Euroopan unioni
Euroopan sosiaalirahasto
Vipuvoimaa EU:lta 2014–2020
Vaasan yliopisto
UNIVERSITY OF VAASA

Hanke rahoitetaan Euroopan sosiaalirahaston REACT-EU tuella.
REACT-EU-hankkeet rahoitetaan osana Euroopan unionin COVID-19-pandemian johdosta toteuttamia toimia.

Moduuli 3: Riskienhallinta osana kyberturvallisuusajattelua

3.1 Kyberturvallisuudella täydennetään riskienhallintaa

Oppimistavoite: Tässä kappaleessa opit, miten kyberturvallisuuden hallinta täydentää riskienhallintaa digitaalisessa toimintaympäristössä. Kyberturvallisuus on laaja aihe ja tässä kappaleessa siihen keskitytäänkin riskienhallinnan näkökulmasta. Kappaleen lopussa vastaat tehtäviin kyberriskeistä. Arvioitu ajankäyttö: 30 min + lisämateriaali.

Moni fyysisen maailman toiminto on riippuvainen kybertoimintaympäristöstä. Kyberturvallisuus on **tavoitteellinen tila**, jossa digitaalisesta toimintaympäristöstä riippuvaisille toiminnolle aiheutuvat riskit ovat hallinnassa myös häiriötilanteissa (VAHTI s. 17). Laajimmillaan kyberturvallisuudessa tarkastellaan **koko digitaalisesti verkottuneen yhteiskunnan toimintoja, jotta ne ovat turvallisia kaikille sen toimijoille**. (Turvallisuuskomitea 2018).

Kyberturvallisuutta toteutetaan t**unnistamalla, ehkäisemällä ja varautumalla digitaalisten järjestelmien häiriöiden vaikutuksiin** (VM 22/2017 Ohje riskienhallintaan). Kyberturvallisuus on varautumista siihen, että digiympäristön häiriöiden vaikutukset voivat esiintyä myös fyysisessä ympäristössä.

Vastuu toimintaympäristön turvallisuuden varmistamisesta on viranomaisilla, mutta myös jokaisella yksittäisellä toimijalla.

Kyberturvallisuuteen kuuluu tietojärjestelmien varassa toimivan infrastruktuurin turvallisuus. Turvallisuuden varmistamiseen kuuluvat esimerkiksi sähköverkkojen ohjausjärjestelmät, teollisuuden prosessiautomaatiojärjestelmät ja itseohjautuvat ajoneuvot. Kyberturvallisuus sisältää myös ne toimet, joilla pyritään ehkäisemään verkkojen kautta tehtävät tietomurrot.

Häiriöt digiympäristössä

Digiympäristön häiriöt voivat olla lähtökohdaltaan esimerkiksi:

- **Ihmisen tahallisesti aiheuttamia**, kuten hakkerointi, verkkohyökkäys, botin luominen häiriöitä ja rikoksia varten.
- **Ihmisen tahattomasti aiheuttamia**, kuten ohjelmointivirhe, tietämättömyydestä tehdystä toimenpiteestä, tai vahinko.
- **Luonnon aiheuttamia**, kuten myrskyn aiheuttama sähkökatkos tai jyrsijän poikki nakertama kaapeli.

Digiympäristön uhkien luokittelusta opit lisää TARA-menetelmää käsittelevästä kappaleesta 3.4. TARA-menetelmässä uhkien arviointi tehdään uhka-agenttien tavoitteiden ja hyökkäysmenetelmien tunnistamisen kautta.

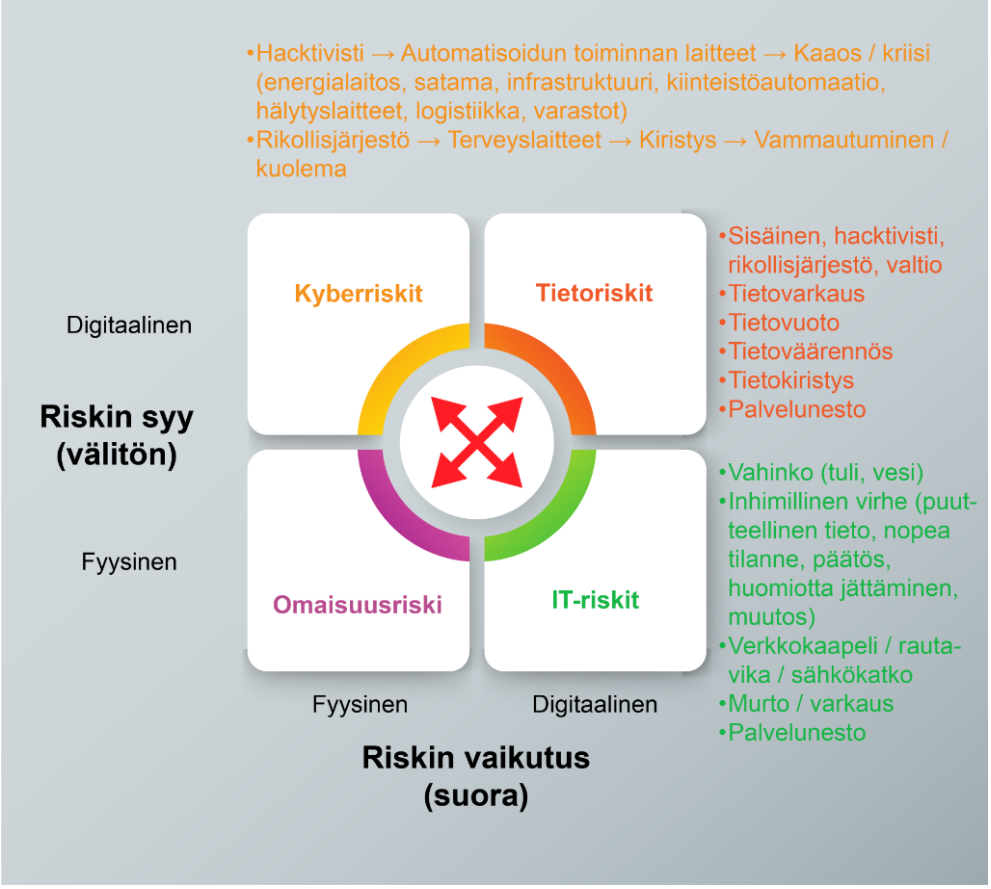
Kyberturvallisuuden riskit

Kyberturvallisuutta rakennetaan osaltaan *digiriskien* hallinnalla, joka on aiheena Riskioppi-ympäristön Moduulissa 1. Digiriskejä voivat olla esimerkiksi kyberriskit, tietoriskit ja IT-riskit.

Alla oleva nelikenttä näyttää, mitkä uhat kuuluvat **kyberriskeihin**. Tämän hahmottaminen on olennaista, jotta voit käsitellä ja keskustella ammattilaisten kanssa oikeista asioista kyberriskeinä.

Nelikentällä tarkastelet **a) Riskin välitöntä syytä** ja **b) Riskin suoraa vaikutusta** sekä digitaalisessa ympäristössä että fyysisessä ympäristössä.

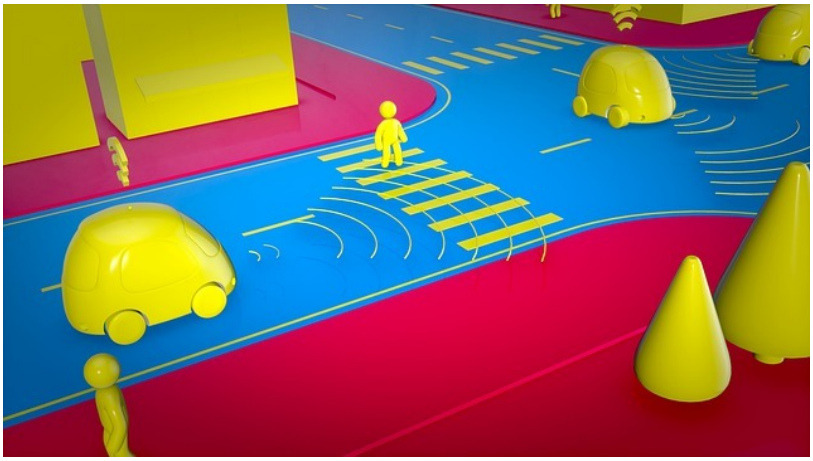
Nelikentän mukaan kyberriskit ovat riskejä, joiden välitön syy on digiympäristössä ja riskin välitön vaikutus fyysisessä ympäristössä.



Riskien nelikenttä. Kuvan lähde: Wihuri (2017).

Kyberriski on esimerkiksi tilanne, jossa itseohjautuvan auton ohjelmistoa häiritään tahallisesti niin, että auto aiheuttaa ihmisille vaaratilanteen. Riskin välitön syy voi olla haavoittuvuus ohjelmistossa sekä suojaamaton ja avoin kanava, jota pitkin häiriön aiheuttava ohjelma siirretään autoon. Tämän riskin kautta voidaan mahdollisesti kiristää tai tahallisesti vahingoittaa ihmisiä tai auton valmistajan mainetta.

Wihuri esittää myös esimerkkejä kyberriskeistä. Jos ns. hackitivisti pääsee murtautumaan automatisoidun toiminnan laitteisiin, voi hän aiheuttaa kriisin tai kaaoksen energialaitoksessa, satamassa, kiinteistöautomaatiossa tai logistiikkaketjussa omien tarkoitusperiensä ajamiseksi. Jos rikollisjärjestö pääsee verkon kautta murtautumaan digitaaliseen terveyslaitteeseen, se voi kiristää uhkaamalla aiheuttaa vammautumisia tai kuolemia.



Nelikenttään palataan myöhemmässä kappaleessa tietoriskien määrittämisestä.

Opi lisää

a. Toimintaohjeita kyberhyökkäystilanteisiin

Kyberturvallisuuskeskus tarjoaa kattavat toimintaohjeet kyberhyökkäystilanteissa toimimiseen ja niistä toipumiseen: 1) yksityishenkilöille; 2) organisaatioille ja yrityksille; 3) tietoturvan ammattilaisille.

Tähän kappaleeseen on lisätehtäväksi koottu linkkejä tärkeisiin toimintaohjeisiin organisaatioille ja yrityksille:

- Tietomurto
- Kiristyshaittaohjelma
- Palvelunestohyökkäys
- Toimitusketjuhyökkäys
- Vuotaneet käyttäjätunnukset

b. Kansalaisen kyberturvallisuus

Maksuton Kansalaisen kyberturvallisuus -kurssi opettaa turvallista toimintaa digitaalisessa maailmassa. Kurssi on suunniteltu ja toteutettu Jyväskylän yliopiston ja Maanpuolustuskoulutus MPK:n yhteistyönä.

c. Kybertuvallisuusharjoitus

Kyberturvallisuusharjoitusten toteutustapaa on kuvattu mm. Ahosen et al. (2019) raportissa. Raportin mukaan hyvä kyberturvallisuuden vertaisverkosto on korvaamaton. Verkostoa ylläpidetään kyberturvallisuusharjoituksilla, jotka ovat erittäin tehokas tapa kehittää verkoston jäsenten kyberturvallisuuskyvykkyyttä. harjoitukset antavat tietoa esimerkiksi äkillisistä uhista ja niiden ratkaisuista.

Kyberturvallisuusharjoitusten toimintamallin pohjalta Vaasan ja Tampereen yliopistojen Riski-Digi -hankkeessa laadittiin prosessi digitalisaatioon liittyvien riskien tunnistamiseen ja hyödyntämiseen liiketoiminnassa.

d. Pienyritysten kyberturvallisuusopas

Traficom on julkaissut erityisesti pienille yrityksille suunnatun oppaan kyberturvallisuudesta.

e. Tietojesiturvaksi.fi -blogi

Tietoturvapäällikkö Matti Laakson blogissa on ajankohtaisia neuvoja tietoturvasta, tietosuojasta, kyberturvallisuuden toteuttamisesta ja riskienhallinnasta digiympäristöissä.

Vastaa alla, mitkä seuraavista kyberriskeihin liittyvistä väitteistä pitävät paikkansa?

- ◊ Digitaalisen ympäristön häiriöt johtuvat ihmisen toiminnasta tai virheestä.
- ◊ Kyberriskien syy on digitaalisessa ympäristössä.
- ◊ Kyberriskin seuraus voi ilmetä fyysisessä todellisuudessa.
- ◊ Ajantasaista tietoa kyberriskeistä on vähän tarjolla.

Hyödynnä yllä kuvattua nelikenttää digiriskeistä ja yhdistä parit seuraavista vaihtoehdoista:

Kyberriski	Sähkökatko tavaratalossa sulkee kassapäätteet, valot, hissit ja automaattiset ulko-ovet ja ostosreissusi päättyy ennen aikojaan.
Tietoriski	Olet vastannut luottamuksellisesti työpaikan henkilöstökyselyyn, mutta seuraavana päivänä kuulet, vastaukset on kerrottu nimien kanssa esimiehelle.
Omaisuusriski	Rikollinen murtautuu sairaalan tietoverkkoon ja kiristää vaarantavansa potilasturvallisuuden.
IT-riski	Maksat bussilipun lähimaksulla puhelimellasi mutta joku rosvo näkee mihin taskuun laitat puhelimen ja nappaa sen matkan aikana.

Vielä edelliseen tehtävään liittyen, **valitse alla olevista sopiva vaihtoehto**.

- ◊ Osasin jaotella riskit nelikentän mukaisiin pareihin.
- ◊ Ihan kaikki parit eivät menneet nappiin.

3.2 Tietosuoja ja tietoturva

Oppimistavoite: Tässä kappaleessa opit, miten tietosuoja ja tietoturva määritellään ja mitkä tyypilliset riskit uhkaavat niitä. Kappaleen lopussa vastaat kahteen valintaruututehtävään tietosuojaan ja tietoturvaan liittyvistä väitteistä. Arvioitu ajankäyttö: 25 min.

Tietosuoja ja tietoturva ovat keskeisiä digiturvallisuuden alueita. Ne on olennaista ottaa huomioon myös fyysisessä ympäristössä toimittaessa.

Tietosuoja on ihmisten henkilötietojen ja yksityisyydensuojan hallintaa. Sen tarkoituksena on pitää hallussa oleva henkilötieto suojattuna asiaankuulumattomalta käytöltä.

Tietoturvallisuus liittyy tietojen luottamuksellisuuteen, saatavuuteen ja eheyteen sekä tiedon käyttövaltuuksien hallitsemiseen ja tiedon kiistämättömyyden todentamiseen. Tietoturvallisuuden tavoite on varmistaa, että tieto on saatavilla ja oikeaa, ja siten turvallista käyttää.

Tietosuoja

Tietosuoja on osa lain takaamaa henkilön yksityisyyden suojaa. Tietosuojan tarkoituksena on varmistaa, että organisaatiot tallentavat ja käsittelevät henkilötietoja lainmukaisesti ja ainoastaan tilanteissa, joissa tietojen tallentamiseen ja käsittelyyn on lainmukainen peruste.

Henkilötietoja ovat esimerkiksi nimi, kotiosoite, puhelinnumero, sähköpostiosoite ja tietokoneen IP-osoite. Tietosuojaan kuuluu oikeus nähdä sekä saada korjattua tai poistettua itsestä kerättyjä tietoja. Tietosuojan tavoitteisiin sisältyy myös se, että tallennetut henkilötiedot suojataan valtuudettomalta tai muulta käytöltä, joka vahingoittaa tiedoissa yksilöityä henkilöä (JOHDA s. 225).

Tietosuojan toteuttaminen tarkoittaa henkilötietojen suojaamista niiden turvallisella käsittelyllä ja tallentamisella, sekä tietojen pitämistä sellaisten tahojen saavuttamattomissa, joilla ei ole niihin oikeutta.

