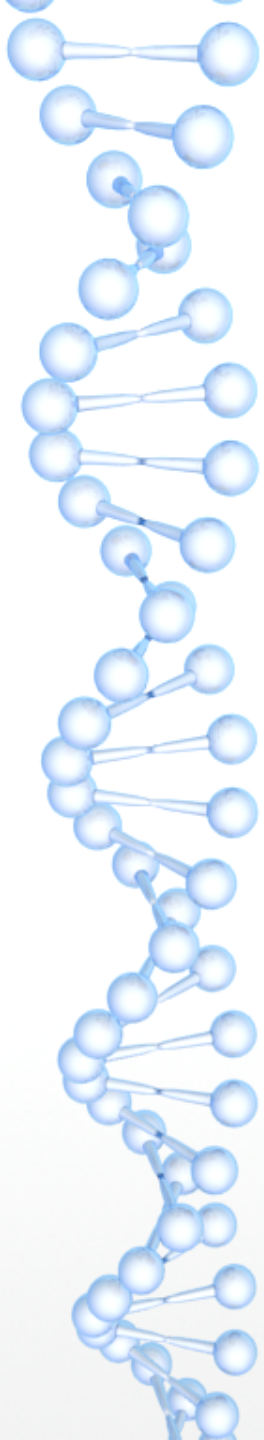


Kybersuojaaminen ja haltuunotto

Tuomas Tenkanen

ITKST55

Määritelmiä

- Kyberturvallisuus – tavoitetila, jossa **kybertoimintaympäristöön** voidaan luottaa ja jossa sen toiminta **turvataan**. Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen **tiedon käsittelystä riippuvaiselle toiminnalle** eikä sen toimivuudelle.
- Kybertoimintaympäristö – sähköisessä muodossa olevan tiedon käsittelyyn tarkoitettu … toimintaympäristö.
- Kybersuojaaminen – toimenpiteitä, joilla turvataan kybertoimintaympäristön toimivuutta ja luotettavuutta
  - hallinnollisia
  - teknisiä

Pari käsitettä alkuun

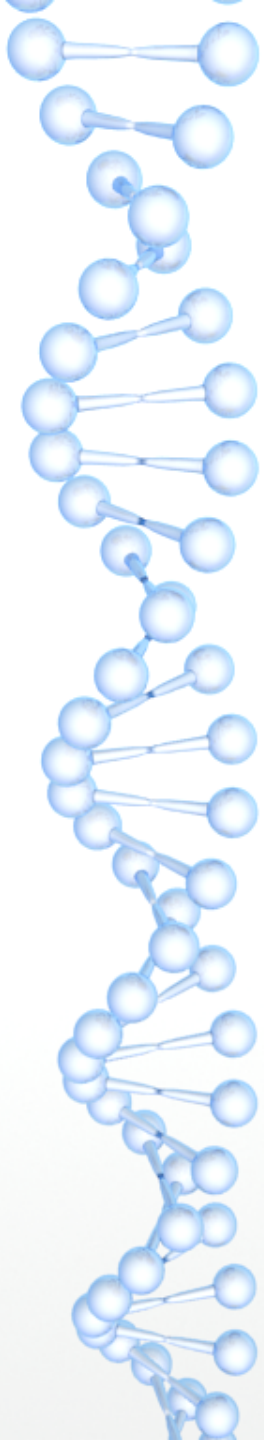
- **Käyttöverkko**, -työasema: verkko, jossa järjestelmän palveluita käytetään tavallisilla päätelaitteilla. Esim. luodaan dokkari ja tallennetaan se palvelimelle.
- **Hallintaverkko**, -työasema: verkko ja työasemat, joilla tehdään ylläpitotoimenpiteitä järjestelmään, esim. asennetaan päivityksiä palvelimille, ruuvataan muureja ja valvotaan palvelutilannetta.
- **Valvontaverkko**, -työasema: verkko ja työasemat, joilla valvotaan ja havainnoidaan kohteen kybertapahtumia, mutta ei vaikuteta kohteeseen mitenkään. Kybervalvonta ohjeistaa ylläpitoa tarvittaessa kovennuksissa ja korjauksissa. Kybervalvontaa ei myöskään pitäisi pystyä havaitsemaan suojattavasta (käyttö-)verkosta mitenkään.

