

**Industry 4.0 & Automation Academy**

# **Tietoturva teknologiassa**

**Tom Tuunainen**

# Kyberturvallisuuden johtaminen

- Organisaation tulee tarkastella muuttuneen kyberturvallisuuden uhkakuvan vaikutuksia omaan toimintaansa
- Vastuu kyberturvallisuudesta kuuluu viime kädessä organisaation johdolle
- Kehotamme:
  - varaamaan riittävät resurssit kyberturvallisuuden varmistamiseksi ja tarvittavien toimenpiteiden toteuttamiseksi. Tässä yhteydessä on huomioitava myös johdon tavoitettavuus kriittisten päätösten tekemiseksi.
  - tarkastelemaan, mitkä ovat organisaatioiden ydintoimintojen kannalta suojattavat digitaaliset palvelut ja ovatko niiden suojaustoimenpiteet ajantasaisia sekä ylläpidettyjä. Toimenpiteissä tulee huomioida organisaation riskien- ja jatkuvuudenhallintaa sekä myös fyysisiä turvallisuusjärjestelyitä koskevat tarpeet.
  - seuraamaan kyberturvallisuuden tilaa viranomaisten (esim. Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen) tiedotteiden ja tilannekuvatuoitteiden välityksellä.

# Määritellään liiketoimintakriittiset ympäristöt

- Johdon tulee määritellä sen toiminnan kannalta kriittiset prosessit sekä niiden vaatimat digitaaliset palvelut ja tieto-omaisuus
- Kyberhäiriötilanteella voi olla vaikutuksia yhtäaikaisesti useisiin organisaation tarvitsemiin palveluihin
  - palauttaminen tulee perustua etukäteen määriteltyyn, dokumentoituun sekä harjoiteltuun suunnitelmaan
  - tulee myös olla selvää, mikä on palveluiden keskinäinen tärkeysjärjestys
- Johdon tulee valmistautua mahdollisuuteen, että toiminta voi keskeytyä
  - esimerkiksi kiristyshaittaohjelman tai tietojen tuhoamiseen tähtäävän hyökkäyksen johdosta
  - tällöin ainoa toiminnan jatkuvuuden mahdollistava keino ovat ajantasaiset ja palautettavissa olevat varmuuskopiot

# Suojataan liiketoimintakriittiset ympäristöt

- Hyökkääjät pyrkivät etsimään ja löytämään organisaation toiminnan kannalta kriittiset digitaaliset palvelut sekä hankkimaan pääsyn niihin
- Organisaatioiden tulee varmistaa, että se torjuu näitä uhkia huolellisella tietoturvyöllä
- Organisaation tulee tarkastella ja priorisoida toimenpiteitä omista lähtökohdistaan

# Otetaan käyttöön monivaiheinen tunnistautuminen

- Kaikissa julkisesta verkosta tavoitettavissa ja kirjautumista vaativissa digitaalisissa palveluissa tulee aina olla käytössä vahva monivaiheinen tunnistautuminen (MFA, 2FA)
- Mikäli monivaiheinen tunnistautuminen ei ole jostain syystä mahdollista, tulee kyseinen järjestelmä suojata jotenkin muuten estämällä sen suora käyttö julkisesta verkosta

# Asennetaan tietoturvapäivitykset viipymättä

- Tietoturvapäivitykset tulee asentaa viipymättä
  - aikaväli haavoittuvuuksien löytymisestä niiden laajamittaisen hyväksikäytön alkamiseen on lyhentynyt koko ajan
- Rikolliset pyrkivät hyödyntämään myös päätelaitteiden haavoittuvuuksia
  - täten laitteiden käyttöjärjestelmät, toimisto-ohjelmistot sekä selaimet tulee päivittää viipymättä
- Suositeltavinta on ottaa käyttöön automaattiset päivitykset
- Organisaation tulee seurata kaikkia oman toimintaympäristönsä kannalta oleellisia haavoittuvuuksia sekä arvioida niiden merkitys oman toiminnan jatkuvuusriskien kannalta

# Varmistetaan tietoliikenteen turvallisuus

- Organisaation tulee määritellä, mikä on sen verkoissa toiminnan kannalta tarpeellista ja normaalia tietoliikennettä
  - palomureilla on estettävä organisaation tietoliikenneverkkojen kaikki tarpeeton tietoliikenne
- Tietoliikenneturvallisudessa tule myös huomioida palvelimet sekä päätelaitteet, jolloin niiden sovelluspalomureilla sallitaan ainoastaan käytössä olevien sovellusten toiminnan kannalta tarpeellinen tietoliikenne
  - menettelyllä vaikeutetaan organisaation verkkoon päässeeseen tunkeutujan etenemistä ympäristöstä toiseen
  - tavoitetta tukee myös verkon jakaminen osiin, eli segmentointi

# Suojaudutaan haittaohjelmilta

- Haittaohjelma muodostaa merkittävän riskin toiminnan jatkumiselle
- Haittaohjelmatorjunnan tulee kattaa organisaation kaikki digitaaliset palvelut, palvelimet ja päätelaitteet
- Kaikki organisaatioon saapuvat ja lähtevät tiedostot tulee tarkastaa haittaohjelmien varalta
- Päätelaitteilta tai palvelimilta tuleviin hälytyksiin tulee reagoida välittömästi
  - hälytys on usein tunkeutumisyrittäksen ensimmäinen merkki
  - hälytyksen kohde tulee eristää verkosta ja tutkia

# Varaudutaan palvelunestohyökkäyksiin

- Palvelunestohyökkäyksessä luodaan tyypillisesti keinotekoisesti ruuhkaa palveluun esimerkiksi täyttämällä palvelun käyttämän nettiliittymän kaista tai aiheuttamalla jollekin laitteelle niin paljon prosessointikuormaa, että toiminta estyy (Distributed Denial of Service, DDoS)
  - pullonkaulaksi voi muodostua paitsi verkkopalvelin myös esimerkiksi palomuuuri
- Tulee arvioida, mihin organisaation digitaalisiin palveluihin voisi kohdistua toimintaa häiritsevää palvelunestohyökkäystä
- Tulee myös kysyä:
  - minkä palveluiden tulee toimia myös kuormitustilanteissa?
  - kuinka kauan palvelunestohyökkäystä voidaan kestää toiminnan häiriintymättä liiaksi?
- Palvelunestohyökkäyksen tehokas torjuminen voi vaatia asiantuntemusta ja laitteistoa, jota ei normaalisti ole käytettävissä
  - jos palvelun toimivuus on organisaatiolle tärkeää, on poikkeustilanteisiin varautuminen otettava huomioon jo palvelun toteutusta suunniteltaessa
  - vähintään on tiedettävä, mistä ja minkälaisella aikataululla asiantuntija-apua on saatavilla

# Suojataan pilvipalvelut

- Pilvipalveluiden osalta tulee varmistaa, että kaikki organisaation kannalta tarpeelliset tietoturvaratkaisut on otettu käyttöön
  - pilvipalvelujen oletusasetukset eivät aina ole tietoturvan kannalta riittäviä
- Ulkoisissa pilvipalveluissa niiden toimittaja vastaa tyypillisesti infrastruktuurin turvallisuudesta
- Vastuu tiedon suojaamisesta pilvipalvelussa on kuitenkin aina loppuasiakkaalla itsellään
  - vaikka käytännön työn tekisikin joku muu, tulee organisaation itse johtaa siihen liittyvää tietoturvaa
  - organisaation tulee määritellä ja ohjeistaa, miten sen tietoa tulee suojata, käsitellä, ja minkälaisia tietoja suojaavia käytänteitä tulee ottaa käyttöön

# Varmistetaan etäyhteyksien turvallisuus

- organisaatioiden tulee arvioida ovatko olemassa olevat etäyhteydet tarpeellisia, esimerkiksi kysymällä:
  - onko organisaatio varmasti tietoinen kaikista etäyhteystavoista, joita sillä on käytössään oman henkilöstön tai kumppanien tarpeisiin?
  - ovatko kaikki etäyhteydet vielä toiminnan kannalta välttämättömiä?
  - tarvitseeko koko henkilöstö tai kaikki kumppanit vielä etäyhteyksiä, vai riittäisikö niiden tarjoaminen esimerkiksi ainoastaan päivystysluonteista työtä tekeville tahoille?
  - jos käytössä on ulkoisten kumppanien etäyhteyksiä organisaation ympäristöön, huomioidaanko niiden yhteydessä riittävästi riski tätä kautta tulevasta tunkeutumisesta?

# Varmistetaan etäyhteysien turvallisuus

- siltä osin kun etäyhteydet katsotaan välttämättömiksi, tulee niiden tietoturvallisuudesta varmistua, ja tällöin seuraavat toimenpiteet ovat oleellisia:
  - varmistetaan, onko etäyhteyksien ratkaisu ylipäätensä riittävän turvallinen käyttötarkoitukseensa, ja onko se valmistajan tietoturvapäivitysten piirissä
  - etäyhteyden toteuttavan tuotteen haavoittuvuuksia seurataan, ja päivitykset asennetaan viipymättä, niin palvelimen kuin päätelaitteidenkin osalta
  - etäyhteyksien ratkaisu on konfiguroitu turvallisesti ja vain toiminnan kannalta välttämättömät toiminnallisuudet on otettu käyttöön
  - etäyhteyksien käyttäjätilejä ylläpidetään aktiivisesti ja tarpeettomaksi käyneet suljetaan välittömästi
  - etäyhteyksien käyttöä valvotaan ja niistä kerätään kattavaa valvontalokia
  - kaikki etäyhteydet on dokumentoitu ajantasaisesti

# Huolehditetaan varmuuskopioista

- Kaikista toiminnan kannalta tärkeistä tiedoista tulee ottaa säännöllisesti varmuuskopiot
  - varmuuskopioihin tulee sisällyttää liiketoimintatiedon lisäksi myös erilaiset järjestelmäasetukset
  - varmuuskopioiden osalta on hyvä noudattaa 321-sääntöä, jolloin tieto on tallennettu vähintään 3 paikkaan, tieto sijaitsee vähintään 2 eri laitteella tai medially, ja 1 varmuuskopio on täysin eri paikassa
- Varmuuskopioiden avulla tulee kyetä palauttamaan toiminta myös tilanteessa, jossa organisaation koko tietotekninen ympäristö joudutaan asentamaan uudelleen
- Varmuuskopioiden palauttamista tulee myös testata säännöllisesti
  - näin varmistutaan, että niiden palauttaminen onnistuu ja myös tarvittavat järjestelmäasetukset on varmuuskopioitu

# Tarkistetaan julkiseen verkkoon näkyvät palvelut

- Rikolliset etsivät jatkuvasti verkosta sellaisia palveluja, joita he voisivat hyödyntää
- Jokin vain sisäiseen käyttöön tarkoitettu palvelu saattaa päätyä julkiseen verkkoon epähuomioissa tai esimerkiksi palomuurin konfiguraatiovirheen johdosta
- On suositeltavaa aika ajoin tarkastaa vastaako organisaation oma käsitys todellisuutta

# Tarkastellaan langattomien teknologioiden muodostamia riskejä

## Langattomat tietoliikenneverkot

- Organisaatioiden tulee huomioida langattomien tietoliikenneteknologioiden muodostamia riskejä niiden kriittisten prosessien yhteydessä:
  - mikään toiminnan kannalta tärkeä tietoliikenneyhteys ei saa perustua pelkästään yhteen langattomaan teknologiaan
  - käytössä tulee olla myös jokin vaihtoehtoinen tapa
  - päätelaitteiden liikkuvissa yhteyksissä tulee huomioida, että julkinen WLAN-verkko tai ulkomaisen operaattorin matkapuhelinverkko ei välttämättä ole aina turvallinen

# Tarkastellaan langattomien teknologioiden muodostamia riskejä

## Sijainti- ja aikatietopalvelut

- Organisaatioiden tulee selvittää minkälaisia vaikutuksia niiden toiminnalle aiheutuu sijainti- ja aikatiedon luotettavuuden heikentymisestä tai saatavuuden katkoksesta:
  - tarkka ja luotettava sijaintitieto on olennainen osa älykkäiden liikenne- ja tilannekuvajärjestelmien kehitystä, joissa eri toimintojen koordinointi pohjautuu henkilöiden tai laitteiden sijaintiin alueella
  - aikatietoa hyödynnetään laajasti mm. tietoliikenne-, tele-, televisio- ja energiansiirtoverkoissa eri järjestelmäosien toiminnan synkronointiin

# Havainnoidaan ja analysoidaan tapahtumia

Organisaatioiden tulee varmistaa kyvykkyys havaita kriittisiin ympäristöihin kohdistuvia tietoturvapoikkeamia

- lokitietoa tulee kerätä sellaisista laitteista, ohjelmistoista ja tietovarannoista, joita hyökkääjä voisi käyttää hyväkseen
- lokitietoa tarvitaan selvittämään, mitä, miksi ja milloin jotakin tapahtui
- mitä suurempi vaikutus vaarantuneella suojattavalla kohteella on, sitä enemmän lokitietoja tulee kerätä kohteesta
- lokitiedot tulee suojata vaikuttamiselta
- lokeista tulee erityisesti etsiä merkkejä seuraavista asioista:
  - käyttäjätietokantojen ja hakemistopalveluiden kirjautumislokeissa (esim. Active Directory tai Azure AD) näkyvistä epänormaaleista tapahtumista, kuten uusien käyttäjätilien luonti, käyttöoikeuksien korottaminen tai kirjautumiset epänormaaleista maantieteellisistä paikoista, päätelaitteilla tai ajankohtina
  - palomuurilokeissa näkyvistä epänormaaleista osoitteista, protokollista, liikennemääristä, tai ajallisesti tavallisuudesta poikkeavista tapahtumista