Tietosuojariskit koskevat henkilöön yhdistettävän tiedon taltioinnin ja käsittelyn riskejä, kuten **tietoturvaloukkauksia**.

Tietosuoja-asetus velvoittaa organisaatiot ilmoittamaan havaitut tietoturvaloukkaukset välittömästi tietosuojavaltuutetulle. Mikäli henkilötietoja käsittävästä tietoturvaloukkauksesta tunnistetaan koituvan rekisteröidyille henkilölle korkea riski, on myös hänelle ilmoitettava loukkauksesta välittömästi.

Ilmoittajansuojelulaki

Yksi tietosuojan osa on whistleblowing- eli ilmoittajansuojelulaki. Sen tarkoituksena on suojella henkilöitä, jotka ilmoittavat työnsä yhteydessä havaitsemistaan väärinkäytöksistä. Laki velvoittaa yli 50 henkilöä työllistävät yksityisen ja julkisen sektorin organisaatiot perustamaan sisäisen ilmoituskanavan väärinkäytöksiä varten. Suomessa laki perustuu EU:n ns. whistleblowing-direktiiviin. Ilmoituskanavan käytön tulee olla anonyymia.

Tietoturva

Tietoturva määritellään VAHTI-sanastossa **tavoitetilaksi**, jossa tietojen ja tietojärjestelmien saatavuus, eheys ja luottamuksellisuus on varmistettu. **Tietoturvallisuus on sama asia kuin tietoturva**. (VAHTI s. 17)

Perinteisessä jaottelussa tietoturvaa rakennetaan kolmen tavoitteen kautta: saatavuus, luottamuksellisuus ja eheys (JOHDA s. 176) seuraavasti:

- **Saatavuus** tarkoittaa, että vain tietoa tarvitsevat pääsevät siihen käsiksi.
- **Luottamuksellisuus** tarkoittaa, että tieto on luokiteltu siten, että tietty tieto on tarkoitettu vain tiettyjen tahojen luettavaksi ja muokattavaksi.
- **Eheys** tarkoittaa, että tieto pysyy muuttumattomana järjestelmässä, johon se on tallennettu.

Nämä tiedon suojaamisen periaatteet ovat myös ISO 27001 - standardin mukaiset. Tavoitteita täydennetään varmistamalla kiistämättömyys ja todentaminen:

- **Todentamisella** tarkoitetaan toimenpidettä, jolla henkilö todistaa IT-järjestelmälle olevansa valtuutettu käyttämään tiettyä järjestelmää tai avaamaan tietyn tiedoston. Todennus suoritetaan minimissään käyttäjätunnuksella ja salasanalla.

- **Kiistämättömyyden** tarkoituksena on väärinkäytön poistaminen. Järjestelmän käyttöä ja siellä tietoon tehtäviä muutoksia seurataan ja tallennetaan esimerkiksi lokipalvelimelle. Näin tietyn käyttäjän tapahtumat tietyllä hetkellä on mahdollista kiistämättömästi todistaa. Lokipalvelimella olevien tietojen luottamuksellisuus ja eheys on turvattava.

Tietoturvallisuus sisältää digiympäristön järjestelyiden ohella myös muita osa-alueita, esimerkiksi paperiasiakirjojen turvallisen tulostuksen ja ohjeistuksen siitä, että tulosteet noudetaan välittömästi, äänen kantavuuden hallinnan sekä näkyvyyden hallinnan laitteiden näytöille.

Tietoturvallisuuden toteuttamisessa eritellään kahdeksan toimenpidealuetta, jotka sisältävät erilaisia tietoturvan järjestelyjä (JOHDA s. 225) esimerkiksi seuraavasti:

1. **Hallinnollinen alue**, kuten määritelty ja valvottu prosessi asiakirjojen turvalliselle säilytykselle ja hävittämiselle;
2. **Henkilöstö**, kuten säännöllinen koulutus ja viestintä uusista tietoturvan uhista;
3. **Fyysinen alue**, kuten toimitilojen ja arkistojen lukitus sekä kulunvalvonta;
4. **Tietoliikenne**, kuten salatut yhteydet ja ohjeistukset olla käyttämättä avoimia WLAN-verkkoja;
5. **Laitteisto**, kuten varajärjestelmät (mm. varavirta, tallennuslaitteet, verkkojärjestelmät varalle);
6. **Ohjelmisto**, kuten tietoturva- ja virustorjuntaohjelmistojen käyttäminen ja säännöllinen päivittäminen;
7. **Tietoaineisto**, kuten tallennettujen tietojen salaus ja varmuuskopiointi;
8. **Käyttöturvallisuus** eli päivittäisten IT-toimintojen ja -rutiinien turvaaminen, esimerkiksi salasanojen hallinnointi, varmenteiden käyttö (mm. kaksivaiheinen tunnistautuminen) ja tietojärjestelmien käytön valvonta ja lokin pitäminen.

Organisaation tavoittelema **tietoturvallisuuden taso** riippuu muun muassa organisaatiolle asetetuista ulkoisista ja sisäisistä vaatimuksista, toiminnan tavoitteista, sekä käytössä olevista resursseista (VAHTI s. 17). Organisaation on täytettävä ulkoiset vaatimukset.

Tietoriskit

Tietoriskit vaarantavat tietoturvallisuutta. Tietoriskit ovat uhkia tiedon aitoudelle, vastuullisuudelle, kiistämättömyydelle ja luotettavuudelle. Tietoriskit vaarantavat tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilymisen (JOHDA s. 176) tai tekevät käyttäjien todentamisen ja käytön kiistämättömyyden epävarmaksi.

Pauli Wihurin (2017) esityksen mukaan tietoriskejä voidaan tarkastella järjestelmällisesti neljän kohteen kautta:

1. Tietoriskin **operatiivinen vaikutus** yksikön toiminnalle
2. Tietoriskin **vaikutus koko organisaatiolle**
3. **Tietosuojariski rekisteröidylle henkilölle**
4. **Vaikutukset rekisteröidylle henkilölle**.

Näkökulmat on koottu seuraavaan taulukkoon

Tietoriski	Operatiivinen vaikutus yksikön toiminnalle	Vaikutus koko organisaatiolle	Tietosuojariski rekisteröidylle	Vaikutuksia rekisteröidylle
Henkilötieto vuotaa sisällä tai ulkopuolelle	Ilmoitusvelvollisuus valvontaviranomaisille ja rekisteröidyille	Maineen menetys, korjauskustannukset, korvausvastuut ja sakot	Salassa pidettävien henkilötietojen luottamuksellisuuden menetys, syrjintä, vapauksien ja/tai oikeuksien menetys	Henkilön arkaluontoiset talous- tai terveystiedot tulevat yleiseen tietoon
Mihinkään henkilötietoon ei pääse (laaja verkko tai tietojärjestelmähäiriö)	Päätöksenteko viivästyy, määräajan ylitys, työajan hukkaaminen ja henkilöstön turhautuminen	Tuottavuuden lasku, maineen menetys, korjauskustannukset, korvausvastuut ja sakot	Pääsy omiin tietoihin estyy, viivästynyt päätös tai toiminta, oikeuksien ja/tai vapauksien menetys	Henkilöstön palkanmaksun viivästyminen

Taulukko pohjautuu lähteeseen Wihuri (2017).

Voit hyödyntää taulukon pohjaa arvioimaan tietoriskien vaikutuksia oman toimintasi kannalta.

Kuten taulukko osoittaa, organisaation tulee kartoittaa tietoriskien vaikutuksia myös tietosuojariskeinä rekisteröidyn henkilön näkökulmasta.

Tietojärjestelmän tietoturvariskit

Tietojärjestelmän tietoturvariskejä voidaan tarkastella **hyökkäyspinnan** (engl. attack surface) kautta. Hyökkäyspinta koostuu kaikista järjestelmän toiminnallisuuksista, joiden kanssa hyökkääjä voi toimia (yleensä verkon kautta etänä) ja joiden kautta hyökkääjä pääsee vaikuttamaan järjestelmään. (Vähä-Sipilä 2021)

Tietojärjestelmässä hyökkäyspinta koostuu tyypillisesti ohjelmallisesti toteutetuista rajapinnoista, kuten käyttöliittymästä sekä sovellusten ja niiden mahdollisten laajennusten rajapinnoista. (Vähä-Sipilä 2021)

Lisäksi hyökkäyspinta koostuu kaikista niistä **fyysisistä paikoista**, joissa hyökkääjä pääsee joko suoraan tai välillisesti yhteyteen siirrettävän/tallennetun tiedon tai suoritettavan ohjelmakoodin kanssa. (Vähä-Sipilä 2021)

Opi lisää tekoälyjärjestelmien tietoturvasta ja riskienhallinnasta tästä selvityksestä.

Nelikenttä tietoriskien tarkasteluun

Alla olevasta nelikentästä näkyy, mitkä uhat toiminnalle kuuluvat tietoriskeihin.

Nelikentän kautta tarkastellaan: **a) Riskin välitöntä syytä** ja **b) Riskin suoraa vaikutusta** sekä digitaalisessa ympäristössä että fyysisessä ympäristössä.

Nelikenttä osoittaa **tietoriskien olevan riskejä, joiden välitön syy on digitaalisessa ympäristössä ja välitön vaikutus on sekin digitaalisessa ympäristössä**.

Riskien nelikenttä. Lähde: Wihuri (2017).

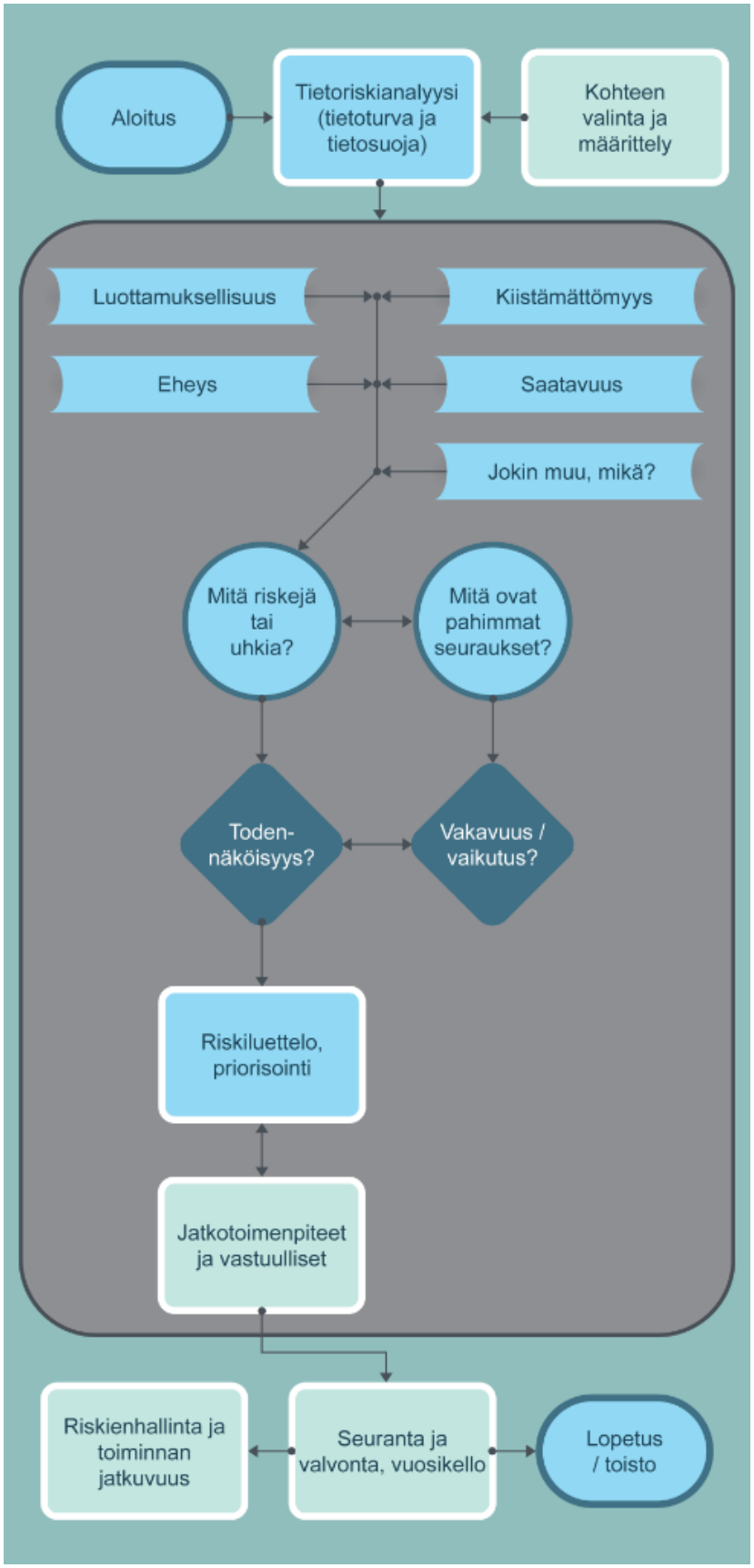
Tietoriskejä ovat esimerkiksi palvelunesto, tietovarkaus, tietovuoto, tietoväärennös ja tietokiristys. Näiden uhkien takana voi olla henkilö organisaation sisältä, hakkeri/hacktivisti, rikollisorganisaatio tai valtiollinen toimija. (WIHURI 2017)

Nelikenttä on hyödyllinen väline tieto- ja IT-riskien erottamisessa toisistaan. Nelikentän mukaan **IT-riskin välitön syy on fyysisessä ympäristössä ja suora vaikutus digitaalisessa ympäristössä**. Ilmeinen esimerkki tästä on tilanne, jossa tietokoneen kiintolevy hajoaa fyysisesti, jolloin sille tallennetut tiedot katoavat, mikäli niitä ei kyetä palauttamaan varmuuskopioista. Uhkia, jotka aiheuttavat IT-riskin, ovat vahingot (tulipalo, vesivuoto), kaapelivika, sähkökatko, murto ja laitevarkaus, palvelunesto fyysisellä välineellä kuten USB-laitteella sekä inhimillinen virhe, jonka taustalla on esimerkiksi puutteellinen tieto, nopea tilanne tai huolimattomuus. (WIHURI 2017)

Tietoriskianalyysi

Tietoriskianalyysissä ennakoit mahdollisia ongelmia tietoturvallisuuden peruskäsitteiden kautta kartoittamalla todennäköisimmät riskit ja kuvaamalla niiden toteutumisen pahimmat seuraukset.

Tietoriskianalyysin voi vähimmäistasolla toteuttaa arvioimalla uhkia, jotka kohdistuvat luottamuksellisuuteen, eheyteen, saatavuuteen ja kiistämättömyyteen, kuten alla olevassa kaaviossa esitetään.



Prosessikaavio **tietoriskianalyysin** yhdelle mahdolliselle toteutustavalle. Lähde: VM 22/2017 s. 15.

Analyysin kohdassa "Jokin muu", voit miettiä mm. uhkia, jotka kohdistuvat käyttäjien todentamiseen. Tällaisia uhkia ovat esimerkiksi puutteelliset ohjeistukset, jotka mahdollistavat salasanojen ja käyttäjätunnusten säilyttämisen samassa paikassa.

Dis- ja misinformaatio

Disinformaation tavoitteena on vaikuttaa ihmisten toimintaan ja ajatteluun. Disinformaatiolla pyritään luomaan **voimakas tunnereaktio**.

Dis- ja misinformaation vastaanottaminen on yleinen digiriski. Se koskettaa kaikkia ihmisiä, jotka toimivat kritiikittömästi vastaanotetun väärän informaation pohjalta. Jakamalla sosiaalisessa mediassa sensaatiomaisen viestin voi osallistua väärän tiedon jakamiseen.

