2022

Riskienhallintasanastoa digitaaliseenkin toimin-taympäristöön - esittely sekä ohjeita riskiviestintään

VAHTI Hyvät Käytännöt -tukimateriaali

2022

Dokumentinhallinta

Omistaja	Juho Reivo
Laatinut	Juho Reivo
Tarkastanut	Kimmo Rousku
Hyväksynyt	

Version hallinta

versionro	mitä tehty	pvm/henkilö
0.1	Ensimmäinen luonnosversio	8.12.2021 JR
0.17	Korjauksia kommenttien perusteella	03.03.2022 JR
0.19	VAHTI Hyvät Käytännöt -tukimateriaalien kommentoitava versio	07.03.2022 JR

VAHTI Hyvät Käytännöt (VHK) -tukimateriaalin julkaisuprosessin mukainen kommentointiversio
Asiakirjaa täydennetään kommentointiajan päätyttyä mm. käännöksillä

Huomiot ja palaute lomakkeella
https://dvv.fi/digiturvajulkaisut

Sisällysluettelo

2022

2022

Riskienhallintasanastoa digitaaliseenkin toimintaympäristöön

Tämä asiakirja on esittely sanastoon sekä siinä esiintyviin riskienhallintaan liittyviin aiheisiin. Nämä on tuotettu Digi- ja väestötietoviraston JUDO-hakkeessa osana VAHTI Hyvät Käytännöt -tukimateriaaleja[1]. Varsinainen termisanasto, jota tässä esitellään, julkaistaan sähköisesti Yhteentoimivuusalustan[2] termipankissa osoitteessa https://sanastot.suomi.fi/ avoimesti kaikkien käytettäväksi. [julkaisu tämän VHK-dokumentin kommentointiajan jälkeen]

Tämä esittelydokumentti on tarkoitettu avaamaan sekä käsitteitä, mutta sen tueksi myös niihin liittyvää toimintaa ja prosesseja, sillä käsitelty sanasto yhdistää useita erilaisia toimijoita ja toiminta-alueita. Dokumentin tavoite on helpottaa sanaston omaksumista, läpikäyntiä sekä hahmottamista yksittäisten ilmausten sijaan hyvin linkittyneenä kokonaisuutena, joka muodostaa osan systeemisestä rakenteesta. Esittely on tarkoitettu erityisesti asiantuntijoille, mutta myös asiaan tutustuville, jotka toimivat esimerkiksi digitaalisen turvallisuuden, kyberturvallisuuden, tietoturvallisuuden, tietosuojan, jatkuvuudenhallinnan, riskienhallinnan, turvallisuuden, huoltovarmuuden, toiminnanohjauksen, johtamisen, hallinnon kehittämisen, viestinnän, sisäisen tarkastuksen, tietohallinnon, hanketoiminnan, tietojärjestelmien kehityksen tai muun vastaavan saralla yrityksissä, yhteisöissä tai julkisessa hallinnossa.

1 Johdanto

Riskienhallinnan alueelta on puuttunut yhteinen kieli tai sen käyttö on ollut epäyhtenäistä eri organisaatioiden välillä, mikä on näkynyt niin sisäisissä kuin ulkoisissakin yhteistyötilanteissa. Eri toimijat voivat lähestyä uhkia ja riskejä eri toimintalinjojen ja tasojen kautta, mutta kaikki pitäisi pystyä tuomaan yhteen osaksi digiturvallisuuden kattavaa rakennetta sekä siitä osaksi niin yhteistyön kuin organisaatioidenkin kokonaisriskienhallintaa. Yhteinen kieli ja tapa sanoittaa tätä on yksi edellytys sen onnistumiseksi ja tehokkaaseen riskienhallinnan hyödyntämiseen toiminnan johtamisen ja ohjauksen tukena.

Aihe on vaivannut eri toimijoita jo jonkin aikaa ja näitä ponnisteluja löytyy myös tämän sanaston takaa. Aikaisemmin määriteltyjä riskienhallinnan sanastoja on luotu standardien kautta, mutta niissä ilmaisut ovat melko abstraktilla tasolla ja rajoittuvat nimenomaisiin osiin esimerkiksi prosessia. Näiden ulkopuolella on kuitenkin paljon keskustelua muun muassa rajapinnoissa, joissa standardoidut riskienhallinnan rakenteet liittyvät toimintaan tai sitä ohjaaviin muihin rakenteisiin. Eli, miten arkiset asiat muuntuvat osaksi riskienhallintaa.

Termejä tarkastellessa on myös ollut selkeää, että joillain niistä on ollut sekä useita lähekkäisiä virallisia ja epävirallisia yksittäisiä määritelmiä sekä vielä enemmän kertaluontoisia ja puhekielisiä soveltavia diskursseja niistä. Tämä johtuu osin varmasti siitä, että ne ovat kehittyneet vuosikymmenten saatossa, kun maailma ja digi ovat kehittyneet teknisesti ja toiminnallisesti. Tämän lisäksi, useimpia standardien

[1] https://dvv.fi/vahti
[2] https://dvv.fi/yhteentoimivuusalusta

ulkopuolisia termejä ei ole koskaan luotu suunnitelmallisesti ja rakennettu suhteessa toisiinsa osaksi systemaattista kokonaisuutta.

Tässä sanastossa on pyritty tähän kokonaisuuden sovittamiseen, mutta on huomattava, että siitä huolimatta se tapahtuu vain rajatussa laajuudessa, erityisesti riskienhallinnan sekä digitaalisen ja turvallisuuden risteämässä. Termisanasto ei ole siis ole varsinaista yleiskieltä ja pelkkiä sanoja kuvaavat määrittelyt aukeavat vasta niitä täydentävissä huomioissa, joiden pohjalta joudutaan aika – kaikesta yrityksestä huolimatta – tekemään tulkintoja. Systemaattisuus ja prosessit, joihin digitaalisuus vahvasti rakentuu, ei voi olla heijastumatta sanastoonkin.

Tämän sanaston pitäisi olla hyvä lähtökohta ankkuroida yhteisiä näkemyksiä, vaikka kattavuus on vain noin 73 käsitettä. ”Noin”, koska näiden termien päälle on viittauksia toisiin termeihin sekä 45 synonyymiä (eli yhteensä noin 120 termiä). Tällainen kiintopiste antaa myös mahdollisuuden poiketa tarvittaessa näistä määrittelyistä perustellusti, mikä on tärkeä käytettävissä oleva mahdollisuus kontekstien ja tarpeiden muuttuessa. Riskienhallinnan pitää kuvata todellisuutta ja sitä kontekstia, jonka näkökulmasta sitä tehdään. Todellisuuden pakottaminen sopimattomiin ilmaisuihin voi vinouttaa näkymämme tai jopa sokaista meidät siltä, mitä ympärillämme tapahtuu, jolloin emme huomaa riskejä ennen kuin on jo liian myöhäistä.

Sanasto pyrkii olemaan neutraali muun muassa näkökulman, teknologian, työkalujen ja käyttäjien suhteen, eikä siten ole sovitettu erityisesti julkiselle hallinnolle vaan kaikille. Tämä on tärkeää, sillä toisiinsa kytköksissä olevien toimijoiden joukko on moninainen ja nykyaikaiset digiriskit (kuten myös muut riskit) siirtyvät ja vaikuttavat noiden kytkösten kautta. Käyttäjäneutraalius on aiemmin mainituista ehkä haastavin, sillä huomioon on pyritty ottamaan eri tasoilla tapahtuva toiminta (jota pyritään avaamaan tasomallilla), mutta myös se, että riskienhallinta täyttää eri tarpeita ja vaatimuksia asioiden ja henkilöiden suojaamisesta johtamisen tiedontarpeeseen, mutta myös sisäisen tarkastuksen ja sääntelyn minimien täyttämisestä taloudelliseen tehokkuuteen. Vähien resurssien maksimointi ja kohdentaminen parhaalla mahdollisella tavalla on tärkeää ja haastavaa digiturvallisuuden luomisessa.

Yhteistyön helpottaminen, systeeminen yhteentoimivuus ja joustavuus muuttuvassa ympäristössä edesauttavat tulevaa. On oletettava, että systeemisempi kieli tukee alati systeemistyvää ja automatisoituvaa toimintaa, kuten kehittyneempiä työkaluja digitaalisen turvallisuuden ja riskienhallinnan toteutukseen. Pelkkä tiedon liikuttelu ei kuitenkaan aiheuta muutosta, vaan tämä tarvitsee rinnalleen (standardinmukaiseen prosessiin kuuluvasti) riskeistä ja riskienhallinnasta viestimisen, johon sanasto myös liittyy. Niin digitaalisen turvallisuuden, kuin riskienhallinnankin näkökulmasta, on tärkeää viestiä uhista, haasteista ja näiden hallintakeinoista oikein. Valitsemamme ilmaukset kertovat jo itsessään miten näemme asiat, miten ne pitäisi nähdä tai näemmekö niitä ollenkaan oikein. Asioiden kohdalla on joskus oltava hyvin tarkka ja osattava tehdä ero siinä, miten rajaa vedetään eri asioiden välillä. Mikä on hyväksyttävää ja mikä ei, mikä kuuluu mihinkin jne. Tämän voi erityisesti nähdä korostuvan, kun viestitään eri hierarkiatasojen välillä, joissa ajatus pitäisi muuttaa tekoja tuottavaksi tiedoksi – ymmärretäänkö molemminpuoliset tarpeet siirryttäessä portaalta toiselle.

Hyväkin ajatus ja tärkeäkin turvallisuustieto voi hautautua huonoon ilmaisuun. Tähän esitelty sanasto tuo yhden parannellun työkalun kaikkien käyttöön – yhteistä kieltä.

2 Sanaston toteutus ja kehitys

Digi- ja väestötietoviraston (DVV) JUDO-hankkeessa[3] toteutettu digiturvallisuuden riskienhallintasanaston määritysprojekti on osa julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmaan 2020-2023 (Haukka) sisältyvää digitaalisen turvallisuuden riskienhallinnan kehittämistä[4]. Sanastoprojektin sisältö on otettu käsiteltäväksi julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja keskeisten palveluiden tuottamisesta vastaavien organisaatioiden laajapohjaisessa yhteistyö-, valmistelu- ja koordinaatioelimessä, VAHTI-toiminnan osana, ja tämä asiakirja julkaistaan VAHTI hyvät käytännöt -tukimateriaalien prosessin mukaisesti, mihin sisältyy mahdollisuus tämän dokumentin päivitykseen tarvittaessa.

Sanasto julkaistaan vapaasti käytettäväksi Yhteentoimivuusalustan[5] sanastotietokannassa osoitteessa https://sanastot.suomi.fi. Sanastot-työkalulla kerätään ja ylläpidetään julkishallinnon yhteisiä terminologisia sanastoja ja käsitteitä. Työkalu tarjoaa myös käsitteiden välisten suhteiden visualisoinnin kuvana, mikä tarjoaa vaihtoehtoisen näkymän kuin mitä tässä dokumentissa esitetyt käsitepuut. Erikseen toteutetaan myös ontologiarakenteet sanastosta mahdollista jatkohyödyntämistä varten.

2.1 Sanastoprojekti

Sanastoprojekti toteutettiin kesä-joulukuussa 2021. Sitä edelsi valmisteluvaihe sekä seurasi esittelymateriaalin ja julkaisun toteutus talvella 2022. Esivalittu sanasto pohjautui useisiin alan sanastoihin, aiempaan riskienhallintasanaston tunnistusprojektiin sekä muihin lähteisiin. Lähtökohtana projektin näkökulmasta toimivat digitaalinen turvallisuus osa-alueineen, tiedolla johtaminen ja systemaattisuus, riskienhallinta prosessina ja siitä viestiminen, riskeistä viestiminen ja niiden vaikutusmekanismien selventäminen, digitaalinen toiminataympäristö, nykyisten riskien kohdalla koetut haasteet ilmaisussa sekä strategia- ja ennakointitöistä nähtävissä olevat mahdolliset tarpeet tulevaisuudessa. Työryhmä valitsi ennakkoon eri lähteissä sekä aiempien sanastojen noin 3000 termin joukosta noin 200 ehdokasta, joista valikoitui noin 60 aihealueen näkökulmasta keskeiseksi katsottua termiä jatkokäsittelyä varten.

Projektin aikana termejä lisättiin ja poistettiin, kun ymmärrys systeemisen rakenteen muodostamisesta kasvoi. Erityisesti huomattava määrä riskien tyyppejä ja erityisten ominaisuuksien kuvauksia rajattiin pois, sillä kattavuutta ei olisi voitu toteuttaa tämän projektin puitteissa. Valinnassa haluttiin projektin näkökulmasta myös varmistaa sellaisten ilmaisujen sisällyttäminen, joilla vastataan tarpeisiin sanoittaa modernien haasteiden käsittely riskienhallinnassa. Lisäksi mukana on ilmaisuja, joilla mahdollistetaan rajanveto helposti toisiinsa sekoittuvien termien välillä. Määrittelyssä huolehdittiin erityisesti yhteensopivuudesta ISO 31000-sarjan riskienhallinnan prosessin standardin kanssa, jolloin yhteentoimivuus toteutuu myös esimerkiksi ISO 27000-sarjan tietoturvallisuuden hallinnan standardin kanssa.

Sanaston määritykseen osallistui projektin työryhmän lisäksi laaja eri alojen ammattilaisjoukko sekä eräitä oman alansa erityisasiantuntijoita. Asiantuntijaryhmä kokoontui

[3] https://www.dvv.fi/judo
[4] https://julkaisut.valtioneuvosto.fi/handle/10024/162191
[5] https://www.suomidigi.fi/ohjeet-ja-tuki/yhteentoimivuusalusta

seitsemän kertaa käsittelemään termejä, minkä lisäksi käytettiin sähköisiä lomakkeita kommentointiin näiden välillä. Ensimmäisen sanastoversion valmistuttua, sille toteutettiin erilliset työryhmän, laajennettu asiantuntijoiden sekä erillinen VAHTI-asiantuntijoiden kommentointikierrokset. Viimeiseltä kommentointikierrokselta saatiin noin 20 huomiota, joiden perusteella tehtiin täydennyksiä lähinnä huomautuksiin sekä puoltava arvio kokonaisuuden laadusta ja sopivuudesta otettavaksi käyttöön laajasti julkisessa hallinnossa sekä sen ulkopuolella.

Tämä esittelydokumentti on osa VAHTI Hyvät Käytännöt -tukimateriaalien julkaisuprosessia, jonka kautta tapahtuu myös laajempi kommentointi itse sanastoon. Dokumentissa esitetään ohjaavaa ja täydentävää tietoa sanaston soveltamiseen käytännössä sekä prosesseissa, että viestinnässä. Tukimateriaalin on tarkoitus auttaa ymmärtämään, miten termit ovat liitoksissa ja mihin ne vaikuttavat. Riskienhallinnan ei tule olla erillinen ja irrallinen toiminnan osa, vaan se on enemmän useita toimintoja yhdistävä solmukohta.

Projektin työ- ja asiantuntijaryhmään ovat kuuluneet:

Juho Reivo, projektipäällikkö, Digi- ja väestötietovirasto
Lassi Väisänen, projektisihteeri, GRC Partners
Kimmo Rousku, VAHTI-pääsihteeri, Digi- ja väestötietovirasto
Esko Mustonen, Controller-toiminto, Valtiovarainministeriö
Antti Nyqvist, Digipooli, Teknologiateollisuus ry.
Markku Rajamäki, Elinkeinoelämän keskusliitto
Ville Knuutila, Kansaneläkelaitos
Jari Ylikoski, Kuntaliitto
Julia Fomin, Kyberturvallisuuskeskus, Traficom
Pasi Koljonen, Puolustusvoimat
Juhani Kuparinen, Tietosuojavaltuutetun toimisto
Pasi Eronen, Turvallisuuskomitea (10.8. asti)
Alexander Zilliacus, Turvallisuuskomitea (10.8. alkaen)
Ville Autero, Työ- ja elinkeinoministeriö
Sanna Eronen, terminologi, Lingsoft Oy
Pia Seppänen, palveluvastaava, Lingsoft Oy

Eri työstövaiheisiin osallistuneet muut asiantuntijat:

Irina Kudasheva, terminologi, Lingsoft Oy
Armi Helenius, Digi- ja väestötietovirasto
Joonas Aitonurmi, Digi- ja väestötietovirasto
Kirsi Janhunen, Digi- ja väestötietovirasto
Erja Kinnunen, Digi- ja väestötietovirasto
Hanna Heikkinen, Digi- ja väestötietovirasto
Juha Kirves, Digi- ja väestötietovirasto
Tuomas Pelttari, Digi- ja väestötietovirasto
Laura Penttilä, Digi- ja väestötietovirasto
Marième Korhonen, Liikenne- ja viestintäministeriö
Ritva Kiiski, Kotkan Kaupunki
VAHTI-johtoryhmä
VAHTI Riskienhallinnan kehittämisen työryhmä sekä riskiprosessin pientyöryhmä

2.2 Terminologin saate

Tässä sanastossa määritellään digitaalisen turvallisuuden ja riskienhallinnan keskeistä käsitteistöä. Käsitteet on huolellisesti valittu siten, että niiden määrittely tukee viestintää ja koulutusta digitaalisten riskien hallinnasta. Aihealue on kuitenkin laaja, ja rajauksen ulkopuolelta on jo tunnistettu eri näkökulmien kannalta keskeisiä käsitteitä mahdollista jatkotyötä varten.

Käsitteiden määrittelyssä on noudatettu terminologisen sanastotyön standardoitua työtapaa (työtapaa kuvataan mm. standardissa ISO 704:2009). Olennaista työtavassa on käsitejärjestelmä sanastotyön lähtökohtana: relevanttien käsitteiden keskeiset piirteet ja niiden väliset suhteet tunnistetaan, ja tämän pohjalta laaditaan keskenään yhteen toimivat määritelmät välttäen esimerkiksi ristiin viittaamista.

Sanastotyön lähtökohtana on käytetty yhteentoimivuusmenetelmän mukaisesti aiemmin tehtyjä sanastoja, joista erityisesti Kyberturvallisuuden sanastoon (TSK 52, 2018), Kokonaisturvallisuuden sanastoon (TSK 50, 2017), ja aihetta käsitteleviin SFS-julkaisuihin (SFS-OPAS 73:2011, SFS-ISO 31000:2018 ja SFS-EN ISO/IEC 27000:2020) on pyritty säilyttämään yhteensopivuus. Aiemmin tehtyjä käsitteiden määritelmiä on lainattu sanastoon sellaisenaan aina, kun se sanaston käsitejärjestelmä, käyttötarkoitus ja tavoitteet huomioiden on ollut mahdollista. Sanaston teksteissä mainitaan joitain termejä, jotka on rajattu tämän sanastotyön ulkopuolelle, ja niiden osalta on varmistettu, että relevanteissa lähteissä julkaistut määritelmät ovat yhteensopivia sanaston kanssa.

Uudet käsitteet on pyritty määrittelemään mahdollisimman yleisellä tasolla, jotta laadittuja määritelmiä voidaan käyttää uudelleen muissa yhteyksissä yhteentoimivuusmenetelmän mukaisesti. Käsitteiden termejä ja määritelmiä on arvioitu asiantuntijaryhmän kanssa työpajoissa eri näkökulmista, minkä lisäksi useilta tahoilta on kerätty kirjallista palautetta, jotta sanasto vastaisi mahdollisimman hyvin eri sidosryhmien näkemyksiä ja tarpeita.

Terminologisessa sanastossa käsitteistä annetaan tarvittaessa lisätietoa huomautuksen muodossa. Huomautuksen tiedot voivat liittyä termeihin, määritelmään tai muuhun sanaston käyttötarkoituksen kannalta oleelliseen asiaan. Etenkin tässä sanastossa huomautus sisältää useimmiten tietoa, jonka tarkoituksena on helpottaa määritelmän tulkitsemista ja käsitteen kontekstin hahmottamista. Lisäksi tässä sanastossa on huomautuksilla tuotu esiin eroja ja yhtäläisyyksiä muiden lähteiden määritelmiin. Etenkin monialaiset ja merkitykseltään abstraktit käsitteet ovat usein haastavia sanaston käyttäjälle, joten huomautuksilla on pyritty varmistamaan tiedon välittyminen tarkoitetulla tavalla. Sanaston syvällinen ymmärrys vaatii kuitenkin myös aihepiirin tuntemusta tai lisäkoulutusta.

Sanasto on laadittu suomen kielellä, mutta taustatietoa on kerätty myös englanninkielisistä ja ruotsinkielisistä lähteistä. Osalle käsitteistä on jo sanastotyön edetessä tunnistettu käännösvastineita, ja lopulliseen julkaisuun vastineita täydennetään niin, että sanastossa on termivastineet kaikille käsitteille ruotsiksi ja englanniksi.

2.3 Digitaalisen toimintaympäristön turvallisuuden käsitteiden kehityksestä

Digiturvallisuuden osa-alueiden eri määritelmiä, eli aiheiden diskursseja, määritetään jatkuvasti – käytännössä jokaisessa keskustelussa. Niitä on jokaisella aiheella monia, ne ovat jatkuvassa muutoksessa, niitä ei voi kutistaa vain muutamiin yhteisesti jaettuihin osiin, ja ne ovat osin päällekkäisiä eri aiheiden välillä. Eri tahot myös pyrkivät aika ajoin vaikuttamaan näiden muodostumiseen suorasti ja epäsuorasti, muun muassa sääntelyn ja standardien kautta – tai viestintäkampanjoilla (markkinoinnista hybridivaikuttamiseen). Suurin muovaaja on kuitenkin ajassa muuttuvat toimintatavat, joiden sisällöt antavat lopulta kattotermeille niiden merkitykset, vaikka kattotermeillä asioita pyritäänkin ohjaamaan.

Termien kehityskulkuja on vaikea ennakoida. Esimerkiksi virukset määrittelivät tietoturvallisuuden sisällön 90-luvulla ja kyber popularisoitui ilmauksena scifi-kirjallisuuden dystopiakuvauksissa jo huomattavasti aiemmin. Digiturvallisuuden käsitteiden kansainvälisyys tuo tähän myös oman leimansa. Erityisesti englannin kielen käyttö eri maiden toimijoiden yleiskielenä tuottaa päänvaivaa merkityksien siirtymisessä. Se, mitä täällä tarkoitetaan kyberillä ei ole aivan sama asia, kuin mitä kymmenien muiden maiden toimijoiden ”cyber”. Erikseen tämän lisäksi on puhekielinen käyttö, jossa on vielä väljemmin luettu asioita eri ilmaisujen sisään. Vaarana on vaikea ymmärrettävyys, rajattomuuden loputon suo ja eri asioiden muovautuminen yhdeksi epämääräiseksi kasaksi, josta ei saada otetta. Tämä lisäksi altistaa sille, että yhteistä merkitystä kaipaavat alkavat tuottaa uusia ilmaisuja, lisäten vain kokonaisuuteen enemmän termejä, sillä vanhat hyvin harvoin katoavat täysin. Keskeisten termien ”inflaatio” on riski digiturvallisuudesta ja sen osa-alueista viestimiselle tehokkaasti, minkä takia ilmaisujen tarkkuuteen tulisi kiinnittää huomiota.

Tulevaisuudessa, kun digitaalinen toimintaympäristö alkaa olla etenevässä määrin osa muuta toimintaympäristöämme, ei liene kaukaa haettua, että seuraavien vuosikymmenten aikana reaalimaailman näkökannat esimerkiksi (digitaalisen) ympäristön suojelusta voisivat siirtyä tällekin saralle. Nämä ovat osin asioita, jotka vaatisivat kaupallisten lainalaisuuksien sijaan demokraattista keskustelua, kuten missä määrin digissä on ”jokamiehenoikeuksia” liikkua avoimessa datassa ja missä määrin kaikki aidataan muurien taakse, mitä säilytetään historiallisina muistoina ja mitä uskalletaan säilyttää, koska muuttumattomuus tarkoittaisi riskienkin säilyttämistä. Ja koska kyse on lopulta ihmisen rakentamasta ympäristöstä, miten se rakentuu turvalliseksi, mikä on digiluonnon suojeltavaa infraa ja mikä on sen hyödynnettävää luonnonvaraa, etenkin mikäli netin rakenteet ja yhteydet katoavat entistä enemmän näkyvistämme. Sekä poliittisista että kaupallisista syistä tapahtuvat ekosysteemien mahdolliset eriytymiset (mistä aiemmin puhuttiin verkkojen ”balkanisoitumisena”) voisivat myös olla merkittävä muutostekijä turvallisuudessakin. Tai ehkä alamme hallita digittömyyden riskejä. Riskit ja näiden hallintatoimet tulevat muuttumaan vastaavasti digin muutosten mukana.

3 Viestinnän ja kielen hyödyntäminen riskienhallinnan eri osissa

Riskienhallinnan prosessin merkittävänä osana on viestintä sen eri vaiheissa. Siitä näkökulmasta riskienhallintaa ei tapahdu, mikäli siitä ja sen tuottamasta tiedosta ei olla tietoisia. Koko prosessia voidaan pitää laadukkaan riskeistä viestimisen prosessina. Tällä selkeällä ja oikein muotoillulla tiedolla tuetaan tietopohjaista päätöksentekoa sekä annetaan koko organisaatiolle käsitys luotettavasta suunnasta toiminnalle. Viestintä ja kieli ovat siten strategisen tärkeitä organisaatiolle.