# Reagoidaan tapahtumiin ja häiriöihin

- Organisaatiolla tulee olla kyvykkyys reagoida välittömästi sen kriittisiin toimintoihin kohdistuviin kybertapahtumiin tai –häiriöihin
  - tilanteisiin tulee olla tunnistettu soveltuvat henkilöt tai roolit
- Tämän toiminnan tärkeimpänä tavoitteena on rajoittaa organisaation toimintaan kohdistuvaa vaikutusta sekä mahdollistaa toiminnan palauttaminen normaaliksi
- kyberhäiriöiden reagoimisen varalle tulee olla suunnitelma, jota pidetään yllä ja joka kattaa koko häiriönhallinnan elinkaaren

# Varmistetaan toiminnan jatkuvuus

- Organisaatiolla tulee olla toiminnan jatkuvuutta koskevat suunnitelmat, joiden avulla toiminta voidaan säilyttää ja palauttaa
- Jatkuvuussuunnitelmissa on tunnistettu ja dokumentoitu ne laitteet, ohjelmistot ja tietovarannot sekä toiminnat, jotka minimissään tarvitaan toiminnan ylläpitämiseksi

# Tiedotetaan henkilöstöä

- Koko henkilöstöllä on tärkeä rooli kyberturvallisuuden varmistamisessa
- Johdon tulee varmistaa, että henkilöstö on riittävän tietoinen kyberturvallisuuden merkityksestä organisaation toiminnalle
- Henkilöstölle tulee antaa koulutuksen ja viestinnän keinoin riittävät valmiudet arkipäiväisten kyberturvallisuusuhkien kohtaamiseen
- Organisaatioissa tulee vähintään toteuttaa seuraavat toimenpiteet:
  - johto viestii selkeästi koko henkilöstölle kyberturvallisuuden merkityksen toiminnalle ja johdon ehdottoman sitoutumisen asiaan
  - johto järjestää henkilöstölle säännöllisesti sen työtehtävien kannalta riittävää tietoturvakoulutusta, jotta se kykenee toimimaan turvallisesti
  - johto järjestää henkilöstölle kanavan, jonka kautta se voi ilmoittaa havaitsemistaan tietoturvapoikkeamista tai niiden epäilyistä

# Kyse on seuraavista...

1. Luottamuksellisuudesta
2. Eheydestä
3. Saatavuudesta
4. Todennuksesta

# Tuotannon kyberturvallisuuskyvykkyyden yleiskartoituksen suunnittelun tarkastuslista

Oletteko muodostaneet organisaatiossanne kyberturvallisuuden, tietoturvallisuuden, tai kokonaisturvallisuuden tiimin, jonka vastuulle kuuluu tietoturvan kehittäminen ja valvonta?

- Onko organisaation johto sitoutunut kyberturvallisuuden kehittämiseen?
  - Miten sitoutuminen näkyy henkilöstön työajan resursoinnissa?
  - Onko kyberturvallisuus säännöllisesti johdon käsiteltävänä?
    - Onko automaatioympäristöjen kyberturvallisuus säännöllisesti johdon käsiteltävänä?

# Tuotannon kyberturvallisuuskyvykkyyden yleiskartoituksen suunnittelun tarkastuslista

- Onko kehitystiimissä mukana henkilöitä kaikilta automaation kannalta kriittisiltä osa-alueilta, esimerkiksi
  - tuotannon (automaation) kunnossapidosta ja kehittämisestä,
  - yritys- ja laitostason ICT-järjestelmien ylläpidosta ja kehittämisestä,
  - automaation hankinnoista,
  - tuotannon järjestelmien pääkäyttäjistä,
  - kokonaisturvallisuudesta ja sen kehittämisestä, ja
  - henkilö- ja ympäristöturvallisuuden kehittämisestä?

# Tuotannon kyberturvallisuuskyvykkyyden yleiskartoituksen suunnittelun tarkastuslista

Oletteko määritelleet tuotannon kyberturvallisuuskyvykkyyden yleiskartoituksen tavoitteet?

- Onko tavoitteena tunnistaa kyberturvallisuuden kehittämiskohteet yleisesti?
  - Vai keskitytäänkö vain tiettyihin tuotantojärjestelmiin?

Oletteko valinneet kartoituskohteen?

- Mitä dokumentaatiota kohteesta toimitatte kartoittajille?
  - Toimitatteko tietoturvapolitiikoita ja käytäntöjä kuvaavaa materiaalia?
  - Toimitatteko teknistä materiaalia kuten verkkokuvia ja inventaarioraportteja?

Oletteko määritelleet mitä menetelmiä kartoittaja saa käyttää ja mitä menetelmiä hänen pitää käyttää kartoituksen aikana?

- Tehdäänkö kartoituksen aikana passiivisia toimenpiteitä kuten esimerkiksi
  - dokumentoinnin katselmuksia,
  - haastatteluja ja
  - avointen lähteiden tiedustelua (Open-Source Intelligence OSINT).

# Tuotannon kyberturvallisuuskyvykkyyden yleiskartoituksen suunnittelun tarkastuslista

- Tehdäänkö kartoituksen aikana aktiivisia toimenpiteitä kuten
  - haavoittuvuusskannausta,
  - penetraatiotestausta (tunkeutumistestaus),
  - kohteessa olevien langattomien verkkojen analysointia,
  - sosiaalista manipulointia,
  - verkkoliikenteen tallennusta ja analyysiä,
  - ohjelmistojen lähdekoodin analyysiä,
  - lokien tutkimista,
  - palomuurisääntöjen tutkimista, tai
  - häiriönhallintaprosessien testaamista testisyötteillä.

# Tuotannon kyberturvallisuuskyvykkyyden yleiskartoituksen suunnittelu

## Tarkastuslista

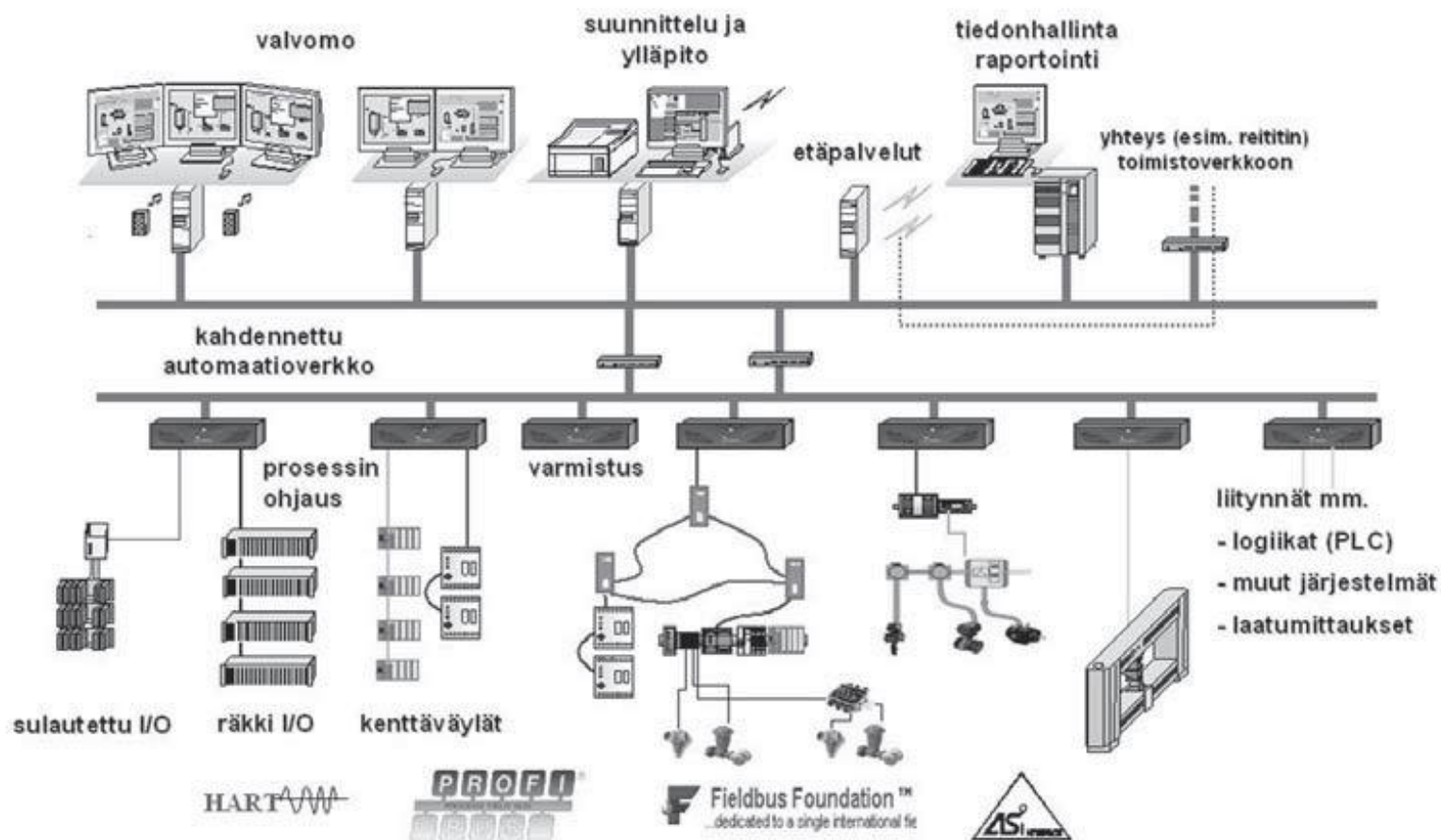
### Hallinnollisiin vaatimuksiin kuuluu:

- automaation tietoturvatietoisuus,
- automaation tietoturvaan liittyvä raportointi ja rekisterit,
- automaatio-omaisuuden hallinta,
- automaation käyttäjien hallinta ja käyttöoikeudet,
- automaation häiriötilanteesta toipuminen ja
- automaation tietojärjestelmien ja sovelluksien hallinta, kehitys ja ylläpito.

### Teknisiin vaatimuksiin kuuluu:

- automaation omaisuuden hallinta,
- automaation päivitysten ja muutostenhallinta,
- automaatioverkon turvavyöhykkeet ja datan suodatus.
- automaatioverkon pääsynvalvonta,
- automaationverkon suojaaminen haittaohjelmia vastaan,
- automaatiojärjestelmän varmuuskopiointi ja niistä palauttaminen ja
- automaation fyysinen suojaus.