Kyber vs ylläpito

- Ylläpito pyrkii varmistamaan, että
  - järjestelmä toimii kuten on suunniteltu
  - käyttäjät saavat palvelut käyttöönsä
  - käyttäjät eivät pääse tekemään hölmöyksiä tahallaan tai vahingossa
  - järjestelmää ei pääse asiattomasti käyttämään tai rikkomaan
  - päivittää ja koventaa järjestelmää

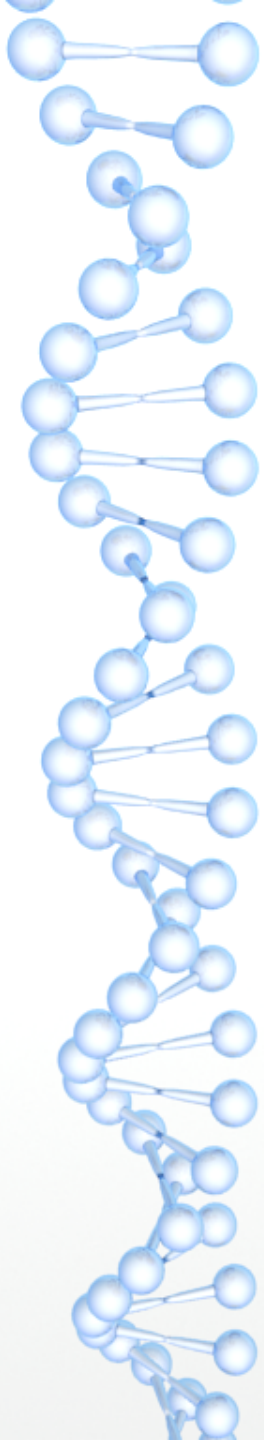
- Kyber
  - huomaa kun joku kuitenkin pääsi tekemään hölmöyksiä, käytti järjestelmää luvattomasti tai esti sen käyttöä
  - huomauttaa ylläpitoa edellisestä ja ohjeistaa korjauksissa

Teknisiä suojauksia käyttöverkossa



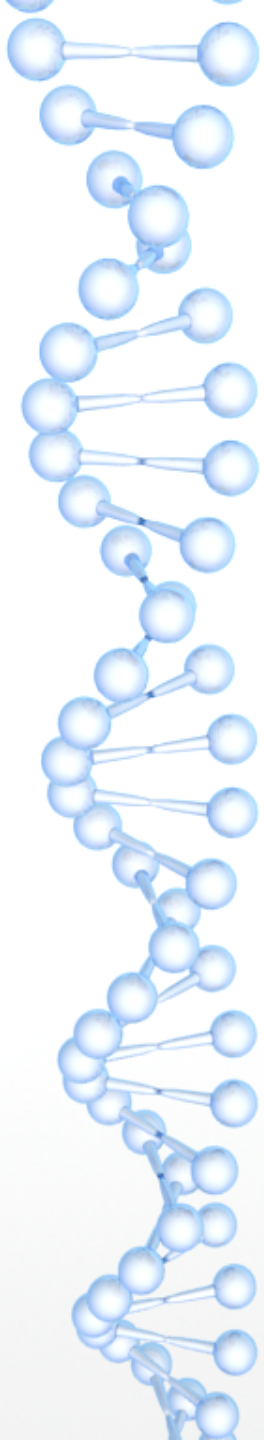
- Käyttäjähallinta
  - hallittu pääsy päätelaitteille, myös mobiili
  - hallittu pääsy tietoon minimiperiaatteella
  - laitehallinta, käyttöoikeudet, käyttäjän tunnistaminen
- Verkon eheyden varmistaminen
  - eriyttäminen: käyttö, ylläpito, valvonta
  - päätelaitteiden tunnistaminen ja pääsyn hallinta
  - palomuurit, segmentointi, porttiautentikaatio (801.x)
- Päätelaitesuojaus: antivirus, hids
- Tiedon suojaus levyllä ja liikkeessä: salaus
- Tapahtumien todentaminen: lokit