Disinformaation lähettäminen on lähtökohtaisesti **pahantahtoista**. Se voi olla osittain vääristettyä dataa (esimerkiksi taloustietoa) tai täysin tekaistua mutta uskottavan näköistä aineistoa (kuten "valeuutinen"), jolla mahdollisesti tähdätään vaikuttamaan ihmisten käsityksiin jostain tahosta, vahvistamaan uskomuksia jostakin asiasta (engl. confirmation bias) tai hidastamaan päätöksentekoa hämmentämisen kautta.

Kysymys ei ole siitä, vastaanotetaanko jossain vaiheessa disinformaatiota, vaan miten siihen varaudutaan ja sen kanssa organisaatiossa toimitaan. Riskienhallinnan näkökulmasta disinformaatio on uhka, koska se on epävarmuustekijä: mistä kanavasta disinformaatiota saadaan, milloin ja miten tieto on väärää, miten tieto todennetaan ja miten kokonaan tai osittain väärän tiedon kanssa toimitaan.

Kuten disinformaatio, **misinformaatio** on väärää tietoa, mutta sen levittämisen tavoite ei aina ole tarkoituksellinen harhaan johtaminen. Misinformaation välittämiseen voi osallistua vahingossa esimerkiksi jakamalla sosiaalisessa mediassa viestin, jonka sisältö vaikuttaa uskottavalta.

Tietoturvayhtiö F-Secure on esittänyt seuraavan käytännönlähtöisen toimintamallin disinformaation tunnistamiseen ja sen kanssa toimimiseen, josta seuraava yhteeveto on osittain KOMPASSI-hankkeen täydentämä maaliskuussa 2023:

- Lue pelkkää otsikkoa pidemmälle.
- Tarkista väitteen lähteet, kuten alkuperäinen julkaisu johon väite viittaa. Käänny luotettavien lähteiden kuten tunnettujen faktantarkastajien puoleen.
- Mieti, onko väite uskottava.
- Tarkista julkaisuajankohta alkuperäisestä lähteestä: vanhentuneet väitteet eivät välttämättä anna todenmukaista kuvaa. Virheellinen väite on jo voitu oikaista alkuperäisessä lähteessä.
- Mieti väitteen taustalla vaikuttavia motiiveja.
- Varo kuvamanipulaatiota. Myös puhe ja videokuva voidaan väärentää erittäin uskottavasti. Deepfaket ovat väärennettyjä videoita, jotka kuvaavat tunnettuja henkilöitä. Huomio tulee siirtää siitä mitä kuva tai video on esittävinään, siihen, miten väitteen oletettu lähettäjä haluaa kuvalla vaikuttaa sinuun ja toimintaasi.
- Kysy itseltäsi: 1) kuka viestin on lähettänyt ja onko hän sinusta luotettava toimija, 2) miten väitteellä halutaan sinuun vaikuttaa, mikäli väitteeseen liitetty kuva on 3) aito, tai jos se on 4) manipuloitu.

Miten toimit rikoksen tapahduttua

Mikäli havaitset tai epäilet joutuneesi verkkorikoksen uhriksi, tee asiasta sekä rikosilmoitus että ilmoitus Kyberturvallisuuskeskukseen.

Tietovuoto tarkoittaa, että tietojärjestelmään murtautunut toimija on saanut haltuunsa suojattavia tai salassa pidettäviä tietoja. Mikäli vuotaneet tiedot sisältävät ihmisten henkilötietoja, on kyseessä **tietosuojarikkomus**, josta on **velvollisuus tehdä ilmoitus tietosuojavaltuutetulle**.

Yksityiset henkilöt, yritykset ja organisaatiot voivat ilmoittaa Kyberturvallisuuskeskukselle koetuista tietoturvaloukkauksista tai niiden yrityksistä, esimerkiksi tietojen kalastelusta tai palvelunestohyökkäyksestä.

Pelihaaste

Oletko valmis testaamaan oppimiasi taitoja Riskivirasto-pelissä?

Pelissä pääset työharjoitteluun ihmisiä kaikissa digimaailman riskeissä palvelevaan Riskivirastoon. Kohtaat virastossa erilaisia digitaalisten toimintaympäristöjen riskejä niin työtehtävien kuin yksityiselämänkin osalta. Opit hyödyntämään teoriassa oppimiasi asioita käytännössä.

Lue lisää Riskivirasto-pelistä.

Mitä seuraavista dis- ja misinformaation muodoista on mielestäsi vaikein erottaa luotettavasta tiedosta?

- ◊ Kuvamanipulaatioita
- ◊ Valeuutisia
- ◊ Tekaistuja somepäivityksiä
- ◊ Väärennettyjä profiileja
- ◊ Tarkoitushakuisesti laadittuja tekstejä
- ◊ Vanhentuneita tietoja
- ◊ Vihapuhetta
- ◊ Väärennettyjä videoita

Mitkä seuraavista ovat mielestäsi tärkeitä tietosuojaan liittyviä asioita?

- ◊ Vain määrätyt henkilöt pääsevät käsiksi tallennettuihin tietoihin.
- ◊ Työpaikalla koulutetaan säännöllisesti henkilökuntaa tietosuoja-asioissa.
- ◊ Esimies pitää tietosuojaa tärkeänä asiana.
- ◊ Paperisten asiakirjojen käsittelyyn ja esimerkiksi tulostukseen on olemassa selkeät ohjeet.
- ◊ Tallennetut tiedot vaativat tunnistautumisen niitä tarkasteltaessa.
- ◊ Ihmiset osaavat tunnistaa väärän tai harhaanjohtavan tiedon oikeasta.

3.3 ISO 27001 -standardi

Oppimistavoite: Tässä kappaleessa opit pääpiirteet siitä, miten toteutat standardien kautta tietoturvallisuutta yhdenmukaisella tavalla, jota noudatetaan kaikkialla maailmassa. Esimerkiksi nostetaan ISO 27001 -standardi, jonka vaatimuksiin tietoturvasta on hyvä perehtyä, vaikkei olisi aikomusta sertifioida standardia. Kappaleen lopussa vastaat pariin tehtävään, jotka liittyvät standardin hyödyntämisen mahdollisuuksiin. Arvioitu ajankäyttö: 30 min.

Standardien tarkoituksena on määritellä yhtenäinen toimintamalli, jonka noudattaminen auttaa eri toimijoita toimimaan yhdenmukaisesti ja tehokkaalla tavalla. Standardi yhdistää yksittäisiä toimijoita suuremmaksi ja voimakkaammaksi joukoksi ja toimimaan yhdenmukaisella tavalla jonkin asian toteuttamiseksi.

ISO (International Organization for Standardization) on kansainvälinen standardisoimisjärjestö, jossa Suomea edustaa Suomen Standardisoimisliitto SFS. ISO on julkaissut yli 22 000 kansainvälistä standardia. IEC on sähköalan standardointiorganisaatio.

ISO/IEC 27001 on **tietoturvallisuuden hallintajärjestelmien standardi**, jossa **kuvataan kattava lähestymistapa tietoturvan toteuttamiseen ja tieto-omaisuuden suojaamiseen**. Standardissa esitettyjen vaatimusten pohjalta organisaatio turvaa tietonsa pitämällä ne virheettöminä, helposti käytettävissä olevina ja hyvin suojattuina. Standardia voivat hyödyntää tietoturvan toteuttamiseen niin kaupalliset yritykset, valtion virastot kuin voittoa tavoittelemattomat järjestötkin.

ISO-standardit määrittelevät dokumentit voit hankkia SFS:n verkkosivuilta: https://sfs.fi/.

ISO 27001 on sertifioitava standardi. Standardin ohjeistusta voidaan toki hyödyntää ilman sertifiointia.

Yleiskuva standardista

ISO 27001 -standardi opastaa organisaatiota asettamaan selkeät tavoitteet tietoturvalle ja sen parantamiselle. Lisäksi standardi auttaa ymmärtämään, miten merkittäviä tietoturvan näkökohtia voidaan hallita ja opastaa toteuttamaan tarvittavat valvontatoimet.

Standardin avulla organisaatio voi hallita velvollisuuksiaan noudattaa oikeudellisia vaatimuksia, kuten GDPR-asetusta (General Data Protection Regulation). Standardin vaatimusten kautta organisaatio tarkistaa säännöllisesti vaatimustenmukaisuuden toteutumisen. Standardin laajennus **ISO 27701** koskee erityisesti tietosuojaan ja henkilötietoihin liittyvien riskien hallintaa.

Standardi ohjaa myös valitsemaan **oikein suhteutettu tapa pienentää riskejä**. Esimerkiksi yrityksen ei kannata käyttää vuosittain tuhansia euroja vakuutuksiin vähäiseksi arvioidun tappion aiheuttavan riskin poistamiseen.

Tavoitteet

ISO 27001 -standardin uusin versio on täydeltä nimeltään **ISO/IEC 27001:2022:fi Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.**

Standardissa siis kuvataan **tietoturvallisuuden hallintajärjestelmä**, joka koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä toiminnoista. Näiden kautta organisaatio suojaa tieto-omaisuuttaan, joka voi olla esimerkiksi:

- Aineetonta omaisuutta
- Taloudellista tietoa
- Työntekijöiden henkilötietoja
- Asiakkaiden tai kolmansien osapuolten organisaatiolle luovuttamia tietoja.

Hallintajärjestelmää ei tule mieltää yksittäiseksi dokumentiksi, vaan se koostuu useasta osasta. Siihen kuuluvat esimerkiksi suunnitelmat riskianalyysille, organisaation tietoturvapolitiikalle, tietoturvalle, jatkuvuudelle ja häiriöistä toipumiselle. Toimivan hallintajärjestelmän tulisi kattaa vähintäänkin tietoturvan johtamiseen, hallinnoimiseen ja valvontaan liittyvät menettelyt ja toimenpiteet.

Hallintajärjestelmä on moniosainen prosessi, jota organisaation tulee jatkuvasti kehittää esimerkiksi PDCA-mallin pohjalta (Plan-Do-Check-Act eli suomeksi Suunnittele-Toteuta-Arvioi-Toimi). PDCA-mallia käsitellään osana jatkuvuudenhallinnan toteuttamista Riskioppi-ympäristö kappaleessa 2.4.

Lähtökohtana organisaation tietoturvapolitiikka

Tietoturvapolitiikka on yritysjohdon laatima asiakirja, joka sisältää yleisellä tasolla kuvaukset organisaation tietoturvan linjauksista ja tavoitteista.

Tietoturvapolitiikkaan kirjattavia asioita ovat esimerkiksi vastuut tietoturvan toteuttamisen osa-alueista, henkilöstön pätevyyden kehittäminen, tietojenkäsittelyn suojaaminen organisaation toiminnassa sekä ohjeistukset laiminlyöntitapausten käsittelyyn.

Tietoturvapolitiikan tarkoituksena on motivoida henkilöstöä tietoturvallisiin toimintatapoihin sekä osoittaa, että myös johto osallistuu prosessiin. Tietoturvapolitiikassa määriteltyihin tavoitteisiin pääseminen edellyttää käytännössä loogista etenemistä.

Tietoturvasuunnitelma

Tietoturvapolitiikka-dokumentissa ei käsitellä teknisiä ohjeistuksia, vaan nämä dokumentoidaan erilliseen **tietoturvasuunnitelmaan**, jossa kuvataan tietoturvan ylläpitämiseksi tehtyjä teknisiä ja hallinnollisia toimenpiteitä organisaatiossa.

Täsmällisempi nimitys tietoturvasuunnitelmalle on **tietoturvakäytännöt ja -periaatteet**, jota muun muassa VAHTI-työryhmä käyttää.

Seuraavassa Tietojesiturvaksi.fi -sivustolla kuvattu käytännön esimerkki tietoturvasuunnitelman toteutuksesta:

- Luodaan asiakirja, eli **tietoturvasuunnitelma**, jossa kuvataan yksityiskohtaisesti organisaatiossa käytössä olevat tietoturvaratkaisut kuten nykyisten IT-järjestelmien suojamekanismit.
- Luodaan edellisestä erillinen asiakirja, eli **tietoturvan kehittämissuunnitelma**, jossa kuvataan, miten tietoturvan ylläpitämisen ja tehostamisen kanssa tullaan vaiheittain etenemään.

- Nämä asiakirjat tulee luokitella luottamuksellisiksi tai salaisiksi niiden arkaluontoisen sisällön vuoksi. (Matti Laakso, Tietojesiturvaksi.fi)

Hallintajärjestelmän suunnittelu

Hallintajärjestelmän suunnittelu aloitetaan tavoitteiden määrittelyllä eli määritellään mitä tietoja, järjestelmiä jne. organisaatio pyrkii suojaamaan. Kuten riskienhallinnassa, on tässäkin kyse resurssien kohdentamista. Resursseja ei ole rajattomasti käytettävissä kaiken organisaation hallussa olevan tai käyttämän tiedon suojaamiseen.

Suojattaviksi määriteltävät **omaisuuserät** voivat olla esimerkiksi digitaalisessa muodossa olevaa tietoa, paperiasiakirjoja, yksittäisten työntekijöiden hallussa olevaa tietoa ja fyysistä omaisuutta kuten tietokoneet, tallennuslaitteet ja tietoverkot.

Suojattavat kohteet luokitellaan niiden **kriittisyyden pohjalta** siten, että liiketoiminnan kannalta oleellisimmat järjestelmät on turvattava ensin. Sen sijaan muut laitteet, kuten henkilöstön tietokoneet, luokitellaan yleensä alempaan kategoriaan.

Suojattavien kohteiden määrittelyn jälkeen pohditaan niitä uhkaavia tekijöitä. Tässä yhteydessä tehdään riskianalyysi, jolla kartoitetaan liiketoimintaa uhkaavia tietoturva- ja muita ongelmia.

Hallintajärjestelmän toteuttamisen jälkeen arvioidaan sen onnistuminen. Tilanteen muuttuessa suunnitelmaa hallintajärjestelmästä päivitetään ja sen toimenpiteitä kehitetään vastaamaan uusia haasteita. Tähän voidaan hyödyntää PDCA-mallia.

Tiedon suojaamisen periaatteet

ISO 27001 **ei koske ainoastaan tietotekniikkaa**, vaan standardi kattaa useat näkökulmat muun muassa tiedon siirtämisestä ja hallitusta jakamisesta.

Standardi auttaa organisaatiota turvaamaan liiketoiminnan jatkuvuutta häiriötilanteissa, joissa organisaation tietoa häviää. Tällaisia tilanteita ovat esimerkiksi tulipalo, laiterikko, hakkerointi ja tahalliset tietovuodot.

Standardissa esitetyt tiedon suojaamisen periaatteet ovat:

1. **Luottamuksellisuus**, jolla varmistetaan, että tiedot ovat ainoastaan niiden henkilöiden saatavilla, joilla on siihen oikeus
2. **Eheys**, jolla turvataan tietojen ja käsittelymenetelmien oikeellisuus
3. **Saatavuus**, jolla varmistetaan, että valtuutetuilla käyttäjillä on tarvittaessa pääsy tietoihin ja niihin liittyvään tieto-omaisuuteen
4. **Tekninen suojaus** tietomurtoja, petoksia jne. vastaan.