# Teollisuusautomaatio, verkottuminen ja tietoturva

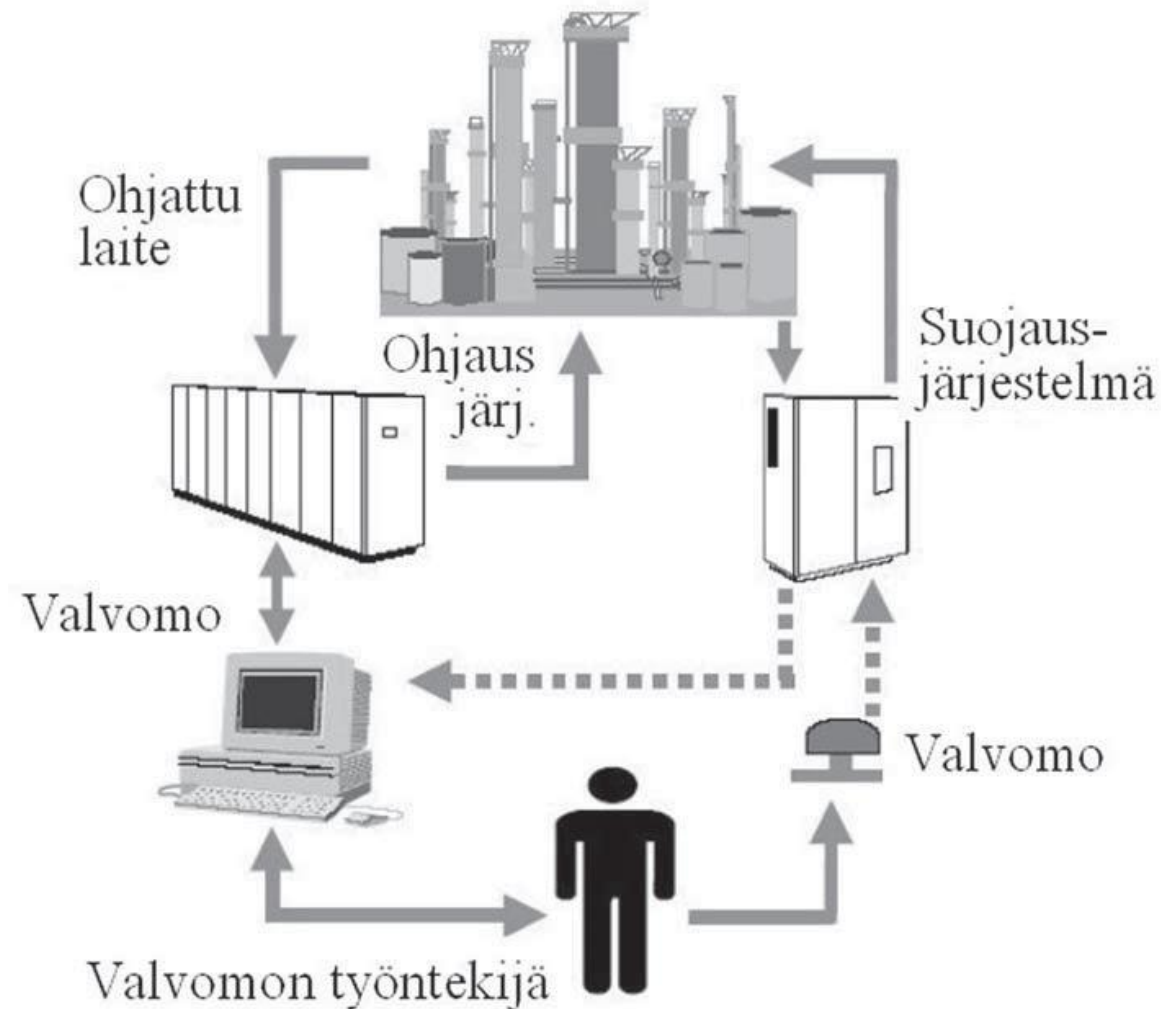


Automaatiojärjestelmä

# Automaatiojärjestelmien luokittelu

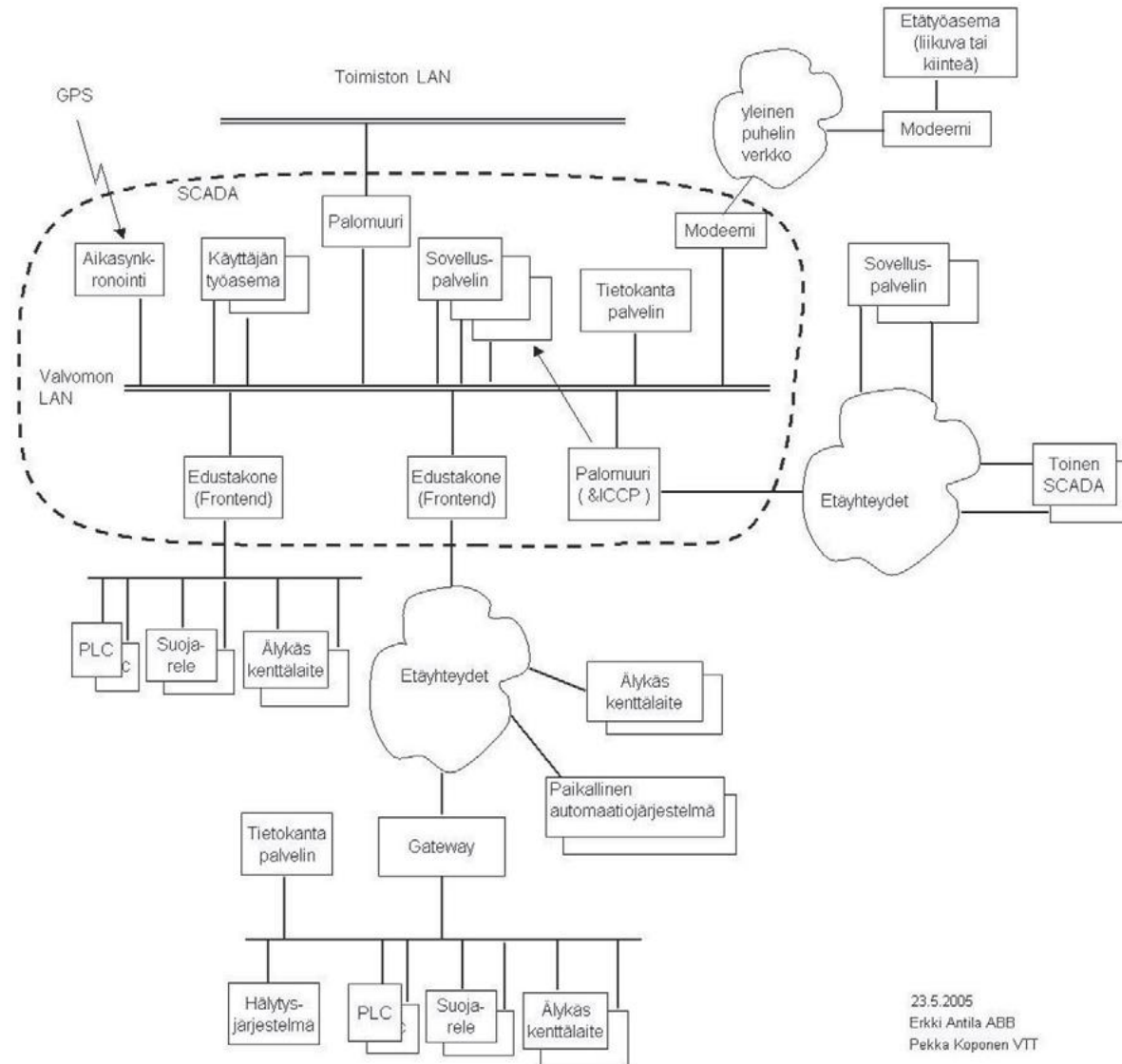
1. Hajautetut automaatiojärjestelmät (Distributed Control Systems, DCS)
2. SCADA-käytönvalvontajärjestelmät (Supervisory Control and Data Acquisition Systems)
3. Ohjelmoitavat logiikkajärjestelmät (Programmable Logic Control, PLC)

# Hajautettu ohjausjärjestelmä



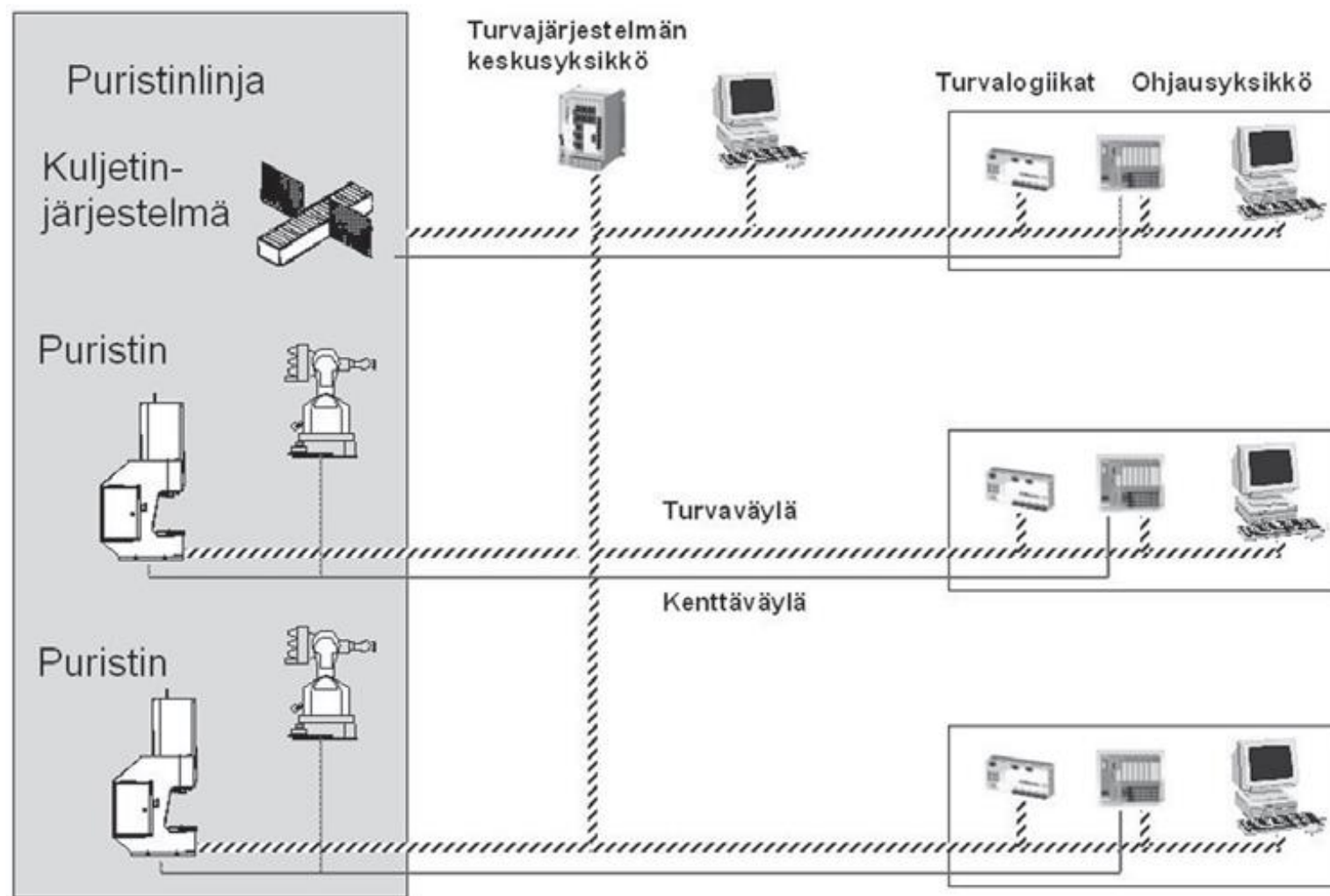
**Prosessiteollisuuden ohjausjärjestelmä (perusjärjestelmä ja turvajärjestelmä)**

# SCADA-käytönvalvontajärjestelmät (infrastruktuuri)



Maantieteellisesti hajautettu SCADA-tyyppinen järjestelmä

# Ohjelmoitavat logiikkajärjestelmät



**Koneiden turvallisuuteen liittyvä ohjausjärjestelmä, jossa on yhdistetty turvaväylä (SafeEthernet) ja tavallinen kenttäväylä sekä työasemia (PC).**

**Puristimien ja kuljetinjärjestelmän turvatoimintoja ohjataan turvaväylällä (paksu viiva), ja muut ohjaukset on toteutettu tavallisella logiikalla. Työasema on yhteydessä turvaväylään, mutta se toimii lähinnä tiedonkeruutehtävissä.**

# Tosiaikajärjestelmät

- Automaatioverkoissa käytettävä verkkoteknologia perustuu alun perin liiketoimintaverkkojen rakentamiseen, joissa välitallennukset olivat tavanomaisia ja hyväksyttäviä
  - tietoturva hoidettiin sovellustasolla, johon se otettiin mukaan jo sovellusten kehityksen varhaisessa vaiheessa
- Koska teollisten tuotantoprosessien ja kappale-tavarateollisuuden automaatiojärjestelmissä vaadittiin tosiaikaista ohjausta, ne suunniteltiin alun perin erillisiksi järjestelmiksi
  - tietoturva hoidettiin erottamalla ne fyysisesti muista verkoista ja toiminnoista, ja tarvittava pääsy järjestettiin hyvin rajoitetusti pääsyn valvonnan avulla
- Tosiaikaiset ohjausjärjestelmät on suunniteltu tavoittelemaan tehokkuutta ja aikakriittistä vastetta (deterministisyys)
  - deterministisessä automaatiojärjestelmässä vasteajat eivät saa häiritä ohjaustapahtumaa, ja siten niillä on pienet vasteajat, jolloin esimerkiksi tietoturvaan liittyvien salausalgoritmien käsittely ei ole aina mahdollista
  - tietoturvatekniset toimenpiteet on monesti suoraan jätetty pois laitteiden suorituskyvyn takaamiseksi
- Perinteiset yritysten toimistotason verkot eivät ole deterministisiä
  - verkot ovat aliverkotettuja ja reititettyjä, jolloin verkkoliikenteen jokaisessa solmussa (kytkin tai reititin) on oma käsittelyviiveensä
  - tämän tyyppisessä verkossa voidaan käyttää salaukseen perustuvia algoritmeja ja tietoturvaa parantavia tekniikoita esimerkiksi pääsyylojen avulla

# Verkkoyhteydet

- Järjestelmät on yleensä suunniteltu toteuttamaan toiminnalliset vaatimukset sekä täyttämään niihin liittyvät luotettavuus-, turvallisuus- ja joustavuusvaatimukset
- Järjestelmät ovat tyypillisesti olleet fyysisesti eristettyjä ja perustuneet niihin soveltuviin laitteisiin sekä tiedonsiirtovälineisiin
- Vertailu eri tietojärjestelmien välillä osoittaa, että järjestelmän korkeimmalla tasolla verkoston arkkitehtuuri on yhtäläistä tuotantolaitoksen kaikkia toimintoja varten
- Täältä tasolta alajärjestelmät jakautuvat paikallisiin verkkoihin
- Järjestelmän osia ovat yleisessä käytössä olevat työasemat, tehtaan tietokannat, sovelluspalvelimet, käyttäjätunnusten hallintajärjestelmät...
- Tietoliikenne tehtaasta ulospäin on tyypillisesti hoidettu palomuurin kautta Internet-verkkoon tai muuhun paikalliseen yleiseen tietoliikenneverkkoon
  - Internet-verkkoon perustuva teknologia on lisännyt teollisuuden tietojärjestelmien haavoittuvuutta
  - Keskitetty ohjaus ja etäkunnossapito on siirtynyt yleisiin puhelin- ja muihin tietoverkkoihin, ja ne ovat sitä kautta uhkana kriittisille infrastruktuureille
  - Hajautetut järjestelmät toimivat kaupallisten laitteistojen ja ohjelmistojen varassa, joita on yhdistetty ulkoisiin tietoverkkoihin, jotka voivat tehdä mahdolliseksi yksinkertaisetkin tunkeutumiset järjestelmiin ja siten vaarantaa yrityksen tuotannon tai jakelujärjestelmien toimintaa

# Uhkakuvat

- Tietomurron tai -hyökkäyksen takana on aina, suoraan tai epäsuorasti, ihminen tai joukko ihmisiä
- Pääosa hyökkäyksistä tapahtuukin yleisen Internet-verkon puolelta, mutta ne voivat yhtä hyvin tapahtua myös yrityksen sisäverkosta käsin
- Taustalla voi olla erilaisia motiiveja, joita perinteisesti ovat olleet ilkivalta, jännityksen ja kuuluisuuden etsiminen, tutkiminen, uteliaisuus, ystäväpiirin painostus, torjuntaohjelmien haastaminen, sosiaalinen arvostuksen etsiminen, turvallisuusaukkojen paljastaminen, ajattelemattomuus, helppous...
- Uhkakuvat koskettavat yhä laajemmin myös teollisuusautomaatiota, koska automaatio on verkottunut osaksi yhteiskunnan järjestelmiä
- Merkittävänä riskinä pidetään toistaiseksi tuntematonta tietoturva-aukkoa, jonka hakkeri voi löytää ja jota hän käyttää hyväkseen

# Toimistojärjestelmien ja teollisuuden automaatiojärjestelmien erot

Automaatiojärjestelmiä voidaan luonnehtia seuraavasti:

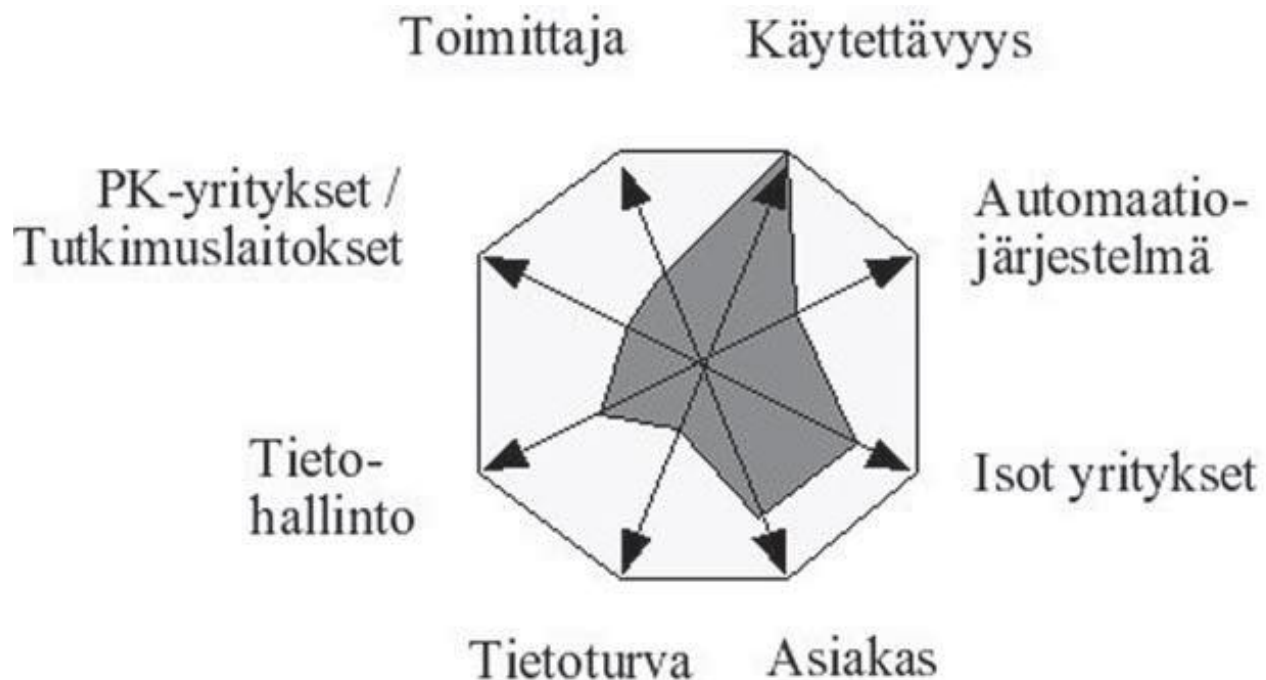
- Automaatiojärjestelmät ovat vakiintuneempia kuin toimistojärjestelmät
- Automaatiojärjestelmissä ei useinkaan ole liiketoimintojen kannalta salassa pidettävää tietoa
- Suoraa yhteyttä Internet-verkkoon ei tavallisesti tarvita
- Automaatiojärjestelmän tietoteknisiä laitteita ei tavallisesti käytetä muihin tarkoituksiin ja useimmiten ne on hajautettu valmistusprosessin mittauksiin sekä ohjauksiin ja turvatoimintoihin
- Pääsyn hallinta on useimmiten tarkasti järjestetty ja henkilöstö on koulutettu näihin tehtäviin
- Automaatiojärjestelmien toimintojen ja henkilöstön valvonta on tiukempaa järjestelmälle asetettavien lisävaatimusten takia, esimerkiksi turvallisuusvaatimukset

# Toimistojärjestelmien ja teollisuuden automaatiojärjestelmien erot

Teollisuusautomaatiolla on muusta tietotekniikasta eroavia erityispiirteitä, kuten:

- Tavoitteet
- Järjestelmän kokoonpano
- Tiedon ja palvelujen saatavuus
- Ei-toivotut seuraukset
- Aikakriittisyys
- Ohjelmistot
- Salaus
- Resurssit
- Tiedon eheys
- Yhteydet
- Ohjelmistojen ja laitteiden päivitykset

# Tietoturva-vaatimusten tasapainotus

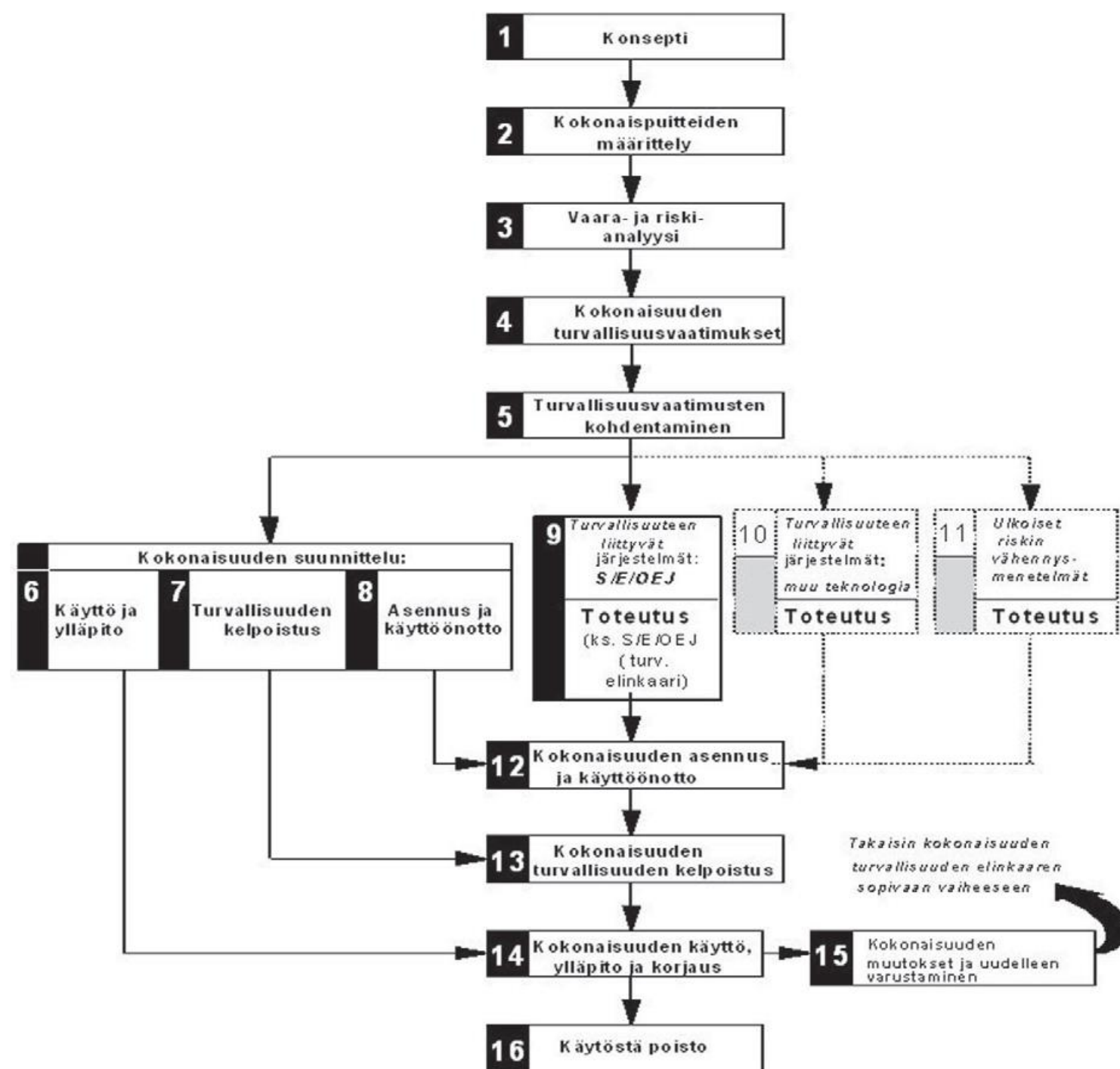


Kuvassa esitetään eri osapuolten ja vaatimusten väliset ristiriidat.

Nuolten päissä on esitetty vastakkain kilpailevat osapuolet ja keskelle muodostuva alue

kuvaava osapuolten tietoturva-vaatimusten tasapainoa. Mitä lähempänä alue on ulkokehää, sitä parempi on kokonaisuus ja mitä lähempänä alue on muodoltaan ulkokehää, sitä tasapainoisempi on kokonaisuuden tietoturva.

# Tietoturvaan ja turvallisuuteen liittyvät säädökset, standardit ja ohjeet



Elinkaarimallin vaiheet (IEC 61508-1)

# Teollisuusautomaation tietoturvaratkaisuja ja -käytäntöjä

Tietoturva voidaan jakaa kahteen alueeseen:

- Ennakoiva tietoturva, jolla pyritään mahdollisimman kattavasti varautumaan ja ehkäisemään ennakoita mahdolliset häiriöt
- Tietoturvahäiriöiden (Security Incidents) hallinta, eli toimintaratkaisut, joilla varmistetaan toiminta häiriötilanteessa sekä korjaavien toimenpiteiden välitön toteutus ja nopea toipuminen

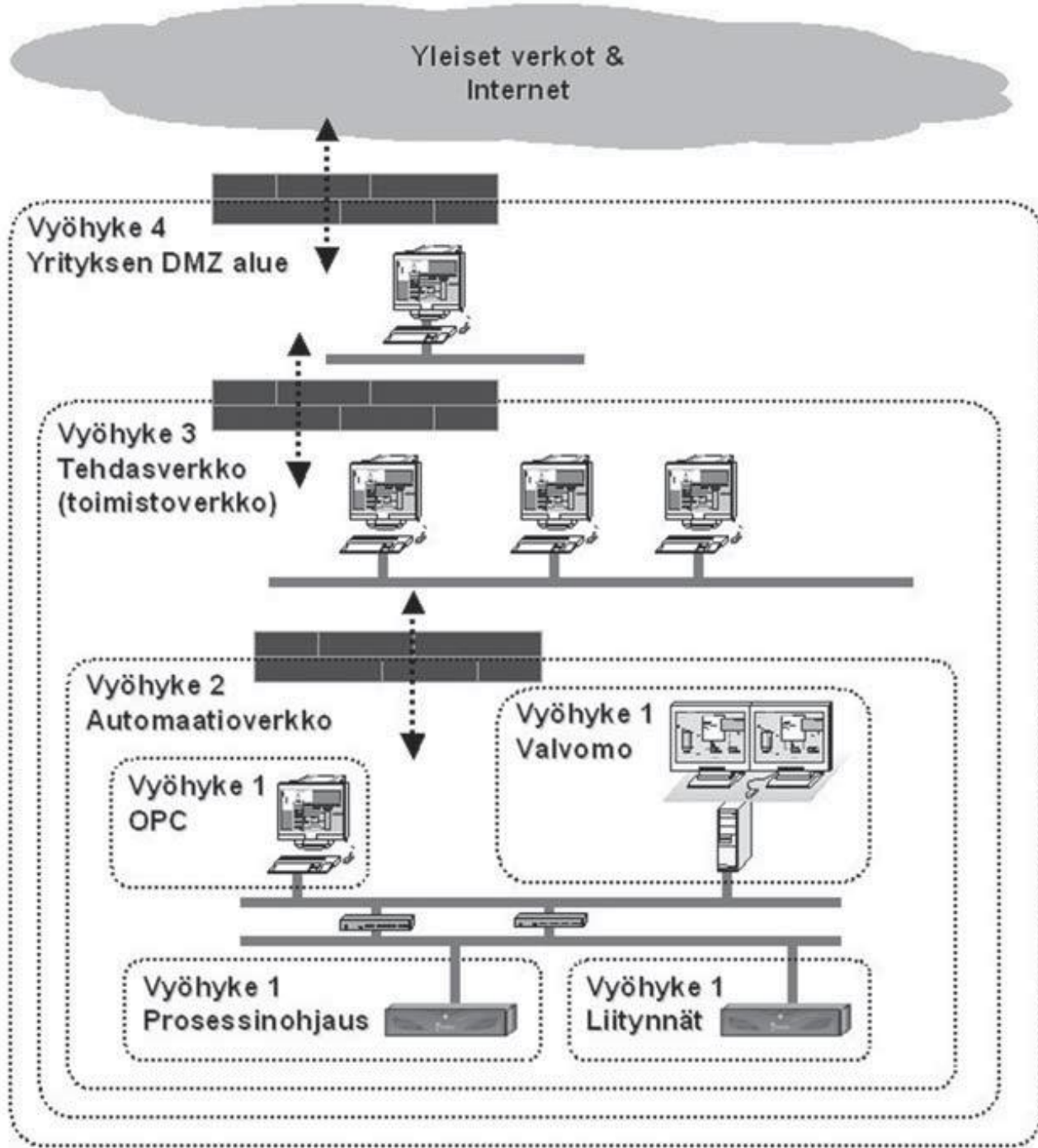
# Vaatimuksia automaatiojärjestelmän tietoturvalle

Yrityksillä on omat tietoturvapolitiikkansa, joiden mukaan toimitaan ja joiden avulla varmistetaan sisäinen tietoturva sekä sen peruseräatteen:

- verkot on erotettu Internetistä palomuurien avulla ja liikenne palomuurin läpi on tarkoin rajattua
- sisäverkossa käytetään virustorjuntaohjelmistoja ja ne pidetään ajan tasalla
- Internet-liikennettä tarkkaillaan, jolloin tyypillisiä toimenpiteitä ovat esimerkiksi selainliikenteen (HTTP) ja sähköpostiliikenteen tarkkailu sekä havaittujen virusten ja roskapostien poistaminen

Järjestelmien korkean käytettävyyden ja riittävän turvallisuuden varmistamiseksi kaikissa olosuhteissa on tietoturva-asiat hoidettava asianmukaisesti. Tämä asettaa erittäin suuret vaatimukset automaatio- ja informaatiojärjestelmille ja erityisesti niiden:

- verkkoarkkitehtuurille
- verkon suunnittelulle (mukaan lukien rajapinnat ja liittynät automaatioverkosta muihin verkkoihin ja sovelluksiin)
- tietoturva-ohjelmistojen käytölle
- tietoturvaparannusten määrittelylle ja toteutukselle
- tietoturvapäivitysten hallintaan



# Syvyyssuuntainen suojaus

# Tekniset menetelmät ja ratkaisut

Yleiset perusperiaatteet, joilla voidaan huomattavasti rajoittaa teollisuusautomaation käytettävyyseriskejä varsinkin kaupallisia komponentteja käytettäessä, ovat muun muassa:

- ratkaisujen vakiointi
- muutosten arviointi ja testaus
- muutosten hallittu toteutus

# Ratkaisujen vakiointi

- Teollisuusautomaation yhteydessä puhuttaessa vakioinnilla tarkoitetaan sekä suunnittelun alussa tehtävien ratkaisujen ja niiden valintaan liittyvää osien vakiointia että valitun ratkaisun säilyttämistä muuttumattomana järjestelmän koko elinkaaren ajan
- Nykyaikainen automaatiojärjestelmä on laaja ja monimutkainen kokonaisuus, johon kuuluu erilaisia laitteita ja ohjelmistoja
  - osana kokonaisuutta käytetään myös komponentteja, joita ei ole alun alkaen suunniteltu käytettäväksi vaativissa teollisissa ympäristöissä
- Jotta kokonaisuuden käytettävyys voitaisiin varmistaa teollisessa ympäristössä, on järjestelmän kokoonpano ympäristöineen pidettävä mahdollisimman muuttumattomana ja tämän kokoonpanon on oltava kattavasti testattu

# Ratkaisujen vakiointi

## KOVENTAMINEN

- Koventamisella (hardening) tarkoitetaan sellaisten perusominaisuuksien, ohjelmistojen, palvelujen ja osuuksien poistoa tai niiden käytön estämistä (sulkemista), joita ei automaatiojärjestelmän toiminnassa välttämättä tarvita
  - se voi myös tarkoittaa jotain muutosta konfiguraatiossa, joka tekee ominaisuuden käytöstä väärin tarkoituksiin hankalaa
- Yleinen koventamisen kohde on itse automaatioverkko
  - yleisinä periaatteina voidaan mainita rajapinnan liikenteen ja pääsyn rajoittaminen sekä automaatioverkon verkkolaitteiden konfigurointi häiriösietoisemmaksi
- Koventaminen on tehtävä aina uudelle järjestelmälle ennen sen käyttöönottoa, ja tämä on normaali toimenpide useimpien automaatiojärjestelmien toimitusvaiheessa
- Koventamisen onnistumiseksi tulisi ottaa huomioon, että:
  - automaatiojärjestelmän koventaminen tulisi tehdä ennen kuin järjestelmä kytketään verkkoon, ja tämä koskee myös sisäverkkoon kytkemistä
  - peruskonfigurointi tulisi tehdä sellaiseksi, että oletuksena käyttäjällä ja laitteella on vain toiminnallisuudelle välttämättömät oikeudet
  - koventaminen ei saa häiritä siinä ajettavien ohjelmistojen toimintaa

# Muutosten arviointi ja testaus sekä muutosten hallittu toteutus

- Koska toimivaan järjestelmään tehtävät toimenpiteet voivat aiheuttaa riskejä, on jokainen toimenpide perusteltava ja hyväksyttävä
  - toimenpiteet, jotka katsotaan välttämättömiksi, on testattava asianmukaisesti ja toimenpiteisiin mahdollisesti sisältyvät riskit on arvioitava
- Aloite tietoturvaparannuksiin ja -toimenpiteisiin tulee yleensä automaatio-osaston ulkopuolelta
  - esimerkkeinä ilmoitus uudesta haavoittuvuudesta käyttöjärjestelmässä, uuden viruksen leviämisestä tai yrityksen uusista IT-vaatimuksista
- Automaatiojärjestelmän toimittajan on seurattava ja arvioitava, mitkä asiat voivat haitata automaatiojärjestelmän toimivuutta, määritellä näihin suositeltavat korjaus- ja parannustoimenpiteet, huolehtia toimenpiteiden testauksesta sekä riittävästä tiedottamisesta asiakaskunnalle
- Teollisuuslaitosten on vastaanotettava ja arvioitava eri tahoilta tulevat suositukset tietoturvan parantamiseen ja uhkien torjumiseen, sekä päätettävä suositusten toimeenpanosta ja toimeenpanojen aikatauluista
  - nykyaikainen automaatiojärjestelmä sisältää monia riippuvuussuhteita ja yhteen osaan tehtävät muutokset voivat vaikuttaa järjestelmän muihin osiin, joten väärin toteutettu toimenpide voi aiheuttaa vakavaa häiriötä koko järjestelmän toimintaan

# Varmennukset ja toipuminen

- Ennakoivan tietoturvan lisäksi on myös varauduttava suunnitelmallisesti tietoturvahäiriöihin ja niiden käsittelyyn
  - tähän on sisällytettävä varmennukset (Backup) ja toipuminen (Recovery)
- Jotta toipuminen tietoturvahäiriöistä olisi mahdollisimman nopeaa, varmennusratkaisujen ja -käytäntöjen on oltava suunniteltuna ja niiden toiminnot testattuna
  - häiriöiden sattuessa ja laitteiden vikaantuessa on ensiarvoisen tärkeää saada automaatiojärjestelmä mahdollisimman nopea palautettua normaaliin tilaan järjestelmän käytettävyyden ja turvallisuuden varmistamiseksi
- Ne osuudet, jotka voidaan varmistaa, on tyypillisesti hoidettu kahdennusratkaisuilla, esimerkiksi kahdennettujen kovalevyjen ja palvelimien käytöllä
- Tietoturvaan liittyvien lokitiedostojen ja –tietojen varmistaminen on tehtävä siten, että tietomurron yhteydessä niihin ei ole suoraa pääsyä

# Automaation tietoliikenneverkot

- Automaatiojärjestelmissä on ryhdytty käyttämään yhä enenevässä määrin yleisiä IP-pohjaisia verkkoteknologioita ja verkkoratkaisujen luotettavuus on täten elintärkeää automaatiojärjestelmien toimivuudelle
  - IP-protokollan käyttö kenttäväylissä tuo mukanaan paitsi sen edut myös sen haittapuolet, joista suurin on laitteen mahdollinen näkyvyys kenttäväylän ulkopuolelle
  - automaatioverkkoratkaisut poikkeavat myös siten normaaleista verkoista, että teollisuusautomaation verkot toteutetaan usein redundanttisesti (eli varmennettuina) ja automaatioverkolta edellytetään riittävän nopeaa vasteaikaa (mahdollisimman nopea, reilusti alle 1 sekunti)
- Yleisiin verkkolaitteisiin ja -tekniikoihin perustuvat ratkaisut ovat asianmukaisesti toteutettuina suhteellisen luotettavia ja hinnaltaan kilpailukykyisiä
  - kaksi tärkeintä automaatioverkkojen suunnittelun ja toteutuksen peruseriaatetta ovat segmentointi (verkkojen erotus) ja liikenteen rajoitus

# Langattomat verkot

- Langattomat verkot, kuten WLAN (Wireless Local Area Network), ovat tehnyt hitaasti tuloaan automaatioverkkojen puolelle
  - suuntaus näyttää olevan, että varsinainen automaatioverkko toteutetaan langallisesti, ja langattomalla verkolla hoidetaan vain joitakin rajattuja toimintoja (kuten esimerkiksi ylläpitoon liittyviä tehtäviä)
- WPA (Wi-Fi Protected Access) –standardi tai uudempi WPA2-standardi on välivaiheen tietoturvateknologia
  - tällä hetkellä odotetaan WPA3-standardia, jota on lähdetty kehittämään WPA2-salauksen ongelmien paljastuttua
- Tietoturvallisin ratkaisu voidaan rakentaa käyttämällä tunnistuspalvelinta, mutta sen käyttöä rajoittaa monesti korkea hinta
- Langattomia yhteyksiä suunniteltaessa on otettava huomioon, että tukiasemien ja mediamuuntimien avulla tehtävä langattomuus sisältää yleensä tarpeelliset työkalut tietoturvallisen langattoman yhteyden muodostamiseksi
  - ongelmallisia kohteita ovatkin lähinnä sulautetut tai vastaavat laitteet, joissa on suora langaton yhteys
  - niissä ei yleensä ole resursseja vahvaan salaukseen tai VPN-yhteyksien muodostamiseen

# Langattomat verkot

## ANTURIVERKOT

- Anturiverkkojen leviäminen lisää kiinnostusta soveltaa niitä myös säätöön
  - säätösovellukset ovat kuitenkin aikakriittisiä ja vaativat myös palvelunlaatuongelmien (Quality of Service, QoS) ratkaisemisen

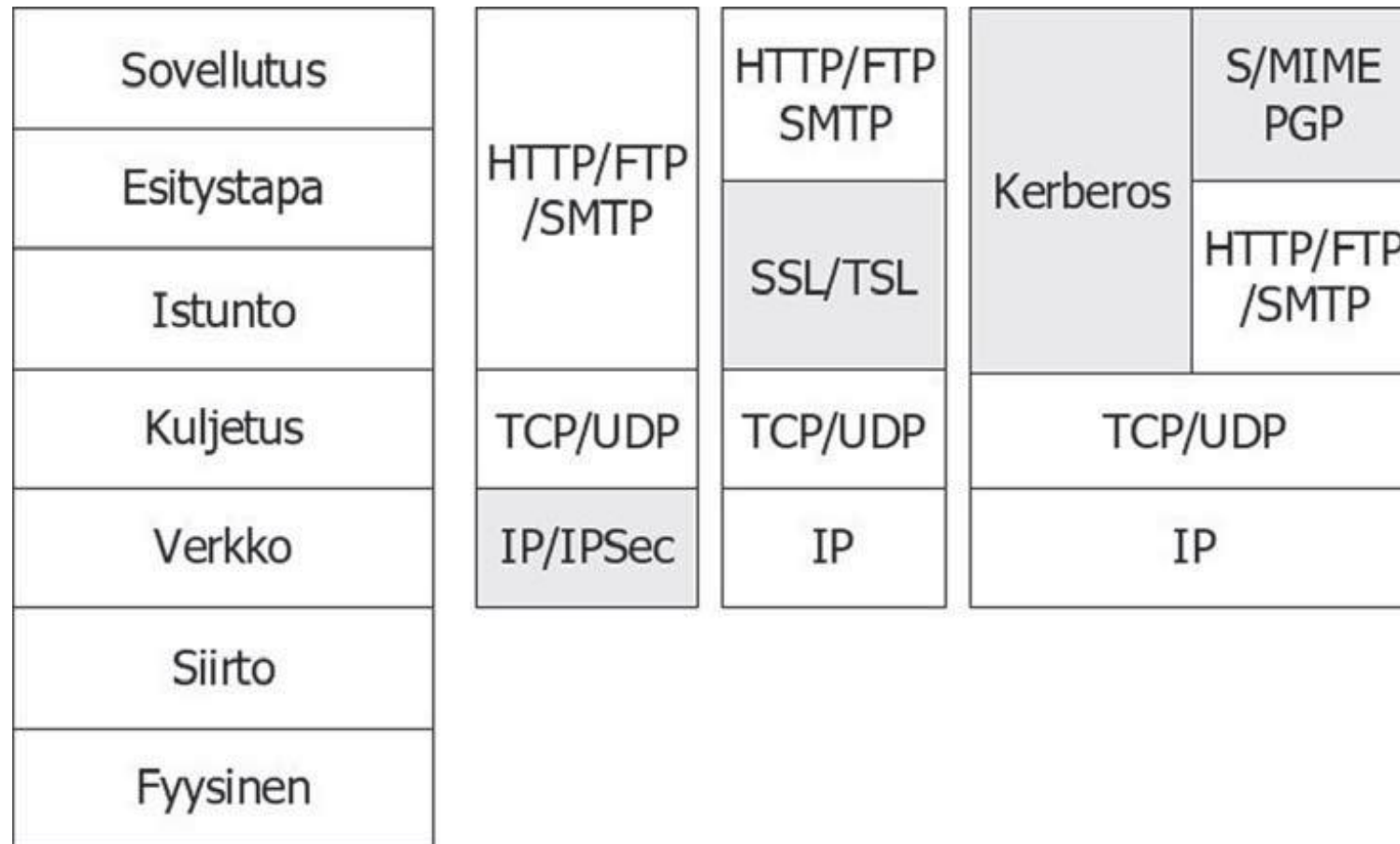
## MOBIILIVERKOT

- Teollisuusautomaatiossa mobiiliverkkoja käytetään rajoitetusti
  - yleisimpiä käyttökohteita ovat hälytysten välittäminen puhelimiin sekä tuotanto- ja diagnostiikkatietojen siirtäminen
- Asioita joihin tietoturvaohaukat liittyvät ovat muun muassa:
  - toimijoiden ja käyttäjien tietoturvatoininnan eritasoisuus
  - toimijoiden (henkilöiden) osaamistasojen erot ja alan nopea muuttuminen
  - palveluun tai laitteeseen kohdistuvat hyökkäykset ja virheet, palvelunesto, monimutkaisuus ja väärät asetukset
  - käyttäjän ja palvelun tunnistus ja tietojen luottamuksellisuus
  - palvelusisältöjen ja ohjelmien käyttöoikeudet ja laiton kopiointi
  - uudenlaiset käyttötavat ja teknologia
  - palvelujen luvaton käyttö
  - haittaohjelmat, kuten virukset ja madot
  - mobiili sähköinen maksaminen

