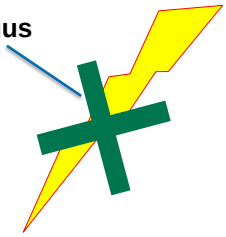
Tieto- ja kyberturvallisuus

Käsitteet ja perusteet

Mitä on kyberturvallisuus (2010)

Kyberturvallisuus



Kyberhyökkäykset

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

Kybertila

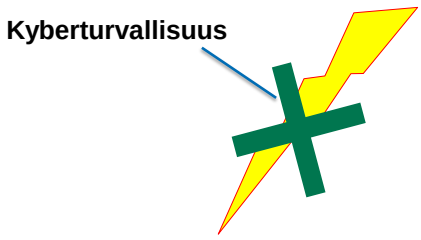
A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers

CNSS Instruction No. 4009, 2010

2

USA:n kansallisen turvallisuusjärjestelmien komitean (CNSS) vuoden 2010 määritelmän mukaan kyberturvallisuus on kybertilan suojaamista kyberhyökkäyksiltä.

Mitä on kyberturvallisuus (2010)



Kyberturvallisuus

Kyberhyökkäykset

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

Tietoturva (CIA)

Kybertila

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers

Vain IT ("toimistotietotekniikka") ei OT ("teollisuusautomaatio")

CNSS Instruction No. 4009, 2010

3

Olennaista vanhassa määritelmässä oli se, että hyökkäys sidottiin perinteiseen IT-infraan (työasemiin, palvelimiin, tietoverkkoihin ym.) sekä näiden sisältämän datan turvaamiseen (luottamuksellisuuteen, eheyteen ja saatavuuteen). Näissä määritelmissä on muutamia haasteita, kuten esimerkiksi teollisuusautomaatiota vastaan hyökkääminen, hyökkäyksen seuraukset ja niiden laajuus sekä tapahtuneen seurauksen tahallisuus.

Kyberturvallisuuden määritelmä tänään?

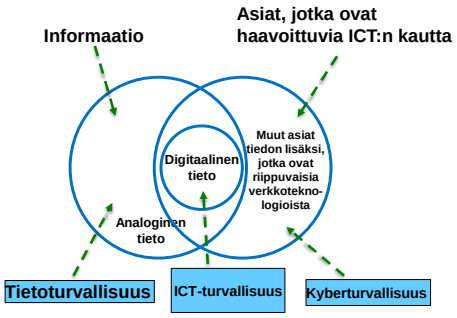
- **Fyysisten uhkien torjunta kyberturvalla**
  - Esim. palveluiden siirtäminen pilveen
- **Kyberuhkien torjunta fyysisin keinoin**
  - Esim. palvelininfran takavarikointi
- **Uhkat laajempia kuin vain ICT ja data**
  - Kriittinen infrastruktuuri
- **Mikä on tarkoituksellista?**
  - Miten tunnistetaan inhimillinen erehdys?
- **Entä tekoäly?**
- **Miten vahinkoihin tulee varautua?**
- **Tietoturvallisuus vs. käyttöturvallisuus**
  - Security vs. safety

4

Fyysinen maailma ja kybermaailma kietoutuvat tiukemmin ja tiukemmin yhteen.
Pelkästään vahinkoja tulkitsemalla on nykyisin entistä vaikeampaa erottaa inhimilliset erehdykset tahallisesta toiminnasta; saati sitten kohdennettu hyökkäys esimerkiksi yleisestä haittaohjelmakampanjasta: Floridan vedenpuhdistamossa käynyt tapaus sisälsi kaikki kyberhyökkäyksen tunnusmerkit, mutta oli lopulta työntekijän virhe.
Perinteiset tietoturvallisuuden suojauksen määritelmät eivät lisäksi ole enää riittäviä tekoälyn kanssa, uhkamallit ovat paljon laajempia.

Kyberturvallisuuden määritelmä tänään?

- **Kyse ei ole vain datasta**
  - … mutta data on kybertoimintaympäristön ja –turvallisuuden ytimessä
- **Tässä käytettävä määritelmä:**
  - Kyberturvallisuus on datan ja datasta riippuvien järjestelmien suojaamista haitallisilta vaikutuksilta, ja muiden järjestelmien suojaamista datan ja datasta riippuvien järjestelmien aiheuttamilta uhilta ja niiden väärinkäytöltä
- **Huom.**
  - Kyberturvallisuus ei aina ole paras suojauskeino → kokonaisriskienhallinta

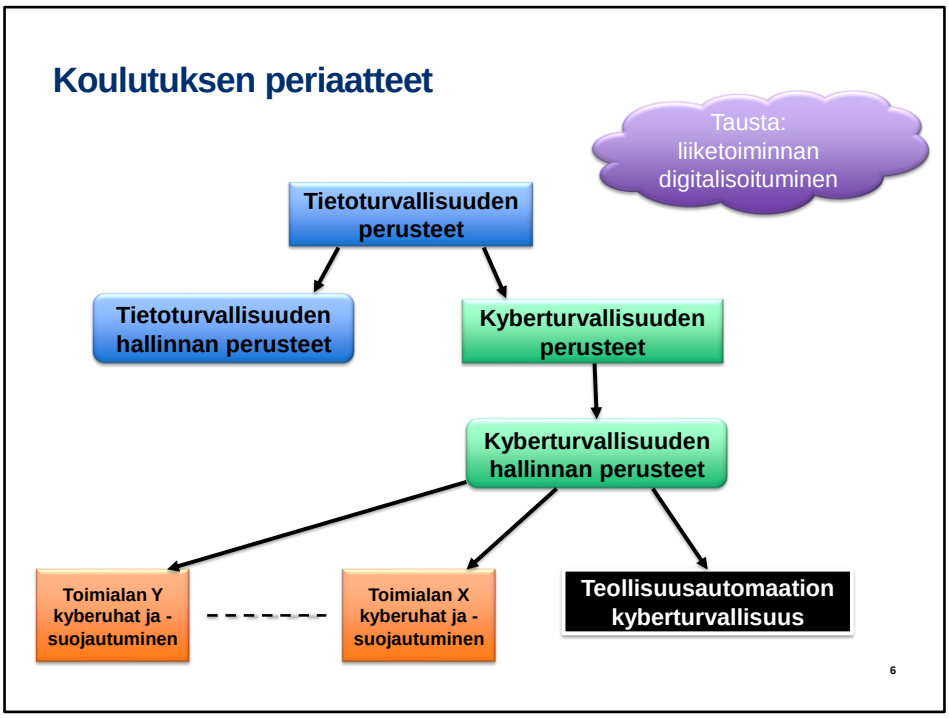


5

Tietoturvallisuus käsittää myös analogisen tiedon, ja toisaalta jättää huomiotta tai ainakin tulkinnanvaraiseksi sen, miten esimerkiksi teollisuusautomaatiota tulisi käsitellä. Data on kyberturvallisuuden ytimessä, mutta se ei ole sen koko kuva.

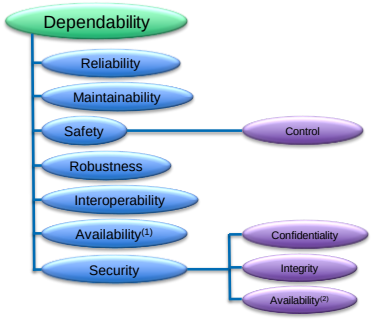
On hyvä huomata, että kyberturvallisuus pitää hallinnollisesti nähdä osana muuta organisaation riskienhallintaa. Kaikkiin kyberuhkiin ei ole kustannustehokasta varautua kybertekniikoilla, vaan esimerkiksi ulkoistamalla riski (vakuutus) tai hallinnollisin sanktioin.

Koulutuksen periaatteet



Datan ja järjestelmien suojaamisen käsitteitä

- **Lähestymistavasta riippuen**
  - Puhdas tietoturva
  - Systeemitieteet
  - Teollisuusautomaatio
  - Tekoäly
- **Suojaamisen käsitteillä sovelluskohtaista priorisointia**



Trustworthy AI goals
(NIST AI-100-1)

7

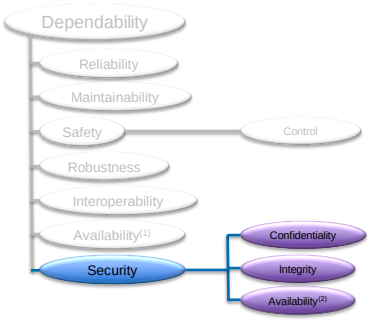
Niinkutsutut CIA-attribuutit ovat kuitenkin melko uusi käsite. Nk. Toimintavarmuus nousi esille jo 1830-luvulla, ja erityisesti ensimmäiset analogiset tietokoneet 1940- ja 50-luvuilla käyttivät epäluotettavia komponentteja ja tärkeintä oli ylipäätään laskennan saaminen päätökseen. Monet toimintavarmuuden käsitteet ovatkin ymmärrettävissä tätä kautta.

Toimintavarmuuden käsitteitä ovat mm.
- Toiminnan luotettavuus ympäristön olosuhteiden heiketessä. RRR-mallissa (reliability, resiliency, robustness) luotettava (resilient) järjestelmä toimii oikein normaaleissa olosuhteissa; vikasietoinen (resilient) järjestelmä toimii, vaikkakin heikommin, myös epänormaaleissa olosuhteissa ja kestävä (robust) järjestelmä toimii normaalisti myös (tiettyjen rajojen sisällä olevissa) epänormaaleissa olosuhteissa.
- Huollettavuus (maintainability), tarkoittaa, että järjestelmää on fyysisesti, teknisesti ja organisaation prosessien kannalta ylipäätään mahdollista huoltaa
- Fyysinen turvallisuus (safety) tarkoittaa sitä, että ihmiset ja järjestelmät säilyvät vahingoittumattomina
- Saatavuutta on kahta lajia: järjestelmän “pysyminen pystyssä” ja tietoturvallisuuden saatavuus vain luvitetuille käyttäjille.

Tekoälyn turvallisuusominaisuuksien katsotaan ulottuvan laajemmalle, ja mukana on tekoälyn luotettavan toiminnan lisäksi myös yhteiskunnallisia ulottuvuuksia, kuten vähemmistöjen suoja.

Datan suojaamisen käsitteitä

- **Tietoturvallisuus**
- **= Datan turvallisuus**
- **Perinteisellä priorisoinnilla:**
  - Luottamuksellisuus (Confidentiality)
  - Eheys (Integrity)
  - Saatavuus (Availability)
- **= C + I + A**



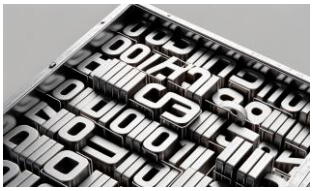
8

Tietoturvan peruskäsitteet ovat
- Luottamuksellisuus (C)
- Eheys (I)
- Saatavuus (A)

Lyhyesti: tiedon pitää olla luotettavaa ja saatavissa vain sen tarvitsijoille

Data and tietoturva nykyisin

- **Datan “liiketilat”**
  - Tietoliikenne (Data-in-transit, perinteinen)
  - Säilöttävä tieto (Data-at-rest, perinteinen)
  - Laskennassa oleva tieto (Data-in-computation/use, uusi)



9

Liikkeessä olevaa tietoa (data-in-transit, esimerkiksi Internetissä kulkeva data tai Netflixistä TV:hen tuleva stream) on suojattava pääosin eri mekanismein kuin paikallaan olevaa, esimerkiksi tietokantoja ja tiedostoja. Tärkein ero suojausmekanismeissa on, että liikkeessä olevaa tietoa suojattaessa suojausmekanismi on helpompi irrottaa itse datasta: data voidaan antaa suojatun siirtomekanismi käyttöön ja poistaa sieltä, kun siirto on tapahtunut. Säilöttävän data suojausprosessi ei ole useinkaan yhtä suoraviivainen.

Laskennassa olevan datan suojaaminen on vielä uutta tiedettä: on vaikeaa tehdä operaatioita datalle, jos datasta ei voi tietää mitään. Tämä on haaste erityisesti tekoälyssä.

Perusattribuuteista johdettuja tavoitteita

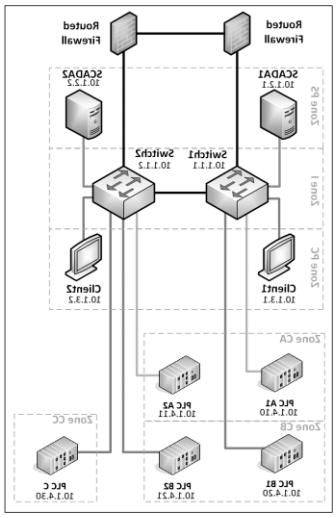
- **Luottamuksellisuudesta johdettuja**
  - Yksityisyys = Tiettyjen henkilöön sidottujen tietojen luottamuksellisuus
  - Yksityinen laskenta = Laskennassa olevan datan luottamuksellisuus

- **Eheydestä johdettuja**
  - Autenttisuus = Esim. lähettäjän identiteetin eheys
  - = Myös: datan alkuperätiedon eheys
  - Kiistämättömyys = Datan luojan/käsittelijän identiteetin eheys
  - IoT-laitteen attestaatio = Koodin tai metatietojen eheys
  - Tietokannan yhtäpitävyys = Tietokantataulujen yhtenevyyden eheys
  - Lohkoketjun konsensus = Tapahtumaketjun järjestyksen eheys

10

Yleisiä tietoturvan periaatteita: eristäminen

- **Idea:**
  - Monimutkaisuuden vähentäminen
  - Hallittavissa oleva määrä tarkastuspisteitä
- **Eri periaatteita eristämiseen:**
  - Politiikkataso: roolinhallinta
  - Politiikkataso: tiedon herkkyysluokat
  - Tekninen taso: verkon segmentointi
  - Fyysinen taso: fyysinen erottelu (“airgap”)



11

Roolinhallinta viittaa auktorisoinnin ts. pääsynhallinnan sitomiseen rooleihin (/tehtäviin) pikemmin kuin henkilöihin. Henkilön yhtäaikaa hyödynnettävissä olevien roolien tyyppeihin asetetaan rajoituksia (nk. Vaaralliset työyhdistelmät). Sama henkilö ei esimerkiksi voi olla laskun tekijän ja laskun hyväksyjän roolissa, ainakaan saman laskun osalta.

Politiikkatasolla voidaan myös luokitella tieto sen herkkyyden perusteella ja perustaa käsittelymenetelmiä luokituksen (esim. “YRITYSLUOTTAMUKSELLINEN”) perusteella.

“Air gap” tarkoittaa, että järjestelmät erotellaan fyysisesti riittävän kauas toisistaan. Tästä ei kuitenkaan välttämättä seuraa turvallisuutta, koska fyysisesti eriytetytkin järjestelmät ovat tekemisissä muiden kanssa esim. USB-median avulla.

Yleisiä tietoturvan periaatteita: virhetilanteiden käsittely

- **Järjestelmän logiikan pettäminen → kyberhyökkäykset**
- **Entä jos…?**
  - Syötteen rajoitukset
  - Järjestelmän käyttöpolitiikan muutokset
  - Rajapintojen muutokset
- **Määrittelemätön toiminto**
- **Määritelty toiminto (mutta tunnistettu)**
- **Määritelty ja käsitelty toiminto**

- **Testaus, validointi, verifiointi ja harjoittelu**

12

Kyberhyökkäykset pääsevät lävitse järjestelmiin kohdista missä järjestelmän toimintalogiikka pettää. Useimmiten tämä pettää juuri kohdissa, joissa toiminnallisuutta ei ole tarkkaan määritelty ja tiedostettu, erityisesti tämä koskee järjestelmän virhetilanteiden käsittelyä.

Entä jos…?

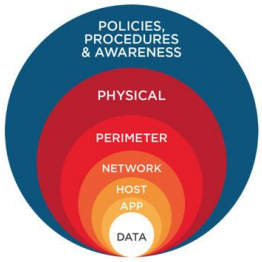
- Järjestelmä saakin “Kyllä/ei”-vastauksen sijasta 2G karttakuvan?
- Henkilön vaihtaessa tehtävää organisaation sisällä vanhat roolit jäävätkin voimaan ja johtavat vaarallisiin työyhdistelmiin (esim. Pääsee hyväksymään omat laskunsa)
- Maksujärjestelmä noudattaakin hieman vanhaa yhteysstandardia

Vaikeampia asioita on ylipäätään tunnistaa erilaiset virhetilanteet. Näitä on kaikilla abstraktiotasoilla koodin kirjoittamisesta käyttövaltuuspolitiikkoihin. Jo se, että virhetilanteet ja muut toiminnot on tunnistettu ja määritelty auttaa hyökkäyksen sattuessa vähintään tekemään korjaavia toimenpiteitä. Parhaassa tapauksessa epäsuotuisasti vaikuttava toiminto on myös korjattu tai vähintään mitigoitu.

Koska kaikkiin järjestelmiin koodista organisaation riskienhallintaan jää virheitä, ainoa ratkaisu on testata ja uudelleenarvioida niitä säännöllisesti ja erityisesti muutospisteissä.