Turvallisuuden kulttuuria luodaan muun muassa kannustamalla tuomalla epäkohtia esiin. Tämä riskientunnistamisen ja heikkojen signaalien käytännön joukkoistaminen ei saa painaa villaisella asioita, auki jäävistä tietoliikenneporteista tai vastaavista haavoittuvuuksista, vaan tulisi kannustaa ja jopa palkita epäkohtien esiin nostamisesta. Palautteesta pitäisi seurata konkreettisia toimenpiteitä, jotta sen antamista pidetään mielekkäänä. Usein keskeistä on kuitenkin tieto siitä, viesti, että palaute on huomioitu ja että sen antaminen ei ollut turhaa. Riskienhallintajärjestelmän kokonaisuuden rakentuminen alkaa tämänkaltaisista pienistä asioista.

Riskienhallinta, kuten digiturvallisuuden, tulisi ulottua kaikkialle, myös meidän vapaa-aikaamme ja arkeemme, myös kotona. Riskeistä viestimisessä tulee kiinnittää huomiota siihen, että puhutaan jokaisen ihmisen arkipäivään kuuluvista asioista. Riskienhallintaa on siis se, että ottaa aamulla sateenvarjon mukaan tai vaihdat talvirenkaat ajoissa, yhtä lailla kuin se että pysähtyy hetkeksi miettimään mikä voisi mennä pieleen tai haitata omaa työtä. Mutta jostain on tultava heräte, muistutus, perustelu, ohjeet, kannustin, varoitus sekä muita vastaavia viestejä, joilla tuetaan tätä. Mitä kiireempää ja tiukalle viritetympää on aikataulujen suhteen tai mitä uudempaa ja poikkeavampaa toiminta on, sitä suurempi kynnys on ylitettävänä ja sitä enemmän tarvitaan suorempaa viestiä ja tukea. Nekin organisaatiot, joissa toimintakulttuuriin on vakiintunut riskienhallinnan huomioiminen osaksi työtä, tarvitsevat muistutuksia laadun ylläpitämiseen ja parantamiseen, uusiutumiseen ja jähmettymisen välttämiseen.

Yksi lähtökohta viestimisessä, kuten koulutuksessa, on käydä asioita läpi kohta kohdalta, aihe aiheelta tai termi termiltä. Joskus nämä ovat yksityiskohtia selventäviä, mutta samalla laajempien keskusteluiden lähtölaukauksia. Mikäli ei täysin hahmoteta, missä on haasteita, voi olla hyvä aloittaa tähän läheisesti liittyvistä käsitteistä ja katsoa, mitä asioita ja ongelman ominaisuuksia rajautuu niiden sisä- ja ulkopuolelle.

Kyse ei ole pelkästään prosessin toteuttamisesta, vaan myös asennoitumisesta ja aiemmin mainitusta kulttuurin luomisesta, jota luodaan suurelta osin johtamisen – niin asiantuntijoiden kuin johtajienkin – sanojen ja esimerkin kautta viestimällä. On siis huomioitava, että riskienhallinnassakin tulee viestiä sekä hallinnollisella, mutta myös johtajuuden tulokulmalla. Tämän päälle sisältöä on osattava kohdistaa, esimerkiksi tässä sanastossa esitellyt tasomallin kautta, johdolle, organisaation asiantuntijoille sekä toteuttavalle tasolle, kullekin niiden strategisina, koordinaatiolle merkityksellisinä ja käytännön toimintaan vaikuttavina viesteinä. Riskienhallinta on se, missä (muun muassa) turvallisuuden ja muun toiminnan pitäisi kohdata ja keskustella.

Kun otetaan vielä huomioon prosessiin liittyvä viestiminen, kuten tilannekatsaukset ja muistutukset, riskienhallinnasta – sekä itse riskeistä ja yleisemmin uhista – viestiminen pitäisi yhä selvemmin näkyä suunniteltavana kokonaisuutena. Käyttäen

vuosikelloa tai taulukkoa voidaan suunnitella milloin mitäkin on viestittävä sekä tarkastella, että viestinnässä katetaan kaikki oleelliset yksityiskohdat. Kun päästään viestinnän suunnitteluun, huomioidaan myös muun muassa kuka viestii, miten ja missä kanavissa sekä mitä muuta digiturvallisuuteen (tai muuhun) liittyvää ollaan suunnitellusti viestimässä. Toki, kuten hyvissä suunnitelmissa yleensäkin, viestintäsuunnitelmaankin on riskiperusteisesti jätetty tilaa venyä poikkeamien varalta.

Strategisessa riskienhallinnassa on olemassa strategiset tavoitteet ja riskit uhkaavat strategioiden toteuttamista. Tämän ymmärtäminen tulee viestiä siten, että kyse on toiminnan jatkuvuuden turvaamisesta eri muodoissaan. Kun halutaan osallistaa tätä tukevaan yhteiseen kulttuuriin, olennaista on osallistaminen. Ihmiset yleisesti haluavat osallistua ja kehittää itseään lähellä olevia ja koskettavia asioita, kuten esim. perhe, harrastuspiirit, työyhteisöt. Riskienhallintaa ei tulisi tiukasti lokeroida eri tasoille (mihin liittyy rajoittamista ja siten on eri asia kuin kohdistaa eri näkökulmiin tarvittavaa tietoa ja toimia) vaan siitä pitää tehdä kaikkien yhteinen asia.

Riskien tilaa tulisi havainnollistaa kaikille. Olisi hyvä keskustella ääneen seurausten vaikutuksista ja luoda kokonaisymmärrystä koko organisaatiossa arvioiduista riskeistä. Esimerkiksi kunnissa, joissa on useita erityyppisiä toimialoja, olisi hyvä tarkastella yli siilojen, miten opetustoimessa on tällaisia riskejä, varhaiskasvatuksessa tällaisia, hallinnossa ja päätöksenteossa tällaisia ja niin edelleen. Pienemmissäkin organisaatioissa voi läheltä löytyä sekä ratkaisuita, että jaettuja haasteita. Kyse ei ole vain johdon raportoinnista - kaikilla on oma roolinsa kokonaisuudessa.

Palveluketjujen näkökulmasta toiminta ei pääty rajapintoihin, siksi yhteinen riskienhallinta ja suunnittelu on tärkeää. Asiakas/käyttäjä/kuluttaja/kansalainen ei välttämättä tiedä kenen riskienhallinta-alueella ollaan. Niin yksilön kuin organisaationkin koko asiakaskokemus voi kaatua huonoon yhteistyöhön tai sen puutteeseen. Asioista tulee keskustella ääneen, jotta ne voidaan järjestää. Tässä keskustelussa kumppani voi tarvita tukea ilmaistakseen asiansa oikein, oikeilla termeillä. Yksi ongelmakohta riskeistä viestimisessä onkin, että puhutaan kyllä samasta aiheesta, mutta toistemme ohi, hieman eri asioista ja kulmista, tarkistamatta mihin tarkalleen viitataan.

Vain omaan napaan tuijottavat riskienhallinta-, turvallisuus- ja valmiussuunnitelmat eivät enää riitä. Ne pitää yhteen sovittaa ja se tapahtuu yhteistoiminnassa. Koska riskejä arvioidaan kunkin omasta kontekstista, mutta toisen tilanne vaikuttaa ketjuuntuneissa rakenteissa tähän, tarvitaan riittävästi tiedonjakoa uhista sekä riskienhallinnan järjestämisestä. Vaarana on, että yksi osapuoli ei riittävästi huomioi riskiä, tai riski muodostuu epäselväksi jäävällä ”harmaalla alueella” toimijoiden rajapintojen välissä.

Riskienhallinta otetaan huomioon palvelusopimuksissa, joissa riskien siirrosta ollaan joissain tapauksissa valmiita maksamaan hintaa, jotta niiltä vältytään, mutta liian usein ulkoistamisessa häviää kuva riskienhallinnasta ja riskeistä palveluketjulle tai kokonaisprosessille. Näistäkin pitää organisaatiossa tunnistaa ja päättää, mitkä ovat avaintoiminnot, niitä tukevat järjestelmät ja liittyykö asiaan palvelusopimuksia, joissa tulee huomioida ja joihin kirjata jotain erityistä. Tämä on polku sopimus- sekä toimittaja(suhteen)hallintaan riskienhallinnan keinoina. Näissä kirjallisissa ”keskusteluissa” on vielä tärkeämpää tulla ilmaistuksi oikein ja tunnistaa nyansseja.

4 Aihealue: Ylätason keskeiset käsitteet

Käsitteet: digitaalinen toimintaympäristö, digitaalisen toiminnan riski, digitaalinen turvallisuus, kyberturvallisuus, tietoturvallisuus

Termien kehityksen seuraamisen ja muutosten ymmärtämisen vuoksi on tärkeää taustoittaa sanaston kehitystä ja siinä tehtyjä valintoja. Erityisesti tässä aihealue-osiossa on huomattava, että sanaston toivotussa käytössä (eli riskienhallinnan toteutuksen tukemisessa) ylätason keskeiset käsitteet ovat vähemmän tärkeitä kuin muu sanasto, joka käsittelee lähempänä prosessia olevia asioita. Nämä kontekstia antavat termit on kuitenkin huomioitava siinä laajuudessa, kuin niitä tarvitaan digitaalisen, riskienhallinnan, turvallisuuden sekä muun käsittelyn rajausten määrittelyyn. Ilman aihealuekohtaista tarkennusta joutuisimme käyttämään hyvin ylimalkaisia ilmauksia. Esimerkiksi palo- ja pelastustoimen tai työturvallisuuden riskienhallinnan sanastoissa on merkittäviäkin eroja joissain määritelmissä.

Tässä sanastossa ei määritetä ylätason kontekstitermejä täydellisesti, laatikoida niitä, vaan vain siinä määrin kuin on tarpeen, muodostaen nähtäville näiden yhteys - eli lähinnä vain ”pari laatikon seinistä”. Tämä jättää tilaa näille termeille toimia ja kehittyä. Tarpeettomassa rajaamisessa on vaaransa, mikä liittyy tärkeään riskienhallinnan periaatteeseen: on kuvattava (tarvittaessa kieltä myöten) sitä todellisuutta, jossa toimitaan, eikä tarkoitus ole pakottaa toimintaa tai toimintaympäristöä sopimaan kielellisiin himmeleihin ja rakennelmiin. Todellisuus ei usein sisällä tarkkoja rajoja ja yksinkertaisia määrityksiä. Vääränlainen tulkinta näistä vinouttaa arvioita riskeistä ja pahimmillaan tämä kertautuu prosessin eri vaiheissa.

Digitaaliseen turvallisuuteen luetaan keskeisinä toteuttamisalueina johtaminen ja riskienhallinta, jatkuvuudenhallinta (sisältäen varautumisen sekä toipumisen), kyberturvallisuus, tietotuoja sekä tietoturvallisuus.[6] Nämä ja muut osa-alueet, joissa digiturvallisuutta voidaan toteuttaa, ovat monisanaisuudessaan osoitus siitä, miten monipuolisesti digi on sulautunut maailmaamme ja miten sen moninaisuus vaikuttaa digiin takaisin. Näistä viidestä jatkuvuudenhallinta otetaan esiin seuraavassa osiossa. Tietosuoja taas on hyvin määritelty jo siihen liittyvässä lainsäädännössä, mikä tekeekin siitä tarkemmin määritellyn kokonaisuuden muihin nähden, eikä sitä siksi ole erikseen otettu sanastoon. Tarkka määrittely myös näkyy sen toteutuksessa, jonka keskeinen osa on riskienhallintaan perustuva. Tuota riskienhallintaa tehdään erityisessä organisaatiokontekstissa (tiedonhallintayksikkö, kts. osio riskienhallinnan konteksteista) ja tietynlaisille riskeille, jolloin siinä käytetään tiettyjä arviointityökaluja ja kriteereitä.

Kyberturvallisuuden määritelmää voi pitää digitaalisen turvallisuuden joukon haastavimpana. Se on ottanut paljon vaikutteita ulkomailta, mutta käännökset perustuvat eri maiden näkemyksiin, vaihdellen tarkoituksissaan digi-, kyber- tai tietoturvallisuudessa – tai jossain näiden sekoituksessa. Eri toimijoilla on omistajuutta termiin ja ne määrittävät termiä oman toimintansa kautta. Sen etuliitteellä on puhekielistä vapaata käyttöä, jonka taustalla on vuosikymmenien historiaa populaarikulttuurista. Se ei myöskään ole neutraali termi siinä mielessä, että sen turvallisuuden tulokulma kehittyi[7]

[6] Digitaalisen turvallisuuden kokonaisuuden laajempi määrittely riskienhallinnan ulkopuolella on liitteissä.
[7] Kts. mm. internetin hakusanojen aihealueiden suosituimmuuden kehittyminen 2004-2022, https://trends.google.com

kybersodankäynnin valtioiden välisistä konflikteista, missä eri toimijoiden kautta usein ajatellaan uhkien tahallisuutta ja kohdistumista sekä (riskienhallinnan termein) mahdollisuuksia huomioimatta.

Nämä ovat vain muutamia vaikuttimia siihen, että kyberturvallisuudella on useita päällekkäisiä määrittelyitä, diskursseja, ja miksi OECD näki tarpeelliseksi laajemman termin, jolla on selkeämpi käyttöalue[8] . Digiturvan kokonaisuudessa kuitenkin kyberturvallisuus on yksi aihealueen tärkeä näkökulma, jonka kautta kohdataan tietyntyyppisiä haasteita. Kyberissäkin on tapahtunut viime vuosina sen moninaisten diskurssien laajenemista digiturvan näkemyksen suuntaan, etenkin puhekielessä, ja se on ollut miltei synonyymi digiturvalle. Tämä on hyvä siihen nähden, että turvallisuuspuheessa joskus tehdään ”turvallistuttamista”, mikä sulkee ja rajaa käsittelyä.

Useiden termien käyttö tukee riskienhallintaa ja riskien hahmottamista, vaikka ne ovat kehittyneet eri lähtökohdista. Pieni päällekkäisyys tuo syvyyttä turvallisuudenkin järjestämisessä ja toisaalta moniulotteisempi tarkastelu tuo esiin ominaisuuksia ja uusia puolia, joiden huomioiminen on usein muistettava kompleksisempien haasteiden edessä[9]. Riskien tunnistaminen ja analysointi sekä käsittelyn suunnittelu tulisi tehdä sisällyttäen useampi kulma.

Digitaalisen toiminnan riskeihin liittyen tulisi kysyä: mikä digissä aiheuttaa erityistä riskiä? Tätä voidaan tarkastella sen tuottamien hyötyjen kautta, kääntäen ne päälaelleen. Digin yleisinä ominaisuuksina tai tavoitteina voidaan nähdä muun muassa:

Tehokkuus
- nopeus (osa- ja kokonaisprosesseissa)
- skaalautuvuus (tarpeeseen helposti suhteessa kuluihin tai vaivaan)
- saatavuus (24h/365)

Laatu
- yhdenmukaisuus (koneelliset säännöt tuottavat osittaista yhdenvertaisuutta)
- tarkkuus (tietyt virheet voidaan korjata ja estää sekä käsittelyssä voidaan olla tarkempia etenkin numeerisissa/koneluettavissa asioissa)
- kattavuus (mahdollisuus laajemman datan käyttöön sekä ”bigdataan”)

Kehitys
- uudet toimintatavat (automatisoidut toiminnot, uudet käyttötavat)
- uudet tekniikat (uudet tavat käyttää dataa ja järjestelmiä)
- synergiaedut (uudet palvelut, uudet palvelutavat, yhteistyö)

Yleistettävyys
- mukautuvuus ja hallittavuus (rakenteisten osien käyttö, kopiointi ja muokkaus automatisoidusti)
- systemaattisuus ja säännönmukaisuus (opittavissa ja toistettavissa)
- globaalius (toiminta eri järjestelmissä ja niiden välillä, verkottuneisuus)

[8] Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi OECD:n suositus ja liiteasiakirja – Valtiovarainministeriön julkaisu 28/2016, erityisesti s.8 ja 30 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75412/OECD_julkaisu_NETTI.pdf

[9] Esimerkkinä digiturvallisuuden riskinäkökulman joidenkin aiheiden käsittelystä Digiturvaviikon aamupäivän paneeli alustuksineen 29.10.2021 (osat 1-7 https://www.mediaserver.fi/live/digiturvaviikko2021).

Se, mitä voidaan yleisesti tarkastella saavutettavan digillä, voidaan lisäksi viedä pidemmälle ja tehostaa vielä kehittyneemmissä järjestelmissä ja prosesseissa, hyödyntäen automatisointia, algoritmeja tai koneoppimista ja niin edelleen. Näin edellä kuvatut digin positiiviset mahdollistajat ja tätä kautta syntynyt digitaalinen toimintaympäristö voidaan kääntää luomaan uhkia kaikille tasoille, yksilöstä yhteiskuntaan. Näistä aineksista syntyy kehittynyt ja tehokkaasti hallittava massiivinen hyökkäys useita järjestelmiä vastaan, joista ohjelma ja hyökkääjä oppivat uutta hyökkäyksen jatkamiseksi tai seuraavan kehittämiseksi. Siksi näille ominaisuuksille ja niistä johdettaville kehittyville riskeille on syytä miettiä tapoja tunnistaa ne sekä luoda niiden vastapainoksi kontrolleja.

Digitaalinen toimintaympäristö, johon kaikki käsitellyt termit liittyvät suoraan tai välillisesti, on luonteeltaan erityinen, ihmisen luomiin sääntöihin perustuva alati muuttuva kokonaisuus[10]. Se on joiltain osin yhtä rajaton kuin mielikuvitus tai kovalevyn koko ja toimii (osin) valon nopeudella, mutta silti se on kiinni reaalimaailmassa, joka asettaa sille rajoja. Reaalimaailman tapahtumat voivat myös luoda riskejä, jotka uhkaavat osia digitaalisesta toimintaympäristöstä – suoraan tai välillisesti. Näitä riskejä voidaan joko tarkastella osana digiriskejä tai muuta riskien hallintaa, riippuen siitä minkä toimintaympäristön kautta se on mielekkäintä omaa toimintaa ja riskienhallintaa ajatellen.

Ylipäätään voi olla mielekkäämpää puhua useista toimintaympäristöistä (mukaan lukien digitaalisen toimintaympäristön sisällä määriteltävät toimintaympäristöt), jotka risteävät kompleksisissa asioissa, mutta samaan aikaan voi toisaalta määritellä, että organisaatiolla (tai muulla tarkastelun kontekstilla) on vain se yksi toimintaympäristö ympärillään, josta voidaan sitten tarkastella digitaalista tasoa. Kumpikin käyttötapa on mahdollinen. Jälkimmäinen tulee esiin, kun tehdään eroa sisäisen ja ulkoisen välillä. Ensinnä mainittuun liitetään muun muassa organisaatiokulttuuri (ja luonnollisesti sen alatermit turvallisuuskulttuuri ja digiturvallisuuskulttuuri), tavoitteet ja käytetty teknologia, kun taas jälkimmäiseen sääntely, politiikka, kulttuuri (paikallinen ja globaali) ja vastaavat. Näiden kahden käyttö on tavallista strategisissa pohdinnoissa. Digiturvallisuudessakin voidaan asemoida omat sisäiset rakenteet ja toiminnot tietyllä tavalla suhteessa ulkoiseen (”minkälaista digiturvallisuutta rakennamme”). Vastaavasti ulkoisessa toimintaympäristössä voidaan ottaa tietty lähestymistapa tai näkökulma siellä vastaantuleviin asioihin, eli miten sisäisiä sovelletaan tai pitäisi soveltaa niiden ratkaisemiseen (”miten rakentamamme digiturvallisuuden tulisi toimia tässä”). Kun nämä strategiset näkökulmat ovat selvillä, niiden toteuttamiseen kuuluu viestiminen oikealla tavalla sisäisesti ja ulkoisesti.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että sisäistää, mitä digitaalisella toimintaympäristöllä tarkoitetaan kaikessa laajuudessaan ja muuntuvuudessaan. Digitaalisen turvallisuuden kattavuus puolestaan tuo esiin eri näkökulmat, joilla voidaan lähestyä eri turvallisuutta monipuolisesti. Haasteena toki on, että termit tai niiden merkitykset eivät ole täysin vakiintuneet ja niiden käyttö on usein

[10] Yleisemmin nykyaikaisesta toimintaympäristöstä käytetty VUCA-akronyymi kuvaa digitaalista toimintaympäristöä hyvin: muutosherkkä, epävarma tulevaisuudenkuva, kompleksia vaikutussuhteita ja tulkinnanvaraisuutta (Volatility, Uncertainty, Compleksity, Ambiquity).

vapaamuotoista, mutta tätä voi pitää yhtenä riskienhallinnan viestinnän ja koulutuksen tehtävänä parantaa jokaisessa organisaatiossa.

4.1 Digitaalinen toimintaympäristö

Synonyymi: kybertoimintaympäristö; digitoimintaympäristö; digitaalinen ympäristö

Määritelmä: *yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö*

Huomautus Muihin toimintaympäristöihin verrattuna digitaaliselle toimintaympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation käsittelyyn viestintäverkkojen avulla. Digitaalinen tietojärjestelmä käsitetään tässä kuitenkin sosio-teknisenä järjestelmänä, joten digitaalinen toimintaympäristö kattaa myös sitä käyttävät ihmiset, heidän toimintatapansa sekä toiminnan mahdollistavat fyysiset laitteet ja rakenteet. Käytännössä digitaalinen toimintaympäristö koostuu erilaisista järjestelmistä ja näiden välisistä yhteyksistä, joihin liittyy toimintaa ohjaavien toiminnallisuuksien lisäksi kulttuurisia käytäntöjä. Esimerkiksi sosiaalisen median kanava mahdollistaa monenlaisia käyttötapoja ja vaikuttamista. Muita esimerkkejä digitaalisista toimintaympäristöistä ovat voimalan tai tehtaan ohjausjärjestelmä, pankki- ja maksujärjestelmät, digitaaliset oppimisympäristöt, verkkovaikuttamisen tiedonkeräysverkostot, ohjelmistoekosysteemit sekä julkiset sähköiset palvelut tietovarantoineen. Kybertoimintaympäristöllä tarkoitetaan samaa kuin digitaalisella toimintaympäristöllä, mutta se sopii terminä parhaiten kyberturvallisuutta käsitteleviin konteksteihin.

4.2 Digitaalisen toiminnan riski

Synonyymi: digiriski; digitaalinen riski

Määritelmä: *digitaalisessa toimintaympäristössä vaikuttava, digitaaliseen toimintaympäristöön kohdistuva tai siitä johtuva riski*

Huomautus: Digitaalisen toiminnan riskejä ovat mm. digiturvallisuuden ja kyberturvallisuuden riskit, digitalisaation ja digitoinnin riskit sekä digitaaliseen viestintään liittyvät riskit. Digitaalisen toiminnan riskiä voidaan tarkastella kapeasti, digitaalisen toimintaympäristön sisäisenä asiana, tai laajasti, jolloin se kytkeytyy toimintaympäristönsä ulkopuolelle ja sitä voidaan verrata myös ei-digitaalisiin riskeihin – esimerkiksi vertaamalla digitaalisia toteutustapoja osin tai kokonaan ei-digitaalisiin toteutustapoihin, kuten tiedonkeräys paperilomakkeella.

4.3 Digitaalinen turvallisuus

Synonyymi: digiturvallisuus

Määritelmä: *tavoitetila, jossa digitaaliseen toimintaympäristöön voidaan luottaa ja toiminta sekä siellä että siihen liittyen on turvallista ja hallittua, myös häiriötilanteissa*

Huomautus: OECD:n määrittelyn mukaisesti digiturvallisuus on laaja kokonaisuus, jonka alle luetaan soveltuvin osin mm. digiturvallisuuden riskienhallinta,

jatkuvuudenhallinta, tietosuoja, tietoturvallisuus sekä kyberturvallisuus; näillä on toisaalta osa-alueita, jotka eivät kuulu digiturvallisuuteen. Siinä missä kyberturvallisuus liittyy kansallisen ja kansainvälisen tason turvallisuuteen, digiturvallisuutta voidaan pohtia jopa yksittäisen henkilön tavoitteiden ja toiminnan kautta. Digiturvallisuus sisältää laajasti mm. teknisiä, sosiaalisia ja taloudellisia kysymyksiä, mutta niitä kaikkia ei aina huomioida. Organisaation tavoittelema digiturvallisuuden taso riippuu muun muassa sen tavoitteista, resursseista ja sille asetetuista vaatimuksista. Digiturvallisuus kuten kyberturvallisuuskin vaikuttavat myös fyysisen maailman turvallisuuteen samoin kuin fyysisen maailman kautta vaikutetaan digiturvallisuuteen.

(Digitaalisen turvallisuuden kokonaisuuden laajempi määrittely riskienhallinnan ulkopuolella löytyy tämän asiakirjan liitteistä)

4.4 Kyberturvallisuus

Synonyymi: -

Määritelmä: *tavoitetila, jossa kybertoimintaympäristöstä yhteiskunnan elintärkeille toiminnoille tai muille kybertoimintaympäristöstä riippuvaisille toiminnoille koituvat uhkat ja riskit ovat hallinnassa, myös häiriötilanteissa*

Huomautus: Digiturvallisuus ja kyberturvallisuus ovat hyvin läheisiä käsitteitä, mutta OECD:n määrittelyn mukaisesti digiturvallisuus on laajempi kokonaisuus, josta kyberturvallisuus muodostaa vain osan; toisaalta kyberturvallisuudella on osa-alueita, jotka eivät kuulu digiturvallisuuteen. Siinä missä digiturvallisuutta voidaan pohtia organisaation tai jopa yksittäisen henkilön tavoitteiden ja toiminnan kautta, kyberturvallisuus sisältää painotuksen kansallisen ja kansainvälisen tason turvallisuuteen sekä yhteiskunnalliseen vaikuttamiseen. Kyberturvallisuutta käsittelevissä konteksteissa digitaalisesta toimintaympäristöstä käytetään yleensä termiä kybertoimintaympäristö. Tässä määritelmässä on mukailtu Kokonaisturvallisuuden sanaston (TSK 50, 2017) määritelmää, joka lähestyy käsitettä riskienhallintaan soveltuvasta näkökulmasta. Kyberturvallisuus on yksi kokonaisturvallisuuden osa-alueista. Kyberturvallisuuden sanastossa (TSK 52, 2018) kyberturvallisuudella tarkoitetaan huomautusten perusteella samaa käsitettä kuin tässä sanastossa, vaikka määritelmä eroaa tässä esitetystä.