Kybervalvonta



- Mitä järjestelmässä pitäisi valvoa?
  - normaalitoiminta: käyttäjät, ylläpitäjät
    - poikkeamaa normaalista ei voi tunnistaa, jos ei tunne normaalia
  - poikkeamien tunnistaminen
- Mitä valvottavassa järjestelmässä tapahtuu?
  - lokit, data flow:t, pakettikaappaukset, hälytykset
- Miten näkyvyyttä järjestelmään rakennetaan?
  - rajoittavat vs näkyvyyttä rakentavat komponentit
  - palomuurit, blacklisting, whitelisting, ACL:t, segmentointi, NAT
  - sensorit, päätelaitesuojaus, lokien keräys ja havainnointi

Tapahtumat, poikkeamat, hälytykset



- Tapahtuma (event), joka ei kuulu normaaliin toimintaan, on poikkeama (anomaly)
- Tapahtumista tai poikkeamista voidaan nostaa haluttaessa hälytyksiä (alert) voimassa olevien sääntöjen mukaisesti tai esim. tunnistettaessa poikkeama tilastollisin menetelmin
- Hälytykset tai poikkeamat käsittelee ihminen, joka päättää onko kyseessä tutkittava asia (case, incident) tai tarvitseeko säännöstöjä päivittää

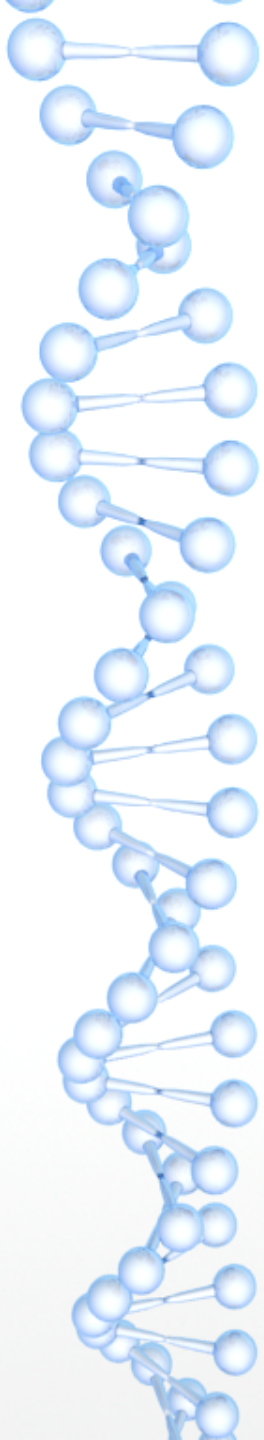
Kyberuhkien ja –poikkeamien torjunta

- Tekninen tutkinta: mitä tapahtui?
  - analyysi
- Haittavaikutusten rajaaminen
  - hallinnollisia ja teknisiä toimenpiteitä
- Poikkeaman toistumisen estäminen
  - ohjeistus, jolla ylläpito koventaa järjestelmää siten, että sama ei pääse tapahtumaan uudestaan

Kybersuojaamisen datalähteitä

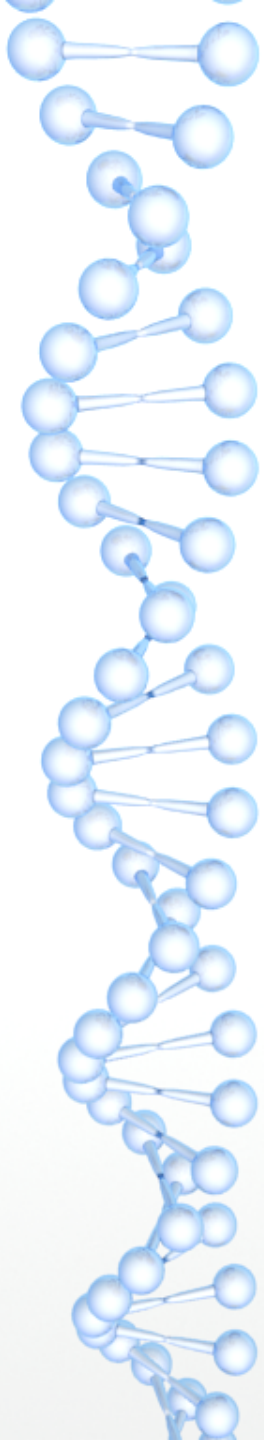
- Lokit, lokien aggregointi, rikastaminen
  - heinäsuopa, josta etsitään neuloja
  - helpottaa huomattavasti, jos lokit ovat saatavilla yhdestä paikasta
- Netflow
  - aktiivilaitteiden näkemät paketit tapahtumiksi verkossa
- Sensorit
  - valitun pisteen liikenne tapahtumiksi verkossa
- Päätelaitesuojaus
  - sallitut ja kielletyt toimet päätelaitteella, lokit/hälytykset näistä
  - etähallinta