ISO 27001 -standardi kattaa kaikki tietoturvallisuuden hallinnan osa-alueet, joita ovat:

- Organisaation toimintaympäristön ja tietoturvallisuuden hallintajärjestelmän kattavuuden määrittely
- Sidosryhmien ja näiden vaatimusten tunnistaminen
- Johdon hyväksymät yrityksen tietoturvallisuuden periaatteet ja tavoitteet
- Riskien arviointi ja riskien käsittely, dokumentaation hallinta
- Tehtävät ja vastuut organisaation sisällä
- Osaamisen ja tietoturvatietoisuuden kehittäminen
- Tietojen, tilojen, tietojärjestelmien ja laitteiden suojaaminen
- Tietokoneiden ja tietoliikenteen hallinta
- Tietojärjestelmien kehittäminen ja ylläpito
- Varajärjestelmät
- Toipumissuunnitelmat
- Lainsäädännön noudattaminen.

Standardin uusin versio

ISO 27001 -standardista julkaistiin uusi versio vuonna 2022.

Uudistettua on muun muassa kappale muutosten suunnittelusta. Standardin uuden version mukaan **muutoksenhallinnassa tulee huomioida koko muutoksen elinkaari**. Muutos voi olla esimerkiksi tietojärjestelmän version päivittäminen.

Uudistetussa standardissa muutoksia tehtiin hallintakeinoihin, jotka on lueteltu standardin Liitteessä A. Aikaisempien hallintatavoitealueiden (joita kuvattiin yllä) tilalle on uudessa versiossa tullut neljä kokoavaa **hallintateemaa**:

- Organisaatio
- Henkilöstö
- Fyysinen
- Teknologia.

Saman aihepiirin hallintakeinot löytyvät standardista yhtenäisen teeman alta. Hallintakeinoja määritellään peräti 93 kappaletta.

Suomen Standardisoimisliitto SFS on julkaissut videon standardin uuden version keskeisistä muutoksista.

Mahdollinen sertifiointi

ISO 27001 on sertifioitava standardi. Sertifioinnilla todetaan järjestelmällisen, kehittyvän ja johdon tukeman riskienhallintatavan uskottava suunnittelu ja toistuva käyttö organisaatiossa. Tämä lisää asiakkaiden sekä yhteistyökumppaneiden luottamusta organisaation toimintaa kohtaan.

Standardin ohjeistusta voidaan toki hyödyntää organisaatiossa ilman sertifiointia.

Opi lisää:

- Sertifioinnista yleisellä tasolla
- Sertifiointiorganisaatioista Suomessa

Täydennykset, kuten ISO 27005 tietoriskeille

ISO 27001:a täydentää kokonainen standardiperhe, joka käsittelee tietoturvallisuuden hallintajärjestelmiä, tietoriskejä ja tietosuojaa, muun muassa:

- ISO 27002 tietoturvallisuuden hallintakeinoista
- ISO 27005 ohjeita tietoturvariskien hallintaan
- ISO 27701 tietosuojalisäys standardeihin ISO 27001 ja 27002
- ISO 29100 tietosuojan perusteet informaatioteknologiassa
- ISO 29190 tietosuojakyvykkyyden arviointimalli informaatioteknologiassa.

Esimerkiksi **ISO 27005** ohjeistaa erityisesti tietoriskien hallintaa. Standardin liitteessä on lueteltu joukko mahdollisia IT-järjestelmien uhkia ja haavoittuvuuksia.

Standardissa on myös kuvattu mallipohja riskien suuruuden määrittämiseksi. Mallipohjassa kunkin tarkasteltavan toiminnon osalta arvioidaan sen varannon arvo, siihen kohdistuvan uhan toteutumisen todennäköisyys ja uhan toteutumisen helppous. Nämä kaksi lukua lasketaan yhteen. Mallipohja on kuvattu alla. Muitakin asteikkoja voidaan käyttää. (Iivari & Laaksonen 2009 s. 126-127)

	Uhan toteutumisen todennäköisyys								
	pieni			keskimääräinen			suuri		
	Toteutumisen helppous								
Varannon arvo	matala	keski-määräinen	korkea	matala	keski-määräinen	korkea	matala	keski-määräinen	korkea
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Mallipohja riskien suuruuden määrittämiseen (Iivari & Laaksonen 2009 s. 127). Taulukossa esimerkiksi matala 'toteutumisen helppous' tarkoittaa, että uhkan toteuttaminen on vaikeaa rikolliselle tai häiriköille. Tältä pohjalta esimerkiksi varanto jonka arvo tulkitaan nollaksi, ja uhka joka arvioidaan matalaksi sen toteuttamisen helppouden kautta, saa mallipohjan mukaan riskin suuruudeksi nolla.

Olennaista on tunnistaa mallipohjan kautta, mitkä ovat arvokkaimmat varannot, joihin kohdistuu suurimmat uhkat.

Täydennä osaamistasi

- Suomen Standardisoimisliitto SFS on julkaissut useita esittelyitä dioineen ja videoineen ISO 27000 -sarjan standardeista.
- ENISA (European Network and Information Security Agency) ylläpitää tietoportaalia riskienhallinnan menetelmistä, työkaluista ja ajankohtaisista teemoista.

Vastaa alla, mikä tai mitkä seuraavista olisivat sinulle tärkein syy hyödyntää ISO 27001 -standardia?

◊ Uskon standardoidun menetelmän käytön lisäävän yrityksen uskottavuutta.
◊ Tarvitsen selkeät ohjeet oman tietoturvani ajantasalle saattamiseen.
◊ Haluan oppia ymmärtämään tietoturvallisuuden laajana kokonaisuutena.
◊ Haluan, että tietoni on asianmukaisesti suojattu mahdollisen häiriötilanteen sattuessa.
◊ Haluan kohdentaa käytössä olevat resurssit mahdollisimman järkevästi.

Yhdistä käsite ja sen määrittely:

Edellinen yhdistelytehtävä oli mielestäni:

- ◊ Helppo - käsitteiden oppiminen käy minulta nopeasti
- ◊ Hiukan haastava - ihan kaikki ei mennyt oikein..

3.4 TARA (Threat Agent Risk Assessment)

Oppimistavoite: Tässä kappaleessa opit TARA-menetelmän periaatteet. Menetelmää soveltamalla voit ennakoida erilaisia uhkia digitaalisessa ympäristössä. Kappaleen lopussa vastaat valinta- ja monivalintatehtäviin TARA-menetelmän soveltamisesta. Arvioitu ajankäyttö: 30 min.

TARA (Threat Agent Risk Assessment) on Intelin tietoturva-asiantuntijoiden kehittämä menetelmä, jonka avulla voit ennakoida uhkia digiympäristössä. Menetelmä on julkaistu jo yli 15 vuotta sitten, mikä voi vaikuttaa pitkältä ajalta kun ajatellaan, miten digiympäristön on kehittynyt samana aikana. Kuitenkin TARA-menetelmän periaatteet ovat edelleenkin päteviä ja toivottavasti myös silmiä avaavia.

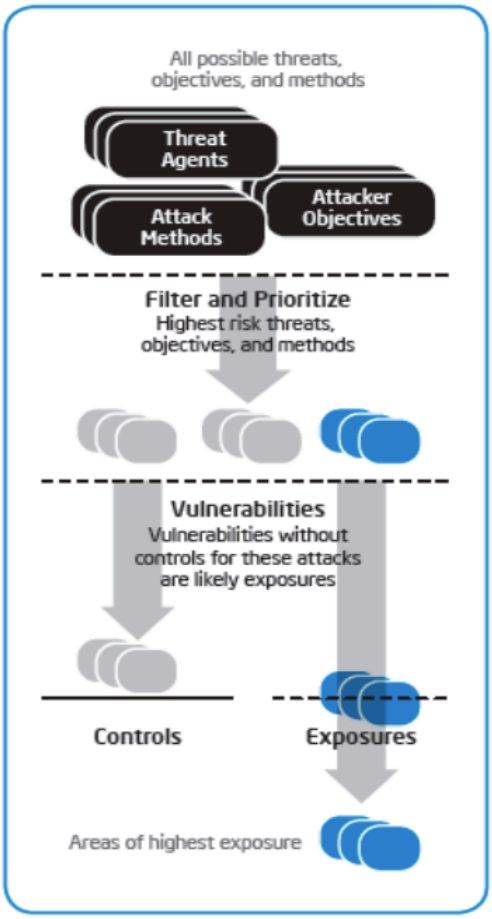
TARA-menetelmä on selkeästi jäsennetty ja sitä on helppo ymmärtää ja käyttää. Menetelmää voidaan mukauttaa kunkin käyttäjän tarpeiden pohjalta ja sen yhteydessä kuvattuja aineistoja tuleekin täydentää omilla havainnoilla ja arvioinneilla. TARA tarjoaa toimivan rakenteen uhka-kirjastoille.

TARA-menetelmän kuvaukset on julkaistu englanniksi. Tässä kappaleessa ei ole käännetty kaikkia menetelmän termejä suomeksi, vaan ainoastaan pääkohtia. TARA-menetelmään kannattaakin

perehtyä lukemalla rinnakkain tämän kappaleen tekstiä ja alkuperäisiä englanninkielisiä määritelmiä menetelmästä. Linkit näihin artikkeleihin ovat kappaleen lopussa.

Yhteenveto menetelmästä

TARA-menetelmän päävaiheet on esitetty seuraavassa kuvassa.



Kuvan lähde: Rosenquist & Casey (2009 s. 4).

Menetelmä pohjautuu kolmen *kirjaston* käyttöön. Kirjastot kuvaavat

1. uhka-agentteja

2. näiden tavoitteita hyökkäyksilleen sekä

3. mahdollisia hyökkäysmenetelmiä.

Kolmen kirjaston analyysin kautta keskitytään erityisesti niihin uhkiin, joilla on **suurin todennäköisyys** toteutua (eli suoritetaan uhkien priorisointi). Niitä ovat esimerkiksi IT-järjestelmän haavoittuvuudet (Vulnerabilities). Muut uhat suodatetaan tässä vaiheessa pois jatkotoimenpiteiltä.

Tämän jälkeen tarkastellaan, mihin valikoiduista uhista ei ole asetettu toimivia kontrolleja, jolloin ne altistuvat (Exposures) hyökkäyksille. Näin kohteisiin, joiden katsotaan ohittavan kuvassa alimman katkoviivan ilmaiseman hyväksytyn riskitason, voidaan osoittaa enemmän resursseja suojaamisen tehostamiseksi.

Menetelmää käyttämällä vähennetään todennäköisinä pidettyjä hyökkäyksiä tai altistumisia keskittymällä vain merkittävimpiin niistä.

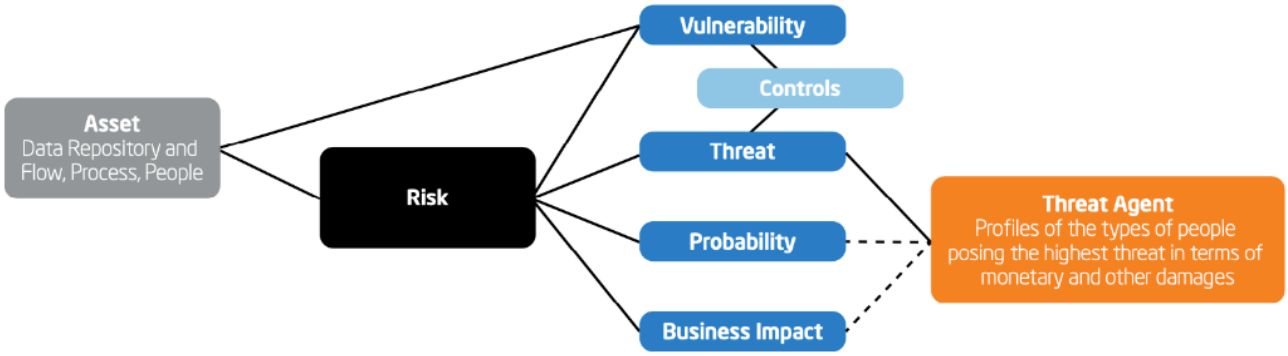
Kirjasto 1: Uhka-agentit

Ensimmäisessä kirjastossa (Threat Agent Library, TAL) kuvataan **uhka-agentit**, joita on yli **20 arkkityyppiä**, kuten *kilpailija, radikaali aktivisti, järjestäytynyt rikollisuus* sekä *huolimaton työntekijä*.

Uhka-agentit jaetaan kahteen pääryhmään näiden oletettujen tarkoitusperien pohjalta:

- **vihamielinen tarkoitus** (Hostile Intent); tai
- **ei-vihamielinen tarkoitus** (Non-Hostile Intent). Tähän ryhmään kuuluu esimerkiksi arkkityyppi *huolimaton työntekijä*.

Alla olevassa kaaviossa esitetään käsitteiden väliset riippuvuudet, joiden pohjalta kunkin uhka-agentin profiili on määritelty kirjastoon.



Kuvan lähde: Houlding et al. (2012 s. 5).

Kaavion mukaan **riskin muodostaa omaisuuden** (Asset) haavoittuvuus, jota agentti voi hyödyntää päästäkseen käsiksi omaisuuteen. Lisäksi riskin määrittelee **todennäköisyys** jolla agentti päätyy hyödyntämään haavoittuvuutta sekä uhan **vaikutus** liiketoimintaan (Business Impact).

Uhka muodostuu siitä, että **haavoittuvuudelle ei ole asetettu riittävää kontrollia**, jolla estettäisiin agenttia hyödyntämästä sitä.

Agentti voi hyödyntää omaisuuden/järjestelmän yhtä ja samaa haavoittuvuutta moniin eri uhkatekoihin, joista jokaisella voi olla eri todennäköisyys ja vaikuttavuus.

TARA-menetelmää käyttämällä tunnistetaan, mitkä mahdollisista uhka-agenteista:

1. Muodostavat uhkan tarkasteltavaan kohdejärjestelmään (ja tätä kautta, uhkan omaan toimintaan)
2. Mitkä ovat tunnistettujen uhka-agenttien motivaatiot
3. Mitä keinoja uhka-agentit todennäköisemmin käyttäisivät uhkateon toteuttamiseen.

Menetelmällä tunnistetaan järjestelmällisesti mitkä näistä kolmen ulottuvuuden yhdistelmistä muodostavat suurimman riskin, eli korkeimman todennäköisyyden ja merkittävimmän vaikutuksen omalle toiminnalle.

Kirjasto 2: Yleiset altistumiset

Toisen kirjaston (Common Exposure Library, CEL) pohjalta kartoitetaan **käytössä olevien** kontrollien altistumista mahdollisille uhkille ja osoitetaan näin, mitkä altistukset uhkille ovat ns. jäännösaltistuksia.

Kontrolleja ovat kaikki työkalut, prosessit ja muut käytössä olevat keinot, joilla pienennetään heikkouksista aiheutuvia menetyksiä.

- CEL-kirjasto pohjautuu Intelin tunnistamiin tietoturvahaavoittuvuuksiin ja altistuksiin, jotka olivat tunnettuja TARA-menetelmän kehittämisen aikaan.
- Varsinainen CEL-kirjasto ei ole ollut julkisesti saatavilla sen luottamuksellisuuden vuoksi.

Omaan käyttöön vastaava kirjasto yleisistä altistumisista rakennetaan luomalla **uhkaskenaarioita**, joilla tunnistetaan kohdejärjestelmän haavoittuvuuksia ja altistumisia. Ajankohtaista tietoa skenaarioihin saa esimerkiksi Kyberturvakeskuksen raporteista.

Tietojärjestelmien haavoittuvuudet muuttuvat jatkuvasti, sillä vaikka vanhoja puutteita paikataan esim. käyttöjärjestelmissä, tulee tai tunnistetaan uusia haavoittuvuuksia.

Kirjasto 3. Keinot ja tavoitteet

Kolmas kirjasto (Methods and Objectives Library, MOL) sisältää kuvaukset **uhka-agenttien mahdollisista tavoitteista teoilleen**, sekä kuvaukset heidän **käyttämistään mahdollisista keinoista teoilleen**.