4.5 Tietoturvallisuus

Synonyymi: tietoturva

Määritelmä: *tavoitetila, jossa tietojen ja tietojärjestelmien saatavuus, eheys ja luottamuksellisuus on varmistettu*

Huomautus: Organisaation tavoittelema tietoturvallisuuden taso riippuu muun muassa organisaation tavoitteista, resursseista ja sille asetetuista vaatimuksista, ja nämä ohjaavat tietoturvariskien hallintaa. Tietoturvallisuutta varmistetaan tietoturvatoimenpiteillä. Tietoturvatoimenpiteet voivat olla hallinnollisia, teknisiä tai muun tyyppisiä. Tietoturvallisuus sisältää digitaalisen lisäksi myös muita osa-alueita, esimerkiksi paperimuotoisten asiakirjojen hallintaa, joka voidaan lukea tarpeen mukaan ja prosesseista riippuen joko digiturvallisuuden ulkopuolelle tai sen alle mm. digitaalisen tiedon tulostuksen, skannauksen ja tiedonsiirron myötä.

5 Aihealue: Kun jotain tapahtuu

Käsitteet: hyökkäyksen aiottu kohde, hyökkäys, häiriö, jatkuvuudenhallinta, poikkeama, tapahtuma

Ollaan jo myöhässä riskienhallinnan näkökulmasta, kun jotain ikävää tapahtuu. Se ei välttämättä tarkoita, etteikö ennen tapahtumaa olisi tunnistettu mahdollisuus tapahtumalle ja panostettu sen käsittelyyn, jotta seuraukset olisivat vähäiset. Riskienhallintaa on myös toivottavasti tehty jatkuvuudenhallinnan osana, jolloin on etukäteen osattu tehdä oikeanlaista varautumista. Tämä helpottaa tapahtuman aiheuttaman tilanteen hallitsemista, jolloin jatkuvuuden hallinnassa päästään tehokkaammin ja nopeammin palautumiseen kohti normaalia – tai muuta tavoiteltua tilaa.

Tapahtuman huomautuksessa on otettu esiin, että voi olla erityyppisiä tapahtumia, riippuen tarkastelluista ominaisuuksista. Määrittely suuntaa toimintaa ja etenkin käsitys tapahtuneesta suuntaa ensireaktiota vahvastikin. Tämä voi ohjata väärään suuntaan valitettavan pitkään, mikäli ensiarvioita ei huomata tarkentaa. Voi selvitä jälkikäteen, että hyökkäyksen aiottu kohde on ollut joku muu, mutta se on usein pidemmän selvittelyn tulos, mikäli jälkiä on yritetty peitellä. Ei ole tavatonta, että samoja järjestelmiä käyttävien joukosta on vaikea tunnistaa kuka tai ketkä ovat olleet kohteena – vai ovatko asiakkaat olleet vain sivullisia uhreja, kun palvelun tuottajassa on ollut maalitaulu.

Näinä päivinä häiriöille haetaan helposti syyllistä, mutta on myös muistettava, että luonto kykenee edelleen – avaruudesta maankuoreen – tuottamaan meille yllätyksiä. Ei toisaalta ole aina selvää, miten kompleksisten järjestelmien rakenteissa asioita pääsee tapahtumaan, sillä niiden toiminnallinen käytettävyys ei aina tue ihmisen tarpeita. Joskus on parempi olettaa tahatonta osaamattomuutta tai inhimillistä erehdystä kohdistetun uhan sijaan. Kaiken kaikkiaan, digitaalisen turvallisuuden kokonaisuus huomioiden, ei tule olettaa, ettei koskaan tapahdu mitään. Täydellisen estämisen ja ehkäisemisen varaan rakennettu riskienhallinta-ajattelu ei ole tehokasta tai kestävää muulle toiminnalle.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että sisäistää, erilaisten tapahtumien kirjon ja osaa valita kuvaavimman ilmauksen käsittelyä varten. Joskus se voi hetkellisesti tarkoittaa hyvinkin ympäripyöreää ja abstraktia kuvausta ensi alkuun, mutta prosessimaisessa toiminnassa tätä tarkennetaan ja kuvaa parannetaan. Erilaisiin tapahtumiin liittyviä merkityksiä voi tarkastella riskin muodostumisen tai niiden rakentumisen ominaisuuksia esittelevien termien kautta myöhemmissä osioissa.

5.1 Tapahtuma

Synonyymi: -

Määritelmä: *tiettyjen olosuhteiden esiintyminen tai muuttuminen*

Huomautus: Tapahtuma voi olla yksittäinen tai koostua monesta tapauksesta, ja siihen voi olla useita syitä. Jos tapahtuman tai tapahtumaketjun seuraukset ovat negatiivisia, kyseessä voi olla hyökkäys, häiriö, poikkeustilanne tai onnettomuus.

Tapahtumaa, jolla ei ole seurauksia, voidaan kutsua vaaratilanteeksi tai läheltä piti -tilanteeksi.

5.2 Häiriö

Synonyymi: -

Määritelmä: *odottamaton tai ei-toivottu tapahtuma, joka haittaa järjestelmän, järjestelmän käyttäjän tai niistä riippuvaisten toimintaa*

Huomautus: Häiriöiksi kutsutaan tavallisesti vain tapahtumia, joista aiheutuva haitta on itsessään tai oikeilla vastatoimilla tilapäistä ja lyhytaikaista. Häiriön voi aiheuttaa esimerkiksi hyökkäys tai odottamaton tapahtumaketju, ja sen usein mahdollistaa jokin heikkous, puute tai vika.

5.3 Poikkeama

Synonyymi: -

Määritelmä: *tarkasteltavan kohteen ero toivottuun tai tavanomaiseen*

Huomautus: Poikkeamien tunnistamista voidaan helpottaa määrittämällä raja-arvoja mittareille, joita kyetään seuraamaan tarvitulla tarkkuudella ja tarkasteluvälillä.

5.4 Hyökkäys

Synonyymi: -

Määritelmä: *teko tai toiminta, jolla pyritään kohteen vahingoittamiseen tai oikeudettomaan käyttöön taikka jolla estetään kohteen tavoitetta toteutumasta*

Huomautus: Hyökkäyksen kohde voi olla esimerkiksi tietoverkko, tietojärjestelmä, laite, tieto, henkilö tai organisaation maine. Hyökkäys on aina ihmisen aiheuttama tahallinen teko, mutta hyökkääjien motiivit vaihtelevat ja tekijöitä voi olla yhden sijaan useita, muutamista henkilöistä jopa suuriin organisaatioihin. Hyökkäyksen aiottu kohde ei välttämättä ole sama kuin kohde, johon hyökkäyksen tunnistetaan vaikuttavan, ja aiottuja kohteitakin voi olla useita. Hyökkäyksellä voi olla vaikutuksia esimerkiksi kohteena olevan organisaation lisäksi sen asiakkaisiin tai yhteistyötahoihin, mikä voi olla tahatonta tai aiottua. Hyökkäysten mahdolliset vaikutukset voivat muodostaa välillisiä riskejä ketjun tai verkoston kautta, minkä takia hyökkäyksiin liittyvät riskit kasvavat tahojen välisten yhteyksien myötä. Joissain tapauksissa tahojen välille voi syntyä riippuvuussuhteita, joissa jonkin tahon kriittiset toiminnot tai järjestelmät ovat riippuvaisia toisen tahon kyvystä hallita hyökkäyksiin liittyviä riskejään.

5.5 Hyökkäyksen aiottu kohde

Synonyymi: -

Määritelmä: *kohde, johon hyökkäyksellä pyritään vaikuttamaan*

Huomautus: Organisaation on riskienhallinnassaan tärkeää varautua myös hyökkäyksiin, joissa organisaatio ei ole hyökkäyksen aiottu kohde, mutta kärsii aiotun kohteen ohella tai sijasta hyökkäyksen vaikutuksista. Todellinen aiottu kohde voidaan esimerkiksi pyrkiä salaamaan tai peittämään hyökkäämällä useita kohteita vastaan. Organisaatiot ja henkilöt, jotka ovat hyökkäyksen aiottu kohde tai muuten sen vaikutuspiirissä, eivät aina ole tietoisia hyökkäyksestä tai kärsi sen vaikutuksista.

5.6 Jatkuvuudenhallinta

Synonyymi: jatkuvuuden hallinta; toiminnan jatkuvuuden hallinta

Määritelmä: *organisaation prosessi, jolla tunnistetaan toiminnan kannalta keskeiset riskit, arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa*

Huomautus: Jatkuvuudenhallinta on organisaation ylimmän johdon hyväksymää strategista ja operatiivista toimintaa, jolla organisaatio ennaltaehkäisee häiriötilanteita ja varautuu reagoimaan niihin siten, että toimintaa voidaan jatkaa ennalta määritellyllä hyväksyttävällä tasolla. Mitä kriittisemmästä toiminnasta on kyse, sitä tärkeämpää sen jatkuvuudenhallinta on. Jatkuvuudenhallintatoimenpiteitä vaativien kriittisyyksien, haavoittuvuuksien jne. tunnistamisessa hyödynnetään riskien arviointiprosesseissa tuotettua tietoa, ja hyvällä riskienhallinnalla voidaan sekä ehkäistä toiminnan jatkuvuuden ongelmia että tarvittaessa tukea vahinkojen minimointia ja toiminnan palauttamista. Jatkuvuudenhallinta on yleensä omaehtoista toimintaa, mutta joillakin aloilla organisaatiot ovat myös lailla velvoitettuja varmistamaan toimintansa eri olosuhteissa. Etenkin huoltovarmuuskriittisissä organisaatioissa jatkuvuudenhallintaan sisältyy oleellisesti huoltovarmuuden turvaaminen.

6 Aihealue: Riskien muodostuminen ja ymmärtäminen

Käsitteet: epävarmuus, haavoittuvuus, heikkous, mahdollisuus, riski, riskikriteerit, riskikäsitys, riskin elinkaari, riskin raja-arvoa välttelevä uhka, uhka, vinouma

Riskien rakentuminen on joskus sattuman kauppaa – tai tältä ainakin vaikuttaa. Mutta mitä systeemisemmässä rakenteessa ollaan, sitä selkeämmin useimmille riskeille voi tunnistaa – jälkikäteen – loogisen kaaren niiden muodostumisessa. Niiden elinkaaren varrella tähän muodostumiseen voidaan liittää erilaisia ilmauksia. Pitää kuitenkin varoa mielikuvaa, että muodostuminen olisi suoraviivaista, sillä useat eri vaikuttimien haarat yhdistyvät tuottaakseen lopullisen tapahtuman ja sen seurausten vaikutukset. Tämän voi ymmärtää niin, että mahdollisessa hyökkäyksessä pitää hyökkääjässä ensin yhdistyä ainakin mahdollisuus, keinot ja motiivi, minkä lisäksi tätä muokkaavat suojauksemme sekä jälkikäteen varautumistoimemme[11].

Kaikkien eri tapahtumien yhdistelmien mahdollisuudet tekevät tulevaisuudestamme epävarman. Emme tiedä mitä tapahtuu. Epävarmuus ja sen sietäminen ovat keskeisiä riskien ymmärtämiselle. Ymmärrykseemme vaikuttavat kuitenkin myös puutteet tiedoissa, joiden perusteella teemme päätelmiämme sekä omaksutut tapamme ja muut tekijät, joilla käsittelemme tätä jo valmiiksi vähäistä ja väärin ymmärrettyä informaatiota. Tähän ehkä kietoutuukin riskienhallinnan yksi keskeisin aspekti. Siinä missä uhkaa voi pitää yleisenä ja epämääräisenä, se muuttuu riskiksi, kun tunnistamme siitä jollain tavalla ja tarkkuudella arvotettavia ominaisuuksia – mitä uhka merkitsee – ja kykenemme arvioimaan riskiä toisaalta suhteessa tavoitteisiimme, kykyihimme ja vastaaviin, sekä toisaalta muihin riskeihin. Näin uhka muutetaan käsiteltäväksi. Ainakin siinä määrin kuin (luulemme) ymmärtävämme sitä. Tämä mahdollistaa toiminnan ja siihen reagoinnin oikeansuuntaisella tavalla.

Haavoittuvuus ei itsessään ole riski. Se on vedenpitävän suojakuoren reikä, kun saatetaan pudottaa puhelin veteen (tapahtuma) sekä menettää tietoa (riski). Haavoittuvuuksia korjaamalla saadaan ehkäistyä monen uhan muodostumista riskeiksi. Erityisesti organisaatioiden hallinnollisten rakenteiden kautta tarkasteltuna, suhteellisia heikkouksia voidaan tunnistaa eri osa-alueilla, sillä panostukset ovat harvoin tasaisia, saati kaikkialle riittäviä, kun pyritään tehokkuuteen. Heikkous usein mahdollistaa haavoittuvuuksien syntymisen tai säilymisen. Esimerkkinä voisi olla puuttuva aika ja osaaminen tarkastaa kaikki omien järjestelmien koodi tai puuttuvat suunnitelmat ja ohjeet erityistilanteisiin. Organisaatioissa heikkouksien hallinta ja korjaaminen voi olla strategisempi ja ennakoivampi lähestymistapa hallita riskejä. Mikäli heikkoja osa-alueita ei muuten tunnista, uhkien ja riskien kautta voidaan analysoida juurisyitä ja löytää taustavaikuttajat.

Riskien määrittely voi olla haastavaa. Riski tulee suhteuttaa tavoitteeseen sekä resursseihin ja tätä kautta yleensä löytyy raja-arvo sille, mitä voidaan sietää ja mitä ei voida hyväksyä. Etukäteen määritellyt kriteerit eri muodoissaan ehkäisevät riskien määrittelyä ja arvotusta satunnaisella tavalla. Yhtenevä arviointi mahdollistaa uskottavan vertailun sekä ehkäisee jotkin vinoumat siitä, miten saattaisimme tuntemuksien, peukkusääntöjen tai vanhentuneen opin perusteella painottaa jotain riskiä suuntaan tai toiseen. Vinoumien ehkäisy on osa laadunhallintaa, jota riskienhallinta

[11] Kyseisen tyyppistä analyysiä voi tehdä niin kutsutulla rusettianalyysillä (”bowtie”).

itsessäänkin on: prosessi luotettavan tiedon tuottamiseksi päätöksenteon tueksi – ja siksi hyvin toimiva prosessi on tavoiteltava asia.

Raja-arvoihin liittyy yleensä myös jokin toimenpide, suoraan tai epäsuorasti. Se on määritys sille, että asiaan pitää reagoida, mutta myös niinkin yksinkertaisille asioille kuin että kykenemmekö edes huomaamaan asioita, jotka eivät nouse tarpeeksi suuriksi. Huomioraja voi olla kirjaimellista (virukset), järjestelmien hälytysasetuksia (väärien salasanayritysten määrä) tai hallinnollista (ilmoitukset poikkeavasta toiminnasta). Se voi myös olla absoluuttista, kuten kriittisten järjestelmien toiminta, mutta myös suhteellista, eli nouseeko jokin esiin kaikkien muiden signaalien ja informaation joukosta.

Datan ja informaation kontrolli eri tavoin on yksi tärkeä osa hyvin toteutettua riskienhallintaa ja turvallisuutta. Pitää varmistaa, että oikeat ihmiset saavat oikeat herätteet, joihin sisältyy riittävästi tietoa siitä, mitä tapahtuu rajapinnan lähellä, mutta siten, että tietoon ei hukuta. Hienosäätöä on myös tehtävä jatkuvasti erilaisissa muutoksissa ja luodattaessa todennäköisiä uusia uhkia, kaikilla organisaation toiminnan tasoilla. Mikäli päätöksentekoa varten ei ole oikeaa tietoa tarjolla, tässä voi olla yksi kehitysalue.

Erityinen haaste ovat uhat ja riskit, jotka jäävät juuri ja juuri erilaisten rajojen toiselle puolelle kertaluonteisina tapahtumina. Niiden luoma kuormitus kuitenkin voi muodostua siitä, että sinänsä harmittomia tapauksia tulee määrällisesti paljon tai jokin muu ominaisuus niissä on poikkeuksellisen korostunut. Se voi olla vain hieman kuluttavampaa tai se voi vaatia resurssien siirtoa toisaalta, aiheuttaen heikkoutta siellä, kuten pullonkauloja, ilman että suuria poikkeamia varten tuntemamme rajanvedot ylittyisivät selkeästi. Hyökkääjä voi myös tarkoituksellisesti yrittää manipuloida raja-arvoja tai niihin liitettävien toimenpiteiden muodostamista. Epäselvät ja epävarmat rajapinnat ovat heikkous, elleivät suoranainen haavoittuvuus.

Mikäli nähdään vain kriisi ja rauha, ei osata toimia näiden väliin muodostuvalla eriasteisten välimallien vyöhykkeellä. Tämän tyyppistä metodiikkaa on hyödynnetty erilaisissa tarkoituksellisissa hybridivaikuttamisen kampanjoissa, joissa uhkaavalta toiminnalta vaikuttavalla hämäyksellä tai normaaleihin prosesseihin tuotetulla lisäkuormalla on häiritty toimintaa. Koska näitä ei ole pystytty erottamaan vastaavan kaltaisista normaaleista tapahtumista ja ilmiöistä, näitä ongelmallisia asioita ei saada myöskään eristettyä tai erotettua tehokkaaseen käsittelyyn. Tämä voi johtaa siihen, että kriisiytyessään ja viimein ylittäessään huomion tai sietokyvyn rajoja, käsittelytoimissa voidaan olla pakotettuja toimimaan tavalla, joka häiritsee tai tuottaa haittaa riskiin liittymättömille tahoille. Tämän tyyppisen toiminnan erikoisuus on sen tavoitteissa, joissa itse riskin toteutuminen ei välttämättä ole tavoite, vaan tuoda esiin organisaation heikkouksia tai manipuloitavuutta (mainehaittoja), tai verkottuneen riskin tavoin aiheuttaa vaikutuksia edellä mainituille riskiin liittymättömille tahoille, jotka voivat olla hyökkäyksen aiottu kohde. Suuremmissa tapauksissa nämä sivulliset voivat olla kansalaisia ja vaikutuksena on arvojen. luottamuksen ja oikeuksien heikkeneminen, mutta todennäköisemmin puhumme kiusaamisesta ja häirinnästä pienemmissä tapauksissa. Näiden riskien hallinnan näkökulmasta tietoisuus on tärkeää, ja se lähtee tunnistamista tukevasta raja-arvojen määrittelystä sille, mikä on normaalia ja mikä ei.

Nykyaikaisessa riskienhallinnassa ei riskejä tule enää käsitellä vain negatiivisina asioina, jotka parhaimmillaan saadaan poistettua tai minimoitua neutraaleiksi

vaikutuksiltaan. Niitä tulee silmäillä siten, että riskeistä joko suoraan tai niiden käsittelytoimien seurauksena saadaan aikaan jotain hyötyä, jotain positiivista yhteistulosta tapahtuman vaikutuksista kokonaisuudessaan. Riskit voidaan nähdä pienemmässä mittakaavassa mahdollisuuksina, jotka ohjaavat korjaamaan haavoittuvuuksia ja vahvistamaan heikkouksia. Tämä voi olla vanhan vahvistamista, mutta useammin se lienee jonkin uuden kehittämistä, uusia mahdollisuuksia. Suuremmassa katsannossa voidaan tarkoittaa kehittyneempää digiturvallisuutta sekä organisaation toiminnan kannalta löydettyjen uusien tilaisuuksien tunnistamista, mikä voi olla vielä arvokkaampaa. On toki eri asia, kyetäänkö ja halutaanko näitä kaikkia hyödyntää. Usein tämän työstäminen vie aikaa, joten uhkien havaitseminen sekä riskien tunnistaminen ja analysointi olisi tapahduttava ajoissa. Riskienhallinnassa tulisi pyrkiä vastaamaan myös kysymykseen, miten tämä asian hallintatoimilla voidaan tukea (strategisia) tavoitteitamme ja saadaan etu. Vain ongelmia painottamalla ja riskeistä negatiivisesti viestimällä tuotetaan pitkässä juoksussa raskasta ilmapiiriä, jossa kulttuuriksi muodostuu välttää ikäviä riskienhallinta-asioita.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että sisäistää riskin kehityksen sekä tapahtumaketjuina, mutta myös miten eri vaiheet tulevat ilmi ja miten nämä eroavat toisistaan. Eri vaiheisiin ja niiden haasteisiin voidaan tarttua eri keinoin. Eri vaiheiden ja ilmiöiden tunnistaminen on kuitenkin haastavaa ja on ymmärrettävä, että eri tekijät vaikuttavat näkemystemme muodostumiseen. Joskus tätä voidaan pyrkiä käyttämään tahallisesti hyväksi, joskus olosuhteet eivät vain mahdollista uhan havaitsemista ennen kuin on liian myöhäistä tehdä sille mitään etukäteen.

6.1 Epävarmuus

Synonyymi: -

Määritelmä: *tiedon puute tulevan tapahtuman luonteesta tai ajankohdasta*

Huomautus: Tulevaisuuteen liittyy aina epävarmuutta, mistä seuraa, ettei tulevaisuutta voida tarkasti ennustaa, vaan on varauduttava useisiin mahdollisiin tapahtumiin ja vertailtava niiden ominaisuuksia ja todennäköisyyttä saatavilla olevan tiedon valossa. Epävarmuutta aiheuttavien tekijöiden olemassaolosta ei välttämättä olla tietoisia, esimerkiksi puutteellinen tietämys omista prosesseista tai tietoturvallisuuden tasosta voi aiheuttaa epävarmuutta. Jos tapahtumaan liittyy epävarmuutta, sen vaikutus voi toteutuessaan olla organisaation kannalta positiivista, negatiivista tai neutraalia. Epävarmuuden positiivisia ja negatiivia vaikutuksia koskevaa tietoa pyritään ilmaisemaan riskeinä, mutta riskitiedot voivat joskus perustua virheelliseen riskikäsitykseen, jopa niin, ettei riskinä pidetty tapahtuma ole ylipäätään mahdollinen. Epävarmuus voi olla täydellistä tai osittaista: epävarmuutta, jonka todennäköisyydestä ja vaikutuksista on tehty perusteltu arvio, voidaan riskin lisäksi luokitella tunnetuksi epävarmuudeksi (known unknown).

6.2 Uhka

Synonyymi: -

Määritelmä: *mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku*

Huomautus: Uhka eroaa riskistä siten, että sen merkitystä ei ole arvioitu ja suhteutettu. Uhka eroaa vaarasta siten, että uhka on epävarmempi kehityskulku ja vaara puolestaan käytännöllinen ja riskienhallinnallisin toimenpitein käsiteltävä asia. Ks. myös riski.

6.3 Haavoittuvuus

Synonyymi: -

Määritelmä: *puute, vika tai toimintatapa, joka altistaa turvallisuuteen kohdistuville uhkille*

Huomautus: Haavoittuvuuksia voi olla esimerkiksi tietojärjestelmissä, prosesseissa tai ihmisten toiminnassa. Haavoittuvuus voi olla esimerkiksi ohjelmassa oleva virhe, joka mahdollistaa väärinkäytöksiä estävien rajoitusten kiertämisen, se, että päätöksenteossa ei edellytetä allekirjoittajan lisäksi toista hyväksyjää tai tarkastajaa, tai se, että sähköpostiviestin salaus ei onnistu, jolloin tietoja joudutaan lähettämään salaamattomassa sähköpostiviestissä. Nollapäivähaavoittuvuus on tietojärjestelmässä oleva haavoittuvuus, joka muodostaa korkean tietoturvariskin, johon ei ole saatavilla korjausta, koska sen paljastumisesta on niin vähän aikaa.

6.4 Heikkous

Synonyymi: -

Määritelmä: *organisaation tavoitteiden kannalta epätoivottu tai haitallinen ominaisuus organisaation toiminnassa tai omaisuudessa*

Huomautus: Heikkouksia voivat olla esimerkiksi prosessien pullonkaulat, puutteet henkilöstön koulutuksessa tai joidenkin toimintojen heikko resursointi. Koska organisaation resurssit ovat aina rajalliset, joitain heikkouksia voidaan poistamisen sijaan vain lieventää tai hyväksyä sellaisenaan. Heikkoudet vaikuttavat organisaation riskinkantokykyyn ja voivat edistää haavoittuvuuksien syntymistä.

6.5 Mahdollisuus

Synonyymi: -

Määritelmä: *mahdollisesti toteutuva tapahtuma tai kehityskulku, joka on toivottava tai hyödynnettävissä*

Huomautus: Mahdollisuuden toteutumiseen voidaan pyrkiä vaikuttamaan, mutta onnistuminen ei ole varmaa. Riskien käsittelyssä voidaan joissain tapauksissa riskin estämisen tai minimoimisen sijaan pyrkiä kääntämään vaikutukset hallintatoimilla osin tai kokonaan positiivisiksi, eli muuttamaan uhka mahdollisuudeksi. Mahdollisuudella tarkoitetaan tässä sanastossa uhkan vastakohtaa. Yleiskielessä mahdollisuus voi olla myös mahdottomuuden vastakohta.

