HSY:n tietoturva

Joonas Väyrynen
Tietoturva-asiantuntija
+358-504728540
joonas.s.vayrynen@hsy.fi

Miten HSY:n tietoturva sai alkunsa?

1. Maailma herää kyberuhkiin
   - Vuonna 2016-2017 maailmalla tapahtui laajasti vaikuttaneita ja uutisoituja kyberhyökkäyksiä. Esimerkiksi Iso-Britannian Wannacry hyökkäys aiheutti paljon kohua mediassa, myös Suomessa, vaikka kiristyshaittaohjelmia on todettu ja nähty Suomessakin jo vuonna 2014. Mikä muuttui?
2. KYBER-VESI hanke saadaan päätökseen
   - Huoltovarmuuskeskuksen, Vesilaitosyhdistyksen ja VTT:n vetämä parivuotinen kyberturvallisuushanke päättyi vuonna 2018 ja tämä nosti monia huolia esiin automaatioympäristön turvallisuudesta.
3. Kyberturvallisuuskeskus (Traficom/KTK) perusti VESI-ISAC ryhmän
   - Kybervesihankkeen tuotoksena KTK lähti perustamaan VESI-ISAC tiedonvaihtoryhmän.
4. Vuoden 2018 ja 2019 kuntiin ja kaupunkeihin kohdistuneet hyökkäykset huolestuttavat
   - Viime vuosina kuntiin ja kaupunkeihin kohdistuneet kyberhyökkäykset ovat myös vaikuttaneet vesialan yritysten toimintaan. Tämä viimeistään on herättänyt monet parantamaan kyberturvaansa.

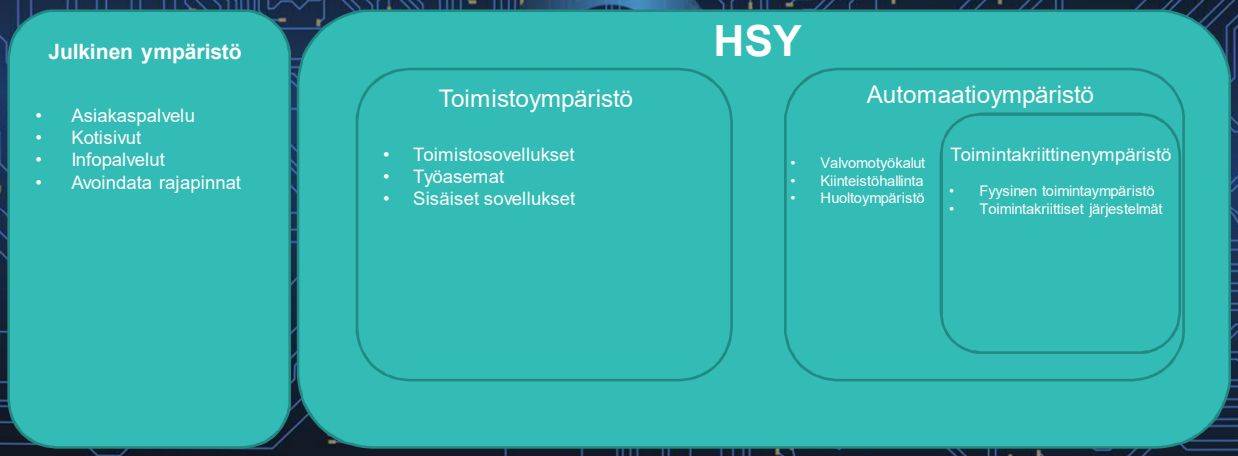
Kuinka tietoturva on HSY:llä organisoitu

- HSY:lle on perustettu tietoturvaryhmä
  - HSY perusti vuoden 2018 lopussa tietoturva-asioille single point of contact ryhmän. Tietoturvaryhmä vastaa käyttäjille tietoturvakysymyksiin, aktiivisiin hälytyksiin ja kouluttaa henkilökuntaa. Kaikki viestintä tapahtuu pääasiassa tietoturva@hsy.fi osoitteen kautta.
  - Tietoturvaryhmä vastaa myös tietoturvan ja palveluiden kehittämisestä HSY:ssä.