Yleisiä tietoturvan periaatteita: syväpuolustus

- **Syväpuolustus = Defence in Depth (DiD)**
- **DiD = "***Useiden eri vastakeinojen soveltamista kerroksellisesti tai peräkkäisin askelin turvatavoitteiden saavuttamiseksi. Metodologia sisältää heterogeenisten turvateknologioiden käyttöä kerrostamalla niitä yhteisten uhkavektorien suunnassa niin, että yhden teknologian pettäessä uhan estää toinen teknologia eri kerroksella***." (IEC 62443)**
- **Tämänhetkinen jaottelu:**
  - *Politiikat*: luo hyvät säännöt, sitouta ihmiset niihin
  - *Tilaturva:* tuki loogisen suojauksen kiertomahdollisuudet
  - *Verkko/reuna:* suojaa virtuaalisen tason pääsyä usealla organisaation rajoilla (ulkoisilla ja sisäisillä)
  - *Työsema/palvelin:* suojaa loppukäyttäjän laite erikseen
  - *Sovellus:* luotettu sovelluksen asennus, päivityksen, käyttäjäntunnistus,…
  - *Data*: CIA, esim. Salaa tiedot luottamuksellisuuden takaamiseksi



13

DiD-periaate on datakeskeistä, mutta käyttäjääkään ei voi unohtaa: myös käyttäjänhallinnan ja todentamisen on oltava monikerroksista. On kuitenkin huomioitava, että monikerroksinen käyttäjän todentaminen EI tarkoita salasanan kysymistä joka viides minuutti, VAAN tietoturvapalveluiden integrointia esimerkiksi SSO:n kautta.

Politiikat: sääntöjen tulisi noudattaa yrityksen prosesseja ja soveltuvaa viranomaissääntelyä. Sääntöjä, eli "hallinnollisia kontrolleja" ei tule keksiä helpottamaan hallintohenkilöstön töitä, koska turhat säännöt johtavat pelkästään niiden kiertämiseen ja tärkeidenkin sääntöjen noudattamatta jättämiseen.
Tilaturvallisuus on kyberturvallisuuden kannalta olennaista, koska esimerkiksi palomuuri (joka on loogisen tason kontrolli) ei suojaa siltä, että joku kävelee ovesta sisään, ja asentaa hakkerityöaseman konttorin sisäverkkoon.

"Reuna" (perimeter) on tietyntyyppisen turvallisuusajattelun käsite, jossa luodaan samaa turvatasoa olevien fyysisen tilan, tietoverkkojen ja tietojärjestelmien kokonaisuuksia, turva-alueita. Tarkastaminen ja toiminnan rajoittaminen tehdään nimenomaan turva-alueiden rajalla tai reunalla. Turva-alueet on luonnollista asettaa organisaation hierarkian mukaisesti, koska

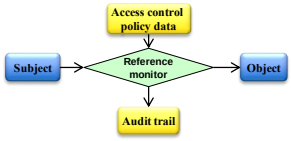
hierarkia *yleensä* noudattelee liiketoimintaprosesseja ja niiden perusteella tehtyjä turva-aluerajoja.

Nykyisissä dynaamisissa organisaatioissa ja projektiluontoisessa työssä joudutaan toimimaan organisaatiorajojen ylitse, ja tietojärjestelmätkin ovat pilvessä. Tämä ei kuitenkaan tarkoita sitä, että syväpuolustus unohdetaan, vaan että pilvipalvelun tarjoaja hoitaa osan esimerkiksi fyysisestä, ja reuna-alueen turvallisuudesta. Tällaisessa toiminnassa turva-alueet ovat dynaamisempia ja muodostavat lisäkerroksia aiempien virtuaalisten turva-alueiden sisälle, esimerkiksi Teams-palvelun pääsynhallintalistojen tai VPN:n avulla.

Tietoliikenneprotokollat ovat nykyisin jo hyvin mietittyjä sitä uhkamallia varten, että hyökkääjä salakuuntelee tai yrittää vaikuttaa itse protokollaan verkon ylitse. Sen sijaan päätelaitteissa on lukuisia muita sovelluksia, jotka eivät ole yhtä hyvin suojattuja. Useimmiten hyökkääjä pyrkiikin murtamaan päätelaitteesta jonkin heikomman sovelluksen, jota kautta saadaan koko päätelaite haltuun. Tämän jälkeen tietoliikennettä voidaan “kuunnella” pelkästään urkkimalla vaikkapa puhelimen mikrofonia tai ottamalla näyttökuvia. Tämän vuoksi myös päätelaitteen suojaaminen on olennaista.

Yleisiä tietoturvan periaatteita: kuristuspisteet

- **Idea: jokaisen tapahtuman tarkastaminen joka paikassa on liian kallista**
  - Vähennä tapahtumia → järjestelmän käytettävyys kärsii
  - Vähennä tarkastuksia → jotkin tapahtumat jäävät tarkastamatta, ja turvallisuus kärsii
- **Pakotetaan suurin osa tapahtumista muutamien kanavien lävitse (kuristuspisteet)**
  - Epäilyttävien tapahtumien tarkastaminen (+karsiminen)
  - Suorituskyky voi kärsiä (esim. IoT)
- **Esimerkkejä: palomuuri, IDS**
- **Toimii turva-alueajattelun kanssa**
  - Turva-alueiden välinen liikenne ainoastaan kuristuspisteiden kautta
- **Tarvitsee tietoturvapolitiikan toimiakseen**
- **Tulee jättää lokitiedot siitä, mitä tapahtui ja millä perusteella**



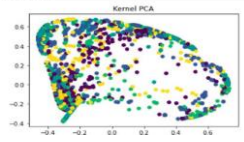
14

Yleisiä tietoturvan periaatteita: poikkeamien havaitseminen

- **Tietojärjestelmien monimutkaisuus → monipuoliset käyttötavat**
- **Luvaton käyttötapa → poikkeava jalanjälki**
  - … kuten myös jotkin käyttäjät ja erikoiset käyttötavat
- **Poikkeava jalanjälki vahva tunnistustapa**
- **Mikä onkaan "normaalikäyttöä"?**
  - Voi vaatia operatiivisessa käytössä olevan järjestelmän seurantaa ja analysointia jonkin aikaa
- **Kuinka poikkeavuudet huomataan?**
  - Määriteltävä metriikat, tilastot ja ulottuvuudet
  - Yleensä valmiiden tuotteiden osana
- **Käyttö niin verkko- kuin päätelaiteturvallisuudessa**
  - IDS/IPS
- **Tekoälyratkaisut tässä hyvin toimivia ja helppokäyttöisiä**

```
#Kernel PCA
kpca = KernelPCA(kernel='rbf', gamma=1)
X_kpca = kpca.fit_transform(X_train)

plt.title("Kernel PCA")
plt.scatter(X_kpca[:,0], X_kpca[:,1], c=y_train)
plt.show()
```



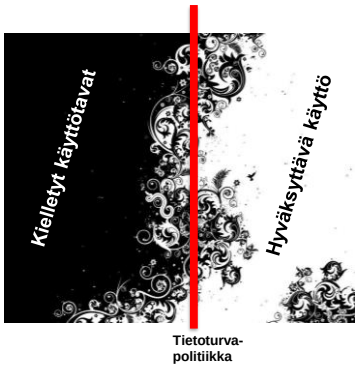
15

Nykyiaikainen organisaatio tarvitsee hyvin monenlaisia tapoja käyttää tietojärjestelmiä. Luvaton käyttö, mikäli tietoturvapolitiikka on asetettu järkeväksi, aiheuttaa jo määritelmän mukaankin poikkeavaa käyttäytymistä tietojärjestelmissä. Tämä on sinänsä hyvin toimiva periaate vahingollisen kybertoiminnan havaitsemiseen (ei siis vielä torjuntaan). On kuitenkin oltava realistinen kuva siitä, mikä on aidosti normaalikäyttöä: pelkkien asetettujen käytänteiden perusteella sitä ei voi päätellä, koska organisaatiossa muodostuu monia hyödyllisiä tapoja virallisten sääntöjen huomioimatta jääneille alueille. On siis kyettävä jollakin tavalla jalkautumaan organisaation jokapäiväiseen toimintaan, nimenomaan tietoliikenteen ja järjestelmien käytön tasolla.

Erilaiset tekoälyratkaisut ovat tällaisessa tarkoituksessa tehokkaita, koska ne kykenevät oppimaan myös tunnistamattomia tapoja käyttää tietojärjestelmiä pelkästään lokitietojen tai tietoliikenneprofiilien perusteella, ja analysoimaan niitä useammassa ulottuvuudessa.

Yleisiä tietoturvan periaatteita: hienojakoinen pääsynhallinta

- **Turvallisuus vs. käytettävyys**
- **Linja hyväksyttävän (ja/tai välttämättömän) ja kielletyn käytön välillä kompleksinen**
- **Lyhyt ja karkeajakoinen tietoturvapolitiikka johtaa sääntöjen kiertämiseen**
- **Ratkaisu: hienojakoinen kontrolli**
  - Esim. RBAC- tai ABAC-säännöstö
  - Vaatii luotettavan käyttäjän tunnistamisen ja todentamisen (/autentikoinnin)
  - Ylläpidettävyys → automatisointi
- **Erilliset toimintoalueet:**
  - Identity- and Access Management
  - Role-/Attribute-based Access Control



16

Turvallisuus ja käytettävyys ovat yleisesti ottaen saman asteikon eri päissä, koska helppokäyttöistä järjestelmää on myös helppo väärinkäyttää. Tämä ei kuitenkaan ole koko totuus: jos järjestelmän turvallisuuden ja käytettävyyden suunnitteluun käytetään riittävästi resursseja, päästään varsin hyviin kompromisseihin.

Jos tietoturvapolitiikka on liian yksinkertainen käyttötapauksiin nähden, normaalikäyttäjät alkavat kiertämään sääntöjä saadakseen hommansa tehdyksi. Tämä johtaa siihen, että sisäiset, auktorisoidut käyttäjät ohittelevat tietoturvakontrolleja.

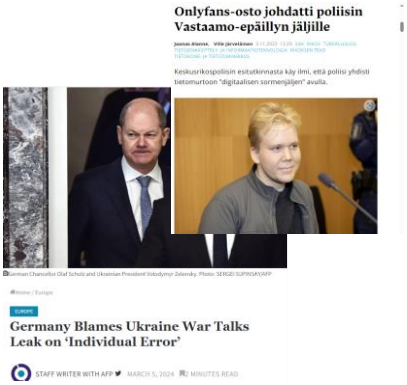
Tietoturvapolitiikka on hyvä rakentaa roolipohjaisuuden ja attribuuttipohjaisuuden varaan. Roolipohjaisessa pääsynhallinnassa (RBAC) käyttäjille annetaan työtehtävän perusteella rooleja, ja luvitus järjestelmiin tehdään roolien perusteella. Attribuuttipohjainen pääsynhallinta antaa luvituksen työtehtävän lisäksi järjestelmän ja ympäristön muiden ominaisuuksien perusteella, esimerkiksi sijainnin, kellonajan ja tietojärjestelmän senhetkisen liiketoimintaprosessin liitynnän kautta.

Automatisointi tarkoittaa tässä sitä, että esimerkiksi uuden käyttäjän

lisääminen järjestelmiin menee HR:n ja esimiehen antamien työtehtävien perusteella automaattisesti HR- ja ERP-järjestelmistä operatiivisten järjestelmien pääsynhallintaan, tai että uudessa projektissa tarvittavat pääsyoikeudet Sharepointiin tulevat automaattisesti projektinhallinnan toimin. Nämä kaikki vaativat järjestelmien välistä identiteettienhallinnan ja todentamisen menetelmien yhteentoimivuutta, esim. SSO.

Yleisiä tietoturvan periaatteita: OPSEC

- **Joka tason 360 astetta turvallisuus →**
- **OPSEC = Operations security**
  - Nimi USA:lta Vietnamin sodan aikana
  - "*järjestelmällisiä ja koestettuja turvallisuus-käytäntöjä, joiden avulla vastustajalta estetään kyky kerätä, analysoida ja käyttää hyväkseen tietoja, mm. puolustajan kyvyistä ja tavoitteista*"
- **Turvaa myös prosessit**
  - Käyttäjän tietoisuus uhista ja koulutus poikkeustilanteissa toimimiseen
  - Vain välttämättömät säännöt
  - … mutta tarkoin toteutetut
  - Hyvin määritellyt poikkeukset (prosesseihin ja sääntöihin)


Onlyfans-osto johdatti poliisin Vastaamo-epäillyn jäljille

Keskusrikospoliisin esitutkinnasta käy ilmi, että poliisi yhdisti tietomurtoon "digitaalisen sormenjäljen" avulla.

EUROPE

Germany Blames Ukraine War Talks Leak on 'Individual Error'

STAFF WRITER WITH AFP · MARCH 5, 2024 · 3 MINUTES READ

17

OPSEC-termi on peräisin USA:n sotilaspuolelta, kun he huomasivat että vihollinen kokosi yhteen yksittäisiä sinänsä viattomia (ja suojaamattomia) tiedonpalasia päätelläkseen etukäteen USA:n operaatioiden toimeenpanoa. Tällaisia olivat esimerkiksi ennustettavat (ja helposti havainnoitavat) joukkojen rutiinit, hallinnollisen tietoliikenteen salaamattomuus, a turha tiedonjako.

Mitä kuuluu kyberturvallisuuteen?

- **Eri näkökulmia**
- **Tekninen**
  - Fyysinen turvallisuus
  - Verkkoturvallisuus
  - Sovellusturvallisuus
- **Järjestelmä**
  - Tietokantaturvallisuus
  - Mobiililaitteiden turvallisuus
  - Pilven turvallisuus
- **Suojattavat kohteet**
  - Liiketoimintatietojen luottamuksellisuus
  - Kriittisten järjestelmien suojaaminen
- **Prosessi**
  - Hyökkäämisen ja suojaamisen vaiheistus
- **Hallintanäkökulma**
  - Turvallisuushallintaohjelma
  - Riskienhallinta
  - Compliance

18

Kyberturvallisuutta voidaan käsitellä monesta eri näkökulmasta, riippuen optimoitavasta asiasta.

Ohessa esimerkkeinä sitä, mitä näkökulmia on ylipäätään olemassa: koska tämä kurssi keskittyy johtamiseen, niin näkökulmaksi valitaan hallinta ja prosessit. On hyvä kuitenkin tietää perusteet eri näkökulmien käsitteistä.

Mitä kuuluu kyberturvallisuuteen 2024?

CISSP	CompTIA Security+	CISO Mindmap 2024	NIST CSF	ISO 27001/2
Turvallisuus ja riskienhallinta	Hallinta, riski ja compliance	Hallinta (govn.)	Uhkan ja kohteiden *tunnistaminen*	Turvallisuus*johtaminen*
Suojattavien kohteiden turvallisuus	Uhkat, hyökkäykset ja haavoittuvuudet	Riskienhallinta	Kohteiden *suojaaminen*	Turvallisuusohjelman (ISMS) *suunnittelu*
Turva-arkkitehtuuri	Arkkitehtuuri ja suunnittelu	Turva-arkkitehtuuri	Toteutuvien uhkien *havaitseminen*	ISMS *liitynnät* organisaatiossa
Turvallisuuden arviointi ja testaus	Operaatiot ja hälytysvaste	Auditointi ja compliance	Hyökkäyksiin *vastaaminen*	ISMS *operointi*
Tietoliikenneturvallisuus	Toteutukset	Automatisointi ja analytiikka	Hyökkäyksistä *toipuminen*	ISMS *arviointi*
Identiteetinhallinta (IAM)		Identiteetinhallinta		ISMS *parantaminen*
SecOps		SecOps		*Organisaation* kontrollit
Turvallinen ohjelmistonkehitys		Tuotekehityksen turvallisuus		*Henkilöön* kohdistuvat kontrollit
		Etätyö		*Fyysiset* kontrollit
		Tekoäly		
		Liiketoimintasov.		
		Kybertiimin hallinta ja brändi		
		HR ja laki		

19

Käytännössä eri näkökulmat kuitenkin suodattuvat eri rooleihin eri tavalla eri aikoina. Tässä taulukossa näkyy jaottelu kolmentyyppisestä näkökulmasta: CISSP ja Security+ ovat yleisiä kyber-/tietoturvallisuuden sertifiointeja; CISO Mindmap on kooste tyypillisen organisaation informaatio-(/kyber-)turvallisuusjohtajan tehtäväkentästä (tarkemmin edempänä) ja kolmantena sääntelijän ohjeistus siitä, millä tavalla kyberturvallisuutta tulisi lähestyä. NIST CSF ja ISO 27k ovat nimenomaan hallinnan standardeja, ja käyn niitä lävitse tarkemmin jäljempänä.

Verrattuna n. 10 vuoden takaiseen, yksittäiset teknologiat tai jopa teknologiaryhmät ovat piiloutuneet toimintojen alle, joita taas nykyisin jaotellaan nk. Kill-chainin mukaisesti (eli tyypillisen hyökkäyksen kulkemisen perusteella) tai turvallisuusfunktioiden perusteella: esimerkiksi kontrollien jaottelu, tai yleinen prosessin kypsyysmallin mukainen jaottelu.