6.6 Riski

Synonyymi: -

Määritelmä: *epävarmuuden vaikutus tavoitteisiin*

Huomautus: Riski ilmaistaan tavallisesti riskin lähteiden, mahdollisten tapahtumien, niiden seurausten ja niiden todennäköisyyden yhdistelmänä. Vaikutus on poikkeama odotetusta. Se voi olla myönteinen, kielteinen tai molempia, ja se voi käsitellä, luoda tai saada aikaan mahdollisuuksia ja uhkia.

Riskit ja riskien vaikutukset voivat kohdistua esimerkiksi ihmisiin, eläimiin, omaisuuteen, tietojärjestelmiin, ympäristöön, yhteisöllisiin arvoihin tai jaettuihin merkityksiin. Riskin toteutuminen voi tuottaa useita erilaisia ja eritasoisia vaikutuksia ja näiden käsittelemiseksi, sekä eri riskien suhteuttamiseksi toisiinsa, voi olla tarpeen jakaa riski pienempiin osasiin tai koota yksittäiset ilmentymät suuremmiksi kokonaisuuksiksi, riippuen riskienhallinnan tarpeista. Riski määritellään tässä samoin kuin useissa lähteissä, mm. standardissa SFS-ISO 31000:2018. Yleiskielessä sekä suomen kielen sanan ""riski"" että ruotsin- ja englanninkielisten vastineiden merkitys on kielteinen."

6.7 Riskikäsitys

Synonyymi: riskin käsitys

Määritelmä: *ihmisen tai organisaation käsitys siitä, millainen jokin riski on*

Huomautus: Riskikäsitykseen vaikuttavat paitsi saatavilla oleva tieto, joka riskien tapauksessa on aina joiltain osin puutteellista niihin liittyvästä epävarmuudesta johtuen, myös vinoumat tiedon tulkinnassa, joten riskikäsitys voi poiketa suurestikin riskin todellisesta luonteesta. Oman riskikäsityksen ja oman organisaation riskikäsityksen lisäksi voidaan tarkastella myös sidosryhmien riskikäsityksiä. Riskikäsityksiin on mahdollista vaikuttaa mm. tiedonhankinnalla, riskien syvällisemmällä analysoinnilla ja viestinnän keinoin.

6.8 Vinouma

Synonyymi: -

Määritelmä: *ihmisten ajattelulle luontaisista vääristymistä johtuva toimijan tai järjestelmän taipumus hahmottaa ja painottaa tietoa tietyllä tavalla*

Huomautus: Vinoumia tunnistamalla ja niihin puuttumalla parannetaan arvioiden objektiivisuutta. Vinouma voi olla henkilökohtainen tai kollektiivinen, ja se voi kertautua järjestelmissä. Vinoumia voi olla eri päätöksenteon tasoilla tai prosessien eri vaiheissa. Vinoumien käsittelytapoja on monia, ja ne voidaan sulauttaa osaksi prosessia. Määritelty, kattava ja kehittyvä riskienhallintaprosessi itsessään on yksi tapa ehkäistä tietyntyyppisiä vinoumia tuotetussa tiedossa.

6.9 Riskikriteerit

Synonyymi: -

Määritelmä: *perusteet riskien merkityksen arvioimiseen yhdenmukaisesti*

Huomautus: Riskikriteerit perustuvat mm. tavoitteisiin, resursseihin ja toimintaympäristöön, ja niitä voidaan soveltuvin osin johtaa standardeista, laeista, toimintaperiaatteista ja muista vaatimuksista. Riskikriteerejä voidaan ilmaista eri tavoin, esimerkiksi tarkkojen raja-arvojen tai yleisluontoisempien sanallisten kuvausten avulla.

6.10 Riskin raja-arvoa välttelevä uhka

Synonyymi: -

Määritelmä: *hyökkäys tai muu uhka, joka pyrkii välttämään vastatoimenpiteitä pysyttelemällä riskien arvioinnissa käytettyjen raja-arvojen alapuolella*

Huomautus: Riskien arvioinneissa käytetty raja-arvo voi olla määrällinen, laadullinen tai näiden yhdistelmä. Arvioinneissa käytetty raja-arvo voi olla liian korkea, liian matala tai jättää huomioimatta yhteisvaikutuksia muiden riskien kanssa, jolloin riskiä ei hallita tarkoituksenmukaisesti. Vaikka riskien arvioinneissa käytetty raja-arvo muuten vastaisi tavoitteita, riskin raja-arvoa välttelevä uhka, joka kertaluontoisena olisi merkityksetön, voi aiheuttaa merkittävää haittaa pitkittyessään tai toistuessaan, jolloin siitä ei välttämättä olla tietoisia tai siihen ei osata, haluta tai kyetä vastaamaan riittävillä seurauksilla. Joissain tapauksissa riskin raja-arvoa välttelevät uhkat jäävät kokonaisuudessaankin organisaation kannalta merkityksettömiksi, mutta aiheuttavat merkittävää haittaa laajemman verkoston tai yhteiskunnan tasolla. Esimerkkejä riskin raja-arvoa välttelevistä uhkista ovat mm. tietomurtoon liittyvien toimenpiteiden naamioiminen harmittomiksi häiriöiksi tai kiristyshaittaohjelmistojen pyrkimys välttää valtiollisia ja turvallisuustoimijoita.

6.11 Riskin elinkaari

Synonyymi: -

Määritelmä: *riskin olemassaolon vaiheet uhkan tai mahdollisuuden muodostumisesta riskin tunnistamiseen ja edelleen aina riskin mahdolliseen poistumiseen asti*

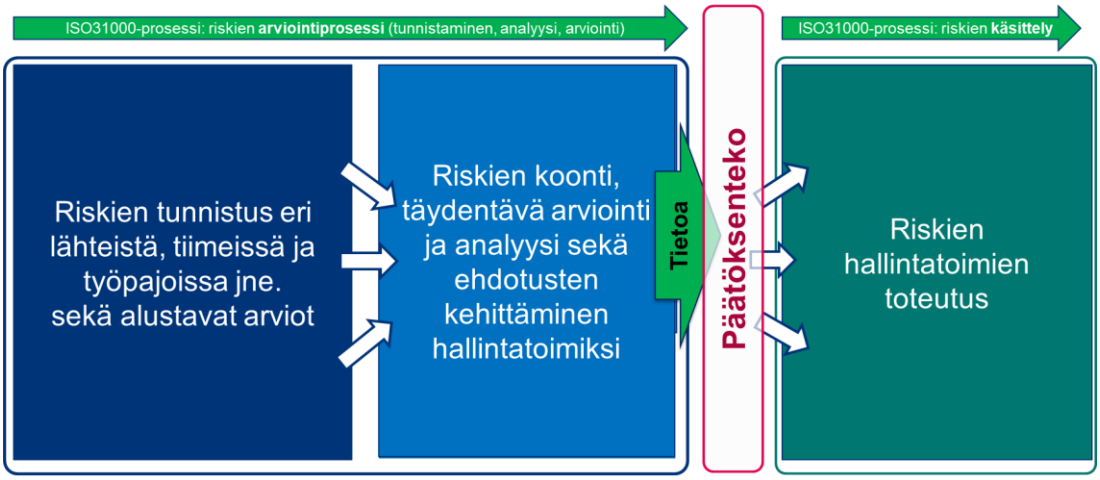
Huomautus: Riskin elinkaaren alkuna voidaan pitää edeltäviä tapahtumia, jotka aiheuttavat uhkan tai mahdollisuuden, joka vuorostaan on tunnistettavissa riskiksi. Riskin elinkaaren loppu on usein vaikeasti määriteltävissä, sillä riski voi muuntua elinkaarensa aikana huomattavastikin, ja monet riskit jäävät elämään vähäisinä jäännösriskeinä. Riskin muuntuessa voivat muuttua esimerkiksi riskin vaikuttavuus, sen todennäköisyys tai jopa kohde, johon riski vaikuttaa. Riskin elinkaareen vaikuttavat sekä toimintaympäristöstä johtuvat muutokset että organisaation toimenpiteet.

7 Aihealue: Riskien arviointi

Käsitteet: alustava arvio, riskianalyysi, riskiarvio, riskien analysointi, riskien arviointi, riskien arviointiprosessi, riskien arviointiprosessin työkalu, riskien luokittelu, tarkentava arvio, uudelleenarviointi

Riskien arviointi on yksi riskienhallinnan haastavaksi muodostuneista käsitteistä. Sitä on käytetty sekä arvioinnin tekemisestä, sen tuloksista, mutta myös kuvaamaan prosessikokonaisuutta, johon kuuluvat erikseen tunnistamisen, analysoinnin ja arvioinnin osat (joihin voidaan soveltaa omia menetelmiään). Puhekielessä esiintyy erilaisia käyttötapoja ja arviointi ja analyysiä saatetaan käyttää toistensa synonyymeinä.

Tässä sanastossa päädyttiin erottelemaan näitä siten, että ISO31000-sarjan mukaisesti prosessin osaa kuvaavalle ilmaukselle valittiin tarkempi vaihtoehto ”riskien arviointiprosessi”. Arvioinnin ja analysoinnin eroa selvennettiin, koska kyse on kahdesta erilaisesta tavasta käsitellä riskeihin liittyvää tietoa, ja tämän hahmottaminen helpottaa oikeanlaisten toimenpiteiden tekemistä.



Kuva1: Osa riskienhallinnan kokonaisprosessista yksinkertaistettuna, eli arviointiprosessi ja käsittelyvaihe sekä niiden välissä tapahtuva päätöksenteko, jolle tuotetaan tietoa ja vaihtoehtoja toiminnan päätöksiksi. Päätöksentekoon vaikuttavat myös muut asiat kuin riskienhallinnan tuottamat tiedot. Arviointiprosessiin luetaan standardin mukaisesti riskien tunnistaminen, analyysi ja arviointi. Tätä edeltää vaihe, jossa määritellään tarkastelun kattavuutta, omia tavoitteita ja toimintaympäristön merkityksiä sekä muita kriteereitä, jotka vaikuttavat tarkasteluun. Käsittelyosuuden jälkeen tulee vaikutusten seuranta ja katselmointi. Tarkempi malli osassa Riskienhallinnan kontekstit ja tasomalli.

Riskien arvioinnissa riskejä arvotetaan ja niitä suhteutetaan sekä toisiinsa, että tavoitteisiin, toimintaympäristöön että resursseihin ja vastaaviin. Tämä on tapa löytää merkittävimmät riskit, ne, joilla on oikeasti merkitystä – mikäli niitä on, sillä olemmehan saattaneet luulla uhista liikoja ennen järjestelmällistä käsittelyä. Samalla muodostuu myös priorisointi siitä missä järjestyksessä käsittelyssä toimitaan tehokkaasti (tämä tosin käsittelytoimia kehitettäessä voi muuttua) ja missä suhteessa mihinkin riskiin tulisi panostaa aikaa, vaivaa ja muita resursseja. Arvioinnissa keskitytään kokonaisuuteen ja kvantitatiivisten arvojen käyttöön.

Riskien analysoinnissa voidaan tarkastella riskijoukon merkitystä, mutta myös yksittäisen riskin rakentumista ja ominaisuuksia. Tässä on tarkoitus oppia tuntemaan riski syvällisemmin, jotta sen eri vaiheet ja vaikutukset saadaan hallintaan. Analysointi on usein kvalitatiivista, mutta suurten joukkojen, verkostojen ja simulaatioiden tapauksessa voidaan tehdä matemaattista analyysiä[12]. Jo eri tavoin tehtävät visualisoinnit itsessään voivat auttaa ymmärtämään merkityksiä ja mekanismeja, mikä on osa analyysiä ja sen tulosten viestintää raportoinneissa – tulokset on tuotava esiin oikein.

Arviot tarkentuvat ajan myötä, kun tieto ja ymmärrys kehittyvät. Siten riskienhallinnassakaan ei tule jämähtää kerran tehtyihin arvioihin. Tätä ei pidä ymmärtää esimerkiksi vuosittain tehtäväksi toisteisuudeksi, jolla on oma tarkoituksensa tiedon pitämisessä relevanttina. Arviointiprosessia, jota usein toteutetaan organisaatioissa, lähdetään tekemään organisaatiokaavion ruohonjuuritasolta, jolloin erilaisten riskien kanssa käytännössä tekemisiin joutuvat tunnistavat riskejä ja tekevät näistä arvioita. Heillä on todennäköisesti paras tuntemus omaan työhönsä ja sen substanssissa vaikuttavista uhista, mutta heidän arvioitaan voi vinouttaa tottumattomuus riskienhallintamallin työtapaan, siinä kuvattuihin raja-arvoihin tai puutteellinen näkemys koko toiminnan kentästä. Täydellisen analyysin toteuttaminen heillä voi myös olla raskasta. Tätä helpottaaksemme, tarvittu ensiarvio otetaan täydennettäväksi ja syvennettäväksi tarkentavissa arvioissa. Näin jo jossain määrin menetellään, kun esimerkiksi riskityöpajojen tietoja kootaan ja uudelleenarvioidaan kokonaisuutena, koko organisaation kontekstista. Toisteisuudella on tarkoitus parantaa riskitiedon laatua.

Arviointiprosessin ensimmäinen kohta ei tarkalleen ottaen ole riskien tunnistaminen. Riskin arviointiprosessi on osa riskienhallinnan kokonaisprosessia, jossa ensinnä todetaan ja tunnistetaan tavoitteet, strategiat näiden saavuttamiseksi, toimintaympäristö ja sen muutosten suunnat sekä muut oletukset ja rajoitteet, jotka on huomioitava riskejä määriteltäessä ja mitä vasten riskien arviointi tapahtuu. Usein tämän kaiken selvitys unohtuu, minkä seurauksena tunnistaminen tai muut toimet tehdään epäyhtenäisen näkemyksen perusteella, eikä esimerkiksi tarvittua kattavuutta tai kohdennusta saada.

Riskin tunnistamiselle, jota ei ole tässä sanastossa erikseen määritelty, voidaan nähdä kaksi perustapaa. Aiempien tapahtumien kautta, eli perustuen historiatietoon uhista, kehityskuluista, syistä ja ulkoisista tekijöistä, joista luodaan skenaarioita siitä, mitä voisi tapahtua. Eli puhutaan siitä, miten aiemmat uhat voisivat toistua, mahdollisesti muuttuneina kehittyvässä toimintaympäristössä. Toinen tapa on tarkastella oman rakenteen suojattavien kohteiden tai haavoittuvuuksien ja heikkouksien kautta. Eli mitä meillä on tai tapahtuu, ja näistä luodaan skenaarioita siitä, mitä näihin voisi kohdistua sekä mitä voisi tapahtua ilman niitä (osin tai kokonaan). Tällä tavalla hyökkäyksen ja puolustuksen näkökulmat voidaan laittaa taulukossa otsikkoriville ja sarakkeeseen, jolloin matriisilla voidaan tehdä järjestelmällinen läpikäynti eri uhkien yhdistelmistä, jotta voidaan tunnistaa omassa kontekstissa merkitykselliset riskit. Tämäntyyppisellä läpikäynnillä tiedetään tunnistamisen kattavuus, minkä ymmärtäminen auttaa ymmärtämään riskienhallinnan merkityksen (sekä puutteet).

[12] Kokoelma erilaisia arviointi- ja analyysimetodeja sekä arvioita näiden käytettävyydestä prosessin eri vaiheissa ja erilaisiin tarkoituksiin löytyy mm. ISO31010:stä, mutta soveltaen voidaan käyttää muitakin strukturoidun analyysin metodeja, mikäli ne tuottavat tarvittua tietoa tai visualisoivat ongelmaa.

Kuten tunnistamisen esimerkistä voi päätellä, prosessin toteutuksen näkökulmasta alkaa erilaista tietoa ja sen käsittelyä muodostua nopeasti, mikä tekee riskitiedon tuottamisesta joskus raskasta. Tätä varten onkin syytä luopua taulukkolaskentaohjelmalla toteutetuista manuaalisista lomakkeista ja ottaa käyttöön riskienhallinnan prosessiin tueksi ammattimainen digitaalinen järjestelmä, työkalu. Tämä voi olla joko tiettyyn prosessin osaan erikoistunut (tai useampi, jolloin tieto liikkuu näiden välillä esimerkiksi tietokantaan rakennetun riskirekisterin kautta) tai laajemman kokonaisuuden kattava järjestelmä, joka voi olla liitettynä organisaation toiminnanohjausjärjestelmään. Oleellista on, että järjestelmä on riittävän pitkäikäinen ja joustava, jotta sitä voidaan kehittää tai muokata sekä riskienhallinnan että organisaation toimintojen kehittyessä. Työkalun tärkeimpiä tehtäviä on pitää tietomassat liikkeessä (tukea prosessia) sekä pitää tieto yhdenmukaisena (vertailtavana ja käsiteltävänä), jolloin käyttäjät ja asiantuntijat voivat keskittyä oleelliseen.

Riskien luokitteluun tulisi kiinnittää erityistä huomiota, sillä sen merkitys joskus unohtuu. Erityyppistä luokittelua voidaan tehdä sekä tunnistamisen, arvioinnin ja analysoinnin että hallintakeinojen kehityksen yhteydessä. Näillä on omat merkityksensä. Tunnistamisessa luokittelu voi olla aiemmin esitetyn matriisin kaltainen työkalu, jolla varmistetaan, että kaikki luokat käydään läpi, tai että kaikista luokista otetaan riski käsiteltäväksi. Käytetty luokittelujärjestelmä, kategoriarakenne, sekä varmistaa kohdennuksen näihin, että voi rajoittaa näkymää, jolloin on syytä muistaa pohtia myös kyseisen laatikon ulkopuolta. Analyysissä erilaisten riskien luokittelu voi auttaa tunnistamaan ilmiöitä, riskien vaikutusmekanismien yhteyksiä tai lähteitä. Tällöin tietyntyyppisiä riskejä voidaan ehkä käsitellä suurempina kokonaisuuksina, joissa vain tietty ennustettava ominaisuus muuttuu. Riskejä arvioitaessa luokittelu yleisimmillään liittyy prioriteettiryhmiin, kriittisyyteen tai vastaavaan toimintaa ohjaavaan arviointiin. Näiden määrittäminen oikein on tärkeää.

Tämän jälkeen, kun aletaan työstämään hallintakeinoja, luokittelulla jaetaan riskejä osiinsa ja tarkastellaan, mihin niiden ominaisuuksiin voidaan vaikuttaa eri keinoin. Erilaiset ja tasoiset riskit voivat tulla käsitellyksi yhdellä hallintatoimella, kun tunnistetaan niitä yhdistävä tekijä. Tämä on se vaihe, jossa riskienhallintaprosessi osoittaa tehokkuutensa. Kunnollisessa hallintaprosessissa, etenkään laajemmassa organisaatiossa, riskejä ei tulisi pääsääntöisesti käsitellä yksitellen. Tehokkaiden luokittelutapojen käyttö prosessin eri vaiheissa mahdollistaa suurtenkin riskitietomassojen käsittelyn tarvittavien hallintatoimien tuottamiseksi sekä niiden ymmärrettävään raportointiin.

Tässä yhteydessä, kun puhutaan arvioinnin kattavuudesta ja luokittelusta, ilmauksen ”digiturvan tasoisesti ja laajuisesti” tulisi tarkoittaa, että silloin on huomioitu digiin liittyvät turvallisuusasiat laajasti. Eli vähintään kaikki viisi keskeistä toteutusaluetta läpi käymällä sekä myös toimintaan liittyvä muut alueet huomioiden. Tällöin tätä luokittelua on käytetty ohjaamaan tarkastelua. Näin toimien mahdollistuu riskien työstö osa-alueittain, mikä voi helpottaa työtä. Mutta, kuten hallintatoimien suunnittelua varten tehtävää kokonaistarkastelua ja luokittelua varten, riskit on koottava yhteen. Tämä voi olla joko digiturvallisuuden oman kokonaisuuden (väli)tarkastelu, mikä tukee aihealueen toimia, mutta myös osa kokonaisriskienhallintaa, mikä tukee strategisia päämääriä ja laajempaa yhteensovittamista. Riskit tulee siis arvioida ja käsitellä hallintaa varten tarvittavissa pienemmissä kokonaisuuksissa, mutta ne on koottava organisaatiossa yhteen kokonaisriskienhallintaan, jotta nähdään niiden yhteiset vaikutukset

organisaation tavoitteisiin. Erillisten riskienhallintayksiköiden tiedot voidaan koota yhteen vain, mikäli ne käyttävät yhteneväisiä luokitteluita sekä raja-arvoja niissä.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että sisäistää riskin arviointiprosessin vaiheet ja niihin liittyvät toisteisuuden, työkalut sekä luokittelut, joilla voidaan tehostaa prosessin toteuttamista. Tätä vaihetta painotetaan usein, mutta on muistettava, ettei tämä ole koko riskienhallintaprosessi. Tarkoituksena on tuottaa tietoa hallintatoimien ja organisaation muun toiminnan ohjaamiseksi, missä huomioidaan riskien lisäksi myös muita asioita, kuten tavoitteet.

7.1 Alustava arvio

Synonyymi: ensiarvio; ensiöarvio; primääriarvio

Määritelmä: *arvio, joka tehdään arviointiprosessin aluksi karkean yleiskuvan saamiseksi*

Huomautus: Alustavan arvion tarkkuustaso voi vaihdella pelkästä tunnistamisesta jopa jonkintasoiseen analyysiin, mutta tyypillisesti se sisältää melko karkean tasoista tietoa perustuen esimerkiksi luokitteluun. Alustava arvio voi olla sellaisenaan riittävä, mutta tarvittaessa sitä voidaan tarkentaa tarkentavalla arviolla ja edelleen uudelleenarvioinnilla.

7.2 Tarkentava arvio

Synonyymi: toisioarvio; sekundääriarvio; jatkoarvio

Määritelmä: *arvio, joka tehdään alustavan arvion jälkeen tarkemman arvion saamiseksi*

Huomautus: Tarkentavia arvioita voidaan tehdä useita.

7.3 Uudelleenarviointi

Synonyymi: -

Määritelmä: *arvio tai arvioiden sarja, jolla pyritään päivittämään tai tarkentamaan aiempaa arviota*

Huomautus: Uudelleenarviointia toteutetaan yleensä osana dynaamisia prosesseja, mutta arvioita voidaan uudelleenarvioida lisäksi säännöllisin väliajoin, jolloin varmistetaan arvioiden päivittyminen vastaamaan toimintaympäristössä havaittuja muutoksia.

7.4 Riskien arviointiprosessi

Synonyymi: -

Määritelmä: *prosessi, joka kattaa riskien tunnistamisen, riskien analysoinnin ja riskien arvioinnin*

Huomautus: Riskien arviointiprosessi on osa riskienhallintaprosessia. Standardissa SFS-ISO 31000:2018 annetaan suosituksia riskienhallintaprosessin eri vaiheisiin, mukaan lukien riskien arviointiprosessi (suosituksessa nimellä "riskien arviointi").

7.5 Riskien arviointiprosessin työkalu

Synonyymi: riskienarviointityökalu; riskienarviointijärjestelmä

Määritelmä: *riskienhallintatyökalu, joka ohjaa toteuttamaan riskien arviointiprosessin osia johdonmukaisesti tiettyjä malleja tai menetelmiä noudattaen*

Huomautus: Riskien arviointiprosessin työkalut ohjaavat keskenään vertailukelpoisten arvioiden tuottamiseen ja varmistavat, että olennaisiksi tiedetyt asiat arvioidaan ja dokumentoidaan. Yksittäinen työkalu voi tukea useita riskien arviointiprosessin osia tai keskittyä yhteen, esimerkiksi riskien tunnistamiseen tai riskien analysointiin.

7.6 Riskien arviointi

Synonyymi: riskien merkityksen arviointi; riskien vaikutuksen arviointi; riskin arviointi; riskin merkityksen arviointi; riskin vaikutuksen arviointi

Määritelmä: *riskien toteutumisen todennäköisyyden ja niiden mahdollisten vaikutusten selvittäminen*

Huomautus: Riskien arvioinnissa hyödynnetään usein etukäteen määritettyjä riskikriteerejä, minkä lisäksi riskejä suhteutetaan toisiinsa. Tuotetut arviot ottavat kantaa esimerkiksi siihen, mihin riskeihin tulisi ensisijaisesti kohdistaa hallintatoimenpiteitä, tai siihen, mitkä riskit tulisi siirtää analysoitavaksi. Arvioita voidaan tarvittaessa päivittää tarkentavilla arvioilla tai uudelleenarvioinnilla sekä syventää vapaamuotoisemmin riskien analysoinnilla. Riskien arviointi on osa riskien arviointiprosessia, jossa sitä edeltää riskien tunnistaminen. Riskien arviointi voidaan tehdä ennen tai jälkeen riskien analysoinnin, ja tarvittaessa riskien analysointi ja arviointi vuorottelevat iteratiivisena ketjuna. Standardissa SFS-ISO 31000:2018 termi riskien arviointi viittaa riskien arviointiprosessiin, kun taas tästä käsitteestä käytetään termiä riskien merkityksen arviointi.

7.7 Riskiarvio

Synonyymi: riskin arvio; arvio riskien merkityksestä; arvio riskien vaikutuksesta; arvio riskin merkityksestä; arvio riskin vaikutuksesta

Määritelmä: *riskien arvioinnin tulos*

Huomautus: Riskiarvion perusteella voidaan suunnitella tarvittavia toimenpiteitä. Raportoinnissa tärkeimmistä riskeistä esitetään riskiarvio, jota tarvittaessa täydennetään syvällisemmällä riskianalyysillä (mm. ominaisuudet ja vaikutustavat sekä mahdolliset hallintakeinot). Valittuja riskiarvion tietoja voi olla tarpeen jakaa sidosryhmien kanssa riskien käsittelemiseksi ja sidosryhmien oman riskienhallinnan tukemiseksi. Riskiarviota voidaan hyödyntää, raportoida, esittää ja tallentaa tarvittavalla tavalla ja valitussa laajuudessa, esimerkiksi tallentamalla keskeiset tiedot riskirekisteriin.