## RFID-TEKNOLOGIA

- RFID-tekniikka (Radio Frequency Identifier) perustuu langattomaan tunnistamiseen, jossa lukulaitteella luetaan mikrosirujen sisältämät tiedot
- RFID-tekniikkaa käytetään muun muassa kulunvalvontajärjestelmissä, autojen lukitusjärjestelmissä ja tavaroiden merkitsemisessä
- RFID-tekniikka mahdollistaa uusia sovellusalueita, mutta samalla se myös tuo uusia riskejä, kuten esimerkiksi yksilöllisen ja henkilökohtaisen RFID-tunnisteiden käytön mukanaan tuomat yksityisyyden suojaan liittyvät ongelmat

# Etäyhteydet ja tietoliikenteen salaaminen



OSI-malli sekä salauksen toteuttamismahdollisuuksia eri kerroksilla (harmaa). Kuvaa tulkittaessa on huomattavaa, että OSI-mallin eri kerrokset ja TCP/IP-protokollaperheen kerrokset eivät ole suoraan vertailtavissa

# Käytönhallinta

- Tietoturvan keskeisenä tarkoituksena on varmistaa automaatiojärjestelmän oikea ja turvallinen toiminta sekä suojata järjestelmässä olevat tiedot
  - tietoturvan toteutuksen eräs keskeinen tavoite on estää valtuuttamaton pääsy laitteisiin ja palveluihin sekä seurata kaikkea pääsyä, eli sekä valtuutettuja että valtuuttamattomia pääsyjä ja pääsyn yrityksiä
    - tämä vaatii asianmukaisen käyttäjien tunnistuksen ja toimivan käytönhallinnan
- Käyttäjien tietoturva käsittää tunnistuksen (authentication), valtuutuksen (authorisation) sekä seurannan (accounting)
- Liikenteen tietoturva voidaan hoitaa palomureilla, salauksilla sekä aktiivisella valvonnalla
- Ongelmana on palvelujen (ohjelmistojen) ja laitteiden hallinta, joka voi vaatia tietoturvan hallitun poiskytkennän
- Käytönhallinnan peruskäsitteet ovat:
  1. Tunnistus (authentication) tarkoittaa sisään kirjautuvan henkilön tai järjestelmään kytkeytyvän laitteen luotettavaa tunnistusta. Normaalisti tämä tapahtuu esimerkiksi käyttäjätunnuksen ja salasanan avulla. Myös vahvempaa tunnistusta voidaan tarvittaessa käyttää, esimerkiksi SecurID-kortti henkilöillä ja varmenteisiin pohjautuvat menetelmät laitteilla. Tunnistuksen luotettavuutta parannetaan ja väärinkäyttö estetään kun:
    - ohjelmistojen ja laitteiden oletussalasanat ei käytetä
    - tyhjiä salasanoja ei käytetä
    - käyttäjien oikeudet pidetään mahdollisimman rajoitettuina
  2. Valtuutus (authorisation) tarkoittaa henkilön tai laitteen pääsyä tarpeen mukaan vain sallittuihin palveluihin ja osoitteisiin.
  3. Seurannan (accounting) tärkein funktio on jäljittävyyden varmistaminen. Ongelmatapauksissa voidaan selvittää, kuka tai mikä ja millä oikeuksilla on käyttänyt palvelua.

# Tietoturvapäivitysten hallinta

- Yksi tämän päivän ongelmista on haavoittuvuuksien hyödyntäminen yhä nopeammin, mikä jättää vähemmän aikaa tietoturvapäivitysten testaamiseen ja asentamiseen
  - myös tästä syystä toimintaprosessien on oltava oikein suunniteltuja ja toimivia!
- Tietoturvapäivityksiä tulee jatkuvasti ja automaatioverkon ylläpitoon liittyvät päivitykset pitäisi havaita, testata ja asentaa mahdollisimman nopeasti
  - jos haavoittuvuuksilla on vaikutusta järjestelmään, testataan korjaavat tietoturvapäivitykset mahdollisimman nopeasti ja kattavasti
    - päivitykset on asennettava kaikkiin tarvittaviin laitteisiin, koska pahimmassa tapauksessa yksi saastunut laite saattaa merkittävästi häiritä ympäristöään
- Koska uhkien vakavuuteen vaikuttavat myös itse teollisuuslaitosten omat tietoturvaratkaisut ja -toimenpiteet, on laitosten pidettävä huolta siitä, että haavoittuvuudet otetaan huomioon ja vaadittavat päätökset tehdään automaatiotoimittajien tiedotusten perusteella mahdollisimman nopeasti
  - tietoturvapäivitysten osalta on tärkeää itse tietoturvaprosessin hyvä ja jatkuva toiminta
- Muun muassa seuraavilla keinoilla voidaan ohjelmistojen päivitykset tehdä turvallisemmaksi:
  - valvotaan tarkasti tuotantoprosessin tilaa ja ohjausten järkevyyttä sekä sitä, miten paljon ohjelmat kuormittavat laskenta-, muisti- ja tietoliikennesresursseja, jotta mahdolliset ohjelman virhetoiminnot havaitaan nopeasti
  - käytetään hyväksi redundanssia ja yksinkertaisia varajärjestelmiä
  - käytetään hyväksi varmuuskopiointia, jotta voidaan tarvittaessa palata nopeasti päivitystä edeltäneeseen versioon
  - arvioidaan onko olemassa käyttökelpoisia vaihtoehtoja tietoturvan parantamiseksi, jos päivitystä ei jostain syystä voida asentaa
- Päivitysten asennusten jälkeen on varmistettava normaalin toiminnan lisäksi myös se, että muu ympäristö on pysynyt muuttumattomana

# Turvallinen tuotekehitys

- Tavoitteena on tehdä laadukkaita ja turvallisia tuotteita. Tuotteen arkkitehtuurissa ja suunnittelussa turvallisuutta lisäävät hyväksi todetut suunnitteluperiaatteet, kuten:
  - hyökkäyspinta-alan minimointi,
  - turvalliset oletusarvot,
  - ulkopuolisten syötteiden tarkistus,
  - oikeuksien minimointi,
  - syvyysuuntainen puolustus,
  - turvalliset virhetilat,
  - epäluottamus ulkopuolisiin palveluihin, ja
  - turvamekanismien yksityiskohtien salailuun pohjautuvien oletusten välttäminen.
- Tietoturva on tietoturvaominaisuuksia mutta myös ohjelmiston laatutekijä
- On tärkeää kiinnittää huomio myös salausta laajemmin tuotteen eri toimintoihin
- Ominaisuuksien lisäksi tietoturvallinen tuotekehitys kattaa myös kehityksen ja ylläpidon aikaiset toimet, kuten:
  - tilaturvallisuuden,
  - käytettyjen järjestelmien turvallisuuden sekä
  - tuotekehityshenkilöstön koulutuksen.

# Turvallinen tuotekehitys

- Uhkamallinnus on tuotteen suunnittelu- ja päivitysvaiheiden tärkeimpiä työkaluja
- Uhkamallissa kuvataan:
  - tuotteen käyttötapaukset,
  - ympäristö uhkien näkökulmasta,
  - järjestelmän tuottamat arvokkaat tiedot ja palvelut, ja
  - kuinka tuote vastaa näihin kohdistuviin uhkiin.
- Tärkeintä on, että uhkamalliin liittyvät asiat käydään läpi osana tuotekehitystä, eikä se millä menetelmällä uhka-arvio tehdään
  - uhkamalli tukee myös tarkastustoimien tehokasta rajaamista ja kohdistamista
- Dokumentoidut ja omaksutut suunnitteluperiaatteet helpottavat, sekä turvallista toteutusta, että toteutuksen turvallisuuden arviointia

# Turvallinen tuotekehitys

- Tuotteen toteutusvaiheessa on tärkeää varmistaa:
  - turvallista tuotekehitystä tukevat työkaluvalinnat,
  - toteuttajien tietoturvaosaaminen sekä
  - valittujen kolmansien osapuolten komponenttien ja alustaratkaisujen turvallisuus.
- Monet tietoturvaongelmat syntyvät ohjelmointivaiheessa
  - turvalliset tekniikat sekä niiden puutteet riippuvat:
    - käytetyistä alustoista,
    - komponenteista,
    - ohjelmointikielistä ja
    - työkaluista.
- Tietoturvaan kuuluu myös kattava testaus, jota pitää suorittaa todellista käyttötilannetta vastaavassa ympäristössä ennen kuin tuote tulee hyväksyntään
- Testauksessa ja laadunvarmennuksessa tulee pyrkiä kohti toistettavia ja automaattisia menetelmiä, joilla saavutetaan suurempi testikattavuus, ja järjestelmään tehtäviä muutoksia pysytään näin testaamaan tehokkaasti ja luotettavasti
  - tuotteen ja sen osakokonaisuuksien helppo testattavuus nopeuttaa myös sen hyväksyntää
- Katselmoinnit ovat tärkeä osa laadunvarmennusta, ja tuote pitää katselmoida myös tietoturvaperspektiivistä

# Tilat ja henkilöstö

- Jos tilat, joissa lähdekoodia, koonti-tuotteita, työkaluja tai työkoneita säilytetään, eivät ole turvallisia, voi hyökkääjä vaarantaa niissä valmistettavien tuotteiden turvallisuuden
  - lähdekoodiin voi esimerkiksi lisätä takaportin
- Turvallisuutta ajateltaessa on ajateltava kaikkia järjestelmän osia, myös henkilöstöä ja tiloja
- Kehityksessä käytettävien työkalujen on vastattava kehitettävien tuotteiden turvallisuusvaatimuksia
  - esimerkiksi versionhallinta, jossa kirjataan kaikki muokkaukset ja niiden tekijät, on välttämätöntä
  - palvelimiin on aina tehtävä viimeisimmät turvallisuuspäivitykset, ja
  - kaikilla käyttäjillä on oltava oma tili lokitietojen tallennusta varten
- Ihmisten pitää tuntea tietoturvahygienian yleiset periaatteet, kuten:
  - älä avaa jokaista sähköpostiviestiä,
  - ole varovainen selaillessasi ja
  - vältä vapaa-ajan selailua työkoneella,
  - älä käytä sattumalta löytämiäsi USB-muistitikkuja koneellasi,
  - pidä järjestelmäsi ajan tasalla ja
  - ole tietoinen käyttäjien manipuloinnin peruspiirteistä.

# Tilat ja henkilöstö

- Kehittäjille on annettava lisäkoulutusta:
  - turvallisesta suunnittelusta,
  - uhkamallinnuksesta ja
  - turvallisesta ohjelmoinnista.
- Kehitysmateriaalia sisältäviin kannettaviin tietokoneisiin on asennettava viimeisimmät turvallisuuspäivitykset ja ne on varustettava levyn salauksella
- Tilojen ja henkilöstön lisäksi on huomioitava myös organisaatiossa käytössä olevat prosessit
  - Lainaus OWASP-järjestön sivustolta ([https://wiki.owasp.org/index.php/Policy\\_Frameworks](https://wiki.owasp.org/index.php/Policy_Frameworks)): "... Turvallisia sovelluksia koskevat seuraavat vähimmäisvaatimukset:
    - turvallisuutta vaaliva organisaation johto
    - riittävät turvallisuustarkistukset ja -toiminnot sisältävät kehittämismenetelmät
    - kansallisiin standardeihin perustuva kirjallinen tietoturvakäytäntö
    - turvalliset julkaisun- ja konfiguraationhallinnan prosessit."
  - OWASP-järjestö toteaa myös seuraavaa: "Tuotekohtaisella kehittämisellä ei saada aikaan turvallisia sovelluksia, sillä se ei ole riittävän järjestelmällistä. Turvallisen koodin luontiin pyrkivien organisaatioiden onkin johdonmukaisesti käytettävä menetelmiä, jotka tukevat kyseistä tavoitetta. On tehtävä huolellisia valintoja – pienten tiimien ei kannata koskaan käyttää raskaita, monia eri rooleja sisältäviä menetelmiä, ja suurten tiimien on valittava menetelmiä, jotka voidaan skaalata niiden tarpeisiin sopiviksi."

# Vaatimukset ja uhkamallinnus

OWASP on julkaissut listan kymmenestä tärkeimmästä verkkosovelluksia koskevasta turvallisuusriskistä:

1. **Injektio:** Sovellus hyväksyy ulkoiset syötteet, mutta ei tarkista niitä kunnolla. Tällöin hyökkääjä voi suorittaa komentoja tai tehdä muuta vahinkoa haavoittuvassa sovelluksessa.
2. **Rikkinäinen todennus:** Käyttäjien todennusta ei ole toteutettu oikein. Salasanoja ei varmenneta, salasanat vuotavat tai järjestelmään voi hyökätä salasanan palautuksen avulla. Todennuksen jälkeen tapahtuva istunnonhallinta voi myös olla rikkinäinen niin, että istuntoja voidaan kaapata.
3. **Arkaluonteisten tietojen paljastuminen:** Arkaluonteisia tietoja säilytetään tai siirretään selkokielistä tai käyttäen heikkoa salausta.
4. **Ulkoiset XML-entiteetit (XXE) (XML external entities (XXE)):** Sovelluksen XML-käsittely ei ole turvallista; esimerkiksi SAML-kertakirjautuminen on toteutettu väärin.
5. **Rikkinäinen käytönvalvonta:** Sovellus sallii käyttäjien suorittaa toimia, joihin heillä ei ole käyttöoikeuksia.

# Vaatimukset ja uhkamallinnus

OWASP on julkaissut listan kymmenestä tärkeimmästä verkkosovelluksia koskevasta turvallisuusriskistä:

- 6. Vääränlaiset turvallisuusasetukset:** Järjestelmän turvallisuutta ei ole kovennettu tai siinä on tarpeettomia palveluja käynnissä, tai alusta on vanha ja haavoittuva ja sisältää turvattomia paikallisia tilejä.
- 7. XSS-haavoittuvuus:** Hyökkääjät voivat suorittaa haitallista HTML- tai JavaScript-koodia.
- 8. Turvaton sarjallistettujen tietojen lukeminen (insecure deserialisation):** Hyökkääjät pääsevät käsiksi sarjallistettuihin tietoihin tai olioihin, jotka sovellus lukee ja käyttää sitten toimiin, joihin vaaditaan valtuudet.
- 9. Tunnettuja haavoittuvuuksia sisältävien komponenttien käyttäminen:** Sovelluksessa käytetään tahallisesti tai tahattomasti komponentteja, joiden tiedetään sisältävän haavoittuvuuksia.
- 10. Riittämätön lokiin kirjaus ja seuranta:** Sovelluksen lokit eivät ole riittävän turvallisia myöhempää tarkistamista varten, tai sovellus ei seuraa mahdollisia hyökkäyksiä tai varoita niistä.