Tavoitteet jakautuvat **yhdistelmiin motivaatioita (Motivation) ja päämääriä (Goal)**. Kirjastossa lueteltuja tavoitteita ovat esimerkiksi *henkilökohtainen hyöty (rahallinen)*, *henkilökohtainen hyöty (emotionaalinen)* ja *sosiaalinen/moraalinen hyöty*. Jotta luettelo olisi kattava, sisältyy tavoitteisiin myös *tahaton/vahinko*.

Uhka-agenttien käyttämien **keinojen tarkastelu jakautuu yhdistelmiksi tekoja** (Acts) ja **rajoitteita** (Limits).

Tekoja ovat esimerkiksi kopiointi, paljastaminen, käytön/pääsyn esto, lunnasvaatimus, tuhoaminen, käyttökelvottomaksi tekeminen, vaurioittaminen, muuttaminen/vääristäminen ja poistaminen.

Kirjastossa kuvataan myös **rajoitteet**, jotka kohdistuvat tiettyjen uhka-agenttien tiettyihin tekoihin.

- Esimerkiksi yksi rajoite *työntekijän virheelle* on *yrityksen menettelyohje*.
- Rajoitteet *huolimattomalle työntekijälle* pohjautuvat lakiin. Rajoitteena toimii siis tosiasia, että yrityksellä on lain mukaan perusteita irtisanoa huolimattomasti toiminut työntekijä ja mahdollisuus vaatia häneltä korvauksia tämän aiheuttamista vahingosta.

Seuraavaksi perehdytään tarkemmin TARA-menetelmän käyttöön uhkien tunnistamisessa.

Uhka-agentti -kirjasto

Uhka-agentti -kirjasto siis koostuu arkkityypeistä, joista jokainen on määritelty jopa yhdeksellä määritteellä seuraavasti:

i. Tavoite (Intent)

- Määritteellä kuvataan, aikooko agentti aiheuttaa vahinkoa. Aikomuksesta riippuen agentti voi olla **vihamielinen tai ei-vihamielinen.**
- Ei-vihamielinen "tavoite" on esimerkiksi tehty tahaton virhe.

ii. Pääsy (Access)

- Määrittää agentin pääsyä organisaation järjestelmiin tai tietoihin. Uhka-agentti voi olla joko **sisäinen tai ulkoinen**.

iii. Päämäärä (Outcome)

- Määrittelee agentin ensisijaisen päämäärän teolleen: varkaus, kilpailuedun saaminen, vahingon tuottaminen, hämmennys ja mustamaalaaminen, teknisen edun saaminen.

iv. Rajoitukset (Limits)

- Määrittää lailliset ja eettiset rajat, jotka voivat rajoittaa agentin toimintaa.
- Esimerkkejä mahdollisista rajoituksista: agentti noudattaa lakia ja käyttäytymissääntöjä, agentti toimii lain puitteissa, agentti on valmis rikkomaan lakia lievästi, tai agentti on valmis törkeään rikokseen.

v. Resurssi (Resource)

- Määrittelee kuinka järjestäytyneesti uhka-agentti toimii.
- Kuvauksia ovat: "yksinäinen susi", kilpailu/kampanja, löyhästi järjestäytynyt kerho, järjestäytynyt ryhmä, organisaatio jolla on käytössään suuret resurssit sekä valtiollinen toimija.

vi. Taitotaso (Skill level)

- Määrittelee minkä erityisen koulutuksen agentti on saanut tai mikä on hänen osaamisensa tiettyyn uhkaan liittyen: ei mitään, vähäinen, toiminnallinen, tai pätevä.

vii. Tavoite (Objective)

- Määrittää teon, jonka agentti aikoo tehdä saavuttaakseen haluamansa tavoitteen: kopioida, tehdä arvottomaksi, haavoittaa tieto-omaisuutta, viedä tieto-omaisuus pois omistajansa käytöstä, tai agentilla ei ole etuikäteissuunnitelmaa vaan hän toimii avautunutta tilannetta hyödyntäen.

viii. Näkyvyys (Visibility)

- Määrittää, missä määrin agentti pyrkii salaamaan tai paljastamaan henkilöllisyytensä ja tekonsa: toimii avoimesti haluten sekä identiteettinsä että tekonsa paljastuvan, toimii salatusti mutta haluaa että tekonsa näkyy, toimii salassa eikä halua tekonsa paljastuvan, ei välitä vaan toimii tilannetta hyödyntäen.

ix. Motiivit (Motivation)

- Hyökkääjän motiivit teolleen. Ne jaetaan **määrittelevään motivaation** ja **henkilökohtaiseen motivaatioon**. Yhteenveto arkkityyppisistä motivaatioista on kuvattu taulukossa alla.
- Analyysissä huomioidaan vähintään määrittelevä motivaatio (Defining Motivation).
- Lisäksi henkilökohtaisen motivaation huomioiminen antaa tietoa arvioida uhka-agenttien yksilöllisiä motivaatioita. Tämä on erityisen tärkeää ryhmässä toimivien uhka-agenttien tapauksissa. (Casey 2015)

Yhteenveto eräiden uhka-agenttien mahdollisista motivaatioista on seuraavassa taulukossa.

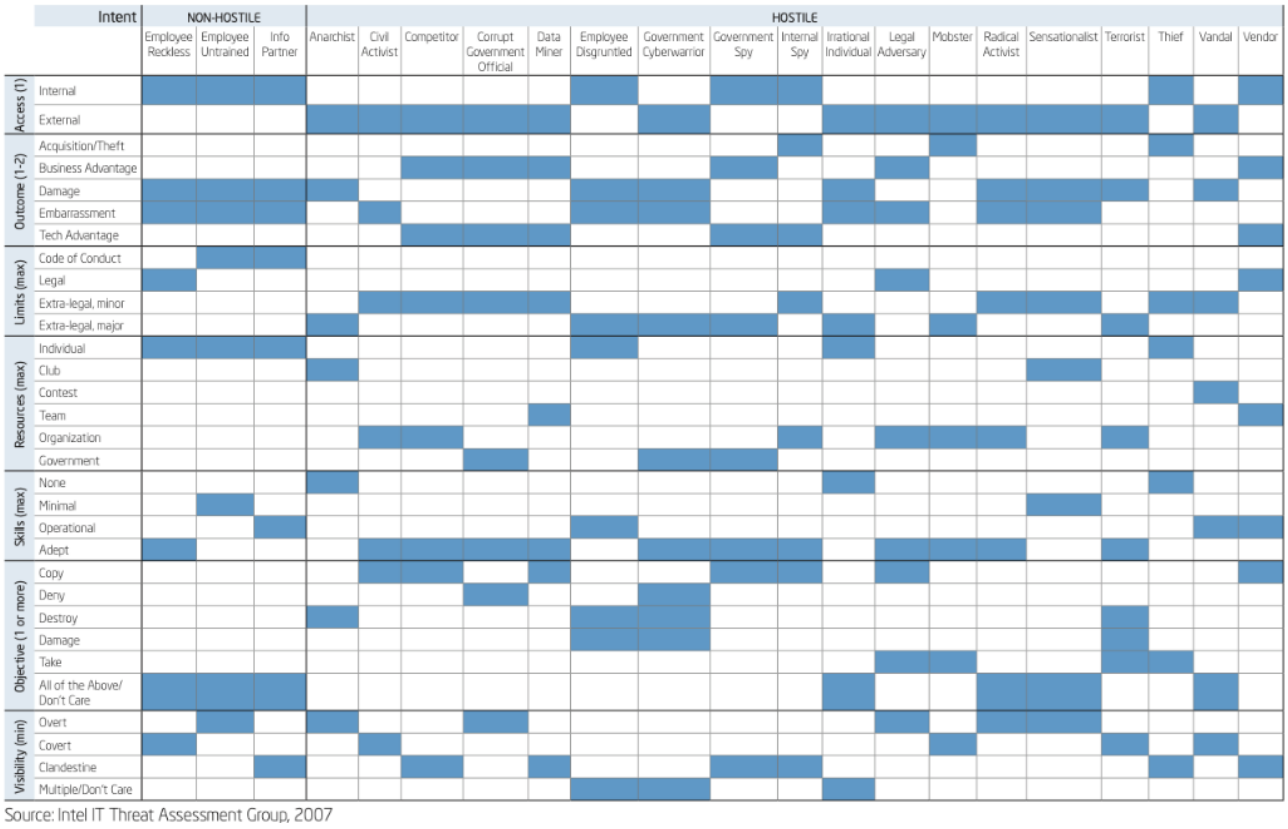
Table 12: Motivations of threat agents in the TAL, adapted from (Casey, 2015)

Threat agent label	Defining Motivation	Personal Motivation
Employee Reckless	Accidental	--
Employee Untrained	Accidental	--
Information Partner	Accidental	--
Civil Activist	Ideology	Ideology
Radical Activist	Ideology	Ideology
Anarchist	Ideology	Ideology
Competitor	Organizational Gain	Personal Financial Gain
Corrupt Government Official	Personal Financial Gain	Personal Financial Gain
Cybervandal	Dominance	Dominance
Data Miner	Organizational Gain	Personal Financial Gain
Disgruntled Employee	Disgruntlement	Disgruntlement
Government Cyberwarrior	Dominance	Ideology, Personal Financial Gain, Personal Satisfaction
Government Spy	Ideology	Ideology, Personal Financial Gain, Personal Satisfaction
Internal Spy	Personal Financial Gain	Coercion, Ideology, Personal Financial Gain
Irrational Individual	Unpredictable	--
Legal Adversary	Dominance	Personal Financial Gain
Mobster	Organizational Gain	Personal Financial Gain, Coercion
Sensationalist	Notoriety	--
Terrorist	Ideology	Ideology
Thief	Personal Financial Gain	Personal Financial Gain, Personal Satisfaction
Vendor	Organizational Gain	Personal Financial Gain

Taulukon lähde: Pushpakumar (2015 s. 50).

Kahdeksan määritelmän pohjalta on rakennettu seuraavassa taulukossa oleva yhteenveto uhka-agentti -kirjastosta.

Table 1: Current Library of Threat Agents and Their Defining Attributes



Source: Intel IT Threat Assessment Group, 2007

Taulukon lähde: Casey (2007 s. 5). Huomaa, että tämä arvio uhka-agenteista kuvaa vuoden 2007 tilannetta.

Uhka-agentti -kirjasto jättää tilaa muuttuville uhkatekijöille taloudellisissa, poliittisissa, yhteiskunnallisissa ja teknologisissa suuntauksissa tapahtuvien muutosten vuoksi. (Pushpakumar 2015)

Yllä kuvatun 'yleisen' TAL-kirjaston lisäksi Houlding kollegoineen (2012) on määritellyt TAL-kirjaston erityisesti terveydenhuoltoalalle.

Menetelmät

Osana menetelmät-kirjastoa (Methods & Objectives Library, MOL) kuvataan uhka-agenttien tavoitteet ja menetelmät: mitä agentit haluavat saavuttaa ja mitä keinoja he todennäköisemmin käyttävät saavuttaakseen tavoitteensa.

Näytteitä MOL-kirjastosta on esitetty alla olevassa taulukossa. Mahdollisia menetelmiä on toki paljon muitakin, kun tässä kuvatut ja uudet teknologiat mahdollistanevat uusien menetelmien kehittämisen.

AGENT NAME	ATTACKER					OBJECTIVE		METHOD								IMPACT				
	Access	Trust				Motivation	Goal	Acts					Limits							
		None	Partial Trust	Employee	Administrator			Copy, Expose	Deny, Withhold, Ransom	Destroy, Delete, Render Unavailable	Damage, Alter	Take, Remove	Code of Conduct	Legal	Crimes Against Property	Crimes Against People	Loss of Financial Assets	Business Operations Impact	Loss of Competitive Advantage, Market Share	Legal or Regulatory Exposure	Degradation of Reputation, Image, or Brand
Employee Error	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X		X				X	X	X	X	X
Reckless Employee	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X			X			X	X	X	X	X
Information Partner	Internal		X			Accidental/Mistake	No malicious intent, accidental	X		X	X						X	X	X	X	X
Competitor	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Radical Activist	External	X				Social/Moral Gain	Change Public Opinion or Corporate Policy	X	X	X	X	X				X		X			X
Data Miner	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Vandal	External	X				Personal Gain (Emotional)	Personal Recognition or Satisfaction			X	X				X			X			X
Disgruntled Employee	Internal		X	X	X	Personal Gain (Emotional)	Damage or Destroy Organization		X	X	X				X			X	X		X

Näytteitä menetelmät-kirjastosta. Kuvan lähde: Rosenquist & Casey (2009 s. 5). Lataa kuvan täysikokoinen versio.

Vaikutukset: Taulukossa on lueteltu joukko vaikutuksia (Impacts), jotka ovat odotettavissa uhka-agenttien motivaatioiden ja tavoitteiden yhdistelmien pohjalta, esimerkiksi ”vaikutus liiketoimintaan”, ”kilpailuedun menettäminen” ja ”maineen, imagon tai brändin arvon alentuminen”.

Tavoitteet (jotka *jakautuvat sarakkeisiin Objective ja Goal)*: Seuraavassa taulukossa on lisää esimerkkejä uhka-agenttien tavoitteiden kategorioista. Kategorioiden kautta voit miettiä mahdollisia uhkia oman toimintasi kannalta.

Table 13: Likely threat agent objectives, adapted from (Rosenquist, 2009)

Objective	Example
Theft/Exposure	Exposure of data resulting in loss of competitive advantage, including loss of IP and personal data.
Data Loss	Destruction or alteration of data including corruption, tampering, denial of access, and deletion, in order to make it unusable or decrease its value.
Sabotage	Willful and persistent attempt to cause damage and disruption, including destruction of systems, capabilities, processes, designs, and brand.
Operations Impact	Negative impact on business operations, including manufacturing, engineering, and research.
Embarrassment	Embarrassment targeted at individuals or corporation including real and fabricated defamation, reputation poisoning, and harassment targeting specific personnel or the corporation.
Accidental	No intentional objective to attack.

Taulukon lähde: Pushpakumar (2015 s. 52.)

MOL-kirjastossa kuvatut menetelmät edustavat todennäköisiä keinoja, joilla uhka-agentti voi toteuttaa hyökkäyksensä. Esimerkkejä menetelmistä on koottu seuraavaan taulukkoon.

Table 14: Likely methods of threat agents, adapted from (Rosenquist, 2009)

Methods	Examples
Copy, Expose	Copying or exposing intellectual property, information etc.
Deny, Withhold, Ransom	Denying access to the system, withholding, and demanding ransom for freeing the system.
Destroy, Delete, Render Unavailable	Destroy, delete, or make unavailable the system, intellectual property, physical assets, information, or its flow.
Damage, Alter	Damage or alter the system, its components, processes etc.
Take, Remove	Take or remove without permission, physical assets, documents etc.