7.8 Riskien analysointi

Synonyymi: riskin analysointi

Määritelmä: *riskien arvioinnissa tai käsittelyssä tarvittavien tietojen selvittäminen riskien luonteesta*

Huomautus: Riskeistä analysoidaan eri menetelmin tarpeita vastaavalla tarkkuudella esimerkiksi riskin rakentumista ja sen eri ominaisuuksia, muutoksia näissä sekä mahdollisia kehityskulkuja. Riskien analysointi on yleensä vapaamuotoisempaa kuin riskien arviointi, ja analysoinnin keinot voidaan valita tapauskohtaisesti. Riskianalyysiä voidaan tarvittaessa syventää ja ajantasaistaa osana tarkentavaa arviota tai uudelleenarviointeja. Riskien analysointi on osa riskien arviointiprosessia, jossa sitä edeltää riskien tunnistaminen. Riskien analysointi voidaan tehdä ennen tai jälkeen riskien arvioinnin, ja tarvittaessa riskien analysointi ja arviointi vuorottelevat iteratiivisena ketjuna. Standardissa SFS-ISO 31000:2018 tästä käsitteestä käytetään termiä riskianalyysi, kun tässä sanastossa riskianalyysillä tarkoitetaan riskien analysoinnin tulosta.

7.9 Riskianalyysi

Synonyymi: -

Määritelmä: *riskien analysoinnin tulos*

Huomautus: Riskianalyysin perusteella voidaan arvioida riskejä ja suunnitella tarvittavia toimenpiteitä. Raportoinnissa riskianalyysillä voidaan avata mm. riskien ominaisuuksia, yhteyksiä, vaikutustapoja sekä mahdollisia hallintakeinoja, ja analyysin yhteyteen sisällytetään myös riskiarvio (usein todennäköisyys ja vaikutus tai riskiluku). Valittuja riskianalyysien tietoja voi olla tarpeen jakaa sidosryhmien kanssa riskien käsittelemiseksi ja sidosryhmien oman riskienhallinnan tukemiseksi. Riskianalyysiä voidaan hyödyntää, raportoida, esittää ja tallentaa tarvittavalla tavalla ja valitussa laajuudessa, ja sen sisällön osia voidaan ottaa seurantaan osana riskirekisteriä ja/tai yleistä toimintaympäristön muutosten seurantaa.

7.10 Riskien luokittelu

Synonyymi: -

Määritelmä: *riskien tehokasta arviointia ja käsittelyä varten tehtävät ryhmittelyt, joiden ansiosta samankaltaisia tai samaan vastuualueeseen kuuluvia riskejä tai niiden osia voidaan tarkastella yhtenä kokonaisuutena*

Huomautus: Riskien luokittelua voidaan tehdä hyvin erilaisin perustein, esimerkiksi aihealueen ja käsittelyssä tarvittavan osaamisen mukaan. Yleisesti tunnettuja riskien luokitteluja ovat tietynlaisten yritysten toimintaan soveltuva PK-RH, jossa riskit jaetaan strategisiin, operatiivisiin, taloudellisiin ja vahinkoriskeihin, sekä tietoturvauhkien luokitteluun tarkoitetut CVSS ja OWASP. Myös jakoa strategiseen tasoon, koordinointitasoon ja toiminnalliseen tasoon voidaan käyttää riskien vaikutuksia tai erityyppisten hallintakeinojen kohdistumista arvioitaessa. Tietoturvallisuuden hallintakeinoja ja niissä käytettäviä kontrolleja voidaan luokitella mm. hallinnollisiin ja teknisiin.

8 Aihealue: Vastuullisuus riskienhallinnassa

Käsitteet: läpinäkyvyys riskienhallinnassa, osallistavuus riskienhallinnassa, riskivastuullisuus

Vastuullisuuden kokonaisuus etsii vielä muotoaan digitaalisessa toimintaympäristössä. Siihen liitetään monia asioita, mutta nämä vaihtelevat asiasta keskustelevan kontekstin mukaan. Perinteisten ympäristöön ja ihmisoikeuksiin liittyvien näkökulmien huomioiminen on osa yhteiskuntaa lävistävää kehitystä, joka tulee jo esiin muun muassa hankintoja tehtäessä, jolloin voidaan esittää eettisten arvojen ehtoja esimerkiksi liittyen työoloihin, materiaalien alkuperään, energian käyttöön tuotannossa tai käytössä, tai imagollisesti rakentuviin ominaisuuksiin. Selkeää määritelmää ei sinänsä tarvita tämän aihealueen olemassaolon tunnistamiseksi ja keskustelun käymiseksi sen kautta.

Digitaalisessa turvallisuudessakin voidaan nähdä vastuullisuuden tulokulma, joka kuitenkin eroaa yleismaailmallisesta esikuvastaan ja sisältää digin erityisyyksiä. Edellä mainitusti, erilaisten teknologioiden ja turvallisuusratkaisuiden ostaminen tai myyminen voi sisältää vastuullisuuteen liittyviä kysymyksiä. Suoremmin näihin liittyvät maineeseen kohdentuvat riskit. Toisaalta samalla suunnalla ovat myös mahdollisuudet ja hyödyt hyvän vastuullisuuden toteuttamisessa, sillä niin sanottu yleisön good will, hyvä tahto, voi olla kriisissä arvokas etukäteen hankittu etu.

Erityinen digitaalisen turvallisuuden vastuullisuusasia on tietysti, miten sen toteutuksen osa-alueet hoidetaan, miten niistä annetaan tietoa ja miten huolehditaan asiakkaista ja muista sidosryhmistä. Erityisesti tietosuojaan liittyy paljon herkkiä rajapintoja, joihin tunnetaan yksityistä ja yhteisöllistä omistajuutta organisaatioiden ulkopuolelta. Ei riitä, että hoitaa tietoturvallisuutensa oman tarpeensa mukaan, vaan on huomioitava muut ja myös riittävästi viestittävä, jotta avoimuuden kautta voidaan rakentaa luottamusta. Tällä on suora yhteys siihen, miten asiakkaat käyttävät (tai eivät käytä) palveluita ja minkälaista julkista keskustelua asian ympärillä käydään – nyt tai kun jotain tapahtuu.

Digitaalisten riskien riskienhallinta on osa tätä käsittelyä. Riskivastuullisuuden kautta voidaan puhua siitä, huolehditaanko asiakkaisiin ja sidosryhmiin kohdistuvista riskeistä ensinnäkään riittävästi, mutta myöskään oikealla tavalla. Osataanko heihin kohdistuvat uhat tunnistaa (ja mikä on riittävää tässä) sekä viestiä näistä ja tarvituista hallintakeinoista. Ovatko riskeille, mutta etenkin vaihtoehdoista päättämiselle asetetut kriteerit ymmärrettävät, päivänvaloa kestävät ja perustellut, kun panokset ovat korkeat ja usea tavoite on ristiriidassa keskenään? Tehdäänkö vain pakollinen, halvimman kautta, myöhässä ja yhteen muottiin pakottaen, vai luodaanko pitkäjänteistä kehittyvää toimintaa, jossa asiat varmistetaan, resursoidaan riittävästi ja oikeasti harjoitellaan?

Organisaation hallintakeinojen valikoima on, etenkin monimutkaisemmissa riskeissä, usein sellainen, että on vaihtoehtoisia tapoja toimia. Näistä osa voi olla muille suotavampia kuin toiset ja olisi löydettävä oikeat tavat määritellä tasapaino vastuullisuuden huomioimisen sekä mahdollisen ylimääräisen ajan tai kustannuksen välillä. Parhaassa tapauksessa vaihtoehtoinen toimintatapa ei edes kustanna merkittävästi ylimääräistä, vaan kyse on toimintatavan muutoksesta.

Läpinäkyvyys riskienhallinnassa painottaa yksinkertaisesti sitä, että voidaan ymmärtää syyt toiminnalle riittävässä määrin. Usein päätöksien muodostumiselle etsitään perusteita, jotka voivat olla hyviä, mutta ilman läpinäkyvyyttä näitä ei voida arvioida. Läpinäkyvyys sinällään ei tarkoita kaiken paljastamista, vaan riittävän informaation tarjolle saattamista, jotta asianmukainen toiminta voidaan tunnistaa. Tälle ei ole määrämuotoa tai -laajuutta. Organisaatioille keskeistä riskienhallinnassa voi yksilöiden sijaan olla sopimuskumppaneihin liittyvä tarve tietää ja ymmärtää heidän riskienhallintaansa, riskejään ja uhkia, jotka voivat ketjuuntuneiden tai verkostovaikutuksien kautta siirtyä organisaatiosta toiseen. Hyvä yhteistyö rakentuu avoimelle viestinnälle, hyvä keskusteluyhteydelle sekä selkeästi määritellylle sopimukselle. Tämä mahdollistaa tarvittavien ja oikeasuhtaisen riskienhallinnan kokonaispalveluun ja palveluprosessiin nähden.

Hyvin lähellä tätä on uhka- ja riskitiedoista viestiminen. On osa hyvä digiturvallisuuden kulttuuria jakaa omien verkostojen, mutta myös laajemman yhteiskunnan kanssa tietoa, joka voi suojata jokaista. Esimerkkeinä ovat ilmoitukset havaituista haavoittuvuuksista tai toisten nimissä leviävistä tietojenkalasteluyrityksistä ilmoittaminen. Erikseen ovat tapaukset, joissa laki velvoittaa tekemään tiettyjä ilmoituksia.

Toiseenkin suuntaan on hyvä olla toimivat kanavat, sillä ihmiset tulevat tulevaisuudessakin kaipaamaan helppoa ja lähestyttävää yhteyttä, jonka kautta olla yhteydessä. Tämä on osa läpinäkyvyyttä. Siihen liittyvä näkökulma on kuitenkin, että hyvän yhteyden kautta voidaan saada monenlaista turvallisuuteenkin vaikuttavaa tietoa, mahdollisesti joukkoistuvalta ja aktivoituvalta havainnoitsijaverkostolta. Kyse voi olla niin organisaation sisäisestä kuin ulkoisestakin kohdennuksesta. Tämä on osa osallistavuudesta riskienhallinnassa, eli ihmisten halusta ja tarpeesta päästä vaikuttamaan itseensä kohdistuviin asioihin, mutta silloin pitää myös osoittaa (vähintään hyvällä viestinnällä) että tällä se on huomioitu jollain tavalla.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että digiturvallisuuden riskienhallintaankin osataan soveltaa hyvän yhteistoiminnan periaatteita luottamuksen rakentamiseksi ja yhteisen hyvän tuottamiseksi. Tämän voi nähdä osana riskienhallinnan keinovalikoimaa, sillä hyvinvoiva ja turvallinen toimintaympäristö niin digissä kuin sen ulkopuolella tukee yksittäisenkin organisaation hyvinvointia ja turvallisuutta, parantaen kaikkien resilienssiä tulevaisuuden kompleksisia uhkia vastaan.

8.1 Riskivastuullisuus

Synonyymi: -

Määritelmä: *muiden toimijoiden etujen tai yleisen edun huomioiminen riskien käsittelyssä*

Huomautus: Riskivastuullisessa toiminnassa riskejä ei esimerkiksi siirretä niin, että vaikutukset kohdistuvatkin sidosryhmään ilman tämän suostumusta. Riskivastuullista on myös muiden toimijoiden pitäminen tietoisina uusista uhista, jotka on havainnut. Käsittelytoimenpiteet voidaan lisäksi valita siten, että niillä tuotetaan yhteistä hyötyä tai minimoidaan yhteistä haittaa sen sijaan, että huomioitaisiin vain oma etu.

8.2 Osallistavuus riskienhallinnassa

Synonyymi: -

Määritelmä*: organisaation riskienhallintaan osallistumisen mahdollistaminen sidosryhmille ja siihen kannustaminen*

Huomautus: Sidosryhmien ottaminen sopivalla tavalla ja oikeaan aikaan mukaan riskienhallintaan mahdollistaa sidosryhmien tietämyksen, näkemysten ja havaintojen huomioon ottamisen. Näin lisätään tietoisuutta riskienhallinnasta ja varmistetaan parhaimpaan saatavilla olevaan tietoon perustuva riskienhallinta. Osallistamisen tavat ja taso riippuvat molemminpuolisista tarpeista liittyen viestintään, uhkatietoon, riskitietoon ja tilannekuviin. Osallistaminen voi itsessään kuulua riskien hallintakeinoihin, tai sen avulla sovittaa hallintakeinoja jaettujen tarpeiden huomioimiseksi.

8.3 Läpinäkyvyys riskienhallinnassa

Synonyymi: -

Määritelmä: *riskienhallinnan arvioinnin mahdollistaminen sidosryhmille ja sisäisille toimijoille siten, että siihen liittyvät tiedot välitetään niiltä osin, kuin tietojen välittäminen ei itsessään tuota merkittäviä riskejä*

Huomautus: Läpinäkyvyys on osa toiminnan vastuullisuutta, minkä lisäksi se edistää tiedon hyödyntämistä itseohjautuvasti eri osissa ekosysteemiä mm. häiriöiden ennakointiin, mikä puolestaan pienentää ketjuuntuneita ja verkottuneita riskejä. Läpinäkyvyyttä riskienhallinnassa voidaan toteuttaa eri toimijoille yhteistyön luonteesta riippuen säännöllisenä raportointina tai tilanteen niin vaatiessa. Riskienhallinnan periaatteita, kattavuutta, päätöksentekoprosessia ja vaikutusmahdollisuuksia voidaan usein avata yleisellä tasolla julkisestikin. Organisaation läpinäkyvyydessä eri toimijoiden suuntaan voi olla suuriakin eroja: toisille sidosryhmille riittävät yleisluontoiset julkaisut, kun taas toisille avataan kahdenvälisessä viestinnässä syvällisesti yhteistyön kannalta relevantteja riskejä ja riskienhallintatoimenpiteitä. Kullakin sidosryhmällä on omanlaisensa riskikäsitykset, joiden pohjalta ne kaipaavat erilaisia tietoja varmistuakseen siitä, että niihin vaikuttavat riskit tulevat käsitellyksi hyväksyttävällä tavalla. Vastaamalla sidosryhmien tiedontarpeisiin vältytään päällekkäisiltä riskienhallintatoimilta, luottamuspulalta ja mainehaitoilta.

9 Aihealue: Tiedonjako ja viestintä

Käsitteet: riskejä koskeva viestintä ja tiedonvaihto, riskiraportointi, riskirekisteri, riskitieto, uhkaprofiili, uhkatieto

Riskeistä ja uhista viestimiseen on esitetty huomiota useassa kohtaa tätä sanaston esittelydokumenttia. Nykyaikaisissa toimintaympäristöissä, joissa koko kentän hahmottaminen omatoimisesti on hyvin haastavaa, yhteistyö on korostuneen tärkeää. Jopa kilpailuasetelmassa olevien tahojen on syytä löytää kanava tietojenvaihtoon toimialueillaan, sillä uhat voivat uhata toimintamahdollisuuksia ja levitä nopeasti – ei vain omaan vaikutuspiiriin vaan asiakkaisiin ja tuotantoketjuihin. Tämänkaltaiset mekanismit tukevat tarvittua stabiiliutta, mikä vuorostaan välillisesti palvelee omaa riskienhallintaa ja tavoitteita, kun huomio ja resurssit voidaan kohdentaa johonkin rakentavampaan. Verkostoituminen myös mahdollistaa tiedon vastaanottamisen.

Tiedonjaossa on ulkoisten tahojen kohdalla aina määriteltävä mitä pitää, mitä voidaan ja miten voidaan jakaa tietoa niin, että se ei tuota tarpeetonta lisäriskiä omalle toiminnalle. Tässä tarkastelussa on syytä erotella ainakin uhkatieto ja riskitieto toisistaan. Ensinnä mainitun kohdalla käsitellään havaitun uhan ominaisuuksia, irrallaan mistään nimenomaisesta toimijasta, tämän haavoittuvuuksista tai muista tiedoista. Jälkimmäisessä tapauksessa samaa asiaa tarkastellaan huomioiden toimijan heikkoudet ja muut vaikuttavat erityisyydet tarvittavilta osin. Uhkatiedon pitäisi siis olla pääosin tietoa, jonka luovuttamisen ei tulisi haitata omaa toimintaa. Riskitiedon suhteen voi olla tarpeen määritellä tarkastikin mitä, miten ja kenen kanssa tietoa jaetaan, sillä pitkälle vietynä siinä voidaan paljastaa asioita, jotka heikentävät turvallisuutta tai toiminnan edellytyksiä (kuten liikesalaisuudet). Tiedonjako tai valikoiva tiedonjako sinänsä ei ole uusi asia, vaan tällä pyritään korostamaan sitä, että se on mahdollista ja tehtävissä hallitusti myös riskienhallinnan kontekstissa.

Sisäisten tahojen kohdalla tiedon jakaminen yleisemmin uhista ja kohdentuvista riskeistä on tärkeää, jotta jokainen voi ottaa nämä huomioon työssään ja toimissaan. Mutta tämän lisäksi on riittävässä määrin myös viestittävä riskienhallinnasta ja sen kokonaistilasta, jottei jatkuvasti esillä olevien yksittäisten asioiden kautta synny vääriä olettamuksia organisaation tilanteesta. Jatkuvat varoitukset ja kertomukset hyökkäyksistä voivat saada epäilemään omien järjestelmien luotettavuutta, mikä vaikuttaa niiden asianmukaiseen käyttöön, mutta toisaalta, vältettäessä uhkia pitkään, saatetaan tuudittautua hyvänolon tunteeseen tai vähätellä varoitusten merkitystä. Myös digitaalisessa turvallisuudessa voi muodostua ero todellisen turvallisuustilanteen ja turvallisuuden tunteen välille (asia, mitä on tarkasteltu digiä laajemmassa käsittelyssä viime vuosina ja jossa digissä tapahtuvalla toiminnalla on ollut osansa[13]).

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että pyrkii löytämään tasapainon siinä, miten pitää omat sisäiset ja ulkoiset sidosryhmät oikealla tavalla tietoisina mitä ympärillä on tapahtumassa. Tämä vaatii tiedon luokittelua sekä hallintaa yhdenmukaisella tavalla, jolloin voidaan toteuttaa prosessia ja kehityksenseurantaa tunnetuille ja kehittyville ilmiöille. Laajan tarkastelun lisäksi, oikein

[13] TUOVI-portaali: https://sisainenturvallisuus.fi/turvallisuuden-tunne-ja-strateginen-viestinta

kohdistettu tutkimus ja selvitystoiminta voi olla strategisen tärkeää riskienhallinnan kannalta sekä riskiymmärryksen kehittämiseksi.

9.1 Riskejä koskeva viestintä ja tiedonvaihto

Synonyymi: -

Määritelmä: *jatkuvat ja toistuvat prosessit, joilla organisaatio antaa, jakaa tai hankkii tietoa ja käy vuoropuhelua organisaation sisällä ja sidosryhmiensä kanssa riskienhallinnasta ja riskeistä*

Huomautus: Riskejä koskeva viestintä ja tiedonvaihto on osa normaalia riskienhallintaprosessia. Viestintää ja tiedonvaihtoa voi tapahtua kahdenvälisesti tai eri verkostoissa. Viestinnän (ml. varoitukset, koulutukset, toiminnan ohjaus jne.) merkitys riskien hallitsemisessa korostuu, kun pyritään muuttamaan toimintaa.

9.2 Riskiraportointi

Synonyymi: riskien raportointi; riskin raportointi

Määritelmä: *riskejä koskeva viestintä ja tiedonvaihto, joiden tarkoituksena on välittää tietyille sisäisille tai ulkoisille sidosryhmille riskien senhetkistä tilaa ja niiden hallintaa koskevaa tietoa*

Huomautus: Raportoinnin syvyys, yksityiskohtaisuus, toistuvuus ja esittämistapa vaihtelevat riskejä koskevan viestinnän ja tiedonvaihdon päämäärien sekä kohdeyleisön mukaan. Esimerkiksi riskiperusteinen päätöksenteko on riippuvaista siitä, että päätöksentekoprosessia tuetaan sen tarpeiden mukaisella riskiraportoinnilla.

9.3 Riskitieto

Synonyymi: -

Määritelmä: *riskiä koskeva tieto*

Huomautus: Riskitiedot eroavat uhkatiedoista siten, että niissä käsitellään mahdollisten tapahtumien vaikutuksia organisaatiokontekstin tavoitteisiin vertaamalla ja suhteuttamalla vaikutuksia resursseihin, kyvykkyyksiin jne., mistä syystä riskitiedot voivat paljastaa heikkouksia tai haavoittuvuuksia. Riskitiedot voivat kuvata esimerkiksi riskin todennäköisyyttä, vaikutuksia, juurisyitä tai hallintatoimia.

9.4 Riskirekisteri

Synonyymi: -

Määritelmä: *rekisteri, johon tallennetaan tunnistetut riskit ja niiden arvioinnit*

Huomautus: Riskirekisteriin voidaan tallentaa tai linkittää monenlaisia lisätietoja, esimerkiksi riskianalyyseja sekä tiedot suunnitelluista ja/tai toteutetuista hallintatoimenpiteistä. Rekisterin muotoa ei sinällään ole määritelty, ja mikäli se on toteutettu erillisenä tietokantana, siihen voi liittyä erilaisia riskienhallintatyökaluja, joilla käsitellään

siinä olevia tietoja ja toteutetaan automatisoidusti mm. luokitteluita. Riskirekisteri kerää riskitiedot yhdenmukaisessa ja päivitettävässä muodossa, mikä mahdollistaa riskien seurannan ja riskien tilannekuvan muodostamisen.

9.5 Uhkatieto

Synonyymi: -

Määritelmä: *uhkaa koskeva tieto*

Huomautus: Uhkatiedot eroavat riskitiedoista siten, ettei niissä suhteuteta mahdollisia vaikutuksia organisaatiokontekstin tavoitteisiin, resursseihin, kontrolleihin tms., vaan tiedot kuvaavat uhkaa yleisellä tasolla lähinnä sen omilla muuttujilla. Esimerkiksi tietoturvauhkien CVSS-arviointi ja näihin liittyvät raportit ovat tapa jakaa uhkatietoa. Uhkatiedoissa voidaan kuvata myös mahdollisuuksiin liittyviä asioita.

9.6 Uhkaprofiili

Synonyymi: -

Määritelmä: *uhkan luokittelua varten laadittu kuvaus uhkan ja uhkan aiheuttajan ominaisuuksista*

Huomautus: Uhkan aiheuttaja voi olla toimija, toisiinsa vaikuttavien toimijoiden joukko tai esimerkiksi luonnonilmiö. Osa riskeihin vaikuttavista tekijöistä voi olla päätteltävissä uhkaprofiileissa kuvatuista ominaisuuksista, kuten uhan sijainti, motivaatiot, resurssit jne. Hyökkääjistä laadittuja uhkaprofiileita kutsutaan hyökkääjäprofiileiksi.

10 Aihealue: Riskienhallinnan rakenteet

Käsitteet: riskienhallinnan puitteet, riskienhallintajärjestelmä, riskienhallintaperiaatteet, riskienhallintapolitiikka, riskienhallintatyökalu

Riskienhallinta rakentuu monesta osasta, mutta jokaisella organisaatiolla se on erilainen ja vastaa eri tarpeisiin. Näiden rakenteiden erittelyllä mahdollistuu sen tarkentaminen, mikä riskienhallinnassa toimii ja mitä pitää kehittää. Painotuksia voi olla, mutta kokonaisuuden tulisi jokseenkin tasaisesti olla samalla kehityksen tasolla. Eri maturiteettitasolta toimiva osa voi haitata tehokasta hallintaprosessia.

Ylimmän tason käsitteistä riskienhallinnan puitteet kuvaavat pitkälti tämän toteuttamiseen määriteltyjä hallinnollisia resursseja ja sen asemaa osana organisaation toiminnan ohjausta ja varmistamista. Sillä tarkoitetaan laajempaa määritystä kuin vain prosessi tai toteutuksen toiminnan mallia. Se eroaa riskienhallintajärjestelmän kuvaamasta kokonaisuudesta siinä, että riskienhallintajärjestelmä sisältää myös varsinaisen toiminnan, jolloin siinä kuvastuu määriteltyjen puitteiden käytännön toteutus. Siinä todellinen toimintakulttuuri, määrittelemättömät harmaat alueet ja epäviralliset toimintatavat täydentävät riskienhallinnan kokonaisjärjestelmää. Tällöin siis järjestelmä pitää käsittää sosio-teknisenä kokonaisuutena, ei vain tietojärjestelminä.

Riskienhallintaa johtavat, suunnittelevat ja kehittävät tekevätkin siis viisaasti sisäistäessään, että riskienhallinnan puitteiden on oltava tarpeeseen nähden riittävät, mutta riskienhallintajärjestelmän todellisen toteutuksen muodostumiseen vaikuttavat useat tekijät. Toteutuksen ja riskienhallintakulttuurin muodostumiseen voidaan pyrkiä vaikuttamaan riskienhallintaperiaatteilla ja riskienhallintapolitiikalla, mutta on muistettava, että näiden kirjaamisen lisäksi niistä on viestittävä – mielellään tavalla, jonka vastaanottaja kykenee hyödyntämään omaan toimintaansa.