Uusimmat teknologiat kulkevat näissä kehyksissä mukana yleensä itsenäisinä, kunnes on selvää, mikä on ko. Teknologian pääasiallinen merkitys turvallisuusfunktioiden kannalta. Näitä teknologioita ovat toistaiseksi tekoäly, pilviteknologiat ja IAM.

CISO Mind map 2024

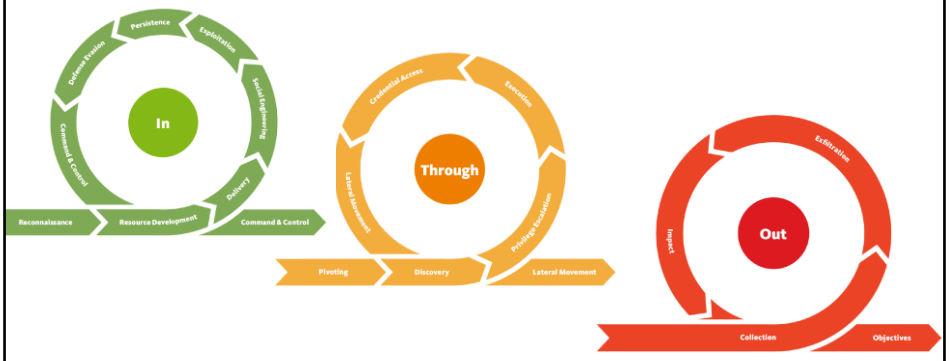
https://rafeeqrehman.com/ciso-mindmap/

(ladatkaa itsellenne kopio, ja tutustukaa alueisiin)

20

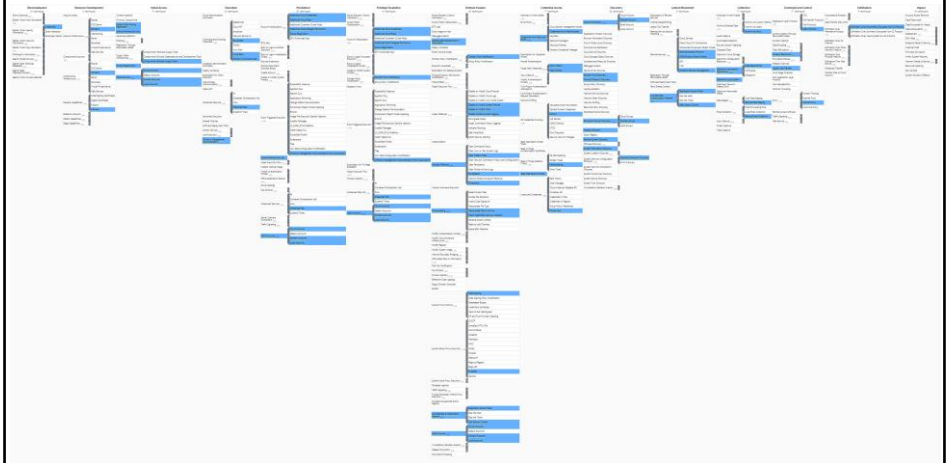
Seuraavissa kalvoissa käyn lävitse kyberjohtamisen osa-alueita kursorisesti. On hyvä tiedostaa, että kovin monet osa-alueet vaativat erityisosaamista, esimerkiksi kryptografia.

Miltä näyttää monivaiheinen kyberhyökkäys?



21

Esimerkki toimitusketjuhyökkäyksestä: Solarwinds



22

Tämä on MITRE ATT&CK-kehikon mukainen näkymä erääseen ohjelmistojen toimitusketjuja vastaan kohdistuneeseen kyberhyökkäykseen (Solarwinds). Solarwinds-hyökkäyksessä. SolarWinds on yritys joka tekee erilaisia verkonhallintatyökaluja organisaation IT-ylläpitäjille. Hyökkääjä oli murtanut ohjelmiston toimitusketjussa useamman organisaation tuotekehityspalvelimia ja saanut ujutettua takaportitettuja ohjelmia kymmeniin tuhansiin organisaatioihin, mukaan lukien USA:n valtionhallinto. Hyökkäyksen tekijä oli todennäköisesti Venäjän SVR:n (ulkomaantiedustelu) rahoittama ja ohjaama uhkatoimija nimeltään Cozy Bear (/ APT29 / Midnight Blizzard).

Kyberturvallisuuden hallinta ja johtaminen

Osana riskienhallintaa

Miksi kyberturvallisuuden hallinta?

- **Johtaminen = governance**
- **Hallinta = management**
- **Yleisluontoisen tilannekuvan pitäminen**
- **Asioiden pitäminen ajan tasalla**
- **Resurssien tehokas kohdentaminen**
  - Osa riskienhallintaa
- **Teknologian kommunikointi päätöksen-tekijöille ja päinvastoin**
- **Koordinoinnin vuoksi:**
  - Eri kyberturvallisuuden alojen kesken
  - Turvallisuuden ja muiden liiketoimintaprosessien välillä
  - Viranomaisten ja organisaation välillä
- **Monimutkaistuvan uhkamaailman ja hyökkäysten vuoksi**

Virallisia määritelmiä: riskienhallinta

- **ISO-31000-2018 (Risk management. Guidelines)**
  - "*Koordinoituja toimenpiteitä ohjaamaan ja kontrolloimaan organisaatiota suhteessa* riskiin"
    - Riski = "*Epävarmuuden tuoma muutos* tavoitteisiin"

25

Virallisia määritelmiä: riskienhallinta

- **ISO-31000-2018 (Risk management. Guidelines)**
  - "*Koordinoituja toimenpiteitä ohjaamaan ja kontrolloimaan organisaatiota suhteessa* riskiin"
    - Riski = "*Epävarmuuden tuoma muutos* tavoitteisiin"

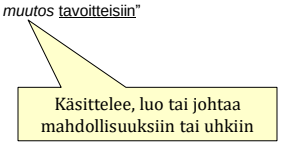
Positiivinen ja/tai negatiivinen

26

Note 1 to ISO31k: muutos (/vaikutus) on suhteessa odotettuun. Muutos voi olla positiivinen negatiivinen tai kumpaakin, ja voi käsitellä luoda tai johtaa mahdollisuuksiin tai uhkiin.

Virallisia määritelmiä: riskienhallinta

- **ISO-31000-2018 (Risk management. Guidelines)**
  - "*Koordinoituja toimenpiteitä ohjaamaan ja kontrolloimaan organisaatiota suhteessa* riskiin"
    - Riski = "*Epävarmuuden tuoma muutos* tavoitteisiin"



27

Note 2 to ISO31k: Tavoitteilla voi olla eri aspekteja ja luokkia ja niitä voidaan soveltaa monella eri tasolla.

Virallisia määritelmiä: riskienhallinta

- **ISO-31000-2018 (Risk management. Guidelines)**
  - "*Koordinoituja toimenpiteitä ohjaamaan ja kontrolloimaan organisaatiota suhteessa* riskiin"
    - Riski = "*Epävarmuuden tuoma muutos* tavoitteisiin"
- **NIST SP-800-37 (Risk Management Framework for Information Systems and Organizations**
  - "*Ohjelma ja tukevat prosessit hallitsemaan riskiä [organisaation] operaatioihin (sisältäen mission, toiminnot, julkisen kuvan ja maineen), suojattaviin kohteisiin, henkilöihin, … ja sisältää kontekstin luomisen …, riskin arvioinnin, riskiin vastaamisen…; ja riskin seurannan ajan myötä*"
    - Riski = "*Suure, joka mittaa sitä, Kuinka paljon kohteeseen kohdistuu uhkaa jonkin mahdollisen tapahtuman tai olosuhteen vuoksi*"
- **EU:n komissio:**
  - "*Jatkuva, proaktiivinen ja järjestelmällinen prosessi tunnistaa, arvioida ja hallita riskejä linjassa hyväksyttyjen riskitasojen kanssa, joka toimeenpannaan joka tasolla… jotta voidaan taata riittävä vakuuttavuus tavoitteiden saavuttamiseksi.*" [1]
    - Riski = "*Mikä tahansa tapahtuma tai asia, joka voi tapahtua ja vaikuttaa negatiivisesti tavoitteiden saavuttamiseen*".

28

[1] Risk Management in the Commission, Implementation Guide (2018-2019), https://wikis.ec.europa.eu/pages/viewpage.action?pageId=50108960

Virallisia määritelmiä: riskienhallinta

- **Wikipedia(EN):**
  - "*Riskien tunnistaminen, arviointi ja priorisointi, jota seuraa koordinoitu ja taloudellinen resurssien allokointi minimoida, valvoa ja kontrolloida epäsuotuisten tapahtumien todennäköisyyttä tai vaikutusta tai maksimoida mahdollisuuksien toteutuminen*."[1]
- **Cambridge sanakirja (vapaa käännös) :**
  - "*toiminta riskin laskemiseksi ja vähentämiseksi, jotta organisaatio ei epäonnistu tai menetä rahaa*"
- **Tärkeimmät elementit määritelmistä:**
  1) Organisaation tahtotila, suojattavien kohteiden arvo ja niiden muutos
  2) Sisäiset ja ulkoiset tapahtumat, joiden todennäköisyyttä ja vaikutusta on osin vaikeaa arvioida
  3) Pyritään minimoimaan negatiivisen tapahtuman vaikutusta ja/tai todennäköisyyttä

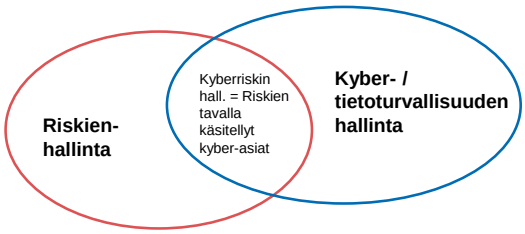
[1] Hubbard, Douglas (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons. p. 46.

29

Huom 1: Tiettyjen riskienhallintajärjestelmien kanssa on edullisempaa laskea liiketoimintamahdollisuuksia samassa kehikossa kuin riskejä "positiivisina riskeinä". Tällaisessa lähestymistavassa monet liiketoimintaprosessit ja –riskit on kiedottu tiiviisti yhteen eri vaihtoehtojen punnitsemiseksi.

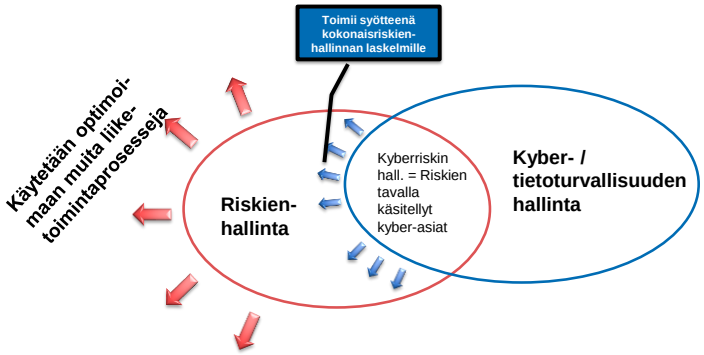
Huom 2: Kompleksisten ja huonosti ymmärrettyjen tapahtumien todennäköisyyden ja vaikutuksen arviointi on itsessään epävarmuuksia sisältävää, ja olisi hyvä huomioida itse riskienhallinnassa.

Määritelmiä: riskienhallinta vs. kyberturvallisuuden hallinta



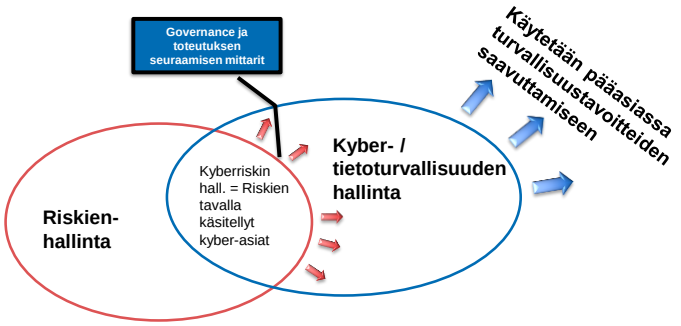
30

Määritelmiä: riskienhallinta vs. kyberturvallisuuden hallinta



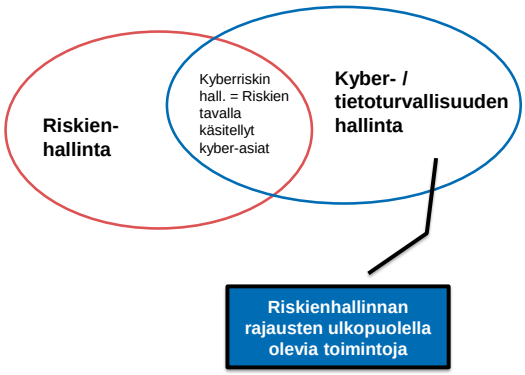
31

Määritelmiä: riskienhallinta vs. kyberturvallisuuden hallinta

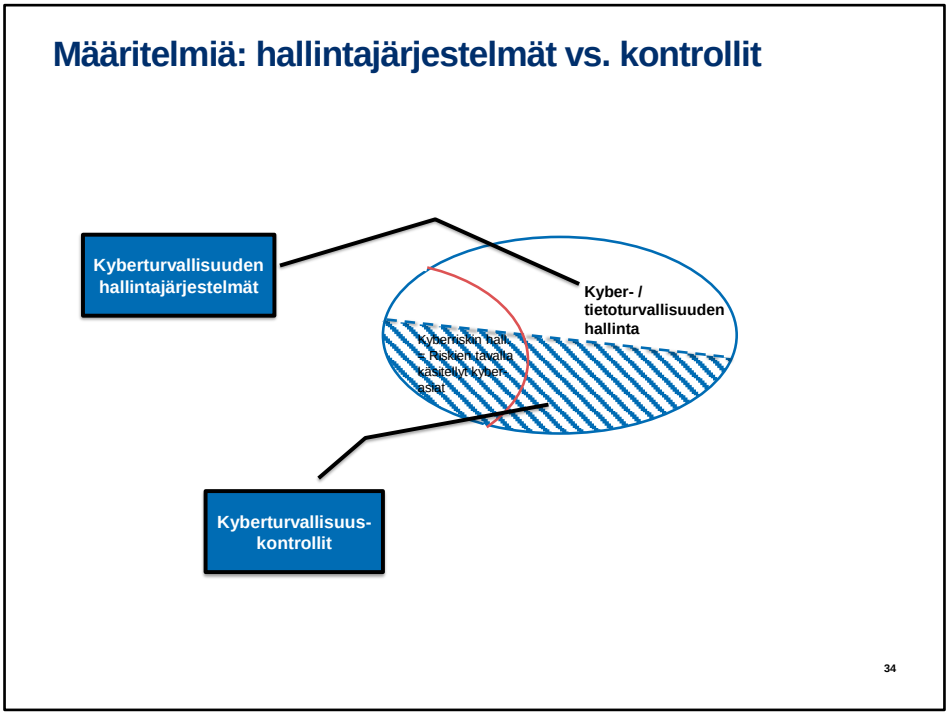


32

Määritelmiä: riskienhallinta vs. kyberturvallisuuden hallinta



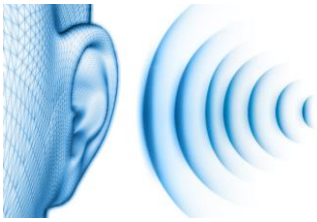
33

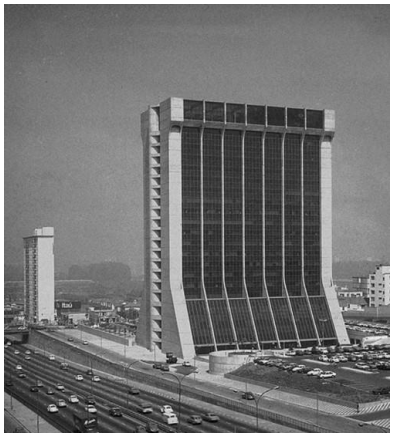


Ei pidä sekoittaa toisiinsa kyberturvallisuuskontrollien luetteloita ja varsinaisia hallintajärjestelmien (Information / Cyber Security Management System: ISMS/CSMS) luontiohjeita. Ensimmäinen toimii mind mappinä tai tarkastuslistana organisaatioille, millaisia kontrolleja ylipäätään on olemassa millaisiin ongelmiin, ja jälkimmäinen kertoo, Kuinka CSMS luodaan, ja miten sitä ylläpidetään ja kehitetään.

Huomioita riskin mittaamisesta

- **Kvantitatiiviset riskitaulukot**
  - R. Courtney Jr., IBM
  - Määritetty odotusarvona R = P*I
- **Oletukset:**
  - Mitattavissa oleva todennäköisyys
  - Mitattavissa olevat vaikutukset
  - Usein osuvat tapahtumat
  - Kokemuksen lineaarisuus





35

Nykyisen kvantitatiivisen riskitaulukon historia ulottuu 1970-luvun IBM:ään, jossa riskien laskenta kehitettiin todennäköisyyslaskennan perusteella niin, että riskiluvuksi muodostui dollareita.