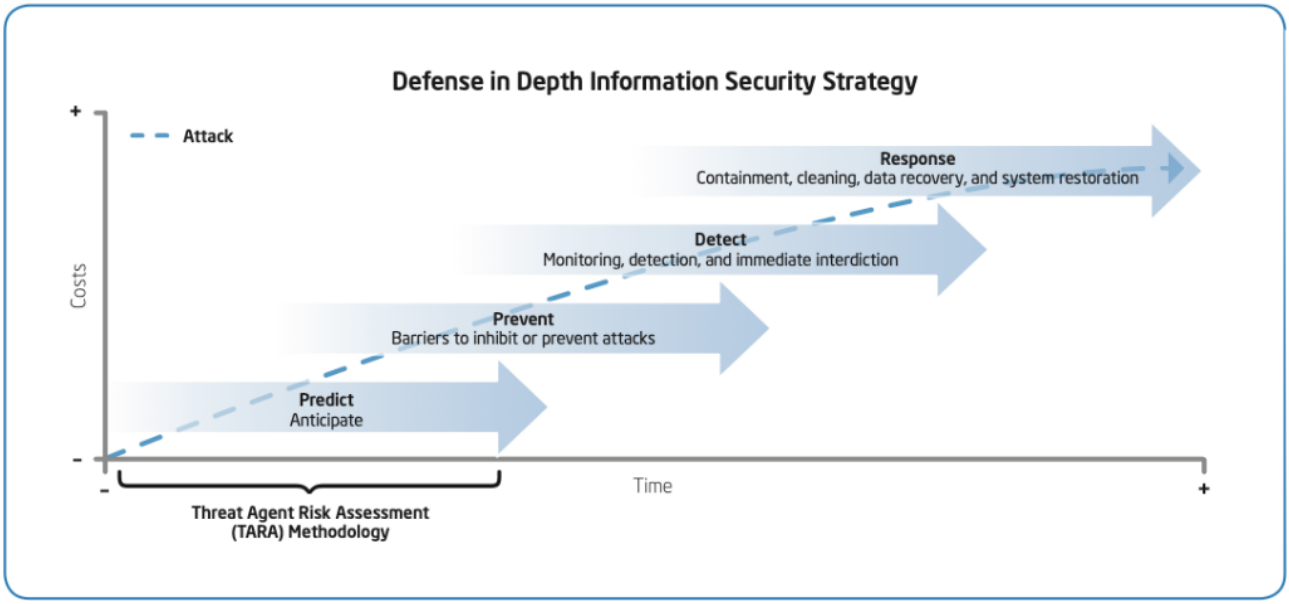
Taulukon lähde: Pushpakumar (2015 s. 52.)

Kun näitä kirjastoja käytetään ristikkäin, voidaan arvioinnissa täsmällisemmin ymmärtää kohdejärjestelmään kohdistuvat todennäköiset hyökkäykset (Rosenquist 2009).

Milloin käyttää TARA-menetelmää?

TARA-menetelmä soveltuu tietoturvan rakentamiseen sen alkuvaiheessa eli uhkien ennakoimisessa, kun tietoturvan rakentamiseen käytettävät kustannukset ovat vielä vähäiset.

Seuraavat vaiheet tietoturvan toteuttamisessa ovat esteiden rakentaminen hyökkäyksille, hyökkäysten seuranta ja tunnistaminen sekä käynnissä oleviin hyökkäyksiin reagointi. Näiden vaiheiden toteuttamisen kustannukset myös kasvavat.



TARA-menetelmä soveltuu tietoturvan rakentamiseen sen alkuvaiheessa. Kuvan lähde: Rosenquist & Casey (2009 s. 3).

Opi lisää TARA-menetelmästä

a.) TARA-menetelmän kuvaukset:

Casey, T. (2007). Threat Agent Library Helps Identify Information Security Risks. Artikkeli ResearchGate-alustalla.

Casey, T. (2015). Understanding Cyberthreat Motivations to Improve Defense.

Rosenquist, M. & Casey, T. (2009). Prioritizing Information Security Risks with Threat Agent Risk Assessment. Artikkeli ResearchGate-alustalla.

b.) Tiivis yhteenveto:

https://cio-wiki.org/wiki/Threat_Agent_Risk_Assessment_(TARA)

c.) TARA-menetelmän soveltaminen IT-hallinnossa:

Pushpakumar, Harikrishnan 2015: Understanding the threat landscape in e-government infrastructure for business enterprises. Delft University of Technology.

d.) TAL-kirjasto terveydenhuoltoalalle:

Houlding, D., Casey, T., & Rosenquist, M. (2012). Improving Healthcare Risk Assessments to Maximize Security Budgets. Solution brief. Intel.

Vastaa alla, **kuinka selkeänä pidit tämän kappaleen kuvausta TARA-menetelmästä?**

- ◊ Kuvaus on selkeä!
- ◊ Vaikeselkoisena
- ◊ Hankala arvioida. Asian sisäistäminen vaatii minulta vielä pohdintaa..
- ◊ Tarvitsen henkilökohtaista opastusta aiheeseen.

Mikä on mielestäsi TARA-menetelmän suurin vahvuus?

- ◊ Menetelmän käyttö ei vaadi suuria rahallisia investointeja
- ◊ Menetelmää voi muokata omiin tarpeisiinsa sopivaksi
- ◊ Menetelmä auttaa huomaamaan todennäköisimmät uhat
- ◊ Menetelmä opettaa tunnistamaan erilaisia uhka-agentteja
- ◊ Menetelmä tarjoaa selkeät toimintaohjeet riskien kartoittamiseen
- ◊ En osaa sanoa

Mikä seuraavista voisi olla todennäköisin uhka omalle tai yrityksesi tietoturvalle?

- ◊ Riittämätön tietotaito
- ◊ Väärän henkilön pääsy tietoihin
- ◊ Paperiasiakirjojen säilytys
- ◊ Etätöiden tekeminen
- ◊ Tahallinen vahingonteko
- ◊ Satunnainen hyökkäys
- ◊ Työntekijän huolimattomuus

3.5 Digitaalisten riskien täydentäviä määritelmiä

Oppimistavoite: Tässä kappaleessa käydään läpi kolme toisiaan täydentävää kokonaiskuvaa digitaalisista riskeistä. Lukiessasi kappaletta vertaile niissä esitettyjä huomioita omaan suhtautumiseesi digiriskien hallintaan uhkana ja mahdollisuutena. Kappaleen lopussa vastaat valinta- ja monivalintatehtäviin. Arvioitu ajankäyttö: 20 min.

Digitaalinen kokonaisturvallisuus rakentuu riskienhallinnasta, jatkuvuudenhallinnasta, kyberturvallisuudesta, tietoturvallisuudesta ja tietosuojasta. Näissä viidessä painopisteessä tehtävillä toimenpiteillä hallitaan digitaalisen toimintaympäristön riskejä.

Tässä kappaleessa käydään läpi kolme toistaan täydentävää kokonaiskuvaa digitaalisen toimintaympäristön riskeistä:

- A. Digitaaliset riskit uhkina
- B. Digitaaliset riskit liiketoimintamahdollisuuksien lähteenä
- C. Tietoriskit: staattinen ja dynaaminen riski

Määritelmillä on päällekkäisiä alueita, kuten yllä olevassa kuvassa näkyy. Usein oivallukset uusista asioista löydetäänkin näistä päällekkäisistä kohdista.

A. Digitaaliset riskit uhkina

de Oliveiran (2020) käytännönläheisen jaottelun mukaan digitaalisia riskejä on seitsemää tyyppiä.

1. Kyberturvallisuusriski

- Tämä riski kuvaa kyberhyökkäysten uhkaa. Usein näissä hyökkäyksissä on pyrkimyksenä päästä käsiksi arkaluontoisiin tietoihin ja käyttää kaapattuja tietoja haitallisiin tarkoituksiin, esimerkiksi kiristykseen tai liiketoiminnan prosessien häiritsemiseen.

2. Työvoimariski (digiosaaminen)

- Työvoimariski on ongelma, joka toteutuessaan aiheuttaa uhan organisaation tavoitteille. Työvoimariskejä ovat esimerkiksi tiettyjen digitaitojen osaamispula. Täsmällistä digiosaamista voi tiettynä hetkenä olla vaikeaa tai kallista saada käyttöön edes organisaation ulkopuolelta ostettavana palveluna.

3. Vaatimustenmukaisuuden riski

- Tämä riski viittaa uuteen teknologiaan liittyviin vaatimuksiin tai sääntöihin. Kun organisaatio ottaa käyttöönsä uuden teknologian, on olemassa uhka ettei teknologian käyttäminen lähtökohtaisesti täytä esimerkiksi liiketoimintaa, tietojen säilyttämistä tai liiketoimintakäytäntöjä koskevia säännöksiä.

4. Kolmannen osapuolen riski

- Nämä riskit liittyvät digitoimintojen ulkoistamiseen kolmansille osapuolille, kuten palveluntarjoajille.
- Kolmannen osapuolen riskejä ovat esimerkiksi immateriaalioikeuksiin, tietoihin, toimintaan, talouteen, asiakastietoihin tai muihin arkaluonteisiin tietoihin liittyvät haavoittuvuudet.
- Kolmannen osapuolen immateriaalioikeuksiin liittyvä riski olisi esimerkiksi tilanne, jossa ohjelmiston osassa käytetään avoimen lähdekoodin komponentteja ilman että selvitetään, millä lisenssillä ne on alkujaan julkaistu. Kaikki avoimen lähdekoodin lisenssit eivät mahdollista ohjelmakoodin mitä tahansa käyttöä.

5. Automaation riski

- Automaation riskejä ovat yhteensopivuusongelmat digiympäristön ja muun käytössä olevan teknologian kanssa, resurssien puute ja hallinnon ongelmat.

6. Resilienssin riski

- Tämäntyyppinen riski viittaa uhkaan negatiivisista seuraumuksista uuden teknologian käyttöönoton yhteydessä. Resilienssin riskejä ovat myös epävarmuudet ennakoida ja minimoida tästä aiheutuneet vahingot, kuten tuotantokatkokset epäonnistuneen ohjelmistopäivityksen yhteydessä.

7. Tietosuojariski

- Tietosuojariskillä viitataan arkaluonteisten tietojen suojaamisen uhkiin ja seuraamuksiin tietosuojan pettäessä. Tämäntyyppiseen tietoon sisältyvät esimerkiksi nimet, sähköpostiosoitteet, salasanat, kotiosoitteet ja syntymäajat. Tietomurtautujat voivat käyttää tietoja helposti väärin henkilöllisyyden väärinkäyttöön tai vahingoittamiseen.

B. Digitaaliset riskit liiketoimintamahdollisuuksien lähteenä (rahoitusalalla)

Rahoitusalan näkökulmasta laadittu konsulttiyritys McKinseyn raportti kuvaa seitsemän digitaalisen riskin ”rakennuselementtiä”. Riskit liittyvät liiketoiminnan digitaaliseen transformaatioon: sen hallitsemiseen ja sen mahdollisuuksista hyötymiseen.

Raportin mukaan digitaalisen riskin 'rakennuselementit' ovat seuraavat seitsemän.

1. Tiedonhallinta

- Tehostettu tiedonhallinta parantaa päätösten pohjana olevan datan laatua ja tekevät riski- ja liiketoimintapäätöksistä johdonmukaisempia. Tiedetään paremmin, mitä dataa ja datalähteitä päätöksentekoa varten tarvitaan. Tietoriski nousee riskitaksonomian avaintekijäksi. Tietoriski linkitetään asetettuun riskinottohalukkuuteen ja tiedon valvonnan viitekehykseen. Päätöksenteon pohjaksi tarjotaan paljon enemmän erilaisia tietoja ja tietolähteitä aikaisempaan verrattuna.

2. Prosessien ja työnkulun automatisointi

- Paremman tehokkuuden lisäksi älykkäät työnkulut luovat asiakkaille saumattoman ja reaaliaikaisen kokemuksen. Toimintoja voidaan toteuttaa pienemmillä kustannuksilla. Automaatio tehostaa myös sääntelyn noudattamisen seurantaa.

3. Kehittynyt analytiikka ja päätöksenteon automatisointi

- Kehittyneet riskimallit (esimerkiksi koneoppimisen algoritmeilla rakennetut mallit) voivat automaattisesti tunnistaa monimutkaisia ilmiöitä, kuten laskutuspetoksia osoittavia tapahtumaketjuja. Niillä voidaan tehdä entistä tarkempia ennusteita muun muassa asiakkaiden maksukyvyttömyydestä ja muista riskitapahtumista.
- McKinseyn selvityksen mukaan erityisesti luotonantopäätöksiin käytettävä aika lyhenee huomattavasti uudella analytiikalla ja osa päätöksistä voidaan kokonaan automatisoida.

4. Yhtenäinen, oikea-aikainen ja joustava infrastruktuuri

- Riski-infrastruktuuria kehitetään tukemaan lukuisia muita ”rakennuspalikoita” kuten innovatiivisia tiedontallennusratkaisuja, uusia rajapintoja, helpompaa pääsyä toimittajaekosysteemiin ja niin edelleen. Toteutukseen hyödynnetään digitekniikoita, kuten sovellus palveluna (software as service).

5. Älykäs visualisointi ja älykkäät käyttöliittymät

- Näkyvyyttä - ja mahdollisesti näkemystä - riskejä kuvaavaan aineiston tarjotaan aikaisempaa intuitiivisemmilla, vuorovaikutteisemmilla ja yksilöllisemmillä visualisoinneilla ja käyttöliittymillä mm. ohjelmistojen hallintapaneelien, lisätyn todellisuuden (AR) ja muiden uudenlaisien käyttöliittymien kautta.

6. Ulkoinen ekosysteemi

- Riskienhallinnassa tehdään yhteistyötä ulkopuolisten palveluntarjoajien kuten Fintech-yritysten kanssa. Yhteistyöllä tehostetaan esimerkiksi asiakashankintaa, luottovakuutusten (merkintäsitoumuksien) sopimista, petosten havaitsemista, viranomaisraportointia ja sääntelyn noudattamisen valvontaa.

7. Osaaminen ja kulttuuri

- Riskienhallinta edellyttää organisaatiossa aikaisempaa enemmän digitaitoja hallitsevaa henkilöstöä, joka hallitsee sekä riskinhallintaa että liiketoiminnan kehittymistä ja kykyä toimia ketterässä, innovaatiota ja kokeilua arvostavassa kulttuurissa. Uusiin osaamisprofiileihin kuuluvat datatieteilijät ja mallintamisen asiantuntijat.
- Kysymys yrityksen johdolle kuuluukin, miten uutta osaamista saadaan organisaatioon: kouluttamalla kokeneita riskienhallinnan osaajia digitaitoihin vai palkkaamalla dataosaajia ja kouluttamalla heitä riskienhallinnan taitoihin?

McKinseyn raportissa esitetään, miten digiriskeistä rakennetaan liiketoimintaa edellä kuvattujen rakennuselementtien avulla. Digitaalisen transformaation riskit nähdään raportissa mahdollisuutena tehdä voittoa, kasvattaa liikevaihtoa tai laajentaa liiketoimintaa.

Tässä näkökulmassa riskin käsite liittyy tuloksen tekemiseen liiketoiminnalla, sijoituksilla, lainoilla ja kaupankäynnillä finanssimarkkinoilla, joihin liittyy epävarmuutta ja joka edellyttää tarkoin mietittyä riskinottohalukkuutta, joka pohjautuu käytössä olevaan dataan ja sen tulkintaan.

Datasta tulkitaan ja tuotetaan tietoa, jolloin tietoa itsessään on suojattava mahdollisilta menetyksen uhilta eli tietoriskeiltä.

C. Tietoriskit: staattinen ja dynaaminen riski

Tieto itsessään on omaisuutta, jolle antavat lainsuojaa esimerkiksi lait liikesalaisuuksista, tekijänoikeudesta, teollisoikeuksista, tietokantaoikeudesta, jne **Toisaalta tieto on väline**, jolla tuotetaan arvoa esimerkiksi liiketoiminnan kautta. Digitaalisessa toimintaympäristössä uhkat

voivat kohdistua tiedon arvoon sekä omaisuutena (staattinen riski) että välineenä (dynaaminen riski). (WIHURI 2017)

Pauli Wihuri (2017) on esittänyt seuraavan tarkastelun tietoriskeistä staattisen riskin ja dynaamisen riskin käsitteiden kautta.