Edellisten käsitteiden abstraktiuden vastapainona on käytännön tekemistä lähempänä oleva riskienhallintatyökalu. Koska tämä alkaa olla nykypäivänä tietojärjestelmäpohjainen, se sekoittuu riskienhallintajärjestelmään. Riskienhallintajärjestelmän ja -työkalun ero on, että työkalulla käsitellään ja hallitaan riskienhallinnan tietoa ja mahdollistetaan määrämuotoinen prosessi. Työkaluja on monenlaisia ja osa on tarkoitettu vain johonkin osaan kokonaisprosessista, jolloin tiedon siirtyminen tapahtuu osin riskirekisterillä ja osin prosessin toteutuksesta vastuutetun henkilön avulla. Yleinen osakokonaisuuden työkalu on poikkeamailmoitusten lomake ja näiden hallintaan tarkoitettu käyttöliittymä. Poikkeamatyökalulla voi olla muitakin tarkoituksia, mutta riskienhallinnalle se on apuväline uhkatiedon keräämiseen sekä joukkoistettuun riskien tunnistamiseen. Ehkäpä tämän takia, koska se on yleisimpiä kontakteja riskienhallintaan monelle, nämä työkalut samaistetaan virheellisesti koko riskienhallintajärjestelmäksi, mikä voi aiheuttaa sekaannuksia.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että tarkasteltaessa riskienhallinnan kokonaisuutta, osataan erottaa tavoiteltu ja todellisuus. Ylätason rakenteiden suunnittelulla ja kirjaamisella luodaan pohja kokonaisuuden rakentamiselle, ylläpidolle ja kehittämiselle, mutta nämä asiat täytyy saada jalkautettua. Riskienhallintatyökalun merkitys sille, miten riskienhallinta ymmärretään, on voimakas ja sitä tulisikin pystyä muokkaamaan – muun muassa siten, että riskienhallinnan periaatteet ja politiikka tulevat esiin toimintaa tukevalla tavalla.

10.1 Riskienhallinnan puitteet

Synonyymi: -

Määritelmä: *riskienhallinnan organisointi, vastuunjako ja tarkennettu toimintamalli, jotka osana johtamisjärjestelmää mahdollistavat riskienhallintaperiaatteiden toteuttamisen organisaation prosesseissa*

Huomautus: Riskienhallinnan puitteet ovat ne hallinnolliset rakenteet, jotka mahdollistavat riskienhallinnan järjestämisen, mutta puitteet voivat myös rajoittaa sen onnistumista, mikäli niissä on puutteita. Riskienhallinnan puitteiden kehittämiseen kuuluu riskienhallinnan sisällyttäminen organisaation johtamisjärjestelmään ja riskienhallinnan suunnittelu, toteuttaminen, arviointi ja kehittäminen koko organisaatiossa.

10.2 Riskienhallintajärjestelmä

Synonyymi: -

Määritelmä: *hallintajärjestelmä, joka kattaa riskienhallintapolitiikat ja riskienhallinnan tavoitteet sekä prosessit ja mahdolliset riskienhallintatyökalut, joilla nämä tavoitteet saavutetaan*

Huomautus: Riskienhallintajärjestelmä on kokonaisuus, joka muodostuu eri osista ja niiden toiminnasta. Kokonaisuus ei välttämättä vastaa aiottua, suunniteltua tai tarvittua, vaan se voi olla esimerkiksi toiminnan tai toimintaympäristön muutosten myötä vanhentunut taikka vuorovaikutusverkostojen monimutkaisuuden vuoksi riittämätön. Riskienhallintajärjestelmän tarkoituksenmukaisuutta voidaan arvioida sisäisen tarkastuksen yhteydessä ja/tai organisaation johdon toimesta. Riskienhallintajärjestelmä voi olla erillinen kokonaisuutensa, mutta sen tulisi liittyä kiinteästi toiminnanohjaukseen ja sen järjestelmiin.

10.3 Riskienhallintaperiaatteet

Synonyymi: riskienhallinnan periaatteet

Määritelmä: *riskienhallinnan tavoitteet ja yleinen toimintamalli, jotka osana johtamisjärjestelmää tukevat organisaation arvon luomista ja säilyttämistä*

Huomautus: Riskienhallintaperiaatteet toimivat pohjana riskienhallinnan puitteiden ja edelleen riskienhallinnan prosessien määrittelyssä. Standardissa ISO 31000 kuvataan periaatteet, joita tarvitaan vaikuttavaan riskienhallintaan.

10.4 Riskienhallintapolitiikka

Synonyymi: -

Määritelmä: *organisaatiokohtainen kuvaus riskienhallintaperiaatteista ja keskeisinä pidetyistä riskienhallinnan puitteista*

Huomautus: Organisaatioissa, joissa riskienhallintaperiaatteet on johdettu suosituksista tai vaatimuksista, riskienhallintapolitiikassa voidaan selventää periaatteiden

suhdetta organisaation tavoitteisiin ja toimintaan. Tyypillisesti riskienhallintapolitiikka dokumentoidaan, mutta se voi käytännössä koostua useista dokumenteista. Organisaation sisällä riskienhallintapolitiikka on keskeinen osa johtamisviestintää. Riskienhallintapolitiikka tai osia siitä voidaan harkinnan mukaan julkaista.

10.5 Riskienhallintatyökalu

Synonyymi: -

Määritelmä: *ohjelmisto, lomake tai muu apuväline, joka ohjaa toteuttamaan jotain osaa riskienhallinnasta johdonmukaisesti tiettyjä malleja tai menetelmiä noudattaen*

Huomautus: Organisaatiolla voi olla käytössään erilaisia erillisiä riskienhallintatyökaluja, jotka parhaimmillaan täydentävät toisiaan. Esimerkiksi riskien arviointiprosessin työkalu kattaa ainoastaan arviointiprosessin, joten se oheen voi olla tarpeellista ottaa käyttöön työkaluja, jotka tukevat muita hallintaprosessin osia.

11 Aihealue: Seuranta ja tilannekuva

Käsitteet: riskien seuranta, riskien tilannekuva, riskienhallinnan seuranta, riskienhallinnan tilannekuva, riskienhallintajärjestelmän seuranta, riskienhallintajärjestelmän tilannekuva

Riskiraportointi, joka otettiin esiin aiemmin, ja tilannekuva ovat hyvin lähellä toisiaan, etenkin puhekielessä. Näitä kannattaa kuitenkin pitää erillään, eri käyttöä varten. Raportointiin voidaan katsoa liittyvän enemmän analyysiä sekä näkökulmaa vaihtoehtoisiin tulevaisuuksiin, jolloin päätöksentekoon tarjotaan vaihtoehtoja. Tähän ei kuitenkaan ole selkeää määrittelyä ja eroa syntyy myös siinä, onko kyse kohdennetusta kertaluonteisesta raportoinnista vai yleisestä, toistettavasta ja määrämuotoisesta.

Tilannekuvasta on hyvin erilaisia määrittelyitä, joista joidenkin mielestä käsitys tilanteesta muodostuu vasta vastaanottajan tajunnassa. Tilannekuva siis kertoo missä ollaan sekä mahdollisesti mihin tästä ollaan suuntaamassa (ja millä varmuudella). Keskeinen komponentti tämän kuvan muodostamisessa on historiallisen kehityksen seuranta, mihin voidaan pyrkiä yhdistämään tulevaisuuden ennakointityön tietoa.

Voidaan ottaa myös näkemys, että tilannekuva on senhetkinen ”päivitys” yksittäisten riskien tai kokonaisuuden tilanteesta, jolloin tilannekuvaa voidaan pitää kevyempänä informaation määrän suhteen, kuin mitä voisi odottaa riskiraportoinnista. Tämänkaltainen tiedon määrän hallinta voi antaa viestintään vaihtoehtoja, jolloin osa riskitietojen käsittelystä ja katselmoinnista voidaan tehdä kevyemmin esimerkiksi kuukausipalavereissa ja raportoinnin läpikäyntiä voidaan keskittää muutamaan kertaan vuodessa. Rajallinen tilannekuva voi myös olla jatkuvasti nähtävissä mahdollisesti riskienhallintatyökalun muodostamissa automaattisissa raporteissa keskeisistä tunnusluvuista. Pitää kuitenkin muistaa, että tunnusluvut eivät ole itse riski tai riskienhallinta – ne ovat vain työkalu muutoksen toteamiseen. Niille määritellyt raja-arvot vain muistuttavat meitä, onko tarve huomioida tai tehdä jotain, selvittää asiaa tarkemmin.

Riskienhallinnan rakenteiden kohdalla tuotiin esiin, miten riskienhallintajärjestelmällä tarkoitetaan laajasti riskienhallinnan toteutusta ja toteutumista. Siinä tarkastelu ei ole niinkään yksittäisten riskien hallinnassa, vaan siinä, miten järjestelmää hyödynnetään osana kokonaistoimintaa. Siihen liittyvä seuranta ja muodostetut näkemykset tilannekuvasta ovat erityisesti johdolle ja sisäiselle tarkastukselle mielenkiinnon kohde. Keskeinen kysymys on, missä määrin koko järjestelmä vastaa tarvittua tai tavoiteltua mallia ja mikä merkitys tällä on strategiassa. Tätä kapeampi tarkastelunsa on riskienhallinnan tilannekuva ja tähän liittyvä seuranta, jossa keskitytään perinteisesti prosessiin ja sen osien koordinointiin. Riskienhallinnan toteutus on käytännössä sitä, miten hyvin prosessia noudatetaan ja tuottaako se tarvittua tietoa ja hallintatoimia niin normaaliin toiminnan ohjaukseen, kuin poikkeustilanteitakin varten. Erikseen näiden lisäksi ovat itse riskit ja niihin liittyvät tiedot.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että tarkasteltaessa riskienhallintaa, osataan erottaa riskit, niiden hallintaprosessi sekä laajempi riskienhallinnan ympärille muodostunut järjestelmä toisistaan. Tämä auttaa kokonaisuuden hahmottamisessa ja hallinnoinnissa, mikä voi vaarantua seuraamalla vain osan kehittymistä. Tehokkaaseen tilannekuvaan kuuluvat kuvaavat ja helposti

hahmotettavat tunnusluvut, joilla voidaan seurata oleellisia muutoksia syvällisempien raportointien välillä.

11.1 Riskien seuranta

Synonyymi: riskitekijöiden seuranta

Määritelmä: *riskien tilan ja muutossuuntien selvittäminen*

Huomautus: Riskien seurannan puitteissa havainnoidaan, mitä vaikutuksia toimintaympäristön muutoksilla ja oman toiminnan muutoksilla on riskeihin, missä määrin riskit toteutuvat ja miten hallintatoimilla onnistutaan niihin vaikuttamaan. Riskien seurannassa olisi hyvä huomioida mm. haavoittuvuudet, riskien todennäköisyys ja suojattavien kohteiden arvo. Riskien seurantaan tulisi käyttää riskirekisteriä ja toistaa seurantaprosessia sopivin väliajoin, jotta mahdollisista muutoksista on riittävä ja oikea-aikainen tieto tarvittavia uudelleenarviointeja varten.

11.2 Riskien tilannekuva

Synonyymi: riskitilannekuva

Määritelmä: *koottu kuvaus riskien seurannan tuloksista*

Huomautus: Seurannan tulosten raportointi ja esitystapa vaihtelevat organisaatiokontekstin ja kohdeyleisön mukaan. Tilannekuvan tulisi sopia sisällöltään ja laajuudeltaan käyttötarkoitukseensa, eli useimmiten riskiperusteisen päätöksenteon tai riskejä koskevan viestinnän tueksi.

11.3 Riskienhallinnan seuranta

Synonyymi: -

Määritelmä: *riskienhallinnan prosessin ja siihen liittyvien toimintojen tilan havainnointi*

Huomautus: Jatkuvan ja/tai säännöllisen seurannan avulla saadaan tietoa siitä, kuinka asianmukaista ja merkityksellistä toiminta on vallitseviin olosuhteisiin ja tarpeisiin nähden. Riskienhallinnan seurannan tehtävänä on tunnistaa, miten tehokas prosessi on ja tuottaako se oikeanlaista tietoa oikea-aikaisesti niin, että siitä saadaan hyötyä. Riskienhallinnan prosessin toimintaa voivat arvioida sekä prosessista vastuussa oleva toimija ("toinen linja" ns. kolmen linjan mallissa) että sisäinen tarkastus ("kolmas linja").

11.4 Riskienhallinnan tilannekuva

Synonyymi: -

Määritelmä: *koottu kuvaus riskienhallinnan seurannan tuloksista*

Huomautus: Seurannan tulosten raportointi ja esitystapa vaihtelevat organisaatiokontekstin ja kohdeyleisön mukaan.

11.5 Riskienhallintajärjestelmän seuranta

Synonyymi: -

Määritelmä: *riskienhallintajärjestelmän soveltamisen tapojen ja laajuuden sekä sen muutoshistorian havainnointi*

Huomautus: Riskienhallintajärjestelmän tarkoituksenmukaisuutta voidaan arvioida sisäisen tarkastuksen yhteydessä ja/tai organisaation johdon toimesta.

11.6 Riskienhallintajärjestelmän tilannekuva

Synonyymi: -

Määritelmä: *koottu kuvaus riskienhallintajärjestelmän seurannan tuloksista*

Huomautus: Seurannan tulosten raportointi ja esitystapa vaihtelevat organisaatiokontekstin ja kohdeyleisön mukaan.

12 Aihealue: Riskienhallinnan kontekstit ja tasomallit

Käsitteet: katsantotaso, koordinointitaso, käsittelytaso, organisaatiokonteksti, strateginen taso, tiedonhallintayksikkö, toiminnallinen taso

Konteksti ja sen määrittäminen oikein on erityisen keskeinen tekijä riskienhallinnan onnistumisessa. Laajemmassa katsannossa konteksti on mukana joka vaiheessa riskienhallintaa, erityisesti siitä syytä, että siinä käytetään paljon tietoa, joka liittyy moneen eri asiaan ja pyrkimys on tarkkuuteen. Riskienhallintaa tehdään aina jostain tarkastelun kontekstista, jolloin pääsääntöisesti tarkastellaan omia riskejä. Riskienhallintaprosessia ja -rakenteita käyttävät ja tuottavat organisaatiot, joten voidaan puhua organisaatiokontekstista. Tämän vuoksi, jonkun toisen tekemän esimerkin kopioiminen ilman lähempää tarkastelua, on riskienhallinnan näkökulmasta uhkapeliä.

Organisaation määrittely ei kuitenkaan ole aina suoraviivaista, sillä kyse voi olla varsin vapaamuotoisestikin yhteen toimivasta ryhmästä. Kyse voi myös olla erilliseksi rajatusta osasta laajempaa organisaatiota tai jostain organisaatioiden muodostamasta ryhmästä. Riskienhallinnan kannata keskeistä lienee, että tunnistaako ryhmä itse itsensä erilliseksi toimijaksi ja onko sillä omat eriävät tavoitteet (tai rajoitteet), joiden suhteen riskejä tulisi arvioida. Usein organisaatioiden yksiköiden tavoitteet ja riskienhallinta voidaan sisällyttää organisaation strategiaan ja kokonaisriskienhallintaan.

Yksi erityinen organisaatiokonteksti on tiedonhallintayksikkö. Sen tulee tehdä riskinarvio erityisesti oman toimintansa osalta, mutta myös omaan toimintaansa liittyvien asiakkaiden osalta, koska tiedonhallintayksikkö käsittelee henkilötietoja. Pääosassa tapauksissa koko organisaatio on tiedonhallintayksikkö, mutta on eräitä, joissa organisaatioon kuuluu useampikin tiedonhallintayksikkö. Lakiin perustuva vaatimus ja määrittely vaatii siis näitä tiettyjä toimijoita huomioimaan toisenkin kontekstin riskit osana organisaation omaa riskienhallintaa, pääosin viestimällä niistä asianmukaisesti.

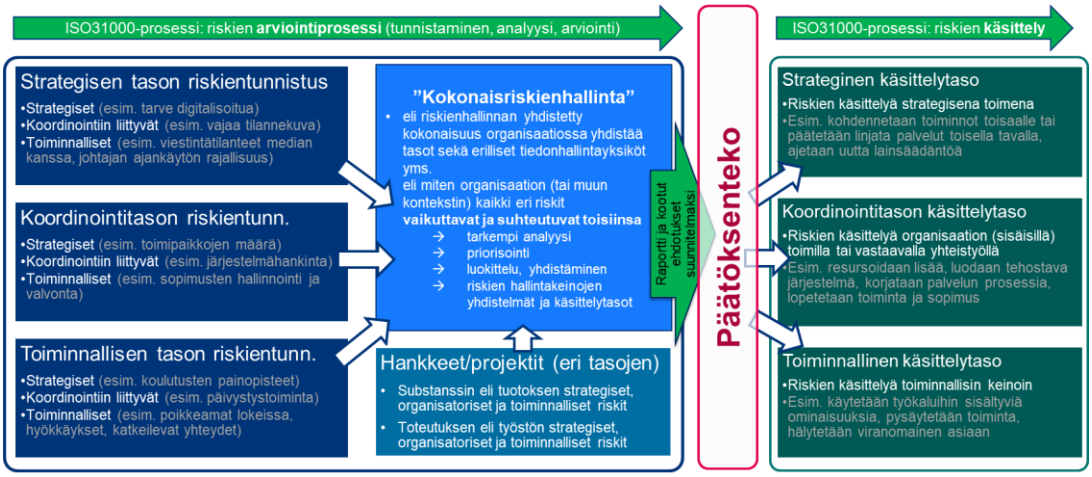
Yksi esimerkki, jossa tietoverkkoja käyttävien asiakkaiden konteksti on organisaation riskikontekstin kanssa nostettu vähintään yhtä tärkeäksi, on 40 artiklan kolmas kohta EU direktiivissä eurooppalaisesta sähköisen viestinnän säännöstöstä (2018/1972). Siinä ”*verkkojen tai palvelujen tarjoajat ilmoittavat niille käyttäjilleen, joihin kyseinen uhka mahdollisesti vaikuttaa, kaikista mahdollisista suojaavista tai korjaavista toimista, joita käyttäjät voivat toteuttaa. Tarjoajien on tarvittaessa tiedotettava käyttäjilleen myös itse uhasta*”, mikä edellyttää uhkien ja riskien tunnistamista eri konteksteissa.[14]

Muiden organisaatiokontekstien huomioimista voidaan pitää riskivastuullisena toimintana, mutta sitä voidaan myös hyödyntää omien näkökulmien avartamiseen sekä mahdollisuuksien tunnistamiseen. On hyvä olla varautunut, jos asiakkaiden, työntekijöiden, sopimuskumppanien ja muiden sidosryhmien kompleksiset ja etenkin maineriskit toteutuvat, sillä niiden vaikutukset voivat heijastua yllättävälläkin tavalla ketjujen ja verkostojen kautta.

Mikäli omaa organisaationkontekstia (keitä me olemme, mitä me teemme, mitkä ovat tavoitteemme jne.) sekä muita taustaoletuksia ei määritellä tarpeeksi tarkasti, tai ne

[14] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A02018L1972-20181217

ovat muuttunut edellisen määrittelyn jälkeen, vaarana on, että riskejä ei tunnisteta tai niitä arvioidaan ja analysoidaan väärin. Usein on tarpeen määritellä minkä tasoisia riskejä halutaan tarkastella. Tällä tarkennetaan sitä, tavoitellaanko riskeissä yhteismitallisuutta, sillä organisaationlaajuiset, pitkäkestoiset ja olemassaoloa uhkaavat riskit nähdään eri tavoin sekä huomioidaan päätöksenteossa toisella tavalla kuin pienemmät ja lyhytkestoisemmat riskit, Katsantotaso eroaa käsittelytasosta siinä, että riskit on voitu tunnistaa ja arvioida yhdellä tasolla, mutta sitä varten luodut hallintakeinot voivat jakautua eri tasoille. Onkin melko tyypillistä, että jokin haavoittuvuus tunnistetaan toiminnallisella tasolla, mutta sekä korjataan toiminnallisella tasolla että vastaavanlaisten ehkäisemiseksi luodaan hallinnollinen ohje tai varoitus koordinointitasolla organisaatiossa. On myös mahdollista, että vastaavien toiminnallisen tason riskien lisääntyessä kehitetään lisäksi strategiaa huomioimaan ne, mikä puolestaan voi poikia koordinaatiotasolla uuden järjestelmän hankinnan ja toiminnallisella tasolla koulutustarpeen kyseisen kontrollin käyttöön. Usean tason kontrollien käyttö luo syvyyttä ja kattavuutta digiturvan hallintaan.



Kuva2: Riskienhallinnan kokonaisprosessin osat arviointiprosessi ja käsittelyvaihe sekä niiden välissä tapahtuva päätöksenteon vaihe. Päätöksenteko ei perustu vain riskienhallinnalla tuotettuun tietoon, vaan siinä huomioidaan myös organisaation tavoitteet, resurssit, toiminta ja muu oleellinen tieto. Keskeistä on huomioida eri tasojen riskitietojen yhdistyminen kokonaisriskienhallinnaksi, jossa kehitetään hallintatoimia toteutettavaksi tarvittavilla tasoilla. Käsittely voi tapahtua eri tasoilla kuin missä riski on tunnistettu.

Strateginen, koordinointi- ja toiminnallinen taso ovat synonyymeineen osa yleisluontoista kolmitasoista mallia[15], jolla avataan sitä tosiasiaa, että kaikki uhat ja riskit eivät ole samanlaisia tai saman arvoisia sen suhteen, miten ne vaikuttavat organisaatioon. Kolmitasoisen mallin sijaa organisaatio voi haluta käyttää muuta jaottelua, joka sopii sen käyttöön paremmin, mutta tasomallin tarkoitus ei ole erotella hierarkioiden tasoa.

[15] Vastaavaa on aiemmin esitetty muun muassa pyramidina, mutta tässä vanhassa mallissa on ollut sisällytettynä myös käsittelyhierarkiaa sekä tiedon siirtymistä, jotka eivät istu kaikkiin käyttötapauksiin, eivätkä tue systeemistä käsittelyä. Tässä yhteydessä on käytetty myös keskimmäisestä ja alimmasta tasosta sekaisin termejä ”operatiivinen” ja ”taktinen”, riippuen organisaation taustasta. Lisäksi näiden sotilaallisen termistön ilmaisuiden ei nähdä istuvan kaikkien toimijoiden käyttöön. Viestinnällisesti erityisiä haasteita on tunnistettu liittyen ilmaisuun ”operatiivinen”, jota käytetään myös eräässä riskien tyyppien luokittelussa, jossa ei oteta kantaa riskien tasoon. Kyseisen termin käyttö yksinään voidaan nähdä merkityksettömänä, pelkkänä puhekielisenä erotuksena ”strategisesta”, mikä liittyy esiteltävään ”kaikki muu” -ongelmaan.

Keskeistä on sisäistää, että määrittelemällä eri katsannon ja käsittelyn tasot sekä niiden väliset rajapinnat (tarkka raja voi olla ongelmallinen), kyetään täsmällisempään riskien kohtaamiseen, luokitteluun ja käsittelyyn.

Yksi ajatusvirhe on, että tunnistetaan vain strateginen taso, sillä ylätaso on yleensä kuvattu eri dokumenteissa melko hyvin. Sen alapuolelle saatetaan kuitenkin mieltää olevaksi ”kaikki muu”, niitä tarkemmin määrittelemättä. Tässä asetelmassa ei synny selkeää prosessia, koska määritellyn toteutusketjun lisäksi rajapinnasta puuttuu keskustelukumppani, jonka kanssa muodostetaan toteutus ja vaihdetaan tietoa, jotta tahtotila muuttuu toiminnaksi. Esimerkiksi, miten riskienhallinnan strategisia linjauksia muutetaan keskimmäisellä tasolla organisaation muutoshankkeiksi ja alemmalla tasolla käytännön toimiksi. Tämän selkiyttäminen on tarpeen hyvässä johdon ja asiantuntijoiden välisessä kommunikaatiossa, mutta myös asiantuntijoiden ja toteuttajien välisessä rajapinnassa. Vaikka tasot pääosin noudattavat päätöksenteossa hierarkiaa, itse riskit voivat muodostua minkä tasoisina vain kaikilla hierarkian tasoilla. Eli, ”johtoyksikölläkin” on omat toiminnalliset ja koordinoinnin haasteensa, joita ei lueta koko organisaation kontekstissa strategisiksi.

Onnistunut määrittely, eli rakenteiden kuvaus, kertoo siitä, miten hyvin organisaation eri kokonaisuuksista muodostuvat toiminnot sekä näiden toiminnan tasot nähdään toisiinsa tukeutuvana systeeminä. Tai huonommassa tapauksessa, miten sattumanvaraisesti, irrallaan ja epätehokkaasti tai vailla tavoitetta ne toimivat. On toki hyvä muistuttaa, että liian tiukkaan määritellyt ja yhteen liitetyt systeemit eivät kykene joustamaan, mukautumaan, kehittymään ja reagoimaan kriiseihin, eli tässäkin on haettava tasapainoa.