Kyberturvallisuus: hallinnollisia termejä

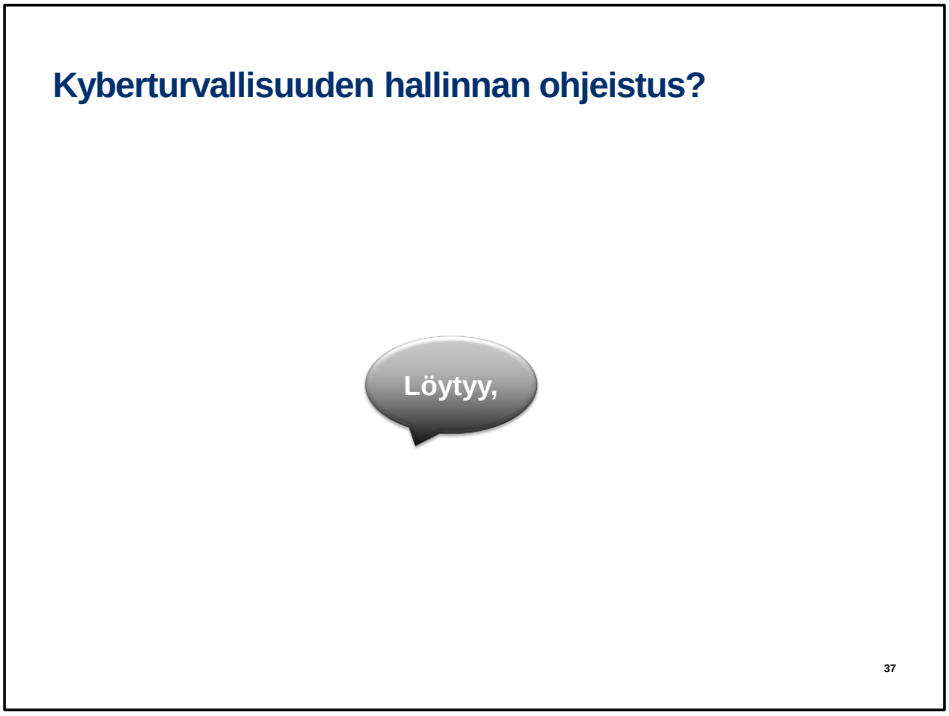
- **Kyberturvallisuuden johtaminen (governance):**
  - Organisaation laajuinen kyberstrategia
  - Politiikkojen / käytänteiden määrittely
  - Säännöstenmukaisuus (compliance)
  - Riskiprofiili (riskinsietokyky)
- **Kyberturvallisuuden riskienhallinta**
  - Riskienhallinnan “kyberaspekti”
- **Kyberturvallisuuden hallinta**
  - Kyberstrategian, käytänteiden ja riskienhallintatoimintojen toimeenpano

36

Johtaminen on organisaatiohierarkiassa korkeammalla kuin hallinta, mutta riskienhallinta kokonaisuudessaan taas on samalla päätöksentekotasolla kuin governance ja compliance.

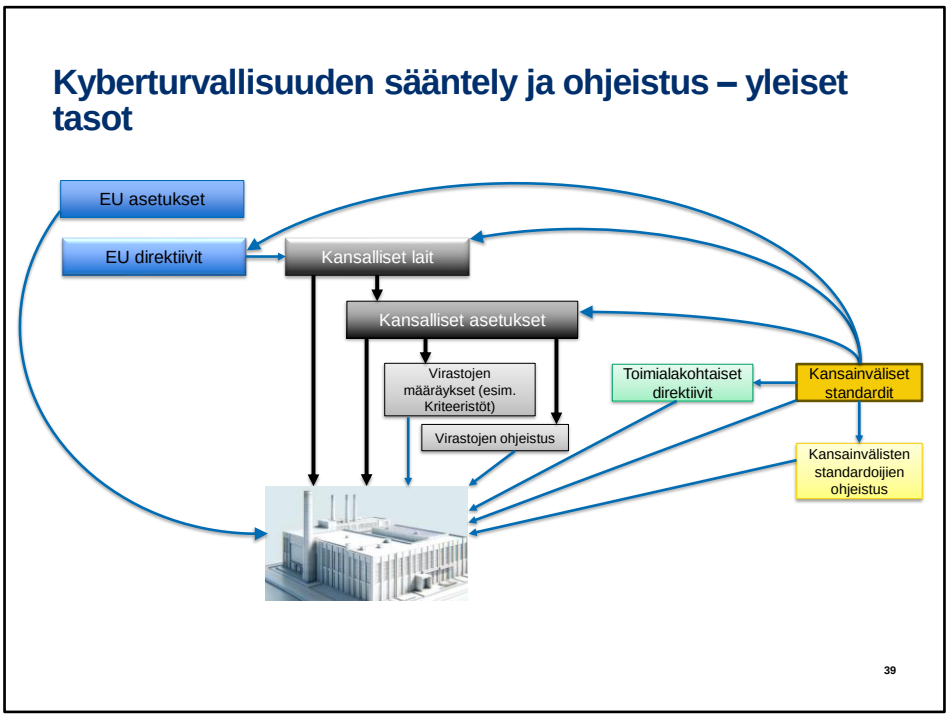
NISTin (USA:n teknologiastandardoinnin organisaatio) kyberturvallisuuden hallinnan kehyssuositus (NIST Cybersecurity Framework) on nostanut governancen normaalin hyökkäyksen torjunnan elinkaaren päälle. Perinteinen torjunnan elinkaari lähtee hyökkäyksen havaitsemisesta ja päättyy hyökkäyksestä toipumiseen.

Governancelle on olemassa myös nk. GRC-malli: Governance – Risk – Compliance, joka korostaa riskinhallinnan ja compliance merkitystä kokonaisjohtamisessa.



Kyberturvallisuuden hallinnasta on olemassa ohjeistusta,

… mutta haasteena on, että sitä on varsin paljon, vaihtelevan laatuista ja vaihtelevia yksityiskohtaisuuden tasoja sekä eri näkökulmia sekä toimialasidonnaisuuksia. On tiedettävä, mistä haluaa lähteä liikkeelle, että voi poimia oman standardinsa.



Velvoittavuuden ja yksityiskohtaisuuden tasoja
Lait eduskunnalta, asetukset ministeriöiltä. EU-asetukset ovat voimassa EU:n päätöksellä sellaisenaan, ja velvoittavia. EU-direktiivit vaativat kansallisen lainsäädännön tullakseen voimaan (esim. NIS2).

Virastot ovat ministeriökohtaisia toimeenpanoelimiä, esimerkiksi LVM:llä on Traficom ja PLM:llä Pääesikunta

Kansainvälisesti on useita toimialakohtaisia globaaleja elimiä, joilla on valta antaa velvoittavaa sääntelyä, esimerkiksi IMO merenkulussa.

Kansainväliset standardointiorganisaatiot antavat lisäksi velvoittavia määräyksiä (siinä mielessä, että jos jokin taho ilmoittaa olevansa standardinmukainen, standardi tarjoaa hyvin yksityiskohtaiset kriteerit siitä, mitä kaikkea pitää olla toteutettuna, ennen kuin väite on pätevä), mutta eniten kuitenkin suosituksia.

Kyberturvallisuuden sääntely ja ohjeistus - esimerkkejä

GDPR (679/2016)

NIS2 (2555/2022)

Tiedonhallintalaki (906/2019)

Asetus turvaluokituksista (1101/2019)

Määräys 72 sähköisistä tunnistus- ja

KATAKRI 2.0

IACS UR E26

ISO 27001

Traficom kybermittari

ISO 27003

40

Huomioita sääntelyn muutoksista: NIS2

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_NIS2_taulukko_230424.pdf

41

Esittelen seuraavaksi hyvin lyhyesti tärkeimmän Suomea ja EU:ta koskevan muutoksen kyberturvallisuuden, erityisesti kybersietoisuuden sääntelyssä: NIS2-direktiivi ja sen kansallinen toimeenpano, laki kyberturvallisuuden riskienhallinnasta.

Standardointiorganisaatioista

- **Standardointiorganisaatioiden pääasialliset tuotteet**
  - Vaatimukset (velvoittavuus, jos yhteensopivuutta vaaditaan)
  - Ohjeistus
  - Tilannekatsaukset
- **Standardien kehitys**
  - Useita eri vaiheita
  - Koko prosessi vuosien mittainen
- **Standardointitoiminnan ohjaus ja rahoitus**
  - Kansainväliset toimijat (ISO, IETF)
  - Valtiolliset toimijat (esim. NIST)
- **Teknisten standardien laaja merkitys**
  - Valtiollinen ja yritysvaikuttaminen

Kyberturvallisuuden hallinnan kehikoita ja suosituksia

- **Riskinhallinnan suositukset**
  - Fokus järjestelmien kyberriskien tai tietojärjestelmien yleisen riskin hallintaan
  - Esim. NIST SP:t 800-39, 37 ja 30, NIST RMF + AI RMF, ISO-27005, IEC 62443-3-2
- **Hallintajärjestelmän luomisohjelmat**
  - Fokus kattavan kyber-/tietoturvallisuuden hallintaohjelman / -järjestelmän luomisessa
  - Esim. ISO-27001, IEC-62443-2-1, NIST CRF 2.0, ENISA ISMS
- **Kontrollien suositukset ja kehikot**
  - Fokus turvallisuuskontrollien vaatimuksissa / ohjeistuksessa
  - Esim. ISO-27002, NIST SP 800-53, IEC-62443-3-1, CIS Controls, Cloud Controls Matrix
- **Jonkin verran päällekkäisyyttä**
  - Hallintajärjestelmien suositukset helposti sisältävät myös kontrollisuosituksia.
  - Program frameworks ⊃ Control frameworks
- **Etenemisjärjestys**
  1) Riskienhallintakehikko (ellei jo ole)
  2) Hallintajärjestelmä (ISMS / CSMS)
  3) Kontrollien valinta

43

NIST SP = NIST Special Publication, käytännössä standardisarja
NIST on velvoittava pääasiassa USA:ssa, mutta kyberpuolella kansainvälisesti ja EU:ssakin velvoittavat ohjeistukset tehdään usein NISTin mallin perusteella. Poikkeuksiakin on, mutta NISTin dokumenttien etuna on niiden ilmaisuus. EU:n direktiivitkin ovat toki ilmaisia, mutta EU harvemmin tekee teknistä standardointia itse, vaan viittaa virallisten, esimerkiksi ISO-standardointiorganisaatioiden teksteihin

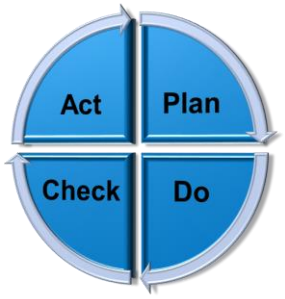
NIST:
800-39 = Tietoturvan riskienhallinta: organisaation, mission ja tietojärjestelmän näkymä (Managing Information Security Risk: Organization, Mission, and Information System View)
800-37 = Riskienhallintakehikko tietojärjestelmille ja –organisaatioille: elinkaarimallin lähestymistapa (Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy)
800-30 = Opas riskin arvioinnin toimeenpanoon (Guide for Conducting Risk Assessments)
800-53 = Turvallisuus- ja yksityisyyskontollit tietojärjestelmiä ja organisaatioita varten (Security and Privacy Controls for Information Systems and

Organizations)

ISO:
27001 = Tietoturvallisuuden hallintajärjestelmät. Vaatimukset
27002 = Tietoturvallisuuden hallintakeinot
27005 = Ohjeita tietoturvariskien hallintaan
62443-3-2 = Tietoturvariskien arviointi järjestelmäsuunnittelussa (Security risk assessment for system design)
62443-2-1 = Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten
62443-3-1 = Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille

PDCA-sykli: miten hallintakehikot yleensä toimivat

- **Suunnittele, toteuta, tarkista, korjaa**
  - Plan-Do-Check-Act
- **Iteratiivinen menetelmä liiketoimintaprosessien parantamiseksi**
- **Kaksivaiheinen toiminta**
  1) Aloitus tyhjältä pöydältä (Plan-Do)
  2) Tarkista ensimmäinen yritys (Check-Act)
- **Siirtynyt riskienhallintaan ja kyberiin**
- **Hyödyt:**
  - Yleispätevä, yksinkertainen
- **Haitat:**
  - Hidas, dokumenttikeskeinen, muutokset ainoastaan syklistä toiseen



44

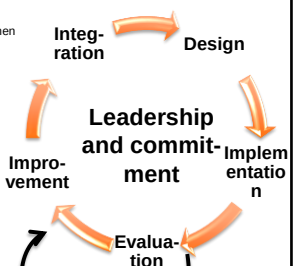
PDCA:n juuret ovat valmistusteollisuudessa

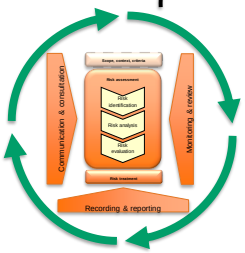
Plan / Suunnittele
Päätä tavoitteet ja luo prosessit, joilla tuotetaan halutut tulokset
Do / Toteuta
Toteuta edellisen vaiheen tavoitteet
Check / Tarkista
Tarkastusvaiheessa, tieto ja tulokset toteutusvaiheesta kerätään ja arvioidaan. Dataa verrataan odotettuihin tuloksiin ja etsitään yhtenevyydet ja erilaisuudet. Itse testausprosessi arvioidaan myös (yleensä ja suhteessa edellisiin kierroksiin).
Act / Korjaa
Tässä vaiheessa prosesseja kehitetään, tiedot aiemmista vaiheista auttavat tunnistamaan kehityskohteet, kuten ongelmat, epäyhteensopivuudet, turvallisuusepäkohdat ym. Pyritään etsimään ja poistamaan kehityskohteiden juurisyyt. Riskit arvioidaan tässä vaiheessa uudelleen, ja tuotetaan uudet, tarkennetut tavoitteet.

Riskienhallintakehyksen ja –ohjelman luominen

- **Riskienhallintajärjestelmä = Risk Management System (RMS)**
- **RMS:n luonti- ja operointikehikot**
- **Tavoite: RMS synnyttäminen, ylläpito ja kehittäminen**
  - Hallintamenetelmä varsinaiselle hallintajärjestelmälle
- **Sisällä: RMS operointi**
- **Esimerkki:**
  - ISO-31000 RMS luominen (“Framework”)
  - ISO-31000 RMS operointi (“Process”)
- **Yleisiä suosituksia ja standardeja:**
  - Velvoittavuus kehikon luonnissa
  - Tarkempi prosessi ja riskien arviointi organisaatiolla

ISO-31000 riskienhallinta-järjestelman luominen, ylläpitäminen ja kehittäminen (establishment system)



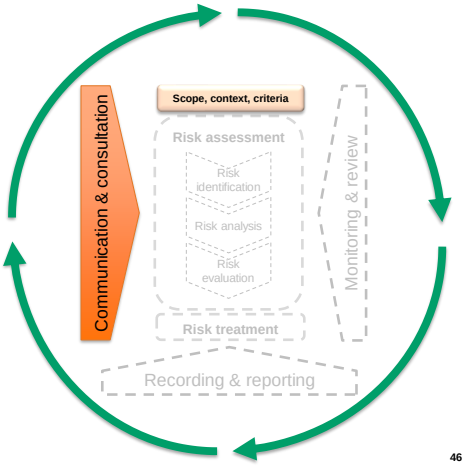


ISO-31000 riskienhallinta-järjestelmän “prosessi” (toiminnassa olevan järjestelmän operointi)

45

Riskienhallinnasta kyberturvallisuuden hallintaan

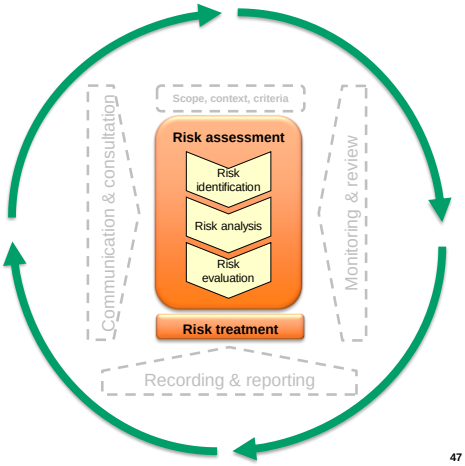
- **Perustuen ISO-31000:2018:een**
  - Yleinen (ei-kyber) riskienhallinnan standardi
- **Kommunikointi**
  - Viestintä asianosaisille *päin*
- **Konsultointi**
  - Palaute asianosaisten *suunnasta*
- **Rajaukset (Scope):**
  - Soveltamisen taso
  - Tavoitteet ja tuotokset
  - Aikaväli, resurssit, toimipisteet
- **Asiayhteys (Context):**
  - Ulkoinen konteksti: esim. sääntelynmukaisuus, teknologia
  - Sisäinen konteksti: esim. organisaation johto, visio
- **Kriteerit (Criteria):**
  - Riskien arvioinnin kriteerit ja mittaaminen
  - Reunaehdot (esim. mikä on “sietämätön riski”)