# Uhkamallinnus

## UHKAMALLINNUS

- Uhkamallinnuksella tarkoitetaan järjestelmän turvallisuuden arviointia
- ”Uhkamallinnukseen on monia erilaisia lähestymistapoja... Paljon tärkeämpi kuin tietty riskien arviointiin käytettävä menetelmä on järjestelmällisen uhkamallinnuksen toteuttaminen käytännössä. Microsoft on todennut, että tärkeintä sen turvallisuuden parannusohjelmassa oli se, että uhkamallinnus otettiin käyttöön koko yrityksessä.” – Threat Risk Modeling – OWASP

- Väliä ei siis ole sillä, miten uhkamallinnus toteutetaan, vaan sillä, että se toteutetaan
  - on ajateltava hyökkääjän tavoin ja sisällytettävä turvallisuusvaatimukset toimintasuunnitelmaan

## SISÄÄNRAKENNETTU TURVALLISUUS / TURVALLISUUS LIITÄNNÄISENÄ

- Sisäänrakennetulla turvallisuudella viitataan yleensä siihen, että turvallisuusvaatimukset huomioidaan kehitysprojektin alusta alkaen, jolloin tuloksena on tuote, jossa turvallisuus on kiinteä ominaisuus
  - sisäänrakennettu turvallisuus on parempi vaihtoehto
- Toinen vaihtoehto on turvallisuus liitännäisenä, jolloin turvallisuuteen kiinnitetään huomiota vasta tuotteen toteutuksen jälkeen ja sen turvallisuus saadaan aikaan lisäämällä uusia suojauskomponentteja ja -ominaisuuksia
  - on aina vaikeaa varmistaa laatua uusia komponentteja lisäämällä

# Suunnittelu

- On toivottavaa, että kehittämisessä sovelletaan toistuvia syklejä ja että vaatimuksiin ja suunnitteluvaiheisiin palataan useita kertoja
- Suunnittelussa määritetään järjestelmän arkkitehtuuri, jota tarvitaan vaatimuksissa määritetyn, suunnittelun toiminnallisuuden aikaansaamiseen

## TURVALLISEN SUUNNITTELUN PERIAATTEET

- Seuraavat säännöt on laadittu OWASPin turvallisen suunnittelun periaatteiden (Security by Design Principles) pohjalta:
  1. Hyökkäyspinnan minimoiminen: Hyökkäyspinnat ovat niitä järjestelmän osia, jotka ovat kosketuksissa ulkomaailmaan joko fyysisesti tai verkon tai tiedostojen välityksellä. Hyökkäyspinta-alaa voi minimoida poistamalla rajapintoja, jotka eivät ole välttämättömiä

# Suunnittelu

2. Turvalliset oletusasetukset: Asiakkaiden ei tarvitse olla tietoturvan asiantuntijoita, jotta he voivat käyttää järjestelmää turvallisesti.
3. Syöteenkäsittely (ei sisälly OWASP periaatteisiin): Jos syötteitä ei tarkasteta, hyökkääjä saattaa pystyä vioittamaan järjestelmän haavoittuvia osia tai kaatamaan ne. Järjestelmään ulkopuolelta tulevat syötteet on tarkastettava aina, kun mahdollista. On otettava huomioon myös rajapinnat, joihin syötteet vaikuttavat epäsuorasti. Kehitystiimin on lähdettävä siitä oletuksesta, että komponentteihin voi tulla haitallisia syötteitä, olipa niiden sijainti mikä tahansa.

# Suunnittelu

4. Erilliset tehtävät: Klassinen esimerkki on tarkastuslokien käsittelyn siirtäminen eri järjestelmään lokit tuottavasta järjestelmästä, jolloin niiden turvallisuutta ei voi vaarantaa samanaikaisesti. Kun tehtävät jaetaan eri komponenteille, voidaan myös komponentteihin liittyviä resursseja ja valtuuksia määrittää ja eriyttää tarkemmin.
5. Mahdollisimman suppeat valtuudet: Kun tehtävät on jaettu eri komponenttien kesken, kyseisiin prosesseihin ja alijärjestelmiin on määritettävä mahdollisimman suppeat käyttöoikeudet. Jokaisen komponentin pitäisi suoriutua tehtävästään mahdollisimman rajallisilla käyttöoikeuksilla. Kun valtuudet määritetään mahdollisimman suppeiksi oikealla tavalla, järjestelmään kohdistuvat hyökkäykset ja hyökkääjän pääsy järjestelmän eri osiin pystytään rajaamaan tehokkaammin.
6. Syväsuojaus: Syväsuojaus tarkoittaa sitä, että järjestelmään suunnitellaan useita suojaustasoja. Syväsuojaus parantaa järjestelmän turvallisuutta, sillä yhden tason vaarantuminen ei vaaranna koko järjestelmää. Syväsuojauksesta puhuttaessa käytetään myös ilmaisua monitasoinen turvallisuus.
7. Turvallisuus vikatilanteissa: Järjestelmä on suunniteltava siten, etteivät häiriöt ja viat vaaranna järjestelmän turvallisuutta. Valittavissa on: "avautuminen" (fail-open) ja "sulkeutuminen" (fail-closed) vikatilanteessa. Eli, pitäisikö järjestelmän sallia vai kieltää käyttö vikatilanteessa? Olennaisinta on, että komponentin vikaantumisen seurauksiin kiinnitetään huomiota.

# Suunnittelu

8. Ei liikaa luottoa ulkoisiin palveluihin: Ulkoisia palveluja on kohdeltava ulkopuolisina toimijoina, niistä tulevat tiedot on aina tarkastettava ja turvallisuuden on säilyttävä vikatilanteessa, jossa palvelu ei ole käytettävissä.
9. Salassapitoon perustuvan turvallisuuden välttäminen: Salassapitoon tai piilotteluun perustuva turvallisuus (security by obscurity) tarkoittaa sitä, että tuotteen turvallisuuden perustana on se, että sen rakenne tai toteutustapa pysyvät salassa. Järjestelmässä ei kuitenkaan pitäisi olla suurta määrää salaisuuksia, jotta se voi täyttää tehtävänsä. Vaikka järjestelmän rakenteen tai lähdekoodin salassapidolla voidaan lisätä järjestelmään yksi suojaustaso, se ei yksinään riitä varmistamaan järjestelmän turvallisuutta.
10. Yksinkertainen järjestelmä: Kun koodia on vähemmän, myös virheitä on vähemmän. Ja mitä enemmän on määritettäviä asetuksia, sitä enemmän on myös niissä tapahtuvia virheitä. Yksinkertaisen järjestelmän arvioiminen ja sen turvallisuuden varmistaminen on helpompaa kuin monimutkaisen järjestelmän.
11. Turvallisuusongelmien korjaaminen oikein: Kun omassa järjestelmässä havaitaan haavoittuvuus, se pitää korjata tai siihen pitää puuttua. Toimivista kehitys- ja testausprosesseista on tällöin hyötyä. On tärkeää, että käytetyt prosessit ja koulutus ovat toimivia ja riittäviä, jotta paikalla oleva henkilöstö pystyy huolehtimaan virheiden korjaamisesta heti, kun se on tarpeen.

# Turvallinen ohjelmointi

- Koodin on oltava hyvin dokumentoitua, modulaarista, luettavaa, testattavaa ja testattua
  - ajan kuluessa koodia on kyettävä ylläpitämään ja korjaamaan sen turvallisuutta vaarantamatta
- Staattisista analysointityökaluista on paljon apua, ja niistä on saatavilla sekä ilmaisia että kaupallisia versioita useimmille ohjelmointikielille
  - työkalujen huono puoli on, että monet niistä varoittavat usein aiheettomasti virheistä
  - tuotekehityksessä on varattava aikaa ja vaivaa staattisen koodianalyysin tekemiseen kun koodikanta on suuri, eikä sitä ole analysoitu aiemmin

## SALAUUS

- Tuotteessa kannattaa hyödyntää hyvin tunnettuja ja korkealaatuisia salauskirjastoja ja noudattaa standardeja sekä parhaita käytäntöjä
- Salaustoimintojen käytössä tapahtuu helposti virheitä ja on suositeltavaa hyödyntää hyvin tunnettuja tekniikoita, sekä selvittää, miten niitä käytetään oikein

# Turvallinen ohjelmointi

## RIIPPUVUUKSIEN HALLINTA

- Ilmaisia avoimen lähdekoodin komponentteja on saatavilla kaikille tärkeimmille alustoille ja ohjelmointikielille
  - salaustoiminnot, erimuotoisten tietojen jäsenys ja järjestelmien välinen integrointi onnistuvat yleensä parhaiten komponentteja liittämällä
- Sille, miten komponentit hyväksytään käyttöön, pitäisi olla olemassa käytäntö tai sovittu prosessi
  - kyseisiä päätöksiä ei tule jättää yksittäisten kehittäjien tehtäväksi
  - jokainen komponentti voi tuoda mukanaan uusia haavoittuvuuksia
  - lisäksi on oltava tietoa käytössä olevien kolmansien osapuolten komponenttien lisensseistä

## KOODIKATSELMUKSET

- Koodikatselmusten avulla voidaan varmistaa, että turvallista ohjelmointia koskevaa ohjeistusta on noudatettu
- Kun huolehditaan myös muista laatuun määrittävistä tekijöistä ei päivitysten toimittaminen ei ole niin työlästä

## JATKUVA INTEGROINTI

- Jatkuva integrointi tarkoittaa, että ohjelmistosta tehdään uusia koontiversioita säännöllisesti
- Jatkuvaa integrointia noudattavan ympäristön luominen on investointi, jota kannattaa harkita

# Testaus ja todentaminen

- Testauksen avulla tarkistetaan, että toteutettu järjestelmä vastaa määritettyjä vaatimuksia
  - Järjestelmän turvallisuusominaisuudet sekä muut tärkeät ominaisuudet on testattava
- **Yksikkötestauksella** tarkoitetaan automatisoituja, kehittäjän suorittamia testejä, joiden kohteena on yksittäiseen komponenttiin sisältyvä koodin osa
- **Komponenttitestauksessa** komponentti suoritetaan eristyksissä ja mahdollisesti niin, että muut simuloitut komponentit edustavat järjestelmää kokonaisuudessaan
- **Järjestelmätestauksessa** testataan koko järjestelmän koontiversio käyttämällä sitä
- **Hyväksymistestauksen** suorittaa riippumaton testaustiimi, asiakas tai kolmas osapuoli
- **Staattinen testaus** suoritetaan itse tuotetta käyttämättä ja tarkastamalla eri komponentteja, kuten lähdekoodia ja binääritiedostoja
  - koodikatselmuksia ja -tarkastuksia voidaan pitää staattisina testeinä
  - automatisoitu lähdekoodianalyysi on staattista testausta
  - verrattain uusi menetelmä on ohjelmistokoostumusanalyysi (software composition analysis), jossa tarkastelun kohteeksi otetaan käännetty binääritiedosto sekä sen kokoamiseen käytetyt komponentit
- **Dynaamisessa testauksessa** tuotetta testataan sitä käyttämällä ja tarkastetaan sen toiminta
  - Fuzz-testaus on turvallisuusnäkökulmaa painottava dynaaminen testausmenetelmä
  - nykyään tuote on testattava myös turvallisuusvaatimusten osalta, ja dynaamisiin testeihin pitäisi sisällyttää tuotteeseen kohdistuvat hyökkäys- ja väärinkäyttöyritykset
  - Kuormitustestaus on dynaamista testausta, jossa keskitytään tuotteen suorituskykyyn

# Testaus ja todentaminen

## FUZZ-TESTAUS

- Fuzz-testaus on turvallisuusnäkökulmaa painottava testausmenetelmä, jossa virheitä etsitään altistamalla tuote odottamattomille ja virheellisille syönteille

## PENETRAATIOTESTAUS

- Penetraatiotestaus on tehtävään nimettyjen turvallisuusasiantuntijoiden suorittamaa turvallisuustestausta, jossa he pyrkivät tunkeutumaan palveluun tai järjestelmään ja havaitsemaan siihen sisältyviä turvallisuusongelmia

## STRESSITESTAUS

- Hyökkääjä voi pyrkiä löytämään tuotteesta haavoittuvuuksia kohdistamalla siihen poikkeuksellista kuormitusta tai poikkeustilanteen
- Usein tällaista on mahdoton estää, joten esimerkiksi seuraaviin kysymyksiin kannattaa miettiä vastauksia:
  - Mitä tapahtuu laitteen käynnistyessä? Onko käynnistyksen aikana hyökkäysvektoreita, joita ei tunneta, tai hyväksyykö laite laiteohjelmistopäivityksen keneltä tahansa käyttäjältä käynnistyksen aikana?
  - Mitä tapahtuu, kun verkkoyhteys katkeaa? Kaatuuko järjestelmä, tai meneekö se turvattomaan tilaan?
  - Mitä tapahtuu, jos tulee sähkökatko ja laite käynnistyy uudelleen sen päätyttyä?