Kaikkien kontekstien ja tasojen kohdalla oman ja toisen suhteellinen sijoittuminen näissä hallinnan tukemiseksi luoduissa rakennelmissa tukee viestinnässä viestin kohdistamista oikein. Tämä koskee niin sisältöä, sisällön muotoilua, kanavaa, ajoitusta sekä muita muuttujia. Erityinen huomio tässä tulee kiinnittää riskitiedon liikkumiseen tasojen ja kontekstien välillä yleisesti. Koska riskeihin tehdyt arviot perustuvat suhteutukseen tiettyjen organisaation tavoitteiden, resurssien, tietotaidon ja muiden ominaisuuksien mukaan, ei näitä tietoja voida suoraan siirtää käytettäväksi toisessa kontekstissa. Nämä tiedot on aina uudelleenarvioitava (kokonaan alusta tai sopivia muuntomekanismeja käyttäen) eri rajapintoja ylitettäessä tai muuten niiden merkitys voi vinoutua.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että osataan tunnistaa oikea konteksti niin organisaation tai muun taustaryhmän mukaan, mutta myös oikea katsantotaso, jotta riskit voidaan tunnistaa kattavasti sekä niiden merkitys voidaan ymmärtää oikein. Näiden lisäksi on muistettava myös muut määrittävät tekijät, kuten digiturvallisuuden eri toteutusalueet näkökulmina riskeihin ja niiden käsittelyyn, missä on myös osattava kohdentaa toimet tarvittaessa usealle tasolle. Väärä kontekstien määritys altistaa puutteelliselle riskien tunnistamiselle. Riskien käsittely yhtenä kokonaisuutena voi olla epätehokasta, vääristää kuvaa niistä sekä vaikeuttaa selkeän hallintakokonaisuuden luomista.

12.1 Organisaatiokonteksti

Synonyymi: -

Määritelmä: *organisaatio tai sen osa, jonka näkökulmasta tarkastellaan*

Huomautus: Kukin organisaatio tekee riskienhallintaa omasta kontekstistaan: se, mitä tunnistetaan riskeiksi, muuttuu sen mukaan missä organisaatiossa – ja missä sen osassa – ollaan. Kullakin organisaation osalla on esimerkiksi omia tavoitteita, resursseja ja vaatimuksia, joiden puitteissa suhtautuminen riskeihin muodostuu. Linjaorganisaatioiden eri toimintayksiköillä tai niiden toimintatasoilla voi suurissa organisaatioissa olla merkittävästikin toisistaan eroavat näkökulmat. Myös käsittelytasot voivat muodostaa omia kontekstejaan. Yksi erityinen organisaatiokontekstin esimerkki ovat tiedonhallintayksiköt, joilla ei välttämättä ole erillistä organisaatiorakennetta taustallaan, mutta joiden lakisääteisen tehtävän kautta määrittyy tarve tehdä riskienhallintaa. Organisaation sisällä eri kontekstien tuottamien riskiarvioiden tulokset tulisi koota yhteen kattavan kokonaisriskienhallinnan tuottamiseksi. Vaihdettaessa riskitietoa on organisaatiokontekstin vaihtuessa – etenkin organisaatioiden välillä – riskeihin liittyvät oletukset ja suhteutukset tarkastettava ja uudelleenarvioitava uuden näkökulman kautta. Organisaatio voi joskus olla epätavallinen, esimerkiksi epävirallinen tai virtuaalinen, jolloin myös organisaatiokonteksti on erityislaatuinen.

12.2 Tiedonhallintayksikkö

Synonyymi: -

Määritelmä: *viranomainen tai viranomaisista koostuva organisaatiokonteksti, joka on velvollinen järjestämään tiedonhallintansa laissa julkisen hallinnon tiedonhallinnasta 906/2019 säädettyjen vaatimusten mukaisesti*

Huomautus: Tiedonhallintayksiköitä ovat valtion virastot ja laitokset; tuomioistuimet ja valitusasioita käsittelemään perustetut lautakunnat; eduskunnan virastot; valtion liikelaitokset; kunnat; kuntayhtymät; itsenäiset julkisoikeudelliset laitokset; yliopistolaissa tarkoitetut yliopistot sekä ammattikorkeakoululaissa tarkoitetut ammattikorkeakoulut (Tiedonhallintalaki 906/2019 2 luku § 4).

Tiedonhallintayksikkö on riskienhallinnan yksi erityisesti määritelty organisaatiokonteksti, joka arvioi käsittelemäänsä tietoon liittyviä riskejä.

12.3 Katsantotaso

Synonyymi: -

Määritelmä: *taso, jonka näkökulmasta riskiä tarkastellaan*

Huomautus: Riskiä voidaan tarkastella esimerkiksi strategisesta, koordinoivasta tai toiminnallisesta katsantotasosta, jos tällainen tasojaottelu on käytössä. Tarkastelussa pyritään tunnistamaan riskin merkitys kyseisellä tasolla suhteuttaen sitä mm. kyseisen tason toimintaan, tavoitteisiin ja vaikutusmahdollisuuksiin.

12.4 Käsittelytaso

Synonyymi: -

Määritelmä: taso, jolla riski käsitellään

Huomautus: Riskiä voidaan käsitellä esimerkiksi strategisella, koordinoivalla tai toiminnallisella käsittelytasolla, jos tällainen tasojaottelu on käytössä. Käytännössä samaa riskiä käsitellään tarpeen mukaan usealla eri tasolla, jotta riskin käsittely ei jää vaillinaiseksi.

12.5 Strateginen taso

Synonyymi: -

Määritelmä: *organisaation päätöksenteon taso, jolla tehdään toimintaympäristöön ja toiminnan rahoittamiseen liittyvät, koko organisaation toimintaa ja kehittämistä koskevat päätökset*

Huomautus: Riskienhallinnassa riskin katsantotaso tai käsittelytaso voi olla strateginen: strategisella katsantotasolla tarkastellaan riskejä koko organisaation kannalta, ja strategisella käsittelytasolla riskejä käsitellään tästä näkökulmasta käsin.

12.6 Koordinointitaso

Synonyymi: koordinoiva taso; organisatorinen taso

Määritelmä: *organisaation päätöksenteon taso, jolla strategisen tason päätökset huomioiden tehdään yksittäisten liiketoiminta-alueiden ja yksiköiden toiminnan järjestämistä koskevat päätökset*

Huomautus: Organisaation koosta ja järjestäytymistavasta riippuen koordinointitasoa ei välttämättä ole mahdollista tai mielekästä erottaa toiminnallisesta tasosta. Riskienhallinnassa riskin katsantotasona tai käsittelytasona voi olla koordinointitaso: koordinoivalla katsantotasolla tarkastellaan riskejä kokonaisten liiketoiminta-alueiden tai yksiköiden toiminnan kannalta, ja koordinoivalla käsittelytasolla riskejä käsitellään tästä näkökulmasta käsin. Päätöksenteon tasoja eroteltaessa käytetään usein termejä strateginen, taktinen ja operatiivinen taso, mutta erityisesti taktinen ja operatiivinen saavat eri yhteyksissä hyvinkin erilaisia merkityksiä, jotka eivät vastaa tässä esitettyä jaottelua eivätkä siis ole synonyymisiä koordinointitasolle ja toiminnalliselle tasolle.

12.7 Toiminnallinen taso

Synonyymi: tuotantotaso

Määritelmä: *organisaation päätöksenteon taso, jolla strategisen tason ja koordinointitason päätökset huomioiden tehdään toteutusta ja toimeenpanoa koskevat päätökset*

Huomautus: Riskienhallinnassa riskin katsantotaso tai käsittelytaso voi olla toiminnallinen: toiminnallisella katsantotasolla tarkastellaan riskejä toteutuksen ja toimeenpanon kannalta, ja toiminnallisella käsittelytasolla riskejä käsitellään tästä

näkökulmasta käsin. Päätöksenteon tasoja eroteltaessa käytetään usein termejä strateginen, taktinen ja operatiivinen taso, mutta erityisesti taktinen ja operatiivinen saavat eri yhteyksissä hyvinkin erilaisia merkityksiä, jotka eivät vastaa tässä esitettyä jaottelua eivätkä siis ole synonyymisiä koordinointitasolle ja toiminnalliselle tasolle.

13 Aihealue: Riskienhallinnan ja riskien merkityksiä

Käsitteet: ennakointi, jäännösriski, kriittisyys, riskinkantokyky, riskitietoinen päätöksenteko, toteutumattoman vaikutuksen arvo

Riskienhallinnan yksi yleinen tarkoitus on tuottaa ennakkovaroituksia mahdollisista ongelmista, jotta ne voidaan ottaa ajoissa huomioon. Tästä näkökulmasta riskienhallinta on osa tulevaisuuden kehityskulkujen tutkimiseen liittyvää ennakointityötä. Ennakointityö on kuitenkin laajempi tehtäväalue, sillä se käsittelee myös yleisempiä kehityskulkuja ja sen aikahorisontti (tai aikaikkuna) on yleensä selvästi pidemmällä tulevassa, kuin mitä riskienhallinnassa. Riskienhallinta on lyhytkestoisempaa ja pääasiassa sen käyttö rajoittuu tämänhetkisen strategisen näkymän kanssa yhtä pitkälle, mikä voi vaihdella.

Ennakointityötä tehdään pääasiassa tuottamaan tietoa ja taustoitusta uusien strategioiden luontiin, eli siihen mitä nykyisten jälkeen tehdään. Tarkoitus on ymmärtää toimintaympäristöjen muutokset ja näiden vaikutukset. Luodut vaihtoehtoiset tulevaisuudenkuvat perustuvat yleensä verrattain heikompiin signaaleihin mahdollisuuksista, kuin mitä riskienhallinnassa tavallisesti käytetään. Näkökulma on usein noin vuosikymmenen tai pari eteenpäin, mutta samalla yleensä valottuu myös kehityskulku sinne. Ennakointityö tuottaa siis syötteitä myös riskienhallinnan taustalle, jotta riskejä voidaan arvioida suhteessa tuleviin muutoksiin ja tarpeisiin.

Aikajanan toista päätä tarkasteltaessa, vaikka varsinaista alarajaakaan ei voida asettaa, riskienhallinnan tarkasteluprosessin läpivientiin käytetty aika – eli miten kauan erilaisten ja -tasoisten riskien havaitsemiseen ja käsittelyyn menee aikaa – määrittelee sen hyödyllisyyttä nykyisyydessä. Aika vaihtelee luonnollisesti sen mukaan minkä tasoisesta uhasta on kyse. Riskienhallintaprosessin ja -järjestelmän tehokkuus ja riittävän nopea syklisyys ovat riskienhallinnan johtamisen kannalta oleellisia asioita.

Uhat, jotka realisoituvat nopeammin, kuin mitä ne ehditään havaitsemaan ja käsittelemään, on hallittava ennakoinnin sijaan reagointina akuuttiin tapahtumaan. Mikäli riskienhallinnan tuottama ennakointi ei ole riittävää, akuutteina kohdattavat tilanteet voivat muodostaa kriisin, mikäli ne ylittävät valmiuteen varatut resurssit. Tätä voidaan ajatella niin havainnointikyvyn puutteena, riskinä riskienhallinnan riittämättömyydestä, kuin myös tavallisesti jatkuvuudenhallintaan kuuluvana varautumisena.

Organisaation omatessa riittävän ymmärryksen riskienhallintajärjestelmänsä kyvykkyydestä, se voi luottavaisemmin mielin hyväksyä ja kantaa jäännösriskejä, sillä näihin sisältyy vähemmän epävarmuutta. Kaikkea ei kuitenkaan voida käsitellä tai tietää, joten epävarmuuden sietäminen sekä pyrkimys niitä aiheuttavien tekijöiden tunnistamiseen ja ymmärtämiseen on osa riskienhallintaa ja johtamista. Riskiä jää jäljelle käytännössä aina ja se pitää jaksaa kantaa, niin henkisesti kuin kykynä tarvittaessa toimia jopa pahimman vaihtoehdon toteutuessa.

Ennakointi ja riskienhallinta tuottavat tietoa päätöksentekoon, jolla ohjataan organisaation toimintaa. Kuten on huomautettu, riskienhallinnan tuottama tieto on vain osa päätöksentekoon tuotetusta tiedosta. Hyvä riskitieto antaa vahvat perusteet toimia ja hallintakeinojen suunnitelmissa tulisi olla vaihtoehtoja, joiden avulla muodostetaan

parhaiten muihin tarpeisiin sopiva päätös. Tätä on hyvä riskitietoinen päätöksenteko yleisellä tasolla.

Päätöksentekoa joissain tapauksissa helpottaa, kun käsiteltävä asia voidaan katsoa erityisen tärkeäksi, sillä silloin valinta on mustavalkoisempi. Asianmukaisesti määritellyn kriittiseksi tunnistetun asian etu on, että tästä ollaan etukäteen tietoisia. Joskus kuitenkin riskin kohteen merkitystä saatetaan alleviivata liittämällä siihen kriittisen leima kevyin perustein. Tässä onkin tarkastettava, käsitelläänkö asiaa tasolla, jossa puhutaan olemassaoloa uhkaavista vaikutuksista vai vaikutuksista, joiden seurauksena menetetään jokin etu tai ominaisuus, kuten toiminnan häiriintyminen tai kyky muuten toimia normaalilla tavalla (verrattuna siihen, että toiminta jouduttaisiin lopettamaan).

Tarkempi tarkastelu voi siis tuoda esiin kriittisyyden asteita, mikä voi olla kyseisen käsitteen suhteen näennäisen epäloogista. Kriittisyyskin voidaan kuitenkin asettaa alisteiseksi tavoitteille, jolloin pelkkä minimaalisen säilymisen ei katsota riittävän, vaan on kyettävä säilyttämään jokin määritelty toiminnan taso, jonka menetys vertautuu katastrofiin. Organisaatiot voivat siis (erityisesti julkisessa hallinnossa) perustellusti määritellä tietyt toimintaansa mahdollistavat asiat kriittisiksi – etenkin, mikäli monen muun toimijan toimintakyky on tästä riippuvainen. Kriittisyyden määrittelyn perusteiden tulisi kuitenkin olla selkeitä ja läpinäkyviä.[16]

Oletettujen tapahtumien toinen puoli on, että hyvällä riskienhallinnalla pystytään ennakolta välttämään ainakin ikävimmät seuraukset tai jopa seuraukset kokonaan. Tapahtumatonta on kuitenkin usein mahdoton todentaa tai löytää suoraa syytä sille, miksi jotain ei tapahtunut. Tämä tekee haastavaksi määrittää toimenpiteille arvoa, sillä taloudelliset seikat ovat merkittävä osa päätöksenteon perusteita. Keskeinen ajatus on, että turvallisuuden arvo, myös digissä, on siinä, miten se tukee tavoitteiden saavuttamista. Tästä voidaan johtaa tapa perustella myös riskienhallinnan merkitys.

Mikäli halutaan arvioida euromääräisiä arvoja riskeille, tähän on kaksi päätapaa. Ensimmäisessä tarkastellaan potentiaalisia menetyksiä riskiskenaarion toteutuessa ja toisessa sen ehkäisemiseksi tarvittavien toimien (investointien) arvoa. Näitä ei tule sekoittaa, sillä molemmat ovat arvioita eri näkökulmista. Kumpikin tuottaa luvun, mutta laskutapoja on useita. Niissä tulisi huomioida, että se mahdollisuuksien mukaan kuvastaa organisaation digiturvallisuuden toimintatapoja ja rakenteita, jotta sillä olisi edes indikoiva yhteys tämän alueen hallintaan. Erikseen on huomioitava, että julkisen ja yksityisen puolen arvon määrittelyssä on eroja muun muassa laillisten velvoitteiden kautta, mikä vaikuttaa myös tapaan arvioida riskejä ja puhua niistä.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että ymmärretään riskienhallinnan merkitys organisaation päätöksenteossa ja johtamisessa. Jäännösriskin käsittely ja hyväksyminen on keskeinen osa tätä. Organisaation ja sen vastuullisten osien tulisi olla tietoisia omista riskeistään, niiden jäännösosista sekä riskinkantokyvystä ja siihen vaikuttavista tekijöistä, jotta ne voidaan huomioida toiminnassa.

[16] VAHTI Hyvät Käytännöt -tukimateriaaleissa on julkaistu kriittisyydenarviointiin työkalu, jota kehitetään seuraajaksi aiemmille Palko- ja BIA-työkaluille. Sen käyttö ei ole välttämätöntä, mutta tunnistaminen voi auttaa kohdentamaan riskienhallintaa. Kriittisten kohteiden luokittelu https://dvv.fi/digiturvajulkaisut

13.1 Ennakointi

Synonyymi: -

Määritelmä: *organisaation toiminnan ja toimintaympäristön muutossuuntien arviointi sekä potentiaalisten kehityskulkujen edellytysten selvittäminen*

Huomautus: Siinä missä riskienhallinnassa tuotetaan tyypillisesti yksityiskohtaista ja käytännönläheistä tietoa suhteellisen rajatuista aiheista ja melko lyhyen aikajänteen näkökulmasta, ennakoinnilla pyritään hahmottelemaan pitkän aikavälin trendejä ja laajojen kokonaisuuksien muutossuuntia. Ennakoinnilla voidaan tunnistaa uhkia ja mahdollisuuksia sekä tapoja vaikuttaa niihin, ja näitä tietoja voidaan hyödyntää edelleen riskienhallinnassa. Ennakointi ei aina ole kokonaisvaltaista, vaan se voi keskittyä esimerkiksi yhden toiminnon tai yhden projektin näkökulmaan. Puhekielessä ennakoinnilla voidaan tarkoittaa paitsi arvioiden ja selvitysten tuottamista, myös niiden pohjalta tehtävää toimintaa.

13.2 Riskitietoinen päätöksenteko

Synonyymi: *riskiperusteinen päätöksenteko*

Määritelmä: *päätöksenteko, jossa on huomioitu riskien arviointiprosessin tuloksi*

Huomautus: Riskitietoinen päätöksenteko ei ole pelkkään riskien arviointiprosessiin perustuvaa päätöksentekoa, vaan päätöksenteossa tulee aina huomioida muitakin tietoja ja näkökulmia, kuten tavoitteet ja muu toiminta. Päätöksentekijöillä on hyvä olla käsitys hyödyntämiensä riskitietojen alkuperästä ja laadusta.

13.3 Jäännösriski

Synonyymi: -

Määritelmä: *riskin käsittelyn jälkeen jäljellä oleva riski*

Huomautus: Jäännösriskillä voidaan tarkoittaa sitä osaa alkuperäisestä riskistä, joka jätetään suunnitellusti hallintatoimien kattaman ulkopuolelle, jolloin voidaan puhua myös riskin säilyttämisestä. Toisaalta jäännösriski ei aina ole käytettävissä olevin keinoin poistettavissa tai siihen voi sisältyä tunnistamatonta riskin osaa, joka voi tulla ilmi vasta riskin toteutuessa. Riskienhallintaprosessissa tunnistetut jäännösriskit tulee hyväksyä tai jatkokäsitellä. Jäännösriskejä arvioitaessa huomioidaan riskinkantokyky esimerkiksi riskeille määriteltyjen raja-arvojen avulla.

13.4 Riskinkantokyky

Synonyymi: riskin kantokyky

Määritelmä: *organisaation kyky sopeutua mahdollisesti toteutuvien riskien seurauksiin*

Huomautus: Riskinkantokyvyllä viitataan yleensä taloudelliseen kantokykyyn, mutta seurauksia voidaan tarkastella myös esimerkiksi maineen tai henkilöstön

hyvinvoinnin näkökulmasta. Riskinkantokyky määrittää ne rajat, joiden puitteissa organisaatio voi ottaa riskejä. Yhdenkään organisaation riskinkantokyky ei ole täydellinen, mutta organisaatio voi selvitä monenlaisten riskien ja niiden yhdistelmien seurauksista. Erityisesti jäännösriskeistä päätettäessä on tärkeää tietää, millaiset riskit tai riskien yhdistelmät uhkaavat organisaation olemassaoloa.

13.5 Kriittisyys

Synonyymi: -

Määritelmä: *välttämättömyys tavoitteiden saavuttamiseksi tai erityisen haitallisten seurausten välttämiseksi*

Huomautus: Kriittisyyttä tarkastellaan riskienhallinnassa yleensä organisaation näkökulmasta, mutta näkökulmana voi olla myös esimerkiksi asiakas, projekti, prosessi, yhteistyöverkosto, kansalaiset tai yhteiskunnan toiminnot. Kriittinen asia, esimerkiksi kriittiseksi tunnistettu järjestelmä, vastaa sen selviytymisen ja jatkuvuuden kannalta keskeisiin tarpeisiin, jonka näkökulmasta se on kriittinen. Kriittisyydelle voidaan joissain yhteyksissä erotella tyyppejä tai tasoja, jolloin kaikki kriittisyydet eivät välttämättä liity selviytymiseen sinällään, vaan esimerkiksi toiminnan mielekkyyteen, tiettyjen kyvykkyyksien säilymiseen tai keskeisen panostuksen menettämiseen.

13.6 Toteutumattoman vaikutuksen arvo

Synonyymi: tapahtumattoman vaikutuksen arvo

Määritelmä: *vältetyn riskin vaikutuksen käänteinen arvo, jonka avulla voidaan kuvata riskienhallinnan vaikuttavuutta*

Huomautus: Toteutumattomien vaikutusten arvojen avulla voidaan kuvata riskienhallinnan kustannustehokkuutta ja sitä, vastaako se tavoitteita. Samassa yhteydessä voidaan huomioida, mikä arvo menetetyillä mahdollisuuksilla olisi ollut. Erityisesti välillisten riskien tapauksessa suuntaa antava arvio on yleensä riittävä. Tapahtumattoman vaikutuksen arvoa ei aina ilmaista rahamääräisesti, vaan se voi olla esimerkiksi maineeseen tai organisaation yhteiskunnalliseen tehtävään liittyvä.

14 Aihealue: Riskin rakentumisen ominaisuuksia

Käsitteet: ketjuuntunut riski, kumulatiivinen riski, verkottunut riski, välillinen riski, välitön riski

Nykyaikainen näkemys digitaalisesta toimintaympäristöstä kattaa sosio-teknisen rakenteen, jossa laitteiden ja verkkojen lisäksi kompleksiseen kokonaisuuteen luetaan mukaan ihminen ja tämän toiminta. Tätä on myös kuvattu VUCA-ajaksi, mikä tulee englanninkielisistä sanoista muutosherkkyydelle, epävarmuudelle, kompleksisuudelle ja tulkinnanvaraisuudelle (Volatility, Uncertainty, Compleksity, Ambiquity). Se kuvaa, miten toimintaympäristö(t) voivat muuttua nopeasti, arvaamattomilla tavoilla, vaikuttaen kompleksisten keskinäisriippuvuuksien kautta sekä ollen monitulkintaisia. Tämä haastaa sekä riskienhallinnan, että muutenkin tulevan ennakoinnin. Monimutkaiset vaikutusrakenteet vaativat enemmän niiden ymmärtämiseksi, nopeutuvaa muutostahtia varten tarvitaan riittävän usein tehtävää uudelleenarviointia, nopeisiin muutoksiin on pidettävä yllä kykyä reagoida nopeasti ja monitulkintaisuus lisää tarvetta osata tulkita eri kontekstien näkemyksiä sekä viestiä nämä huomioiden.

Selkeät välittömät riskit voidaan ottaa joskus itsestäänselvyyksinä. Ne voivat edelleen olla riskilistojen kärjessä, mutta suoraviivaisina vaikutusten ja hallintakeinojen suhteen, ne saattavat kiinnostaa vähemmän. Tällöin on syytä tarkastella, mitä sivuvaikutuksia ja näistä syntyviä odottamattomia seurauksia voisi syntyä riskin toteutuessa – erityisesti, mikäli samaan aikaan toteutuu jokin toinen riski. Hyökkäyksissä pyritään löytämään keinoja toteuttaa tunkeutuminen yksinkertaisella tavalla, sillä usean kontrollin ohittaminen on haastavaa. Erilaisten kombinaatioiden määrä voi olla liian suuri täydelliselle kattavuudelle, jolloin on kehitettävä tapoja ja työkaluja seuloa merkittävimmät ja todennäköiset jatkokäsittelyä varten.

Vaikutusketjujen domino-ilmiöt voivat siirtää riskiä ja vaikutuksia toisilta toimijoita tai järjestelmien välillä odottamattomasti. Erityisesti ulkoisia palveluita käytettäessä tulisi yhteistyötahojen kanssa olla toimivat kommunikaatioyhteydet, jotta osapuolet ovat tietoisia toistensa merkittävistä riskeistä sekä niihin liittyvistä kontrolleista ja riskinkantokyvystä. Suoria ketjuja monimutkaisempia ovat verkottuneet vaikutukset, joissa ilmiöt voivat vaikuttaa erikoisemmilla tavoilla, esimerkiksi usean pienemmän tapahtuman kautta, joiden yhteinen vaikutus on merkittävästi suurempi. Näihin odottamattomasti kehkeytyviin ilmiöihin liittyy usein kerrannaisvaikutus tai skaalautuminen kokoluokkaan, joka ei ole normaalin varautumisen tai järjestelmän rajojen sisällä käsiteltävissä. Samaan aikaan hallintakeinoissa tulisi ottaa huomioon, mitä sivuvaikutuksia niillä voi olla verkostossa ja miten ne voivat vaikuttaa muihin.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että ymmärretään riskien erilaiset tavat rakentua ja miten vaikutukset voivat siirtyä epätavallisilla tavoilla. Koska jokaisella toimella ja tapahtumalla on sivuvaikutuksia omaan tai muiden tilanteeseen, tulisi pyrkiä ennakkoon tarkastelemaan näitä sopivimman valitsemiseksi. Jatkuvan muutoksen vuoksi on syytä uudelleenarvioida riskejä ja toimintaympäristöä riittävän usein.

14.1 Välitön riski

Synonyymi: suora riski

Määritelmä: *riski, jonka lähde vaikuttaa suoraan kohteeseen*

Huomautus: Organisaatiossa välittömän riskin vaikutuspiiriin kuuluvat mm. organisaatiossa työskentelevät työntekijät sekä organisaation käytössä olevat laitteet ja materiaalit. Välitön riski voi vaikuttaa myös organisaatiorajojen yli.