46

Riskienhallinnasta kyberturvallisuuden hallintaan

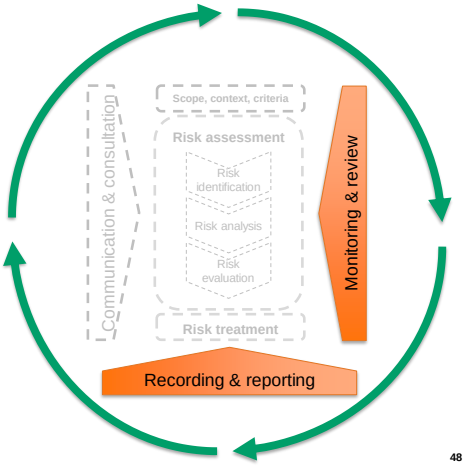
- **Riskin tunnistaminen**
  - Riskin lähteet
  - Syyt, haavoittuvuudet, uhat,…
- **Riskianalyysi**
  - Suojattavien kohteiden (asset) tunnistaminen ja arvottaminen
  - Riskin todennäköisyyden arviointi
  - Riskin vaikutusten arviointi,…
  - Voi olla laadullinen tai määrällinen
- **Riskien evaluointi**
  - Analyysin tuloksien vertaaminen kriteeristöön
  - Voi johtaa tai ei, riskien hoitamiseen
- **Riskien hoitaminen**
  - Vähennetään vaikutusta (suhteessa hoitamisen kustannuksiin)
  - Muutetaan todennäköisyyttä (asentamalla kontrolli)
  - Muutetaan vaikutuksen kohdetta tai suuruutta (varasuunnitelmien teko)
  - Riskin välttäminen tai poistaminen (muuttamalla omaa toimintaa)
  - Riskin jakaminen, hyväksyminen tai ulkoistaminen (esim. vakuutukset)



47

Riskienhallinnasta kyberturvallisuuden hallintaan

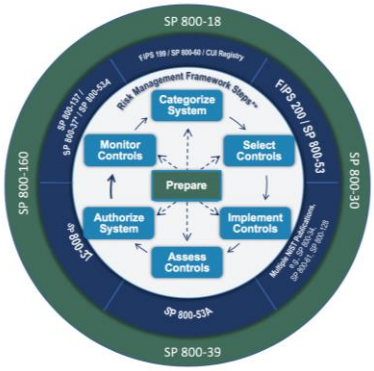
- **Monitorointi**
  - Alemman tason toiminto
  - Kerätään dataa läpi koko prosessin
  - Tuottaa syötettä raportointiin ja kommunikointiin
- **Katselmointi (review)**
  - Monitoroinnin tulosten analyysi
  - Palautteen tuottaminen
  - Tuottaa syötettä raportointiin ja tallennukseen sekä kommunikointiin
- **Tallennus (recording)**
  - Operatiivisen tason toiminto
  - Prosessin ja sen tulosten dokumentointi
  - Tarvitaan liiketoimintaprosessin päätöksiin
- **Raportointi**
  - Strategisen tason / johtamisen toiminto
  - Viestintä ylimmälle johdolle ja asianosaisille



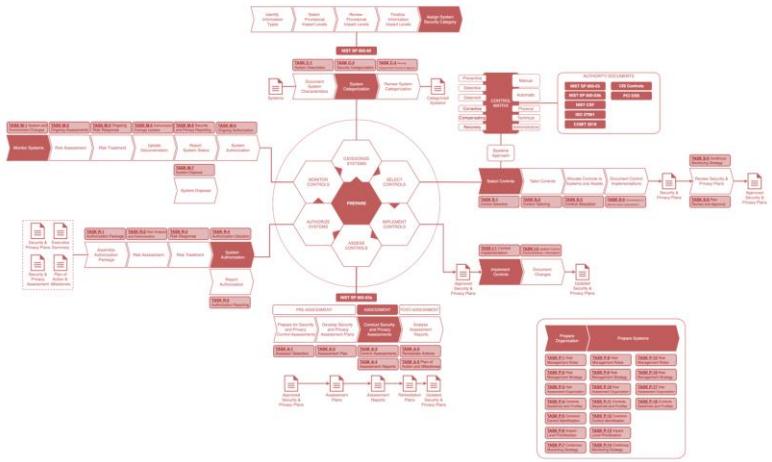
48

Tietoturvallisuuteen suuntautuva riskienhallinta: NIST RMF

- **NIST Risk Management Framework (RMF)**
- **Tarkoitettu USA:n valtionhallinnolle**
  - Soveltuu myös muille organisaatioille
- **Suositellaan käytettäväksi NIST CSF:n kanssa (kyberturvallisuuden hallintasuositus)**
- **Jaettu usean NIST SP-dokumentin kesken**
  - Päädokumentti SP 800-37

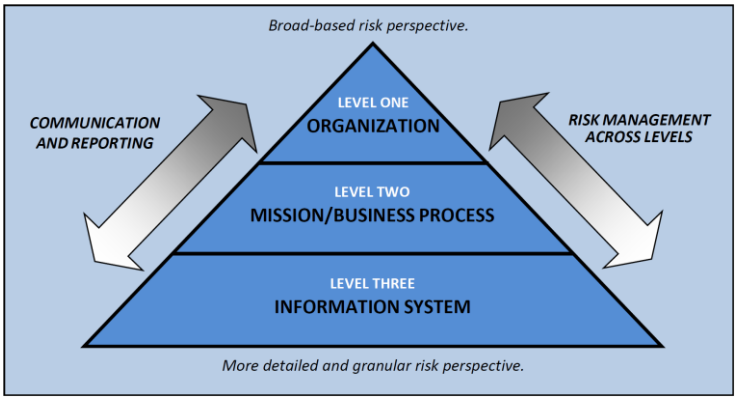


NIST RISK MANAGEMENT FRAMEWORK



50

NIST RMF sovellettavuuden tasot



51

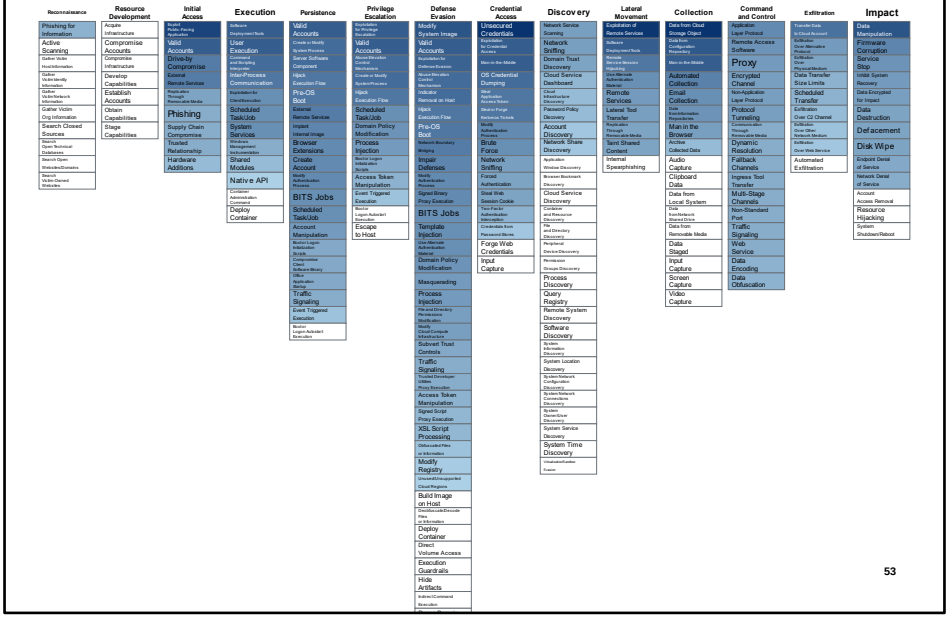
NIST RMF kontrolli”perheet” (800-53)

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

52

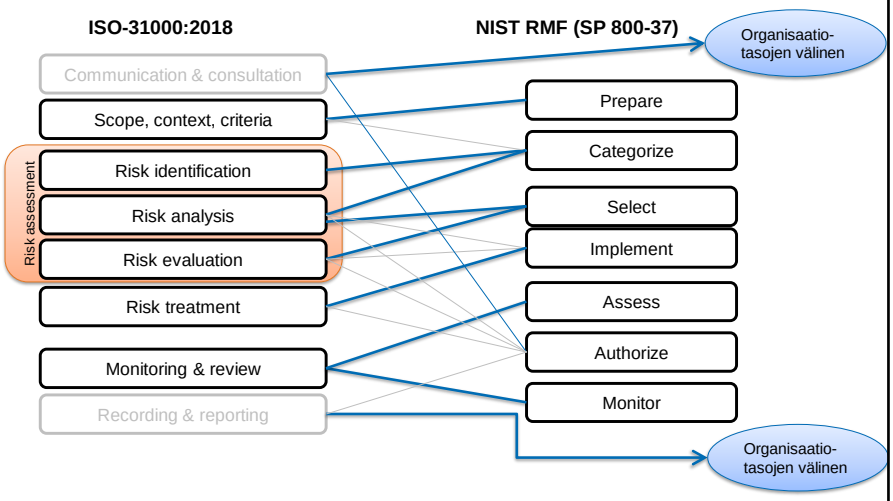
NIST RMF kontrollien kattavuus suhteessa MITRE ATT&CK-kehikkoon



NIST RMF on yleinen tietoturvallisuuden hallintakehikko, joten on hyvä tehdä ristiinvertailua uhkamallin suhteen, ts. Esim. Mihin tyypillisiin kyberhyökkäysmenetelmiin olisi voitu vastata, jos riskienhallinnassa olisi käytetty kaikki NIST RMF:ssä listattuja kontrolleja.

Kaavion perusteella RMF:n kontrollilistaus on kattava *siitä asti, kun aktiivinen toiminta alkaa*. RMF ei siis ota kantaa tiedonkeruuseen järjestelmistä, joihin organisaatio kyllä voi itsekin vaikuttaa.

Tietoturvallisuuden riskienhallinta vs. yleinen riskienhallinta



54

Kyber-/tietoturvallisuuden riskienhallinnan erityispiirteet

- **Laadullinen suojattavien kohteiden ja uhkien arvottaminen**
  - Uhkan todennäköisyys usein tuntematon
- **Useita riskilukuja ja -tasoja**
  - Riskiluvut voivat olla tuntemattomia tai epävarmoja
- **Kontrollien ja mitigoinnin vaikutustasot tuntemattomia tai ei voida muuttaa**
- **Korostuu: riskianalyysin sijaan kontrollien valinta ja sijoittelu**
- **Kyberturvallisuutta korostava lähestymistapa organisaatiossa**
  - Formaalisti määriteltävä hyväksymismenettely ja jäljitettävät luvitusprosessit

55

Kyberturvallisuuden hallinta ja johtaminen teollisuusautomaatiossa

Teollisuusautomaation kyberturvallisuuden hallintamalli ja turvallisuusohjelman luominen

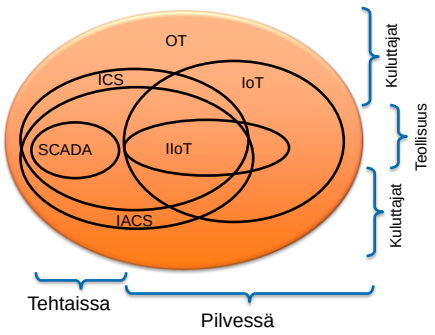
Tässä osiossa mennään lähemmäs toimialakohtaista kyberturvallisuutta. Kerron tarkemmin, mitä teollisuudessa käytettävien tieto- ja hallintajärjestelmien kyberturvallisuus nähdään ja mitä se tarkoittaa. Ensin on kuitenkin hyödyllistä Saada käsitteet kuntoon ja vähän kouriintuntuvia esimerkkejä siitä, mistä oikein on kyse.

Termistöä: OT / käyttötekniikka

OT:

Org.	Definition
[IIoT-laitetoimittajat]	Operational Technology, "Käyttötekniikka" (vs. IT = informaatioteknologia)
NIST	Laaja teknologia-alue ohjelmoitavia järjestelmiä ja laitteita, jotka ***vuorovaikuttavat fyysisen ympäristönsä*** kanssa tai hallitsevat laitteita, jotka vuorovaikuttavat fyysisen toimintaympäristön kanssa. Nämä järjestelmät ja laitteet ***havaitsevat*** tai ***aiheuttavat*** suoria ***muutoksia*** fyysisiin kohteisiin valvomalla tai säätelemällä laitteita, prosesseja ja tapahtumia. Esimerkkeinä on: *teollisuusautomaatio, fyysiset pääsynhallintajärjestelmät, ympäristömuuttujien [esim. Lämpötila] valvonta ja mittaaminen*.
ISO	Laitteistoja tai ohjelmistoja, jotka ***havaitsevat*** tai ***aiheuttavat muutoksia*** organisaation järjestelmiin, prosesseihin tai tapahtumiin suoralla ***fyysisten laitteiden*** säätämisellä tai valvonnalla.
Gartner	Laitteistoa ja ohjelmistoa, joka havaitsee tai aiheuttaa muutoksia ***teollisuuden kaluston, prosessien, assettien ja tapahtumien*** suoran valvonnan tai kontrollin kautta.

Muut käsitteet:



57

SCADA: esimerkki valvontatoiminnosta

58

SCADA: PLC-laitteet

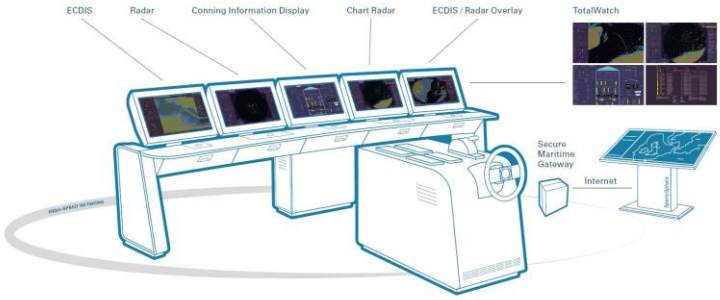
59

PLC tarkoittaa Programmable Logic Controlleria, eli ohjelmoitavaa logiikkayksikköä. Nämä ovat erityiskäyttöön rakennettuja prosessoreita tai jopa pieniä tietokoneita OT:n käyttötarkoituksia varten. PLC-komponentteja on myös pilviratkaisuissa (IIoT:ssä) eli ei rajoitu pelkästään SCADAan.

PLC ottaa syötteensä sensoreista ja ohjaa esim. Aktuaattoreita, venttiilejä, tuottaa lokitietoja ja informaatiota SCADAn valvontatasolle. Sisäinen laitteistoarkkitehtuuri on yleensä optimoitu kutakin käyttötarkoitusta varten, ja mitään suoraa käyttöliittymää näihin ei kuulu, vaan tarvitsevat erillisen HMI:n (Human-Machine Interface)

PLC:tä on kaiken kokoisia ja muotoisia, jotkut voivat olla itsenäisiä yksikköjä, mutta suurin osa on integroitu muuhun laitteistoon tai osana IT-palvelimia palvelinhuoneessa.

SCADA: Human-Machine Interfaces



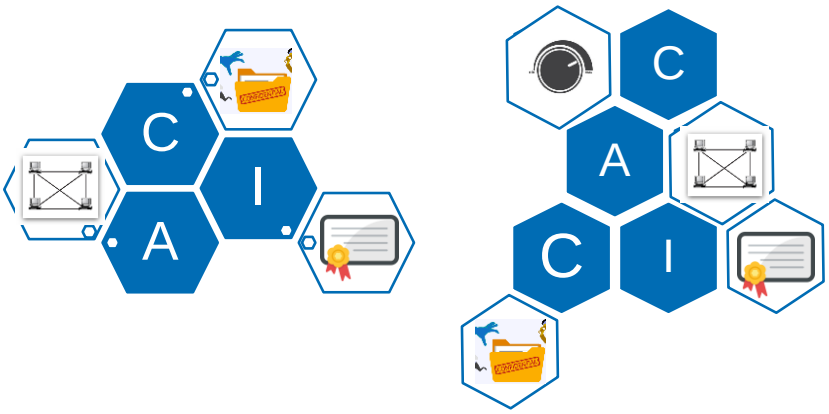
Aalto University

Prof. Mikko Kivilharju
mikko.kivilharju@aalto.fi

60

OT:ssä käyttöliittymän (UI) virallinen termi on “ihminen-kone-rajapinta” (HMI), pääasiassa historiallisista syistä ja siitä, että HMI on paljon muutakin kuin ruutu. HMI:hin kuuluu esimerkiksi ratteja, vipuja, kosketusnäyttöjä ym. Markkinat ja laitteistot ovat voimakkaammin jakautuneet PLC:hen ja HMI:hin OT:ssä kuin IT:ssä, jossa UI on yleensä integroitu kokonaisuuteen.