Suojaamisen tietotarpeita



- Järjestelmän toiminnan tarkoituksen tunteminen
  - miksi järjestelmä on olemassa
  - **suojattavan tiedon tunnistaminen**, vaarantumisen hinta
  - kenen käyttöön järjestelmä on tarkoitettu: käyttövaltuudet, pääsynhallinta
- Järjestelmän komponenttien tunnistaminen
  - **mitä järjestelmään kuuluu**
  - inventaario, dokumentaatio
  - muutokset, dokumentaatio
  - haavoittuvuudet, hallinta
- Uhkamallit
  - mitä, kuka, miksi, millä resursseilla

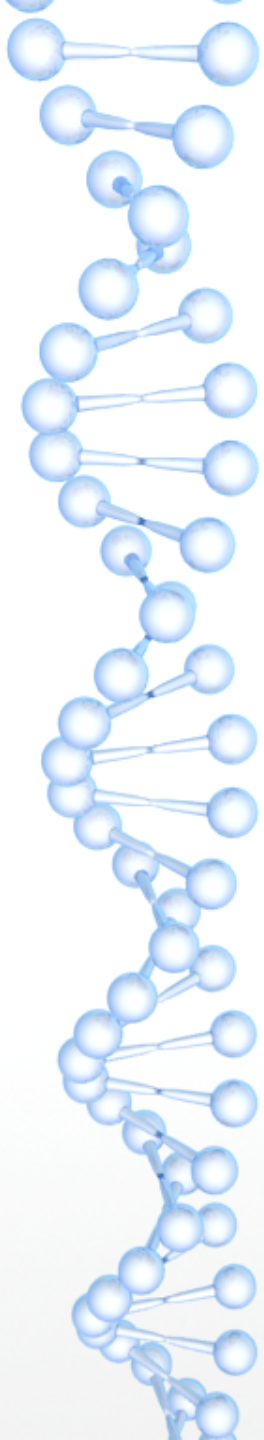
Suojattavan tiedon (asset) tunnistaminen



- Toiminnan kannalta tarpeelliset tiedot, palvelut ja toiminnot
- Käytettävissä olevat resurssit
- Kaikki, jolla on jotakin arvoa – joko itselle tai jollekin muulle
- Riskiarvion perusta

Mitä järjestelmään kuuluu

- Verkkoyhteydet
- Interfacet
- IP-osoitteet
- Gatewayt
- Reitit
- Nimipalvelimet
- Käyttäjätunnukset
- Ylläpitotunnukset
- Palvelimet
- Palvelut
- Työasemat
- Ohjelmistoversiot
- Tunnetut haavoittuvuudet
- Verkonvalvonta
- Saatavilla olevat päivitykset
- Avaimistot
- Palomuuriasetukset
- Lokit
- Avoimet yhteydet
- Baseline, normaali