Staattinen riski	Dynaaminen riski
Riski **kohdistuu omaisuuteen**	Riski **kohdistuu tavoitteeseen**
Tieto on **omaisuutta**	Tiedon käsittely, hallinta ja kehittäminen ovat (dynaamisia) **tavoitteita**
Tieto-omaisuudella on **haavoittuvuuksia** eli ominaisuuksia, jotka asettavat omaisuuden alttiiksi riskeille	Tavoitteen saavuttamisen toteutuksessa voi tapahtua ennakoimattomia asioita
Omaisuuden suojaaminen optimoidaan riskien mukaisesti	Suunnitelmassa tavoitteiden saavuttamiseksi huomioidaan riskit etukäteen

Tietoriski

Riski k**ohdistuu tietoon tai tiedon olomuotoon** (esim. paperiarkistoon tai tietojärjestelmään).
Tietoon ei päästä käsiksi tai sen käsittely voi olla vaikeaa.
Tieto voidaan menettää tai se voi vuotaa asiaankuulumattomille.
Tieto voi olla virheellistä tai tieto ei jalostu ketterästi toiminnan tavoitteiden mukaan.

Esimerkkejä:

- Paperiarkistosta ei päästä hakemaan tietoa. Paperiarkisto voi mennä epäjärjestykseen eikä tietoa löydy. Arkisto voi tuhoutua tulipalossa. Arkistoon voidaan jättää laittamatta tietoa tai laittaa väärää tietoa.
- Tietojärjestelmä voi lakata toimimasta. Tietojärjestelmään ei päästä kirjautumaan. Tietojärjestelmä voi olla monimutkainen ja vaikeasti käytettävä. Tietojärjestelmä voi tuottaa virheellisiä tuloksia. Tieto voi vuotaa asiaankuulumattomille.
- Organisaation digitaalinen omaisuus ja tavoitteissa onnistuminen riippuvat tiedosta ja tietojärjestelmistä.
- Tiedon varmentaminen ja suojaaminen optimoidaan riskien perusteella.

Tieto-omaisuuden haavoittuvuuksia ovat kaikki sellaiset tiedon ominaisuudet, jotka altistavat omaisuuden alttiiksi riskeille.

Wihurin esittämä yhteenveto **tietoriskin neljästä tyypistä** kohdistuu yhtäältä tietoon itsessään ja siihen miten ihminen käyttää sitä, sekä toisaalta tietojärjestelmään, johon tieto on tallennettuna ja jonka kautta tietoa käytetään.

Tietoriskin tyyppi	Tieto (uhkan vaikutus)	Tietojärjestelmä (uhkan vaikutus)
Pääsy (Access)	Tietoon pääsy on hankalaa tai hidasta. Tietoon pääsy ei onnistu.	Tietojärjestelmään pääsy on hankalaa tai hidasta. Tietojärjestelmän pääsy ei onnistu.
	Tieto vuotaa asiaankuulumattomille.	Asiattomat pääsevät tietojärjestelmään.
Tarkkuus (Accuracy)	Tieto ei ole käyttökelpoista. Mahdollisia syitä: tieto on puutteellista, virheellistä tai hävinnyt	Tietojärjestelmä tuottaa virheellisiä tuloksia tai hävittää tietoa.
Ketteryys (Agility)	Tieto ei jalostu. Tietoa ei pystytä käyttämään tarpeiden mukaisesti.	Tietojärjestelmä ei kehity samassa tahdissa toiminnan kehityksen kanssa.
Ketteryys (Agility)	Tieto ei ole käytettävissä	Verkko tai tietojärjestelmä ei toimi

Näin voidaan esittää yhteenveto, jonka mukaan tietoriskejä torjutaan tarkastelemalla mahdollisia uhkia sekä tiedon että tietojärjestelmän näkökulmista.

Esimerkiksi jatkuvuuteen liittyvä tietoriski saattaa aiheutua, kun tietoverkko ei toimi katkoksen vuoksi. Tällöin organisaation jäsenillä pitää olla käytettävissään jatkuvuussuunnitelma, miten toimitaan tilanteessa, jossa toimintaan tarvittava tieto ei ole käytettävissä normaalilla tavalla.

Jos joudut valitsemaan vain yhden, mikä seuraavista kolmesta digitaalisten riskien luokittelusta on sinulle käyttökelpoisin?

- ◊ Digitaaliset riskit uhkina
- ◊ Digitaaliset riskit liiketoimintamahdollisuuksien lähtökohtana
- ◊ Tietoriskit: staattinen ja dynaaminen riski

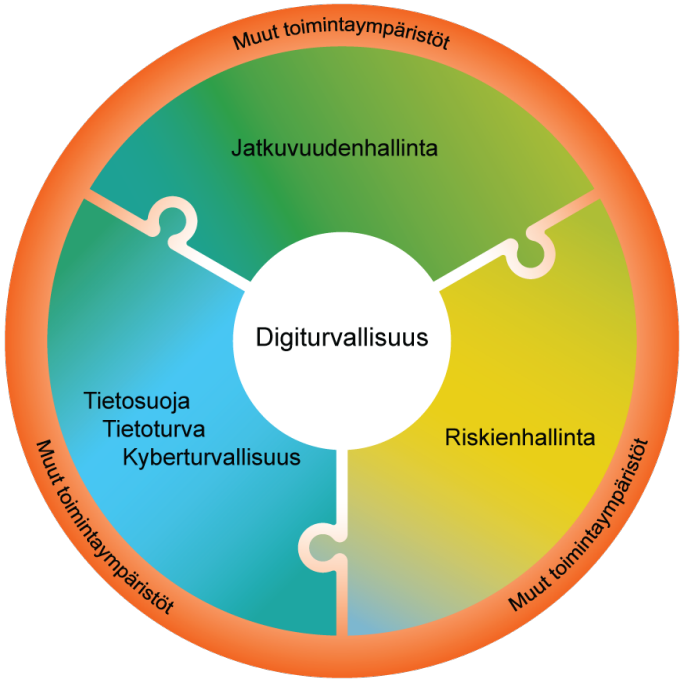
Mitkä seuraavista voisivat olla sinulle tai yrityksellesi digitaalisten riskien tuomia mahdollisuuksia?

- ◊ Digitaalinen maailma helpottaa näkyvyyden saamista.
- ◊ Digitaaliset riskit pakottavat oppimaan uusia asioita.
- ◊ Voin myydä osaamistani digiriskien asiantuntijana.
- ◊ Työtehtävien automatisointi tuo säästöjä ja nopeuttaa työtä.
- ◊ Kehittyneet ohjelmistot nopeuttavat taloushallintoa.
- ◊ Työntekijöiden osaamisen parantaminen digikoulutuksilla.

Päätöstehtävä: riskitiedon rajoilla

Oppimistavoite: Tässä kappaleessa kertaat kyberturvallisuuden, jatkuvuudenhallinnan ja riskienhallinnan periaatteet, jotta voi käyttää niitä tehokkaammin toiminnassasi. Opit myös, että osana digiturvallisuuden rakentamista on tietämisen rajallisuuden tunnistaminen ja operoiminen "tiedon ja luulon miinakentällä". Kappaleen lopussa testaat tietosi yhdistämällä käsitepareja ja jokaisesta oikeasta vastauksesta saat 10 pistettä - pääsetkö pistelistan kärkeen? Arvioitu ajankäyttö: 30 min.

Digiympäristön kokonaisturvallisuutta eli digiturvallisuutta rakennetaan riskienhallinnan, jatkuvuudenhallinnan ja kyberturvallisuuden kautta, kuten on esitetty alla olevassa kuvassa. Riskioppi-ympäristön aineistossa olet keskittynyt digitaaliseen toimintaympäristöön. On kuitenkin hyvä muistaa, että myös muut toimintaympäristöt vaikuttavat digiturvallisuuteen, sillä monenlaiset vaikutukset voivat heijastua digiympäristöstä fyysiseen maailmaan ja päinvastoin.



Tässä päätöskappaleessa esitetään käytännön vinkkejä, joiden avulla on mahdollista tehostaa jatkuvuudenhallintaa ja ratkaista yleisiä riskienhallinnan haasteita.

Digiturvallisuuden rakentamiseen ja johtamiseen kuuluu oman tiedon rajojen tunnistaminen ja operoiminen ”tiedon ja luulon miinakentällä”.

Vinkkejä jatkuvuudenhallinnan tehostamiseen

Riskienhallintaratkaisuja tarjoava Granite-yritys antaa kuusi käytännön neuvoa, joiden avulla organisaatio voi tehostaa jatkuvuudenhallintaansa.

1. Tee säännöllisiä riskiarviointeja

- Toimivan jatkuvuudenhallinnan ensimmäinen askel on tunnistaa organisaation toimintaan kohdistuvat riskit.
- Riskit muuttuvat ajan kuluessa, ja muutoksessa on pysyttävä mukana.
- Riskiprofiilin säännöllinen arviointi ja päivittäminen auttaa organisaatiota tunnistamaan uusia riskejä sekä varmistamaan, että jo seurattavat riskit ovat edelleen ajankohtaisia ja että niiden hallintaan on jatkossakin tarkoituksenmukaista kiinnittää resursseja.

2. Organisaation kaikki tasot tulee osallistaa jatkuvuudenhallintaan

- Jatkuvuudenhallinnan ei saa olla yhden henkilön tai organisaation tason vastuulla.
- Henkilökunnan osallistuminen jatkuvuudenhallinnan prosessiin organisaation kaikilla tasoilla auttaa varmistamaan, että jokainen ymmärtää roolinsa jatkuvuudenhallinnan toteuttamisessa.

3. Testaa ja päivitä jatkuvuussuunnitelmia säännöllisesti

- Jatkuvuussuunnitelmien tulee olla ajan tasalla.
- Jatkuvuussuunnitelmien säännölliseen päivittämiseen sisältyy viestintäsuunnitelmien, poikkeamanhallinnan prosessien ja palautussuunnitelmien testaaminen.
- Testauksessa havaitut puutteet korjataan päivitetyissä suunnitelmissa.

4. Kouluta jatkuvuudenhallintaan

- Organisaation jäseniä tulee tiedottaa sekä kouluttaa heidän jatkuvuudenhallintaan liittyvistä vastuistaan ja rooleistaan poikkeus- ja häiriötilanteiden varalta.
- Koulutuksen kautta jaetaan henkilöstölle myös laajemmin tietoa organisaation jatkuvuussuunnitelmista ja toimintamalleista.

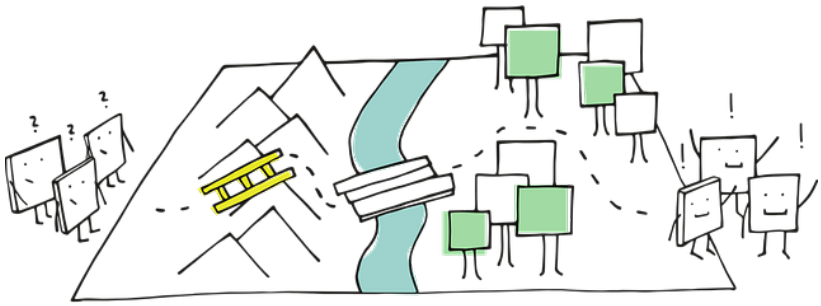
5. Toteuta kriisiviestintäsuunnitelma

- Välittömästi häiriön alettua on keskeistä, että organisaatiolla on käytettävissään kriisiviestintäsuunnitelma. Kriisiviestintäsuunnitelma antaa suuntaviivat sille, miten häiriöstä tiedotetaan työntekijöitä, asiakkaita ja muita sidosryhmiä.
- Kriisiviestintäsuunnitelma auttaa pienentämään häiriön kielteisiä vaikutuksia organisaation toimintaan.

- Lopulta kriisiviestintäsuunnitelma myös edistää normaalien toimintojen palauttamista, kun tiedotetut tahot tulevat tietoisiksi häiriöstä ja pystyvät sopeuttamaan omaa toimintaansa.

6. Paranna säännöllisesti jatkuvuudenhallinnan prosesseja

- Jatkuvuudenhallinnan prosessien tehokkuutta ja toimivuutta tulee tarkastella ja arvioida säännöllisesti.
- Jatkuvuussuunnitelmiin tehdään tarvittavia parannuksia arvioimalla toteutuneita häiriöitä ja testaamalla olemassa olevia suunnitelmia. Päämääränä on oltava, että suunnitelmissa kuvatut toimintamallit vastaavat aina liiketoimintaympäristön muuttuneisiin tarpeisiin.



Riskienhallinnan yleisten haasteiden ratkaiseminen

Graniten toinen esitys kokoaa käytännön neuvoja digiympäristössä tapahtuvan riskienhallinnan toteuttamiseen. Neuvoja seuraamalla ratkaiset neljää yleistä tehottomuutta, jotka liittyvät riskienhallintaan digiympäristössä.

I. tehottomuus: käytetyt työkalut eivät vastaa riskienhallinnan tarpeisiin --> ratkaisu: *valitse työkalut tarpeen mukaan*

- Riskienhallinnan onnistuminen pohjautuu organisaation kulttuuriin ja vastuuhenkilöiden halukkuuteen kehittää toimintaa riskienhallintakeskeisemmäksi. Tähän tarvitaan oikeat ja tarkoituksenmukaiset työkalut.
    - Kysy itseltäsi, onko esimerkiksi Excel-taulukko riittävä työkalu riskienhallintaan. Miten taulukko käytännössä jaetaan useamman tahon kesken ja miten sen päivittäminen hallitaan? Edelleen pohdi, riittääkö sähköposti jakamiseen ja versionumerointi tiedostonimessä version hallintaan vai tarvitsetko käyttöösi erityisen riskienhallintaohjelmiston.
- Riskienhallintaan on tarjolla monenlaisia ohjelmistoja.

II. tehottomuus: riskiä ei ole määritelty oikein --> ratkaisu: *määrittele riskit organisaation tavoitteiden kautta*

- Ainoastaan osa riskeistä on yhteisiä kaikille organisaatioille ja yrityksille tietyllä toiminnan alueella.
- Riskienhallinnan kannalta oleelliset riskit ovat aina tavalla tai toisella suhteessa niihin tavoitteisiin, joita yrityksen tai organisaation toiminalle on asetettu. Määritelmät yleisistä toimialalle tyypillisistä riskeistä ovat siten vasta riskienhallinnan ensimmäinen askel.
- Riskienhallintaa tehdään organisaatiota itseään varten. Ainoastaan organisaation jäsenet tietävät, mitä riski organisaatiolle tarkoittaa.

III tehottomuus: riskejä ei ole luokiteltu --> ratkaisu: *hyödynnä riskien luokittelua*

- Riskien luokittelu on keskeinen osa riskienhallintaa. Riskejä luokittelemalla opitaan tunnistamaan riskejä aiempaa täsmällisemmin. Riskien luokittelu tekee riskien jatkuvasta tunnistamisesta ja hallitsemisesta helpompaa. Lisäksi riskien luokittelu auttaa organisaatiota hahmottamaan oman liiketoimintaympäristön ominaispiirteitä.
- Riskien luokittelun tarkoitus on ymmärtää jokaisen tunnistetun riskin muodostumisen syyt ja ilmenemisen muodot.
- Järjestelmällisestä riskien luokittelemisesta huolimatta eri riskilajit voivat esiintyä joissakin tapauksissa limittäisinä. Suositus onkin, että riskien luokittelussa sovelletaan eri kategorioita.