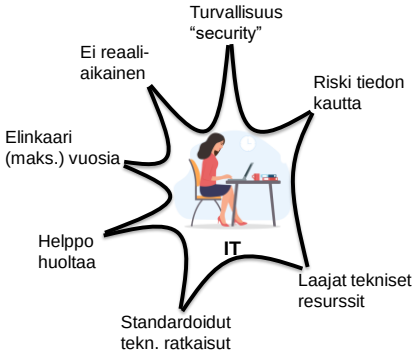
IT vs. OT turvallisuuden tavoitteet

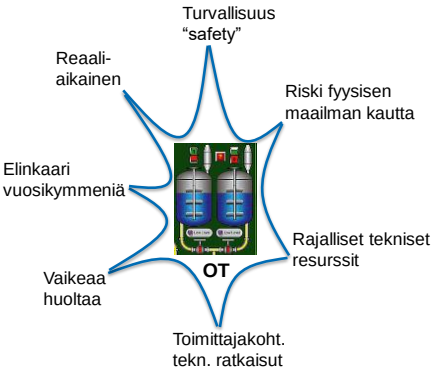


61

IT vs. OT

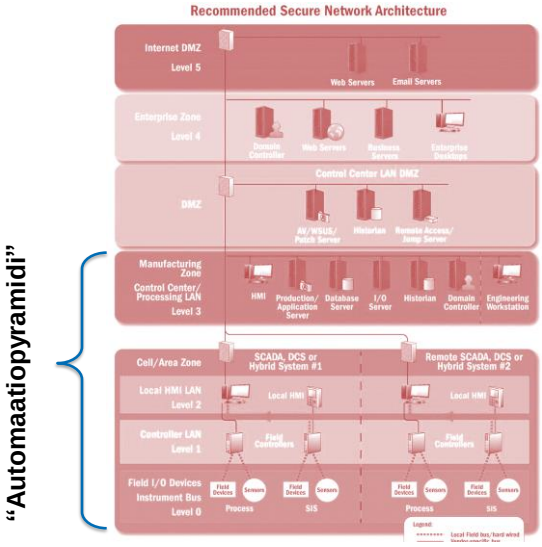
IT vs. OT


Turvallisuus
“security”
Ei reaali-
aikainen
Riski tiedon
kautta
Elinkaari
(maks.) vuosia
Helppo
huoltaa
IT
Laajat tekniset
resurssit
Standardoidut
tekn. ratkaisut


Turvallisuus
“safety”
Reaali-
aikainen
Riski fyysisen
maailman kautta
Elinkaari
vuosikymmeniä
Rajalliset tekniset
resurssit
Vaikeaa
huoltaa
OT
Toimittajakoht.
tekn. ratkaisut

63

OT-verkkoarkkitehtuurit: Purdue



"Automaatiopyramidi"

IEC 62264!

64

Teollisuusautomaatio on perinteisesti rakennettu kerrostamalla (koska automaatio ja SCADA-järjestelmät ovat olleet itsenäisiä järjestelmiä ja vasta myöhemmin kytketty toimistojärjestelmiin). Tämä ei ole kyberturvallisuuden kannalta mikään ideaalimalli, mutta löytyy edelleen valitettavan monesta järjestelmästä, eikä sen päivittäminen modernimmaksi ole helppoa.

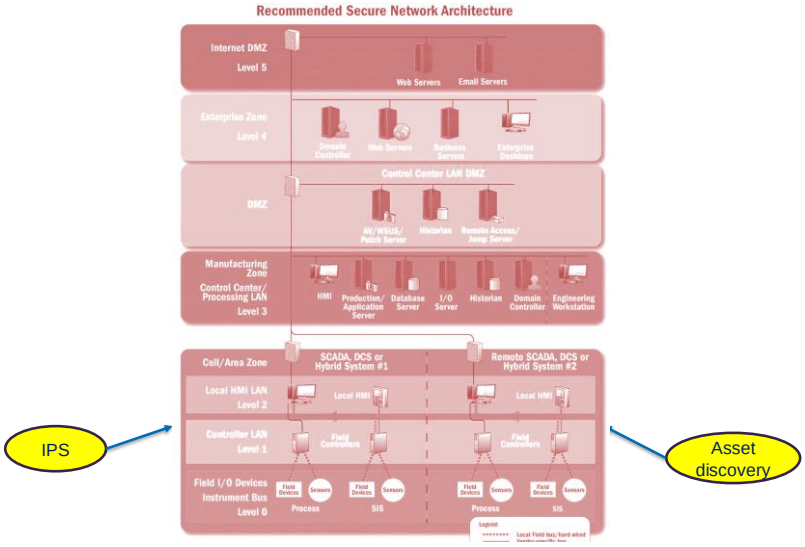
Perus kerrosmallia OT-arkkitehtuureille sanotaan Purdue-malliksi, tarkemmin PERA: Purdue Enterprise Reference architecture. Malli on standardoitu IEC62264:ssä. Mallia on ensin käytetty mm. prosessiteollisuuden teollisuusautomaatiolle. Purdue-malli on ollut pohjana ensimmäisen aallon teollisuusautomaation kyberturvallisuudelle, ja varsinkin OT-järjestelmien käytännön turvaamisen terminologia ja peruskäsitteet tulevat edelleen tästä mallista. Tasoja mallissa oli historiallisesti 4, mutta uusien lisäysten jälkeen 6 tai jopa 7.

Jos Purdue-mallissa lähdetään liikkeelle alhaalta, ensin tulevat itse sensorit ja aktuaattorit. Näitä ohjaavat erilaiset PLC:t tasolla 1 lähes kokonaan valmistajakohtaisten tietoliikenneprotokollien ja ratkaisuiden kautta. PLC:t ovat yhteydessä HMI:hin tasolla 2, jossa on käytössä jo jonkin verran avoimiakin tietoliikennestandardeja.

Tuotannon valvonta operatiivisine tehtävineen tapahtuu tasolla 3. Tämä on yleensä normaalissa lähiverkossa. Toimistojärjestelmät ja toiminnan optimointi ovat tasolla 4 ja Internetiin päin yhdistetyt järjestelmät tasolla 5.

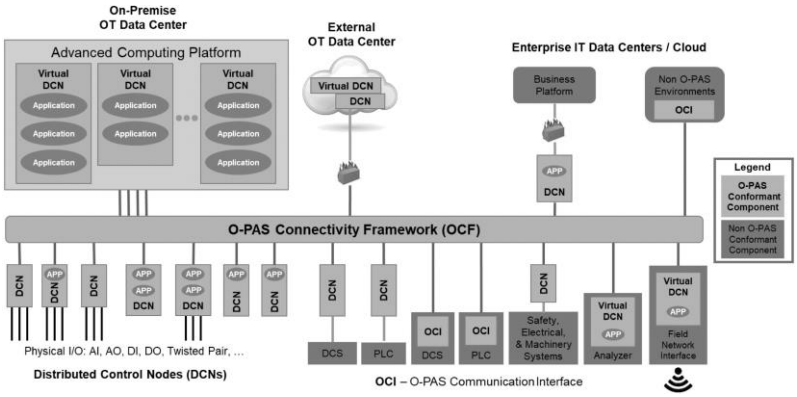
DCS = Distributed ICS, first attempt to network ICS or early SCADA systems
DMZ = Demilitarized Zone, a subnetwork realizing the “air gap” or “choke point”-principle: all traffic to the external world will have to travel through DMZ with hopefully sufficient examination and filtering

OT-verkkoarkkitehtuurit: Purdue



65

OT-verkkoarkkitehtuurit: O-PAS

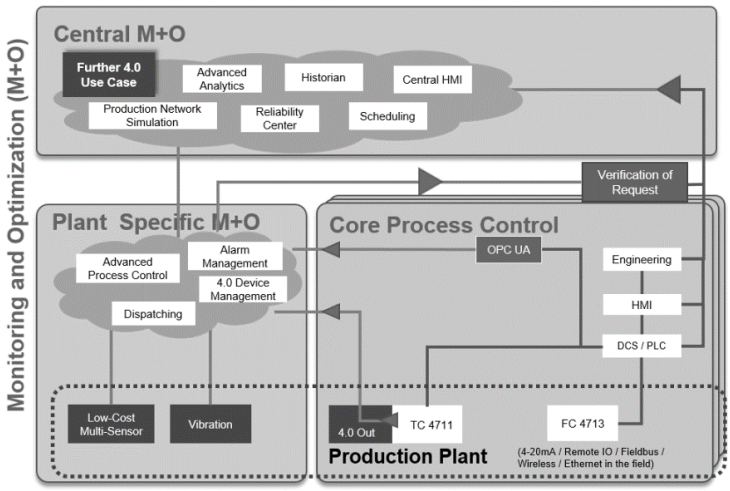


R. Donald Bartusiak, Stephen Bitar, David L. DeBari, Bradley G. Houk, Dennis Stevens, Bridget Fitzpatrick, Patrick Sloan. "Open Process Automation: A standards-based, open, secure, interoperable process control architecture, Control Engineering Practice, Volume 121, 2022, 105034,ISSN 0967-0661, https://doi.org/10.1016/j.conengprac.2021.105034.

66

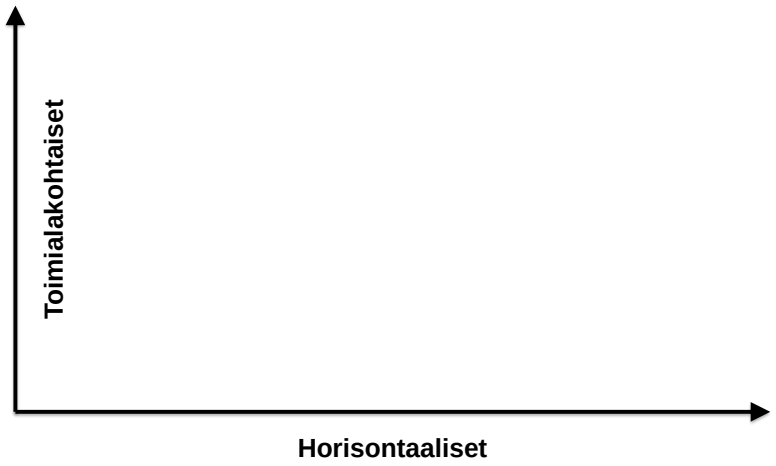
O-PAS eli Open Group:in Open Process Automation Forumin Open Process Automation Standard kytkee Purdue-mallin alakerrosten (tasojen 1-3) toiminnat yhteiseen avoimeen kommunikointikehikkoon (OCF), josta on yhteys (palomuurin kautta tarvittaessa) muille tasoille joko paikallisesti tai pilvessä, tai jopa vastaavan tason järjestelmiin pilvessä.

OT-verkkoarkkitehtuurit: NOA



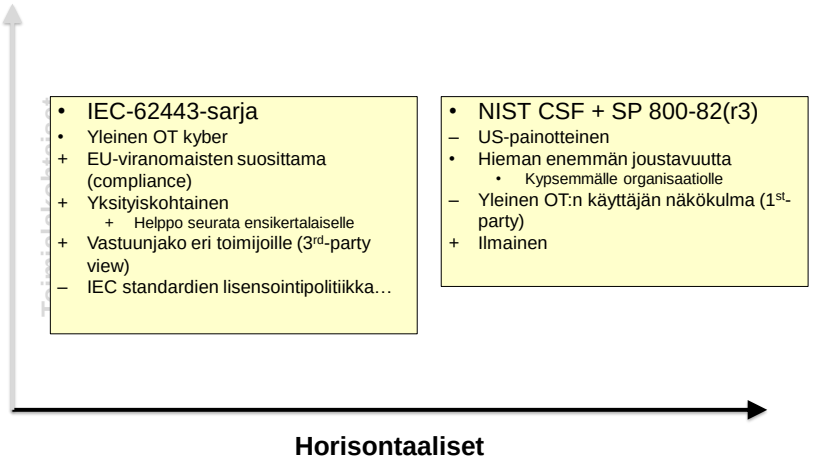
NOA, eli NAMUR Open Architecture, virallisesti NAMUR suositus NE 175 (-179), on saksalaisen NAMUR-organisaation (“Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V.“) sta konsepti, malli ja turva-aluemäärittely. NOA:n periaatteena on pitää teollisuusautomaatiodomain (Core Process Control, harmaa alue) itsenäisenä, mutta lisätä sen ympärille toinen „datakanava“ (Keskitetty ja aluekohtaiset valvonta- ja optimointikomponentit, pinkki). NOA tarjoaa lisäksi teollisuusriippumattomuuden standardoitujen tietomallien kautta, ja nojautuu muutenkin avoimiin standardeihin. NOA väistää Purdue-mallin haasteet liiketoiminnalle ulottamalla datakanavan alimpiin kerroksiin asti (kuten myös O-PAS)

IT vs. OT kyberstandardointi



68

IT vs. OT kyberstandardointi



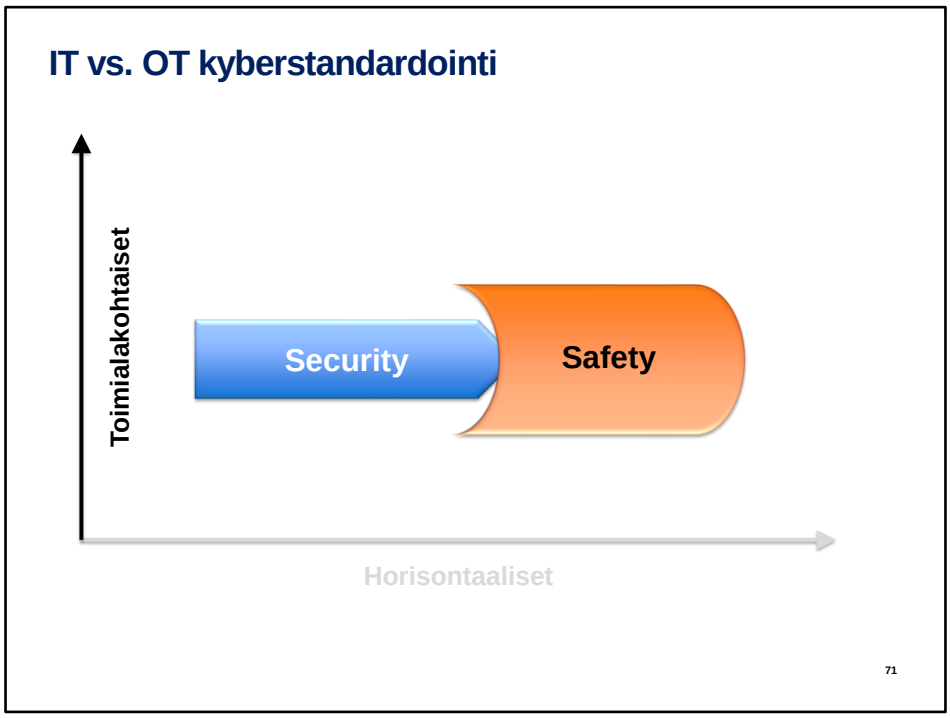
69

IT vs. OT kyberstandardointi

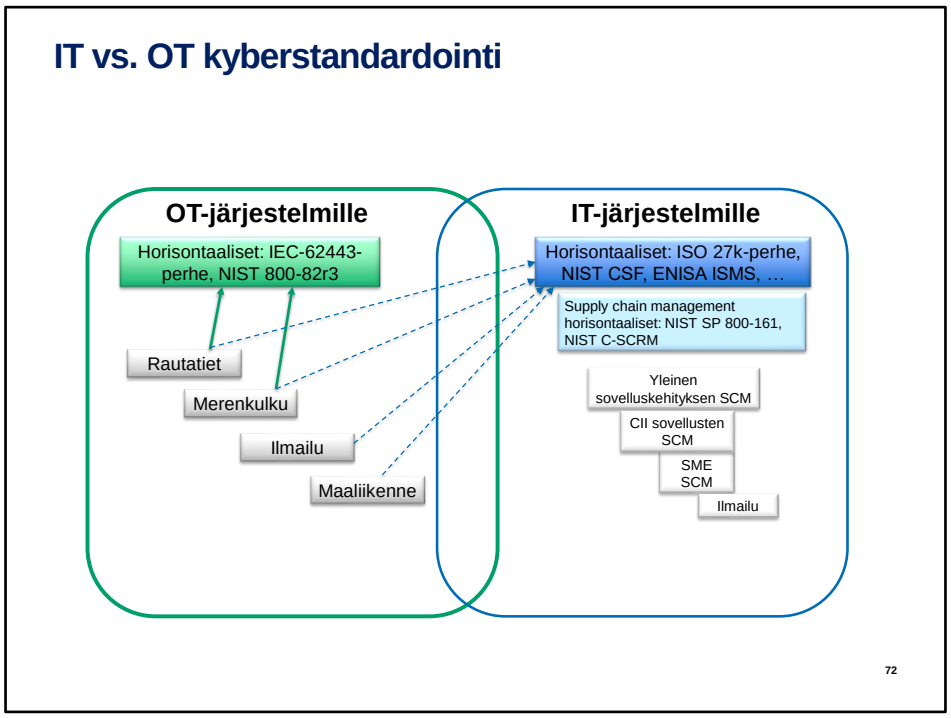
Standardi	Toimiala
CENELEC TS50701	Rautatiet
IACS UR E26-27	Laivat
EUROCAE ED202A	Lentokoneet
UL 2900-2-2	Toimitusketjut (ohjelmistot ja teoll.automaatio)
ISO-28004-2	Toimitusketjut (yleinen turvallisuus)

70

Toimialakohtaiset teollisuusautomaation kyberturvallisuusstandardit pyrkivät ottamaan huomioon kunkin toimialan, kuten esimerkiksi logistiikan tai alihankintaketjun kyberturvallisuuden. Nämä standardit ovat kyseisen toimialan katto-organisaatioiden varassa



Toimialakohtaiset standardit ottavat yleisemmin ja paremmin huomioon OT:n perusominaisuuden: CAIC ennen CIA:ta, ts. Safety ennen Securityä, unohtamatta jälkimmäistä kuitenkaan. Kyberturvallisuusstandardit on ikäänkuin paketoitu käyttöturvallisuusstandardien sisään.