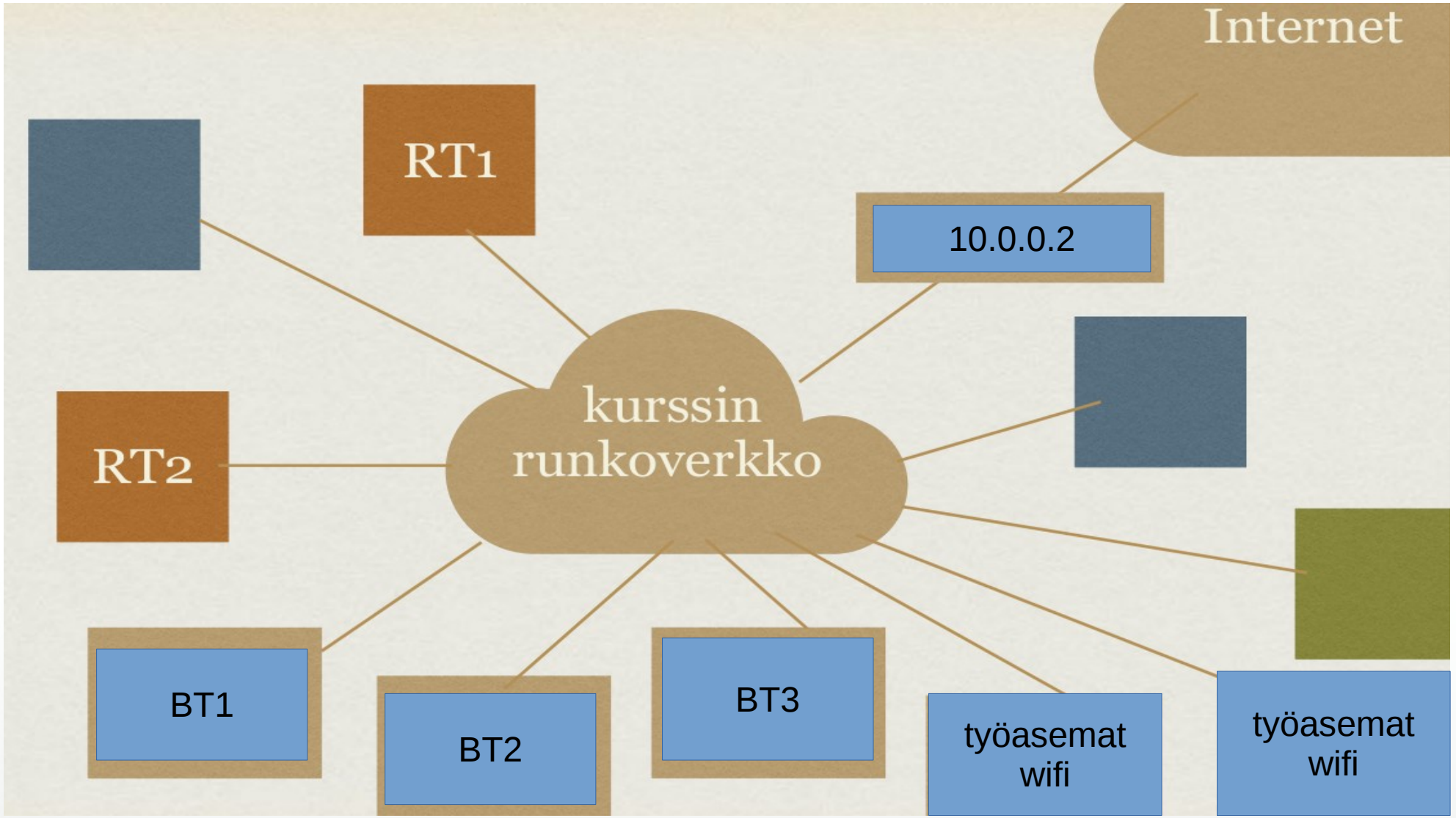
Miten selvitetään

- Dokumentaatio
- Reaalimaailman havainnointi
- Virtuaalimaailman havainnointi
  - koneiden verkkoasetukset, ping, nmap, konffitiedostot, nimipalvelukyselyt
- Tukipyynnöt

Lähtötietoja

- Pienen firman verkko: Arttu kertoo taustat
- Työasemia, palveluita, kaikki ei samassa verkkoalueessa
- Oma ylläpito aivan kaikelle
  - Voitte tehdä omassa verkossa mitä tahansa
  - Palvelut täytyy pitää toiminnassa
- https://www.io

Iso kuva


Internet
RT1
10.0.0.2
RT2
kurssin
runkoverkko
BT1
BT2
BT3
työasemat
wifi
työasemat
wifi

Tehtävä

- Määritä oma organisaatio ja tehtävät jokaiselle
- Kartoita suojattava verkko
- Tunnista järjestelmän komponentit
- Tee riskiarvio järjestelmän osista, priorisoi
- Suunnittele suojaus- ja kovennustoimet edellisten perusteella
- Dokumentoi
- Palautus wikiin MA 1700 mennessä
- Valmistaudu esittämään oma ratkaisu TI 0815