# Testaus ja todentaminen

## TAKAISINMALLINNUS

- Tuotteen turvallisuuden ei pitäisi perustua ohjelman tai sen algoritmien salassapitoon (security by obscurity)
  - yksi hyvä syy siihen on se, että ohjelmatiedostojen, laiteohjelmistojen ja verkkoliikenteen takaisinmallintamiseen on olemassa monia työkaluja
- Ei ole realistista olettaa, että järjestelmän suunnittelun yksityiskohdat pysyvät salassa
- Takaisinmallinnukseen voi tutustua tarkemmin takaisinmallintamalla omia tuotteita ja esimerkiksi seuraavista työkaluista voi tähän olla hyötyä:
  - Wireshark verkkoliikenteen nuuskimiseen ja analysoimiseen
  - Nmap isäntäkoneiden, avointen porttien ja palvelujen etsintään verkosta
  - Strings merkkijonojen tulostukseen mistä tahansa tiedostosta (esim. ohjelmatiedostot ja laiteohjelmistot)

# Tietoturva vaatimusten standardointi

	<b>Sähköala</b>	<b>Yleinen standardointi</b>	<b>Teleala</b>
<b>Maailmanlaajuinen taso</b>	<b>IEC</b> International Electrotechnical Commission	<b>ISO</b> International Organization for Standardization	<b>ITU</b> International Telecommunication Union
<b>Eurooppalainen taso</b>	<b>CENELEC</b> European Committee for Electrotechnical Standardization	<b>CEN</b> European Committee for Standardization	<b>ETSI</b> European Telecommunications Standards Institute
<b>Kansallinen taso</b>	<b>SESKO</b>	<b>SFS</b> Suomen Standardisoimisliitto SFS toimialayhteisöineen	<b>Liikenne- ja viestintävirasto</b>

# Auditointi, akkreditointi ja sertifiointi

## SERTIFIOINTI

- Tietoturvallisuuden vaatimustenmukaisuuden todistettavasti täyttävälle toteutuksille voidaan myöntää standardin mukainen hyväksyntä, eli sertifikaatti, jonka myöntää puolueeton kolmas osapuoli
- Standardeja voidaan käyttää tietoturvallisuuden parantamiseen ilman sertifiointiakin mutta sertifiointi on selkeä tapa viestiä standardiin sitoutumisesta
- Organisaatio voi sertifikaatin avulla osoittaa asiakkailleen ja sidosryhmilleen, että jatkuva kehittäminen ja toiminnan parantaminen kuuluvat sen toimintatapoihin
- Hallintajärjestelmät ja niiden sertifiointit ovatkin usein edellytyksenä asiakkaan valitessa toimittajia tai kumppaneita, erityisesti kansainvälisessä liiketoiminnassa

## ARVIOINTI JA AUDITOINTI

- Arviointi sisältää tulkintamahdollisuuden, mutta tarkastus ei, koska siinä keskitytään ainoastaan vaatimusten toteutumiseen (kyllä/ei)
- Kolmas osapuoli voi arvioida tai auditoida organisaation toimintaa sen dokumentteja tarkastelemalla, fyysisinä tarkastuskäynteinä tai molempien yhdistelmänä

# Auditointi, akkreditointi ja sertifiointi

## AKKREDITOINTI

- Akkreditointi tarkoittaa pätevyyden toteamista puolueettomasti ja riippumattomasti
- Suomessa akkreditointielin on FINAS (Finnish Accreditation Service)
- Turvallisuus- ja kemikaalivirasto Tukesiin kuuluva FINAS on kansainvälisen akkreditointijärjestön IAF:n (International Accreditation Forum) jäsenjärjestö
- Liikenne- ja viestintävirasto puolestaan hyväksyy ja valvoo arviointilaitoksia, jotka tarjoavat viranomaisille puolueetonta tietoturvallisuuden arviointipalvelua
- Akkreditointi viestii asiakkaille toiminnan pätevyydestä, uskottavuudesta ja luotettavuudesta sekä yhdenmukaistaa vaatimusten tulkintaa ja lisää yhteentoimivuutta

## SERTIFIOINTIEN MERKITYS LIKETOIMINNALLE

- Kustannukset vaikuttavat sertifiointien käytön laajuuteen ja vaikutukseen
- Edullisten, niin sanottujen kevytsertifikaattien merkitys liiketoiminnalle voi olla vähäinen, kun taas raskaammissa vaatimuksissa ja niiden todentamisissa kustannukset voivat olla suuria
- Raskaammat sertifiointit painottuvatkin pääsääntöisesti isoihin toimijoihin ja niiden tuotteisiin
- Oikein tehtynä puolueettoman osapuolen tarkastus ja hyväksyntä lisäävät kuitenkin merkittävästi sidosryhmien luottamusta vaatimusten noudattamiseen

# Tärkeää tietoa NIS 2 direktiivistä

## Keitä direktiivi koskee?

Direktiivin kohteena olevat organisaatiot on pääpiirteissään kuvattu Kyberturvallisuuskesksen Excel-taulukossa, joka löytyy osoitteesta:

[https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM\\_NIS2\\_taulukko\\_230424.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_NIS2_taulukko_230424.pdf)

Taulukossa kuvatun lisäksi NIS 2 direktiiviä sovelletaan toimijoihin niiden koosta riippumatta myös, kun:

- toimija tarjoaa ainoana jäsenvaltiossa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen.
- häiriö toimijan tarjoamassa palvelussa voisi vaikuttaa merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen.
- häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia.
- toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

Lisäksi NIS2-direktiiviä sovelletaan CER-direktiivin nojalla kriittisiksi toimijoiksi määritettyihin toimijoihin niiden koosta riippumatta. Lisätietoa löytyy osoitteesta:

<https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=fi>

# Mitä vaatimuksia direktiivi asettaa?

## Kyberturvallisuuden riskienhallintavelvoitteiden noudattaminen

- Toimijalla on oltava käytössä ajantasainen kyberturvallisuuden riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta.
- Toimijoiden on toteutettava kyberturvallisuuden riskienhallinnan toimintamallin mukaiset oikeasuhtaiset tekniset, operatiiviset tai organisatoriset hallintatoimenpiteet viestintäverkkojen ja tietojärjestelmien turvallisuudelle kohdistuvien riskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.
- Kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on huomioitava ja ylläpidettävä ajantasaisena vähintään NIS 2 direktiivin 21 artiklan sisältämän luettelon kymmenen keskeistä kohtaa:
  1. riskianalyysijä ja tietojärjestelmien turvallisuutta koskevat politiikat;
  2. poikkeamien käsittely;
  3. toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta;
  4. toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat;
  5. verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen;
  6. toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta;
  7. perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus;
  8. toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä;
  9. henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta;
  10. tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.
- Riskienhallinnan toimenpiteet on suhteutettava toiminnan laatuun ja laajuuteen, toimijan poikkeamasta kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeamien todennäköisyyteen ja vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä ajantasainen kehitys huomioiden käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

# Hyviä käytänteitä

Hyviä perustason tietoturvakäytäntöjä ovat:

1. Toimija on ohjeistanut perustason tietoturvakäytännöt henkilöstölle, alihankkijoille ja muille kumppaneille,
2. Toimija on tunnistanut kriittisimmän omaisuutensa,
3. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä,
4. Toimija on erottanut kriittiset ja haavoittuvat viestintäverkot ja tietojärjestelmät muista ympäristöistä,
5. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä haitallisia ja luvattomia ohjelmistoja vastaan,
6. Toimija on järjestänyt tunnistautumisen sisäisiin ja ulkoisiin palveluihinsa ja laitteisiinsa turvallisesti,
7. Toimija on erottanut järjestelmiensä pääkäyttäjätunnukset ja korotettujen oikeuksien tunnukset muista tunnuksista,
8. Toimija on varmistanut, että sen luottamuksellista tietoa käsitellään turvallisesti,
9. Toimija on huolehtinut, että sen järjestelmiä päivitetään säännöllisesti ja kriittiset päivitykset asennetaan viivytyksettä,
10. Toimija on huolehtinut, että sen palvelut ja laitteet on turvallisesti konfiguroitu,
11. Toimija on huolehtinut, että sen kriittiset palvelut ja tieto-omaisuus on varmuuskopioitu,
12. Toimija on varautunut, miten sen toiminta voidaan ylläpitää vakavissa poikkeamissa ja
13. Toimijalla on käytössään kriittisten toimintojen tapahtumakirjaus.

Täydennä käytäntöjä riskiarvion perusteella!

# ISO/IEC 27001

- vain toimintakuntoiset tietoturvakontrollit voivat suojata organisaatiota
  - jotta organisaatio voi varmistua tietoturvallisuuden systemaattisuudesta, voi se ottaa toimintansa tueksi ISO 27001 -standardin käytännöt, säännöt ja ohjeet
  - ISO 27001 -standardissa määritellään vaatimukset, jotka koskevat organisaation tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä, ja jatkuvaa parantamista

# ISO/IEC 27001

- ISO 27001 –standardin hallintajärjestelmä ei tarkoita mitään erillistä tietojärjestelmää
  - se on kokoelma ohjeita, toimintatapoja sekä teknisiä ratkaisuja tiedon suojaamiseen ja toiminnan jatkuvaan kehittämiseen
  - usein näitä ohjeita ja tietoturvaa tukevaa teknologiaa on jo paljonkin käytössä, mutta niitä ei ole vain koottu yhteen hallituksi kokonaisuudeksi – ja niitä ei välttämättä kehitetä systemaattisesti
- Jos jatkuvan parantamisen kulttuuri ei toimi, se ei vastaa enää jatkuvasti ympärillä muuttuvan maailman vaatimukseen
- mutta, mitkä ovat sitten ydintoimintojen kannalta suojattavat digitaaliset palvelut, ja ovatko niiden suojaustoimenpiteet ajantasaisia sekä ylläpidettyjä?
  - on huomioitava organisaation riskien- ja jatkuvuudenhallintaa sekä myös fyysisiä turvallisuusjärjestelyitä koskevat tarpeet

# Miksi ISO 27001 –standardia kannattaa noudattaa?

- tietoturvallisuuden tavanomainen hallinta ei ole kaikkia uhkia vastaan riittävä
- on myös mahdollista, että tietoturvaa ei kehitetä pitkäjänteisesti ja yhtä nopeasti kuin maailma ympärillä tai omat tarpeet muuttuvat
- jotta organisaatio voi varmistua tietoturvallisuuden hallintansa systemaattisuudesta, kannattaa sen ottaa toimintansa tueksi ISO 27001 –standardin käytännöt, säännöt ja ohjeet
  - johdon tulee myös määritellä vastuuhenkilö(t) hallintajärjestelmän ylläpitämiseen

# Mitä standardi käytännössä vaatii?

- ISO 27001 –standardissa määritellään vaatimukset, jotka koskevat tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä, ja jatkuvaa parantamista
- Hallintajärjestelmä on kokoelma ohjeita, toimintatapoja, sekä teknisiä ratkaisuja, suojan luomiseen ja toiminnan jatkuvaan kehittämiseen
  - suojattavia kohteita ovat erityisesti tieto
  - lisäksi halutaan suojata mm. henkilöstöä, tiloja, järjestelmiä, ja tietoverkkoja
- Keskiössä on jatkuvan parantamisen kulttuuri
  - tietoturvassa havaittuja epäkohtia nostetaan esille, ja niitä käsitellään sekä korjataan jatkuvasti
    - organisaatioiden tarpeet ovat erilaiset, mutta ISO 27001 –standardi on suunniteltu kattamaan kaikenkokoiset organisaatiot kaikilta aloilta
      - soveltaminen tehdään tietoturvallisuuden hallinnan näkökulmasta, riskienhallinnan avulla, sekä organisaation omien sidosryhmien vaatimusten pohjalta

# Mitä standardi käytännössä vaatii?

- Tietoturvan hallintakeinojen avulla suojaudutaan konkreettisesti uhkia vastaan
  - esimerkiksi kyberhyökkäyksiä, tietämättömyyttä, tai tulipaloa vastaan
  - myös ihmisten käyttäytyminen huomioidaan
    - esimerkiksi henkilöstön kouluttaminen ja käytänteiden noudattaminen on mukana kokonaisuudessa
- Kokonaisuuteen sisältyy myös toiminnan säännöllinen arviointi mm. sisäisillä auditoinneilla

*ISO 27001 –standardi on kuin arkkitehdin piirrokset ja yksityiskohtaiset työohjeet, jotka auttavat rakentamaan suojattavien kohteiden turvaksi jyvän kivitalon*

- Jatkuva kehittäminen ja parantaminen pitää huolen siitä, että hyödyt eivät katoa ajansaatossa
  - tämän vuoksi sertifiointikaan ei ole kertaluontoinen, vaan jatkuva prosessi

# Mitä sertifiointi vaatii?

- Sertifikaattia varten organisaation tulee noudattaa kaikkia standardin vaatimuksia, ja todistaa tämä arviointiprosessin aikana
- Koko prosessiin sisältyy vaadittavan dokumentoinnin ja käytänteiden luominen, henkilöstön koulutus, sisäiset auditoinnit, sekä ulkoinen auditointi
  - sisäinen auditointi voidaan suorittaa organisaation omasta toimesta
    - se vastaa täysin ulkoista auditointia
    - tehdään tyypillisesti kaksi kertaa ennen ulkoista auditointia
  - ulkoisen akkreditoidun auditoinnin kesto riippuu organisaation henkilöstömäärästä ja hallintajärjestelmän laajuudesta
    - se sisältää sekä haastatteluja että dokumentoidun tiedon läpikäyntiä
  - jos sertifikaatti myönnetään ulkoisen auditoinnin seurauksena, tehdään kahden seuraavan vuoden aikana suppeammat seuranta-arvioinnit
    - kolmantena vuonna sertifikaatti uusitaan jälleen vähän laajemmalla arvioinnilla, minkä jälkeen prosessi toistuu säännöllisesti kolmen vuoden sykleissä

# Sertifiointinin hyödyt

1. Osoittaa selkeän sitoutumisen tietoturvaan
2. On vetovoimatekijä
3. Mahdollistaa tuottoisammat sopimukset
4. Mahdollistaa erottautumisen muista
5. On vankka valinta



**Tom Tuunainen**  
**Centria SecuLab**  
**seculab@centria.fi**  
**<https://seculab.fi>**