On hyvä muistaa, että useimmat OT-järjestelmät eivät toimi yksin, vaan osana esimerkiksi rahtilogistiikan prosesseja. Suurin osa logistiikankin järjestelmistä ovat normaalia toimistoympäristöihin ja palvelinsaleihin tarkoitettua tietotekniikkaa, esim. BI- tai ERP-järjestelmiä. Näille taas on jo olemassa yleisen IT-puolen ohjeistusta ja standardeja.

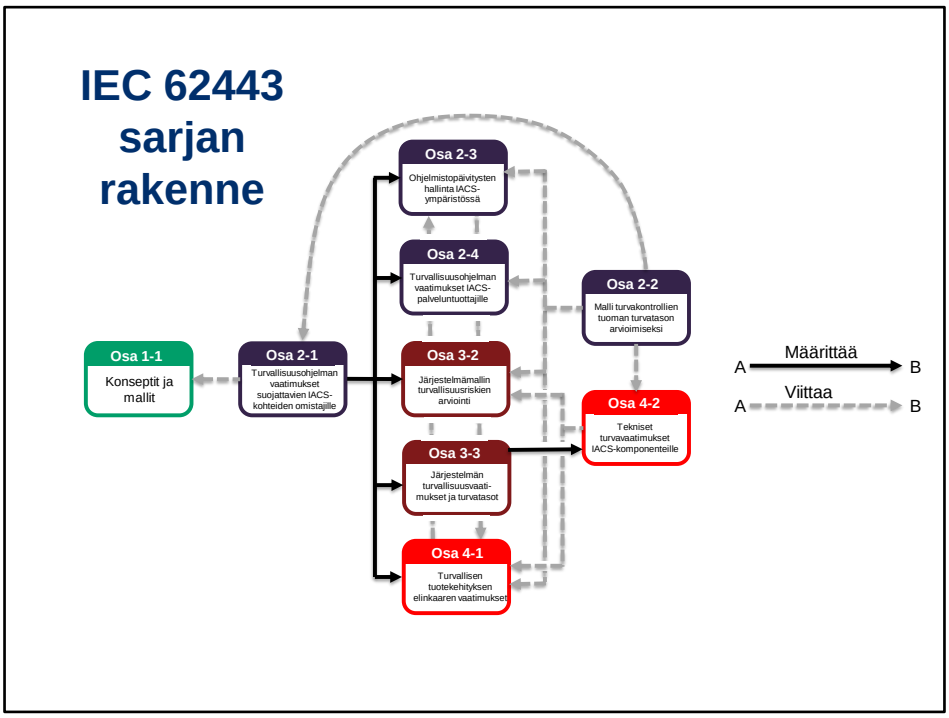
IT-puolen kyberturvallisuudessa suurimmalle osalle toimialoja pätevät horisontaaliset standardit. Poikkeuksena on toimitusketjujen hallinta, jolle on paljonkin omaa ohjeistusta.

OT-puolen toimialastandardit nykyisin viittaavat pääasiassa OT-puolen (osaksi myös IT-puolen) horisontaalisiin standardeihin.

ISO/IEC 62443

- **Standardisarja**
  - Yht. 15-18 eri dokumenttia (tällä hetkellä)
  - Eri statuksilla ja kehitysvaiheissa
- **Koskee teollisuusautomaatiota ja ohjausjärjestelmiä (IACS)**
  - "*kokoelma henkilöstöä, laitteistoja ja ohjelmistoja, joka voi vaikuttaa teollisuusprosessin turvalliseen, tietoturvalliseen ja luotettavaan toimintaan*" (IEC 62443-1-1, määritelmä 3.2.57)
  - Sisältää erityisesti: DCS, PLC, RTU, SCADA, älykkäät elektroniset laitteet, verkotettu elektroninen havaitseminen ja ohjaus, sekä seuranta- ja diagnostiikkajärjestelmät
- **Elinkaaren mittainen kattavuus:**
  - Järjestelmäkohtainen elinkaari
  - Tuotekohtainen elinkaari

73



IEC-62443-perhe on jaettu neljään eri sarjaan ja kussakin sarjassa maks. Viiteen eri dokumenttiin. Läheskään kaikilla dokumenteilla ei ole standardistatusta (johtuen joko prosessin keskeneräisyydestä tai dokumentin taustoittavasta luonteesta). Dokumenttisarjojen jakautumisperiaate on: 1: yleiset dokumentit, 2: politiikat ja toimintatavat, 3: järjestelmiä koskevat teknisemmät asiat ja 4: yksittäiselle komponenttitasolle menevät vaatimukset.

IEC 62443 eri rooleille

- Suojattavan kohteen omistaja
  - Turvallisuusohjelman luominen
  - Zones & Conduits
  - Vaatimusmäärittely ja hankintaprosessi
  - Operointi, huolto ja turvallisuusohjelman seuranta
- Integraattori/ palveluntarjoaja
  - Turvallisuusohjelman luominen
  - Turvallisten järjestelmien tuottaminen asiakkaan määrittelyjen mukaisesti
  - Turvallisuuspäivitysten hallinta
- Huoltopalvelu
  - Turvallisuusohjelman luominen
  - Huolto- ja muiden palvelujen kyberturvallinen tuottaminen asiakkaan vaatimusten mukaisesti
- Komponenttituottaja
  - SDLC:n luonti
  - Ohjausjärjestelmien tuottaminen tietylle turvatasolle
  - Komponenttien tuottaminen tietylle turvatasolle
  - Elinkaaren mittainen tuki komponenteille ja ohjausjärjestelmille

75

62443-sarja ottaa nk. Kolmannen osapuolen näkymän OT:n standardointiin. Tällöin se pyrkii ottamaan huomioon koko OT:n tuotantoketjun komponenttivalmistajasta käyttäjään. Käyttäjästä (asset owner) lähtien eri roolit ja niiden tehtävät ovat:

Tärkeimmät käsitteet IEC 62443:ssa

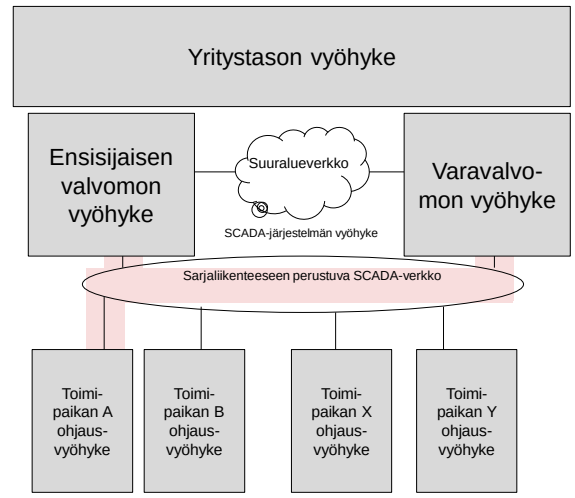
- ***Zone / vyöhyke*: Tietoturva-domain**
- ***Conduit / tietoväylä*: Vyöhykkeiden välillä kulkeva yhteyksien joukko**
  - Luottamussuhteet vyöhykkeiden ja väylien välillä riippuvat tietoturvatasoista
  - Koostuu *kanavista* (/ *channel*)
- ***Security Level / Tietoturvataso* / SL:**
  - Target SL / Tavoite-SL / SL-T: Zone/Conduit tavoitetaso (esim. AO määrittelyssä)
  - Capability SL / Kyky-SL / SL-C: Kontrollin kyky toteuttaa tietty taso
  - Achieved SL / Saavutettu SL / SL-A: Z/C saavutettu taso (AO:lla olevassa toteutuksessa)

76

77

IEC 62443 Zone / Conduit

- Esimerkki: SCADA
- Vyöhykkeet
- Eräs tietoväylä (punaisella)



Tässä kuvassa on esimerkki IEC 62443:n Zone-Conduit-ajattelusta. Vyöhykkeiden muodostamisen taustalla on usein edelleenkin Purdue-arkkitehtuuri, joskin itse vyöhykemalli ei estä käyttämästä moderniampiakin arkkitehtuureja. Käytännössä yhden vyöhykkeen muodostaa yhtenäisesti hallinnoitava, samaan käyttötarkoitukseen oletettujen järjestelmien kokonaisuus, jotka ovat samalla turvatasolla.
Kun puhun turvatasosta, viittaan nimenomaan käyttäjän / Asset Ownerin asettamaan tavoiteturvatasoon (SL-T, eli Target-SL). Kyseessä on siis ensisijaisesti järjestelmän käyttäjän

tavoitteiden mukainen kuvaus kokonaisuuden kyberturvallisuudesta. Integraattori ja ylläpitäjä voivat tämän kuitenkin muodostaa ja muokata, mutta vain AO:n hyväksynnällä.

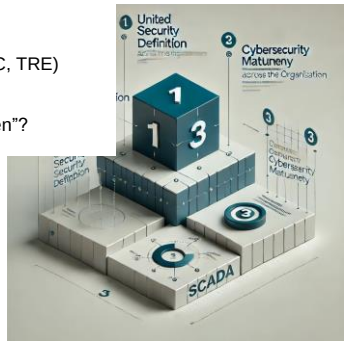
IEC 62443 perusvaatimukset

- **“Foundational requirements” (FR)**
- **OT-kyberturvallisuudelle priorisoituja kyberturvallisuusvaatimuksia**
- **7 pääluokkaa**
- **FR:iin sidottu useita järjestelmävaatimuksia (SR, 51 kpl) ja näiden tarkennuksia (RE)**
  - SR + RE: ~100 kpl

78

Tietoturvatasojen ominaisuuksia

- Organisaatio määrittelee tason merkityksen
  - Määritelmä sama organisaation ylitse
- Kvalitatiivisesta kvantitaviiseen
  - Organisaation kyberturvallisuusohjelman kypsyyden mukaan
- Kukin turvatason tyyppi ilmoitettavissa suhteessa perusvaatimuksiin (FR) ja elementtiin / kontrolliin
  - Esim. Zone “SCADA”, **`SL-T = [3,3,3,1,2,1,3]`**
  - Esim. Kontrolli “IDS/FW”, **`SL-C = [0,3,0,0,0,2,0]`** (UC, TRE)
- Tavoite-SL (SL-T):
  - Riskiperusteisesti: “mitä ***jos*** hyökkääjä pääsee tähän zoneen”?
- Kyky-SL (SL-C):
  - Järjestelmille FR-/SR-taulukko (Osa 3-3)
  - Komponenteille omat turvatoiminnot (osa 4-2)
- Saavutettu SL (SL-A):
  - Toteutuskohtainen määritys ja tulos
  - Aikariippuvainen
  - Ympäristön (koti- ja naapurivyöhykkeet) turvatasot



79

Turvatasojen oletetut hyökkääjäluokat

- Useimmiten perusvaatimusten osa-alueiden tasolla
- SL-4 vastaa valtiotason hyökkääjää vastaan olevaa turvallisuutta

SL #	Murron tyyppi	Tekniikat	Taidot	Resurssit	Motivaatio
SL-0	-	-	-	-	-
SL-1	Huolimattomuus/ Sattuma	-	-	-	-
SL-2	Tarkoituksellinen	Yksinkert.	Yleiset	Pienet	Alhainen
SL-3	Tarkoituksellinen	Monimutk.	IACS-tekniset	Keskikok.	Keskimäär.
SL-4	Tarkoituksellinen	Monimutk.	IACS-tekniset	Suuret	Korkea

80

Kyberturvallisuuden turvallisuusohjelman luominen

Teollisuusautomaation turvallisuusohjelma IEC 62443 perusteella

Nyt, kun IEC-62443 peruskäsitteet ja ideat ovat tuttuja, käyn seuraavaksi lävitse varsinaisen turvallisuusohjelman (CSMS, Cyber Security Management System) luomisen.

IEC 62443 Turvallisuusohjelman perustaminen

- **Cyber Security Management System (CSMS) program**
  - Vrt. ISO 27001 ISMS
- **Määritelty IEC 62443-2-1:ssä**
- **Käytännössä OT:n käyttäjän (AO) näkökulma riskienhallintaan**
- **Pohjana ISO/IEC 17799 ja 27001**
  - OT-ympäristössä huomioonotettavat erityispiirteet
- **Suurin osa organisaatiolle yleisiä riskienhallintaprosessin ja kyberturvallisuuden hallinnan osia**

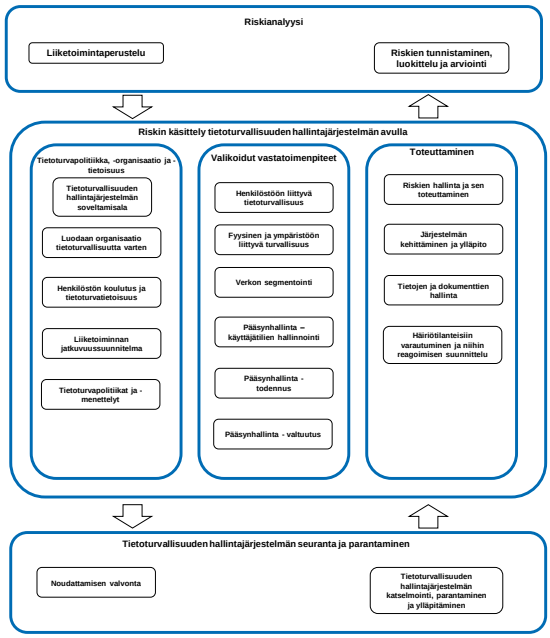
82

IEC 62443-2-1 on standardiperheessä turvallisuusohjelman perustamisesta vastaava osa. Jos muistatte, kyber- ja tietoturvallisuuden hallinnan kehikkoja oli kolmenlaisia: kontrollisuosituksia, riskienhallintajärjestelmiä ja turvallisuushallintaohjelman perustamisohjeistusta. IEC 62443 CSMS-ohjelma kuuluu jälkimmäisiin.

62443:n CSMS-ohjelman perustamisohjeet ovat suurimmaksi osaksi organisaatioille yleisiä riskien ja kyberturvallisuuden hallinnan prosessien perusteita. Pohjana näissä on käytetty yleisempää ISO 27001:stä (jossa luodaan ISMS-ohjelma IT-teknologiaa CIA-mallilla hallinnoivalle organisaatiolle).
Seuraavilla dioilla nostetaankin esille asioita, joissa OT:n erityispiirteet tulevat esiin.

Koska kyseessä on CSMS-ohjelma, tämä tarkoittaa, että 62443-standardiperheen kannalta kyseessä on järjestelmän omistajan ja käyttäjän (Asset Owner) näkökulma asiaan.

IEC 62443 turvallisuus-ohjelma teollisuusauto-maatiolle



IEC 62443-2-1 standardi kuvaa sen, miltä CSMS-ohjelman tulee näyttää, mikäli halutaan väittää standardiyhteensopivuutta. Standardi EI velvoita tiettyä sapluunaa kehittää CSMS-ohjelma, mutta tarjoaa esimerkkejä siihen, Kuinka sellainen ohjelma luodaan.

