
  - Poikkeamien havainnointi ja käsittely (ml. toimittajan ilmoitus- ja raportointivaatimukset);
  - Jatkuvuus- ja toipumissuunnittelu;
  - Henkilöstöturvallisuus;
  - Salausmenetelmät;
  - Pääsynhallinta;
  - Viestintäverkkoihin ja tietojärjestelmiin liittyvä fyysinen ja tilaturvallisuus.

XAMK
Kaakkois-Suomen ammattikorkeakoulu

KYMEN LAAKSON LIITTO

Euroopan unionin osarahoittama

DITTMAR & INDRENIUS