IV. tehottomuus: riskejä ei ole arvioitu yhteismitallisesti --> ratkaisu: *arvioi riskejä yhteismitallisesti*

- Osa riskeistä on sellaisia, että niiden voikin antaa toteutua ilman, että niillä on merkittävää vaikutusta toiminnan tavoitteisiin.
- Kaikki riskit eivät ole lähtökohtaisesti samanarvoisia. Harkituista hallintatoimenpiteistä huolimatta jotkut riskit toisinaan realisoituvat, eikä asialle voi mitään.
- Riskienhallinnan toimenpiteet vaativat priorisointia. Priorisoinnin lähtökohtana tulisi olla riskien vaikutusten keskinäinen vertailtavuus. Lisäksi riskien vaikutuksia tulee arvioida suhteessa vaikutusten toteutumisen todennäköisyyteen.
- Haasteena on Graniten mukaan se, että vaikutusten kirjo saattaa vääristyä, kun organisaation eri vastuualueet tekevät arviointeja ja niitä tehdään eri näkökulmista. Organisaatiolle saattaa muodostua todellisuudesta irrallaan oleva joukko kriittisinä pidettyjä riskejä, joka vesittää koko arvioinnin lähtökohtia.
- Ratkaisuksi Granite esittää, että ensin määritellään pahimmat realistiset vaikutukset, jotka riskillä on. Sen jälkeen arvioidaan sen todennäköisyys, että nämä pahimmat vaikutukset toteutuvat.

Oikea työkalun valitseminen sopivaan käyttöön on keskeistä myös onnistuneessa riskienhallinnassa.

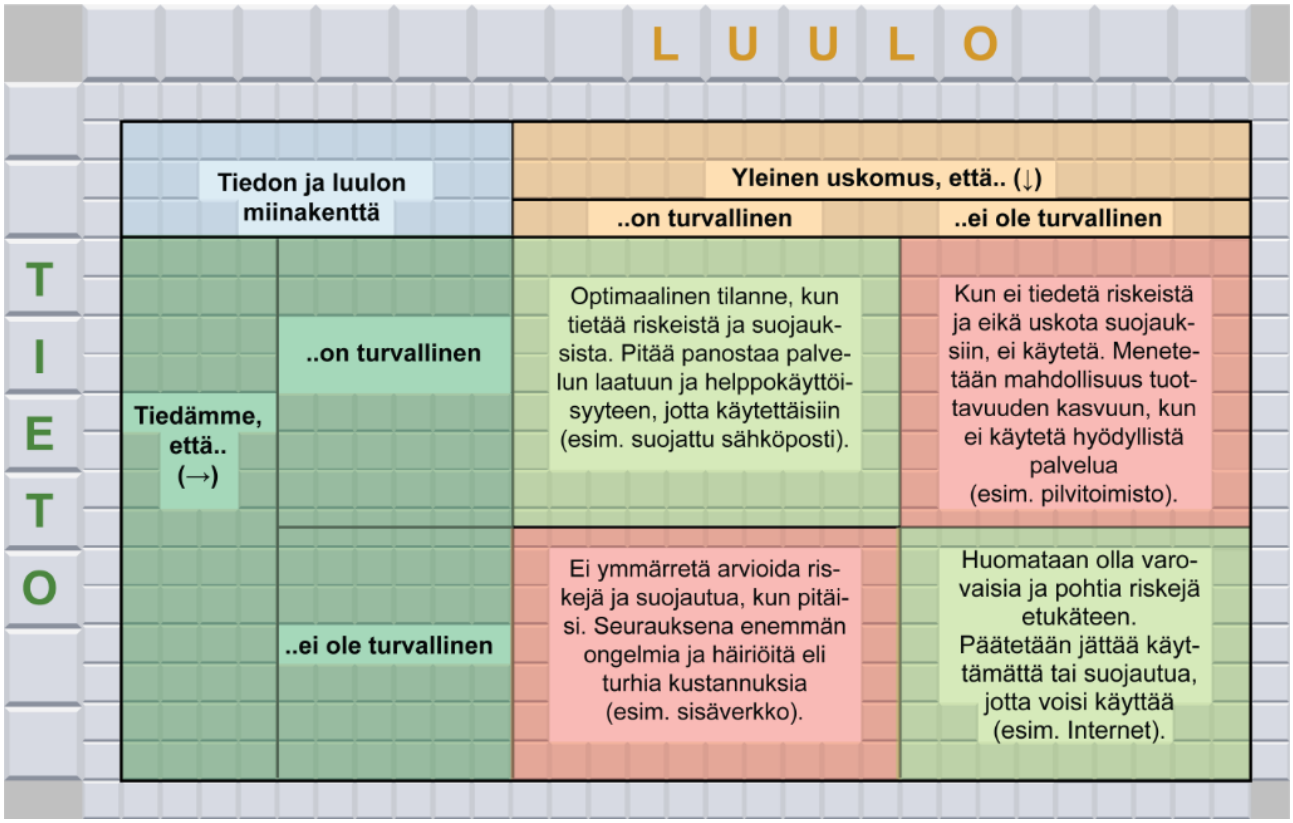
Itsearvioinnin miinakentät kokonaisturvallisuuden hallinnassa

Miinakenttä saattaa aluksi vaikuttaa hurjalta metaforalta kokonaisturvallisuuden hallinnalle. Asiaa tarkemmin miettiessäsi saatat huomata ilmeisen yhtäläisyyden: kuten miinakentällä, osa tulevista ongelmista voidaan vain ennakoida parhaimman käytössä olevan tiedon ja sen tulkitsemisen avulla.

Riskienhallinnan, jatkuvuudenhallinnan ja kyberturvallisuuden rakentaminen perustuu tietoon siitä, millaisia uhkia omaan toimintaan kohdistuu: mikä voi olla uhkaksi ja millä tavoin, ja mitä organisaation toimintoja ja omaisuutta tulee suojata uhkilta.

On tärkeää tiedostaa myös se, että kaikkea ei voida tietää. Joskus voi käydä niin, että lähtötiedot tulkitaan väärin tai jotain olennaista jää huomaamatta. Tietämättömyyden tunnustaminen voi olla viisauden alku.

Tiedon ja luulon miinakentällä on nimensä mukaisesti kaksi ulottuvuutta: se mitä tiedetään ja se mitä uskotaan (WIHURI 2017). Tämä nelikenttä on kuvattu alla olevassa kuvassa.



Tiedon ja luulon miinakenttä (mukaeltu WIHURI 2017).

Mahdolliset vaarat – eli kuvassa punaisella merkityt ”miinoitetut” alueet – ovat vaarallisia tiedon ja luulon yhdistelmiä siitä, kuinka turvallista toimintaa rakennetaan ja ylläpidetään:

i. Tiedetään, että jokin asia ei tietyissä olosuhteissa ole turvallinen, mutta luullaan, että tällaiset olosuhteet ovat harvinaisia eivätkä kosketa omaa toimintaa.

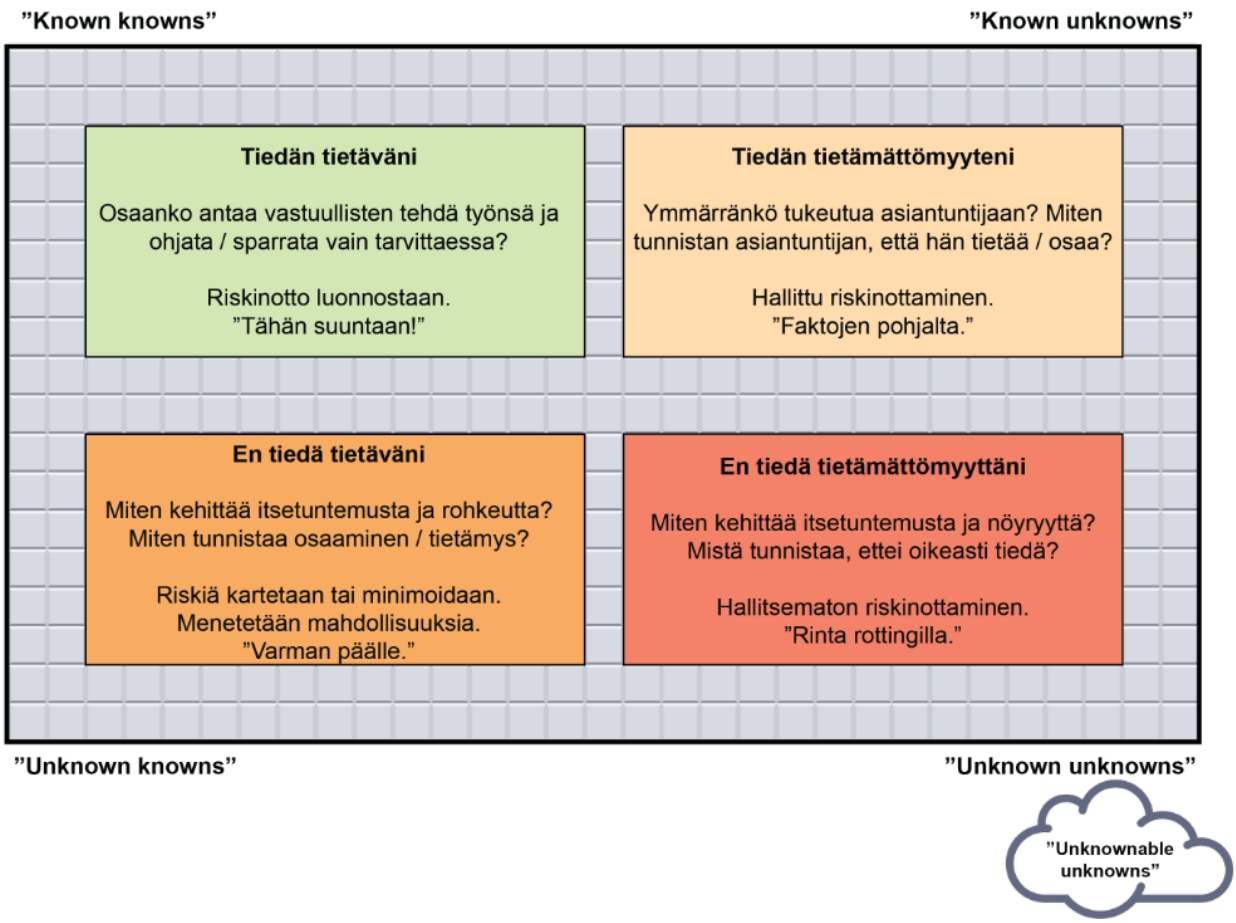
ii. Tiedetään, että jokin asia on turvallinen, mutta luullaan, että asia ei olisikaan turvallinen.

Toiminnassa tulisikin pyrkiä pysymään vihreällä merkityillä alueilla, eli tunnustetaan tietämättömyys asian turvattomuudesta ja se, että asiassa toimitaan luulojen varassa. Näin toimimalla voidaan huomata alue tai asia, jonka kanssa on oltava varovainen ja johon liittyviä riskejä tulee pohtia etukäteen.

Riskien tunnistaminen riippuu käytössä olevasta tiedosta, ja tiedolla on rajansa. Riskejä voidaan hallita myös tiedostamalla oman tiedon rajat eli pohtia, mitä kaikkea ei tiedetä ja mitä vaikutusta tällä tietämättömyydellä voi olla lopputuloksena tehtävään tulkintaan.

Pohdi, onko uhka mielestäsi asia, jota ei tiedetä.

Oheinen nelikenttä auttaa hahmottamaan tätä kysymystä.



Nelikenttä (mukaeltu WIHURI 2017).

Yllä oleva nelikenttä kuvaa erilaisia yhdistelmiä **riskin tuntemisen** ja **riskin vaikutusten tuntemisen** välillä käytettävissä olevan tiedon perusteella. Lisäksi viidentenä mahdollisena riskin tyyppinä on kokonaan nelikentän ulkopuolelta määrittyvä riski.

Nelikenttä pohjautuu viiden kohdan jaotteluun riskien ennakointitiedon tiloista (engl. states of risk forecasting knowledge). Seuraavassa yhteenveto niistä (pohjautuu lähteeseen Manning et al. 2020).

1. ”Known knowns”

- Riski ja sen vaikutukset voidaan tunnistaa.
- Vaikka riski vaikutuksineen tunnistetaan, voi se silti olla uhka, jos riskin käsittelemistä vältetään sen vaikutusten merkittävyyden vuoksi tai riskin käsittelyn vaatimien resurssien vuoksi.

2. ”Known unknowns”

- Riski tunnetaan, mutta ei voida arvioida sen vaikutuksia eikä näiden vaikutusten toteutumisen todennäköisyyttä.

3. ”Unknown knowns”

- Riskiä ei tunneta kovin hyvin, mutta siihen kiinnitetään huomiota, koska sen vaikutukset omalle toiminnalle arvioidaan merkittäviksi.

4. ”Unknown unknowns”

- Riskiä ei tunnisteta, koska siitä ei ole saatavilla riittävästi tietoa. Näin ollen myöskään riskin vaikutuksia ei voida arvioida.

5. ”Unknowable unknowns”

- Riskiä ei voida tunnistaa, koska sen aiheuttajaa ei joko tunneta tai osata ajatella riskin lähteenä. Tällöin myöskään riskin vaikutuksia ei pystytä arvioimaan. Tällaisia riskejä kuvataan ”mustina joutsenina”.
- Vasta realisoitumisensa jälkeen tällainen riski näyttäytyy siinä valossa, että se olisikin voinut olla tunnistettavissa. Tällöin riskiä voidaan jatkossa tarkastella kategorian 1 kautta.

Päätöstehtävänä, muodosta seuraavissa ryhmissä parit käsitteen ja sen määrittelyn kanssa. Käsitteet ovat eri kohdista Riskioppi-ympäristön moduuleita, eli käsittelevät digiturvallisuuden kokonaisuuden 'rakennuspalikoita'.

Ryhmä 1: Jatkuvuudenhallinta ja kyberturvallisuus

Poikkeama	Tilanne, jossa asiat eivät etene suunnitellusti tai odotetulla tavalla
Poikkeusolot	Syy digiympäristössä ja vaikutus on fyysisessä ympäristössä
Kyberriski	Syy fyysisessä ympäristössä ja vaikutus digitaalisessa ympäristössä
IT-riski	Sisältää kirjalliset määrittelyt vastuista ja toimenpiteistä häiriötilanteiden varalle
Jatkuvuussuunnitelma	Kansainvälisestä tilanteesta tai suuronnettomuudesta johtuva vakava vaara

Ryhmä 2: Häiriöiden kartoittaminen ja tietosuoja ja tietoturva

Häiriö	Heikkous, puute tai vika, joka mahdollistaa häiriön
Hyökkäyspinta	Tapahtuman yleisyys * tapahtuman vaikutuksen arvioitu merkittävyys
Riski-indeksi	Tilanne, joka aiheuttaa suunnittelemattoman negatiivisen poikkeaman
Mahdollistaja	Koostuu kaikesta järjestelmän toiminnallisuudesta, jonka kanssa hyökkääjä voi toimia
Tietoriskianalyysi	Arvio uhista, jotka kohdistuvat luottamuksellisuuteen, eheyteen, saatavuuteen ja kiistämättömyyteen

Ryhmä 3: Elinkaariajattelu

Elinkaariajattelu	Menetelmä, joka pienentää tuotteen/palvelun ympäristövaikutuksia
Ekosuunnittelu	Tuotteen/palvelun ympäristövaikutukset, jotka pienentävät esim. asiakkaan päästöjä
Kestävä kehitys	Ympäristön kantokyky otetaan huomioon taloudellisessa kasvussa ja hyvinvoinnissa
Hiilikädenjälki	Tuotteen tai palvelun elinkaaren aikana syntynyt ilmastokuormaa
Hiilijalanjälki	Tarkastelee tuotteiden/palveluiden elinkaarta, alkaen raaka-aineiden hankinnasta hävittämiseen asti

Lähteet

Lähdeluettelo on koottu tälle sivulle.