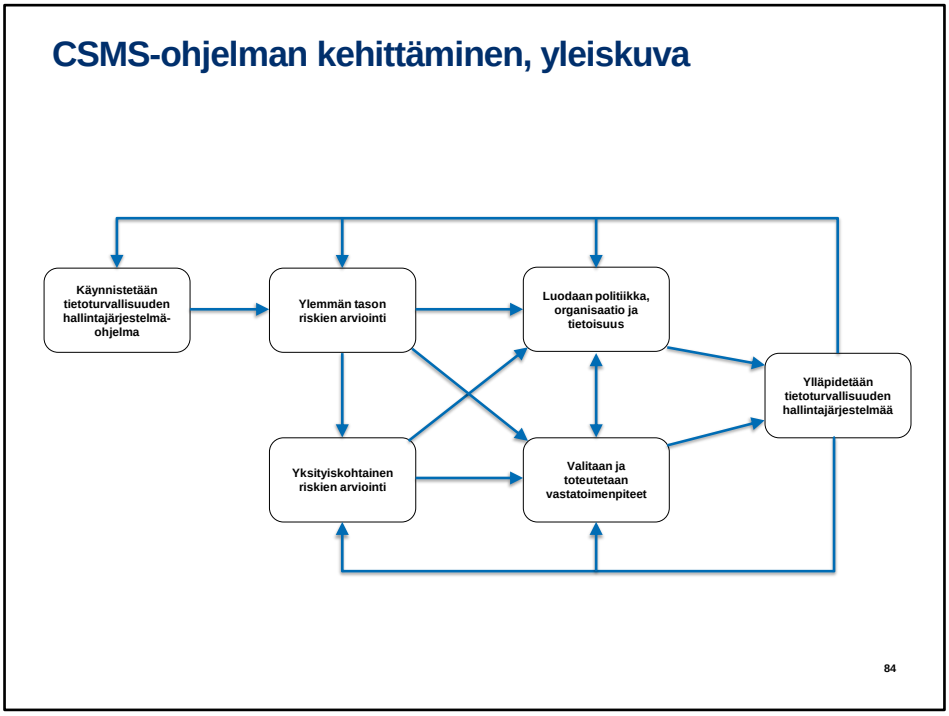
Oheinen kuva esittää valmista CSMS-ohjelmaa ja sen toimintoja. Valmiissa, käynnissä olevassa CSMS:ssä on kolme pääosaa

1) Riskianalyysi
2) Riskin käsittely CSMS:n (keskimmäinen laatikko) avulla
3) CSMS:n seuranta ja kehittäminen

Riskianalyysin liiketoimintaperustelu on koko prosessin kivijalka. Monet käsiteltävät asiat ja päätöspisteet palautuvat riskianalyysiin (tämä ei ole mitenkään ominaista nimenomaan OT-kyberturvallisuudelle pelkästään), ja riskianalyysin perustana on asioiden ja teknologioiden Liiketoimintaymmärrys.

Liiketoimintaperustelu vaatii: ymmärryksen OT:n merkityksestä organisaatiolle, jossa auttaa tietous tapahtuneiden häiriöiden historiasta ja LL (Lessons Learned) oppiminen mulita toimijoilta

Liiketoimintaperustelussa on otettava huomioon otettava: Taloudelliset, terveys-, turvallisuus (safety)- ja ympäristövaikutukset (mikäli johtuvat OT:n CIA:n vaarantumisesta);
OT:lle ominainen asia ovat OT:n osien vaihtelevat elinkaaret – vaihteluväli on paljon suurempaa kuin IT-järjestelmissä.



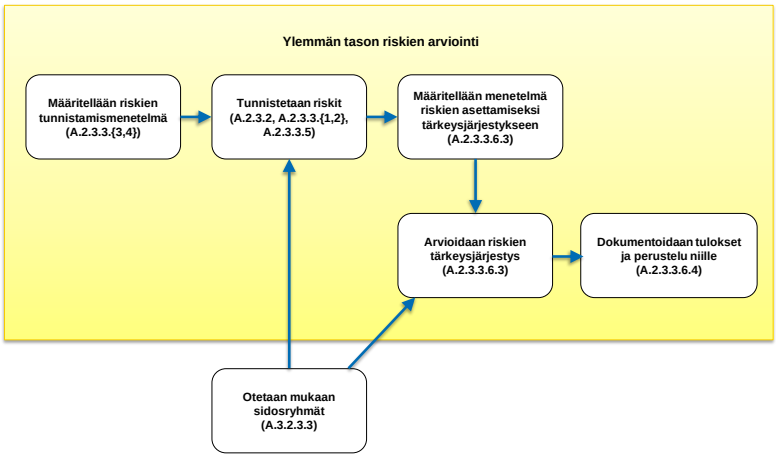
Tässä käydään lävitse yleisesti, miten CSMS-ohjelma kehitetään.

Menetelmä on top-down, eli yleisistä periaatteista yksityiskohtaisempia kohti. Esimerkiksi haav.kuvaukset ja tapahtumaketjut tulevat vasta yksityiskohtaisessa tarkastelussa esiin.

Ylemmän tason riskienarvioinnissa on tärkeää ilmaista rajaukset – CSMS-ohjelma voi olla hierarkkinen koko organisaatiosta yksittäisiin valmistuksenohjausjärjestelmiin. Yksittäisen CSMS-ohjelman osalta tulee selkeästi ilmaista kohde, ja tunnistaa rajapinnat muihin järjestelmiin.

Vastatoimenpiteet ja policy/koulutus on suunniteltava rinnan: sellaisella politiikalla ei ole mitään merkitystä, mitä ei voida käytössä olevin kontrollein toteuttaa, ei sellaisilla kontrolleilla mitään Tekoa, joita kukaan ei osaa käyttää.

CSMS-ohjelman kehittäminen, ylemmän tason riskienarviointi

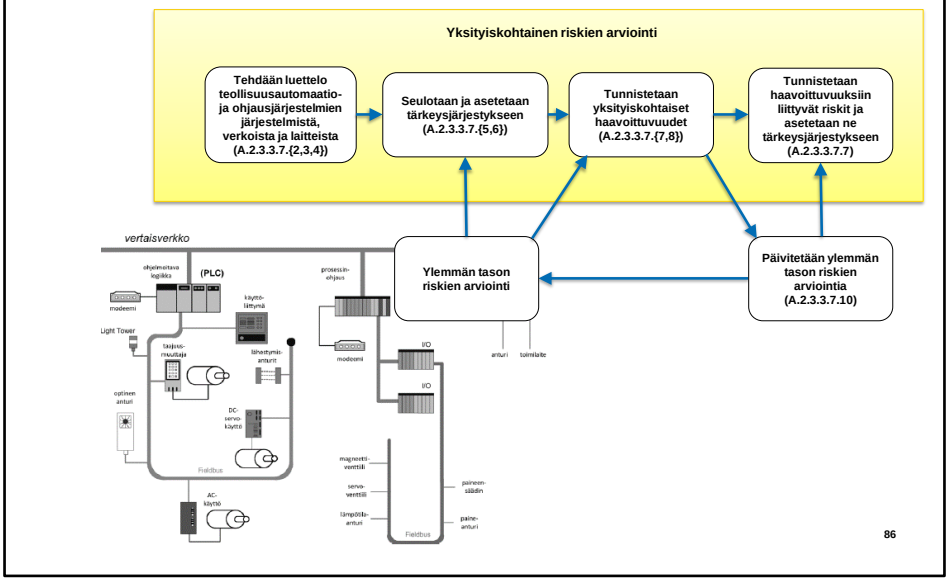


85

Tunnistamis- ja arviointimenetelmissä on hyvä päättää esimerkiksi, käytetäänkö kvalitatiivista vai kvantitatiivista menetelmää, mennäänkö kohde- vai skenaariokohtaisella analyysillä (vai molemmilla); käytetäänkö omaa arviointikehikkoa vai lainataanko (/ ostetaanko) muualta?
Riskien luokittelussa on hyvä kyetä yhdistelemään eri tapahtumien todennäköisyyksiä (suurin osa tapahtumista ei ole itsenäisiä tai yksinään merkittäviä) ja tarvittaessa kalibroida omia riskianalyysin asteikkojaan, esimerkiksi keräämällä ensin data omasta ja muiden organisaatioista.

Todennäköisyys- ja vaikutusluvut voivat kyllä muuttua, mutta niiden vaihteluvälin pitäisi tulla liiketoimintaperusteista etukäteen.

CSMS-ohjelman kehittäminen, yksityiskohtainen riskienarviointi



Yksityiskohtaisessa riskienarvioinnissa tullaan usein sitten laitetasolle.

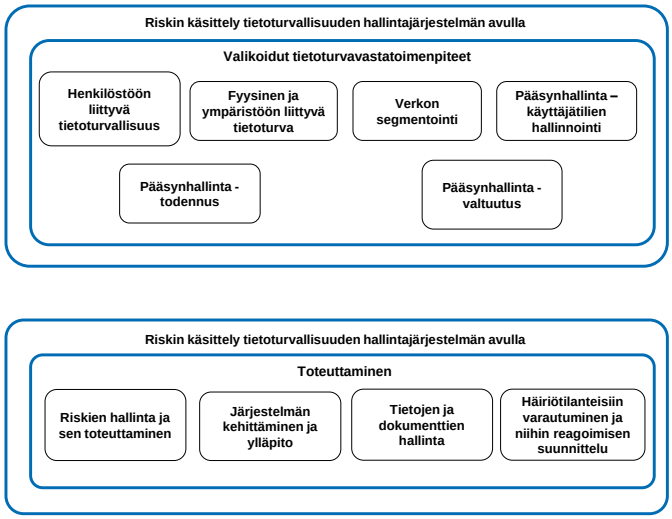
Laitetasolla tärkeää on yhtenäinen ja yhteismitallinen tilannekuva (esim. Zone-Conduit-kaaviota varten), kuten luokittelu vakiokriteereiden perusteella:

- Level 0/1: Ana/Digi?
- Kytkentäisyys? Verkkojen tyypit?
- Turva-alueet?
- Häiriötoiminnan seuraukset?

Tilannekuvassa auttaa verkkokaavion kehittäminen (kuten kuvassa vasemmalla alhaalla).

Nykytilanteen selvittämisen jälkeen on kartoitettava haavoittuvuudet ja haavoittuvat rajapinnat erikseen, esimerkiksi ulkoiset kytkennät ja etäyhteydellä tehtävä ylläpito.
OT-järjestelmien kanssa on erityistä huomiota kiinnitettävä seuraaviin teknologioihin: *modeemiyhteydet, etäkäyttöinen ikkunointi, telemetriaverkot, FR-verkot*

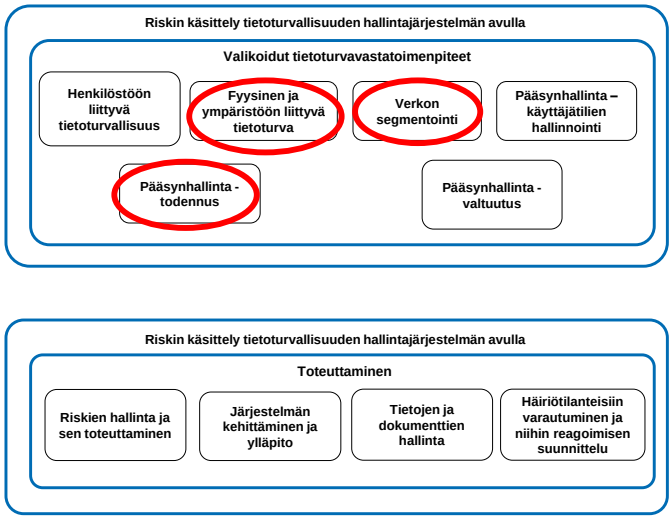
CSMS-ohjelman käyttö: riskien käsittely



87

Yksi tapa käsitellä riskejä on pienentää uhkien todennäköisyyttä. Tämä tehdään kontrollien eli vastatoimenpiteiden avulla.

CSMS-ohjelman käyttö: riskien käsittely

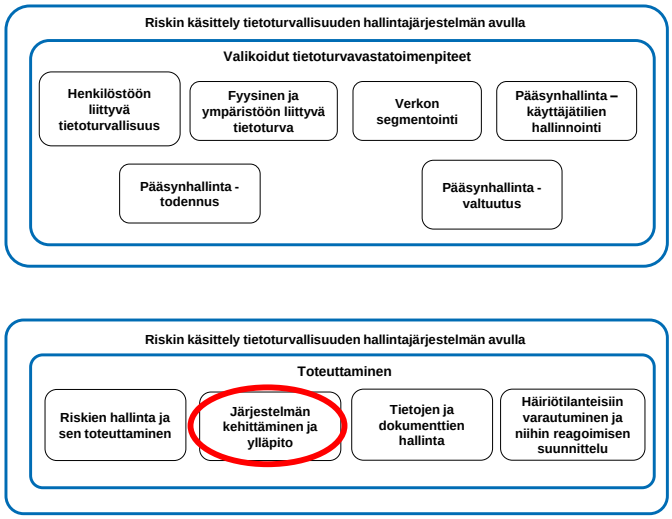


88

Vastatoimenpidevalikoimassa on näkyvissä OT:n perinteiset turvakontrollit:

- Käyttäjien- ja pääsynhallinta
- Verkon segmentointi
- Fyysinen turvallisuus

CSMS-ohjelman käyttö: riskien käsittely



89

Riskinkäsittelyn toteutustavoissa korostuu päivitystenhallinta ja (vastaanotto-)testaus, jotka ovat pääasiassa järjestelmän kehittämisen ja sen vaatimuksen alla.
Riskien hallinnan valvonnassa määrällisin keinoin käytetään standardin Zone-Conduit-mallin turvatasoja (SL) ja perusvaatimuksia (FR/SR)

IEC 62443 riskien käsittely, pääsynhallinta

- **Pääsynhallinta**
  - Hallinnointi
  - Todennus
  - Valtuutus
- **OT:n erityispiirteitä**
  - Valvomotyön roolipohjaisuus (esim. RBAC)
  - Fyysisen sijainnin merkitys (esim. ABAC)
  - Todennusstrategia
  - Valtuutuspolitiikka
    - Hienojakoisuus riskitason mukaan

90

Pääsynhallinnan kolme näkökulmaa ovat käyttäjätilien hallinnointi, todennus ja valtuuttaminen.

Käyttäjätilien hallinnointi tarkoittaa pääsynhallinnan periaatteiden ja yleisten tietoturvasääntöjen, kuten vaarallisten työyhdistelmien, roolipohjaisuuden, minimioikeuksien periaatteen ym. Valvomista tilejä ja rooleja luotaessa sekä ylläpitoa vallitsevan tilanteen (esimerkiksi vyöhykkeen turvatason nostamisesta tai henkilön irtisanoutumisesta johtuen) mukaisesti.

Todentaminen viittaa laitteiden, henkilöiden ja roolien identiteetistä varmistumiseen eri tilanteissa, erityisesti etäkäytössä ja vyöhykkeen ulkopuolelle mentäessä.

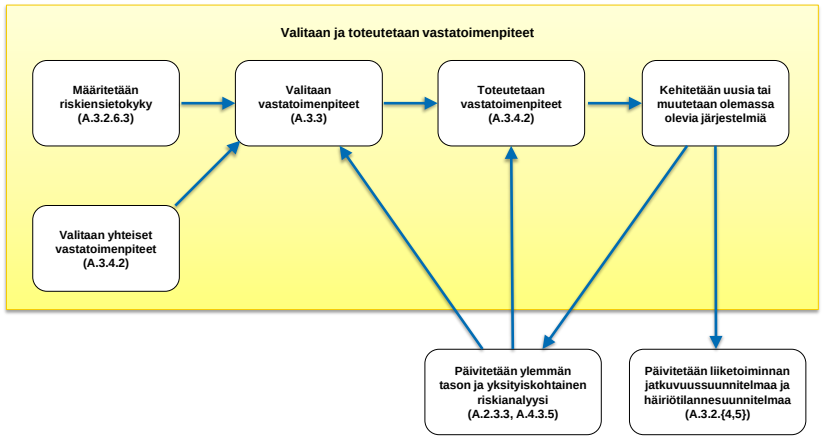
Valtuuttamiseen sisältyvät mm. ne säännöt ja politiikat, joiden perusteella varsinainen pääsy järjestelmään myönnetään, ja se voi olla riippuvainen paitsi roolista, myös ajankohdasta tai henkilön fyysisestä sijainnista.

OT-puolella tyypillistä on sääntöjen roolipohjaisuus esim. Valvomotyössä, ja ympäristötekijöiden merkitys. Tällöin luonnollisia tapoja hallita valtuutusta ovat RBAC (roolipohjainen pääsynhallinta) tai jopa ABAC (attribuuttipohjainen

pääsynhallinta). Valmistajat tosin antavat OT-laitteilleen tällaisia toteutusmahdollisuuksia varsin vaihtelevasti.

Riskienkäsittelymenetelmiä OT-ympäristöön luotaessa olisikin tärkeää luoda erikseen todennusstrategia ja valtuutuspolitiikka, joilla nämä funktiot kytketään korkeamman tason riskianalyysiin. Valtuutuspolitiikassa on suositeltavaa asettaa hienojakoisuus riskitason perusteella – alhaisen turvatason järjestelmiin voi riittää jopa yleinen pääsy kaikilta osaston työntekijöiltä kaikkiin järjestelmiin.

CSMS-ohjelman kehittäminen, kontrollien luonti riskinkäsittelyyn



91

Vastatoimenpiteet valitaan tiiviissä yhteistyössä riskianalyysin kanssa. Yhteisiä vastatoimenpiteitä ovat esimerkiksi ennalta valitut organisaation laajuiset toimenpiteet, ja yksityiskohtaisten vastatoimenpiteiden on voitava toimia näiden kanssa yhteen ja niiden asettamissa kehyksissä.

OT:lle erityisesti ominaisia asioita vaikkapa kenttälaitteiden (fyysisten turva-alueiden ulkopuolella olevat laitteet) turvallisuudessa on niiden fyysisen turvallisuuden takaaminen tai sen loukkaamisen käsitteleminen.

Zone-Conduit-malli auttaa toteuttamaan segmentoinnin ja reunaturvallisuuden (perimeter security) kontrollit