14.2 Välillinen riski

Synonyymi: epäsuora riski

Määritelmä: *riski, jonka lähde vaikuttaa epäsuorasti kohteeseen*

Huomautus: Välilliset riskit ovat usein välittömiä riskejä vaikeampia tunnistaa ja hallita. Välillinen riski voi johtua ketjuuntumisesta (ks. ketjuuntunut riski), verkostoista (ks. verkottunut riski) tai toimintaympäristön rakenteellisesta muutoksesta.

14.3 Ketjuuntunut riski

Synonyymi: -

Määritelmä: *välillinen riski, joka on siirtynyt toiselta kohteelta*

Huomautus: Ketjuuntunut riski voi siirtyä dominoilmiönä monien kohteiden kautta tarkasteltavalle kohteelle. Riskin siirtyessä sen toteutumisen todennäköisyys ja seuraukset voivat muuttua.

14.4 Verkottunut riski

Synonyymi: verkostomainen riski

Määritelmä: *välillinen riski, jonka lähteenä on monimutkaisten vaikutusketjujen verkosto*

Huomautus: Verkottunut riski on usein seurausta toimintaympäristön kompleksisuudesta. Toisin kuin ketjuuntuneella riskillä, verkottuneen riskin vaikutukset voivat esimerkiksi haarautua ja monistua (skaalautua), eikä niiden alkuperä ole useinkaan tunnistettavissa. Verkottuneiden riskien käyttäytymistä on tyypillisesti mahdotonta täysin ennustaa.

14.5 Kumulatiivinen riski

Synonyymi: kasautuva riski

Määritelmä: *riski, jonka suuruus muodostuu useiden riskitekijöiden yhteisvaikutuksista*

Huomautus: Kumulatiivisen riskin vaikutus voi olla riskitekijöiden vaikutusten summa, mutta usein riskitekijät vuorovaikuttavat siten, että yhteisvaikutus on tätä suurempi. Esimerkiksi yksittäisiin henkilötietoihin ei yhteenlaskettuna liity yhtä merkittäviä riskejä kuin näistä henkilötiedoista koostuvaan laajaan tietokantaan.

15 Aihealue: Riskeihin vaikuttaminen

Käsitteet: kontrolli, toiminnallinen käytettävyys, vähäriskiseksi suunniteltu

On tärkeää tietää uhista ja tunnistaa riskit, mutta riskienhallintaa tehdään, jotta riskejä voitaisiin hallita, eli toteuttaa hallintatoimia niiden käsittelemiseksi. Erilaisia kontrolleja on monia. Vain harva niistä nykyisissä kompleksisessa toimintaympäristöissä yksi yhteen täydellinen ja ainutlaatuinen vastinparina olevan riskin kanssa. Kontrollit voivat, kattaa useita riskejä kerralla, mutta myös tuottaa sivuvaikutuksinaan haittaa muulle toiminnalle sekä kattaa vain vaillinaisesti osan riskistä. Tämän vuoksi on osattava valita kontrollien kokonaisuus, jossa useat yhdessä tuottavat riittävän kattavan ja aukottoman suojan vaikutuksilta, ilman liioiteltua päällekkäisyyttä. Toisaalta, juuri päällekkäisyys tuottaa syvyyttä ja siten varmuutta hallintakeinoihin.

Kontrollien takana ovat teoreettiset riskienkäsittelytavat, joita voidaan usein yhdistellä. Riski voidaan torjua lopettamalla jokin toiminta tai olemalla aloittamatta toimintaa, jolloin ei myöskään oteta riskiä. Riskin kohdistumisen maalitaulu tai haavoittuvuus, jota se käyttää kanavanaan, voidaan poistaa. Riskin toteutumisen todennäköisyyttä voidaan muuttaa eri tavoin, samoin kuin sen vaikutuksia. Riski voidaan myös jakaa tai siirtää sopimuksilla tai vakuutuksilla jollekin kolmannelle osapuolelle. Riski voidaan, pitää, ottaa tai sitä voidaan jopa kasvattaa entistä suuremmaksi, mikäli siinä nähdään riittävästi tavoiteltavaa ja hyödynnettävissä olevaa. Viemällä tätä pidemmälle, yksi erityinen lähestyminen hallintakeinojen joukossa on pyrkimys muuttaa niitä mahdollisuuksiksi ja vaikutuksiltaan positiivisiksi lopputulemiksi. Siinä voidaan innovoida uutta ja sopeuttaa olemassa olevaa. Mitä enemmän näin vielä tuetaan laajempia tavoitteita, sen parempi. Tällöin digiturvallisuus muuttuu mahdollistajaksi.

Erityinen sovellus riskien hallitsemiseksi ovat jo etukäteissuunnittelussa sovelletut periaatteet, joilla pyritään tuottamaan laitteita ja järjestelmiä, joista on pyritty poistamaan keskeiset riskiä luovat ominaisuudet. Tämän ilmauksen kääntämiseen englannista ei ole suoraviivaista, sillä sille puuttuu selkeä vastine (security by design). Huomioiden erityisesti tietosuojan, tämän rinnalle on muodostunut myös muun muassa vastaava yksityisyydestä huolehtimisen periaate (privacy by design) sekä lähtökohtaisesti turvallisen ja yksityisen periaatteet (security by default, privacy by default). Puhuttaessa organisaatioiden järjestelmien riskeihin vaikuttamisesta, mahdollisesti joukkoon tulisi lisätä hallittavaksi ja kontrolloiduksi suunnittelu.

Esiin voitaisiin nostaa useita näkökulmia kontrolleihin liittyen. Yksi on toiminnallinen käytettävyys, jonka puute erityisesti tulee esiin monissa turvallisuuden toteutuksissa, joissa ei ole huomioitu käyttäjää riittävässä määrin. Huono toiminnallinen käytettävyys ohjaa kohti vääränlaista käyttöä ja toimintaa, päinvastoin, kuin mitä on mahdollisesti yritetty estää. Käyttöliittymien monimutkaistuessa on ihmisen – etenkin stressaavissa tilanteissa – mahdollista jopa sivuuttaa turvallisuuteen liittyvät toimet. Tätä voidaan tulkita sen kautta, että käyttäjät ovat valmiit käyttämään vain rajallisesti aikaa ja vaivaa turvallisuuden eteen. Voidaan siis törmätä siihen, että käyttäjät kokevat kuilun tarpeellisiksi katsottujen hallintakeinojen sekä saaduksi koetun turvallisuuden välillä.

On myös muistettava, että oli prosessimme, järjestelmämme tai tuotteemme kuinka turvallinen tahansa ominaisuuksiltaan, raskas tai muuten huono käytettävyys voivat

rampauttaa tai vinouttaa niiden käytön. Viestintään nämä liittyvät epäsuorasti. Hyvin suunniteltu ja käytettävä kokonaisuus, jonka tarkoitus ymmärretään ja joka ei tuota riskejä, tarvitsee vähemmän viestintää tuekseen esimerkiksi ohjeiden, selitysten ja motivoivien viestien avulla.

Näiden termien tehokas ja tarkoituksenmukainen käyttö tarkoittaa, että riskien kontrolloimiseksi kehitettävien hallintakeinojen taustalla vaikuttavat periaatteet on ymmärretty. Hallintatoimenpiteitä suunniteltaessa olisi syytä pyrkiä ottamaan ensisijaisesti huomioon toteutustavat, joissa riskin kehittymiselle ei ensinnäkään anneta sijaa, minkä lisäksi turvallisin vaihtoehto on jo oletusarvoisesti käytössä.

15.1 Kontrolli

Synonyymi: hallintakeino; hallintatoimi

Määritelmä: *toimenpide, jolla pyritään muuttamaan riskiä tai säilyttämään se*

Huomautus: Kontrollit voivat olla prosesseja, toimintaperiaatteita, laitteita, käytäntöjä, kertaluonteisia toimenpiteitä tai muun tyyppistä toimintaa. Ennakkoon tehtävät kontrollit pyrkivät yleensä pienentämään riskien todennäköisyyttä, kun taas jälkikontrolleilla pienennetään riskien vaikutusta. Termiä hallintakeino käytetään joskus kontrollin synonyyminä, mutta usein hallintakeino viittaa kokonaisratkaisuun (esim. tunnistautuminen tai hyvä hallintotapa), joka voi sisältää useita konkreettisia kontrolleja. Kontrolleja voidaan tarkastella tyypeittäin tai suojeltavan kohteen mukaan, esimerkiksi valvontatoimenpiteet eli valvontakontrollit omana ryhmänään tai tiedon saatavuutta suojaavat kontrollit kokonaisuutena.

15.2 Vähäriskiseksi suunniteltu

Synonyymi: riskit minimoivaksi suunniteltu; sisäänrakennettu riskien minimointi

Määritelmä: *tuotteelle, palvelulle tai prosessille etukäteen suunniteltu ominaisuus tai toteutustapa, jossa tietyt sille ominaiset riskit on huomioitu*

Huomautus: Suunnittelussa huomioidaan yleensä jonkin riskityypin riskit, kuten tietosuojariskit (eng. privacy by design) tai laajemmin turvallisuusriskit (eng. safety by design, security by design). Esimerkiksi kyselyssä voidaan välttää kysymyksiä, joiden vastauksiin liittyy tietoturva- tai tietosuojariskejä, jos niiden kerääminen ei ole välttämätöntä. Jos kuitenkin kerätään tietoja, joihin liittyy tietoturvariskejä, voidaan keräys toteuttaa niin, että kaikki tiedot kulkevat suojattuina viesteinä ja talletetaan tietoturvallisesti sen sijaan, että tietoja kerättäisiin vaikkapa pahviseen keräyslaatikkoon julkisessa tilassa. Lisäksi kulku- ja käyttöoikeuksien hallinta voidaan suunnitella vähäriskiseksi esimerkiksi siten, että tiettyjen oikeuksien antamiseen vaaditaan useamman henkilön suostumus. Jos erilaisten tarpeiden takia tuotteessa tai prosessissa on sallittava myös vaihtoehtoja, joissa riskejä ei ole minimoitu, samankaltainen vaikutus voidaan saada aikaan siten, että vähäriskisin vaihtoehto on aina oletusarvona (eng. security by default, privacy by default jne.), kun taas riskien ottaminen vaatii erillisiä toimia.

15.3 Toiminnallinen käytettävyys

Synonyymi: -

Määritelmä: *tietojärjestelmän, laitteen tai prosessin ominaisuus, joka ilmentää sitä, että se on helposti opittava, sen toimintalogiikka on helposti muistettava, sen toiminta tukee niitä tehtäviä, joita käyttäjän pitää sillä tehdä ja se edistää sen turvallista ja helppoa käyttöä*

Huomautus: Puutteet toiminnallisessa käytettävyydessä ovat heikkous: jos toiminnallisessa käytettävyydessä on puutteita, se voi lisätä virheellistä käyttöä, mikä puolestaan voi johtaa haavoittuvuuteen.

16 Hakemistot ja liitteet

Termien ja synonyymien hakemisto käännöksineen ruotsiksi ja englanniksi täydennetään asiakirjan kommentointiajanjakson jälkeen julkaistavassa versiossa

16.1 Suomi

Termit ja synonyymit	Päätermi	Sivu
alustava arvio	Alustava arvio	32
arvio riskien merkityksestä	Riskiarvio	33
arvio riskien vaikutuksesta	Riskiarvio	33
arvio riskin merkityksestä	Riskiarvio	33
arvio riskin vaikutuksesta	Riskiarvio	33
digiriski	Digitaalisen toiminnan riski	18
digitaalinen riski	Digitaalisen toiminnan riski	18
digitaalinen toimintaympäristö	Digitaalinen toimintaympäristö	18
digitaalinen turvallisuus	Digitaalinen turvallisuus	18
digitaalinen ympäristö	Digitaalinen toimintaympäristö	18
digitaalisen toiminnan riski	Digitaalisen toiminnan riski	18
digitoimintaympäristö	Digitaalinen toimintaympäristö	18
digiturvallisuus	Digitaalinen turvallisuus	18
ennakointi	Ennakointi	55
ensiarvio	Alustava arvio	32
ensiöarvio	Alustava arvio	32
epäsuora riski	Välillinen riski	58
epävarmuus	Epävarmuus	25
haavoittuvuus	Haavoittuvuus	26
hallintakeino	Kontrolli	61
hallintatoimi	Kontrolli	61
heikkous	Heikkous	26
hyökkäyksen aiottu kohde	Hyökkäyksen aiottu kohde	21
hyökkäys	Hyökkäys	21
häiriö	Häiriö	21
jatkoarvio	Tarkentava arvio	32
jatkuvuuden hallinta	Jatkuvuudenhallinta	22
jatkuvuudenhallinta	Jatkuvuudenhallinta	22
jäännösriski	Jäännösriski	55
kasautuva riski	Kumulatiivinen riski	58
katsantotaso	Katsantotaso	50
ketjuuntunut riski	Ketjuuntunut riski	58
kontrolli	Kontrolli	61
koordinointitaso	Koordinointitaso	51
koordinoiva taso	Koordinointitaso	51
kriittisyys	Kriittisyys	56
kumulatiivinen riski	Kumulatiivinen riski	58

Termit ja synonyymit	Päätermi	Sivu
riskin merkityksen arviointi	Riskien arviointi	33
riskin raja-arvoa välttelevä uhka	Riskin raja-arvoa välttelevä uhka	28
riskin raportointi	Riskiraportointi	39
riskin vaikutuksen arviointi	Riskien arviointi	33
riskinkantokyky	Riskinkantokyky	55
riskiperusteinen päätöksenteko	Riskitietoinen päätöksenteko	55
riskiraportointi	Riskiraportointi	39
riskirekisteri	Riskirekisteri	39
riskit minimoivaksi suunniteltu	Vähäriskiseksi suunniteltu	61
riskitekijöiden seuranta	Riskien seuranta	45
riskitieto	Riskitieto	39
riskitietoinen päätöksenteko	Riskitietoinen päätöksenteko	55
riskitilannekuva	Riskien tilannekuva	45
riskivastuullisuus	Riskivastuullisuus	36
sekundääriarvio	Tarkentava arvio	32
sisäänrakennettu riskien minimointi	Vähäriskiseksi suunniteltu	61
strateginen taso	Strateginen taso	51
suora riski	Välitön riski	58
tapahtuma	Tapahtuma	20
tapahtumattoman vaikutuksen arvo	Toteutumattoman vaikutuksen arvo	56
tarkentava arvio	Tarkentava arvio	32
tiedonhallintayksikkö	Tiedonhallintayksikkö	50
tietoturva	Tietoturvallisuus	19
tietoturvallisuus	Tietoturvallisuus	19
toiminnallinen käytettävyys	Toiminnallinen käytettävyys	62
toiminnallinen taso	Toiminnallinen taso	51
toiminnan jatkuvuuden hallinta	Jatkuvuudenhallinta	22
toisioarvio	Tarkentava arvio	32
toteutumattoman vaikutuksen arvo	Toteutumattoman vaikutuksen arvo	56
tuotantotaso	Toiminnallinen taso	51
uhka	Uhka	25
uhkaprofiili	Uhkaprofiili	40
uhkatieto	Uhkatieto	40
uudelleenarviointi	Uudelleenarviointi	32
verkostomainen riski	Verkottunut riski	58
verkottunut riski	Verkottunut riski	58
vinouma	Vinouma	27
vähäriskiseksi suunniteltu	Vähäriskiseksi suunniteltu	61
välillinen riski	Välillinen riski	58
välitön riski	Välitön riski	58

16.2 Svenska

-

16.3 English

-

16.4 Digitaalisen turvallisuuden kokonaisuuden yleinen määrittely

Erityisesti asiantuntijoiden ulkopuolella kuulee kysyttävän, kuinka digiturvallisuus eroaa kyber- tai tietoturvallisuudesta. Näitä termejä ei ole aikanaan luotu tai määritelty toistensa suhteen ja ajan saatossa ne ovat myös kehittyneet omillaan. Niiden toteuttamisessa on tehty joitain rajanvetoja käytännössä ja on erillisiä määritelmiä, mutta yksittäistä vastausta ei ole. Tässä sanastossa näitä on käsitelty riskienhallinnan rajatussa kontekstissa ja siten suuri osa kyseisten aiheiden eri muodoista, ilmenemistä, poikkeuksista ja ominaisuuksista jää määrittelyssä huomiotta.

Osittainen vastaus aiempaan kysymykseen on kuitenkin työstetty, perustuen sanaston määrittelytyöhön, mutta erityisesti sekä valtioneuvoston periaatepäätökseen[17] että OECD:n määrittelyyn[18]. Keskeistä on, miten nämä eri asia-alueet muodostavat digitaaliseen toimintaympäristöön liittyvän loogisen rakennekokonaisuuden turvallisuuden osa-alueelle ja tämä on asiantuntijaryhmän työhön perustuva näkemys siitä, miten digitaalisen turvallisuuden kokonaisuutta voidaan tulkita.

Kuva3: Digiturvallisuuden kokonaisuus tiivistyksenä, jossa painotetaan viiden keskeisen toteutusalueen muodostamaa kattavuutta, tarpeenmukaisesti määrittyviä rajauksia sekä täydentäviä toteutus- ja merkitysalueita. Digi- ja väestötietoviraston digiturvallisuuden toiminta keskittyy tässä kokonaisuudessa näiden osa-alueiden hallinnan kehitykseen ja tukeen, erityisesti strategisella- sekä koordinaatiotasolla.

Digitaalinen turvallisuus on laaja kattokäsite, joka kokoaa useita osa-alueita ja käsittelee näitä Suomen kontekstissa. Määrittelytavan rakenteen tarkoitus on antaa tilaa eri käsitteille kehittyä toimintatapojen ja tekniikan mukana, sillä näkökulmat turvallisuuteen ja digiin kehittyvät paljon jo vuosikymmenessä.

Digiturvallisuus ei keskity vain digitaaliseen toimintaympäristöön, vaan liittyy myös kaikkeen, mikä vaikuttaa digitaaliseen toimintaympäristöön sekä kaikkeen, mihin

[17] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162169/VM_2020_23.pdf
[18] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75412/OECD_julkaisu_NETTI.pdf

digitaalisesta toimintaympäristöstä vaikutetaan. Tämä voi tarkoittaa reaalimaailmaa tai abstraktimpia merkitysrakenteita, kuten luottamus, politiikka tai vapaa-aika. Siten, digiturvallisuus ulottuu itse digitaalista toiminta-aluetta laajemmalle.

Digiturvallisuuden kaikkia eri toteutusalueita, eli näkökulmia turvallisuuden aiheisiin, tarvitaan, jotta eri puolet tulevat katettua ja voidaan kohdata erityyppisiä haasteita. Viisi painopistettä on valittu julkisen hallinnon ohjauksessa digiturvallisuuden keskeisiksi toteutusalueiksi. Niiden muodostama kattavuus on nähty välttämättömäksi ja kaikki toimijat yhdistäväksi, jotta voidaan tuottaa uskottavaa ja hallittua digitaalista turvallisuutta. Lyhyesti ilmaistuna:

- Johtaminen ja riskienhallinta kytkevät eri osa-alueet hallittavaksi kokonaisuudeksi sekä liittävät ne muuhun johtamiseen ja toimintaan tavoitteellisella tavalla.
- Jatkuvuudenhallinnassa varaudutaan ennakolta sekä toimitaan häiriötilanteiden sattuessa niiden vaikutusten hallitsemiseksi.
- Kyberturvallisuudessa, jolla on puhekielessä ja kansainvälisesti monia merkityksiä, painotetaan verkottunutta ympäristöä, laajoja ilmiöitä, monimutkaisia vaikutuksia sekä vaikuttamista digissä ja digillä.
- Tietosuoja on yksityisyydensuojaa ja tietojen hallintaa - niin omien kuin toisten.
- Tietoturvallisuuden perinteinen fokus on tietojen luottamuksellisuus, saatavuus ja eheys sekä käyttövaltuudet ja kiistämättömyyden todentaminen.

Näiden viiden lisäksi digiturvallisuutta toteutetaan muillakin toiminnan alueilla, esimerkiksi sääntelyllä, standardeilla, eettisillä valinnoilla, osaamisen kehittämisellä, käytettävyyteen liittyvissä asioissa, vastuullisuusnäkökulmalla, fyysisten ilmiöiden rajoissa, viestinnän kentällä, teknologisissa valinnoissa, ohjelmistokehityksessä, hallinnon rakenteissa sekä muissa vastaavissa toteutuksen mahdollistajissa.

Digitaalinen toimintaympäristö ei ole tarkkarajainen. Kuten todettua, digillä voidaan vaikuttaa moneen asiaan sen ulkopuolella, mutta myös ulkomaailma voi vaikuttaa digiin. Rajanveto digin ja muiden toimintaympäristöjen välillä voi vaihdella kompleksisessa maailmassamme. Selkeää määritelmää ei ole myöskään toteutusalueiden sisällä. Niihin liittyy ulottuvuuksia, joita ei pääsääntöisesti lueta osaksi digiä tai digiturvallisuutta. Esimerkkejä toteutusalueiden ei-digitaalisista ulottuvuuksista:

- Johtamista ja riskienhallintaa tehdään myös muihinkin asioihin liittyen.
- On digin ulkopuolisiakin asioita, joiden jatkuvuuden varmistaminen on tärkeää.
- Kyberiin liitetään valtioiden välisiä ulottuvuuksia ja sodankäyntiä, joita ei tavallisesti käsitellä digiin keskittyvinä asioina.
- Tietosuojassa ja tietoturvallisuudessa tiedot paperilla eivät ole digitaalisia.

Rajanveto ei ole selvää ja sen määrittämistä on tehtävä tapauskohtaisesti, tavoitteisiin perustuen. Muun muassa, edellä mainitut paperit voivat olla osa digiturvallisuutta, kun huomioidaan tietoa luoneet järjestelmät, tulostimet ja tiedonsiirto niille. Määrittämisen joustavuudella varmistetaan, ettei asioita jää harmaalle alueelle, mutta myös huomioidaan muutokset tekniikassa ja toimintatavoissa.

Digiturvallisuus kattaa kaikki eri tasot, sekä yhdistää laajasti kaikki digissä toimijat ja siihen liittyvät asiat. Digiturvallisuus tulee huomioida osana muuta toimintaa.

16.5 EU:n tulevassa NIS2-direktiivissa käytetty riskienhallintatermistö

EU:ssa kehitteillä olevalla NIS2-direktiivillä[19] tulee olemaan vaikutuksia digiturvallisuuteen ja sen riskienhallintaan erityisesti infrastruktuuriin liittyen. Siinä on viitattu riskiperusteisuuteen sekä muutamiin muihin sanastossa esiin nostettuihin termeihin määrittelemättä niitä kuitenkaan tyhjentävästi. Sen voidaan katsoa täydentävän eri tapoja soveltaa ilmaisuita, erityisesti omassa kontekstissaan, ja näistä on hyvä olla tietoinen.

Riski tarkennetaan NIS2:ssa sanastossa käytettyä ilmaisua konkreettisemmaksi tapahtumaksi, jota kuitenkin käsitellään samalla tavoin, kuin mitä sanastossa ja standardeissa. NIS2 viittaa uhkien alakategoriaan, kyberuhkiin, määritellyllä tavalla[20], jota täydennetään ”merkittävillä kyberuhilla” (significant cyber threat). Selkeä poikkeama määrittelyssä on vain haavoittuvuuden ja heikkouden kohdalla, sillä direktiivin työstöversiossa (loppuvuodesta 2021) nämä määritellään samaksi, kun taas sanastossa tunnistetaan mahdollisuus heikkoudelle, ilman että se välttämättä olisi haavoittuvuus, tai ainakaan vielä sellaiseksi kehittynyt, millä voidaan välttää yksioikoinen tulkinta. Huomioitava on myös direktiivin esiin ottama ”läheltä-piti” -tilanteen määritelmä, joka sanastossa nähdään ”tapahtuman” erikoistapauksena ja voidaan kääntää myös ”vaaratilanteeksi”, mutta joka direktiivin työversiossa on määritelty vain onnistuneesti estetyksi tapahtumaksi, eli tarkoituksellisen toiminnan tuloksena.

Edellä mainitut termit muodostavat määritelmäpohjan riskiperustaisuudelle päätöksenteossa ja priorisoinnissa, kuten se NIS2:n kontekstissa määritellään. Riskiperusteisuuden tueksi tehtävien riskiarvioiden sisältö määritellään jäsenvaltioissa, mutta tähän luetaan erityisesti välillisten ketjuuntuneiden (sekä verkottuneiden) riskien tarkastelu keskinäisriippuvuuksia silmällä pitäen, kuten esimerkiksi tuotantoketjuissa muodostuvat riskit. Direktiiviluonnoksen kriteerit toimitusketjujen riskinarviointiin sisältävätkin selkeästi kriittisten riippuvuussuhteiden tunnistamisen, vaihtoehtoisten tuotteiden ja palveluiden saatavuuden selvittämisen, koko elinkaaren mittaisen häiriötilanteiden siedon suunnittelun, järjestelmien tulevaisuuden ennakoinnin sekä mahdolliset eritysvaatimukset EU:n ulkopuolisten maiden tuotteille.

Toinen arvioihin liittyvä näkemys on, että asiat on osattava suhteuttaa oikein mm. riskin vaikutuksiin ja todennäköisyyksiin, toimijoiden kokoon, (parhaisiin saatavilla oleviin) hallintakeinoihin, vaikutuksiin yhteiskuntaan ja niin edelleen. Riskiperusteisuutta voitaisiin siis soveltaa sekä riskienhallintaan, että näiden riskienhallintatoimien valvontaan ja muihin priorisoinnista hyötyviin toimiin.

[19] https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_FI.html
[20] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32019R0881