- Automaatioympäristössä valvomo vastaa viestimisestä
  - Koska automaatioympäristöstä ei saada helposti viestejä ulkoisiin lähteisiin on ympäristöjen tarkkailu ja mahdollisista poikkeamista ilmoittaminen päivystäjälle valvomon vastuulla.
  - Automaatioympäristöissä toiminta on yleensä toimittajalähtöistä, joten heidät tulee sitouttaa Tietoturvalliseen toimintaan.

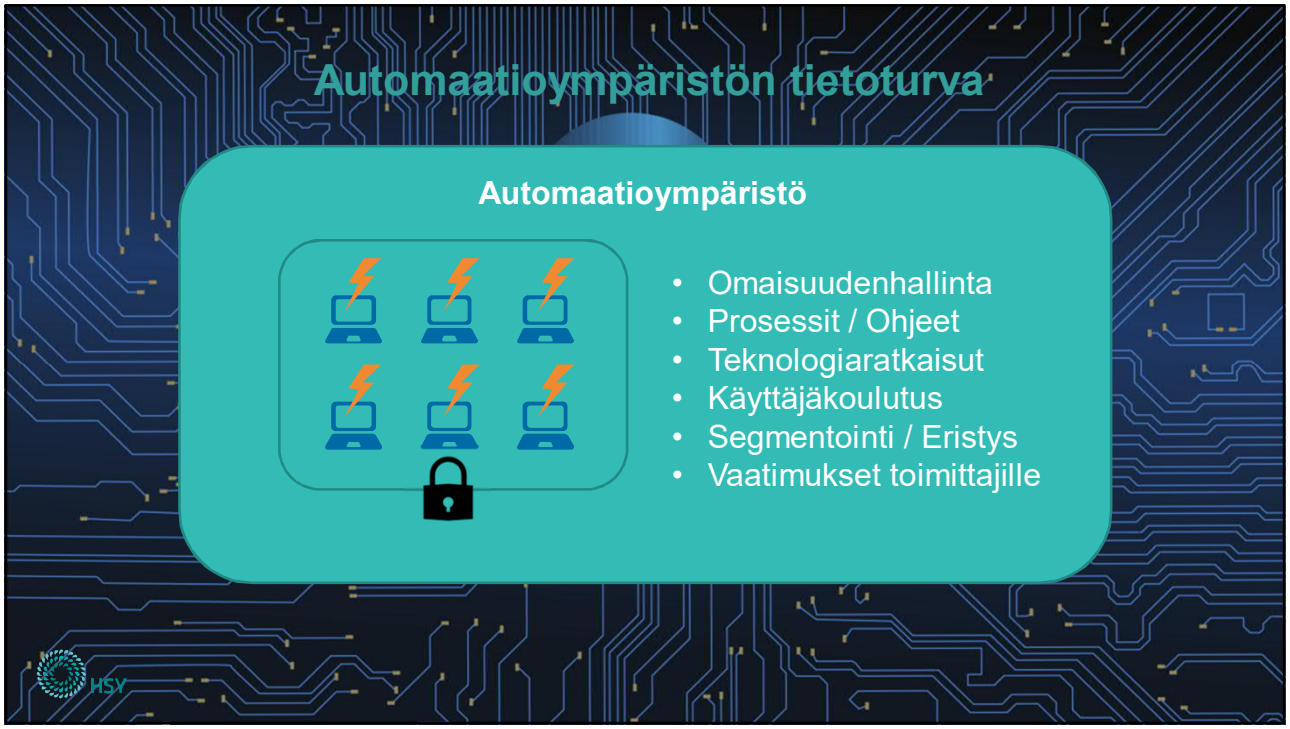
HSY

Toimintaympäristöt



HSY


Tietoturvan kontaktointi
Toimistoympäristö
Käyttäjät
Hälytykset
Ulkoiset viestit
HSY tietoturvaryhmä
Yksi kontaktirajapinta
Ohjeistukset näkyvillä
Valmiit prosessit
Näkyvyys ympäristöön
Automaatioympäristö
Automaatio
Monitorointi
Valvonta
Valvomo
Päivystäjä
HSY


Automaatioympäristön tietoturva
Automaatioympäristö
Omaisuudenhallinta
Prosessit / Ohjeet
Teknologiaratkaisut
Käyttäjäkoulutus
Segmentointi / Eristys
Vaatimukset toimittajille
HSY

Toimistoympäristön tietoturva

Toimistoympäristö

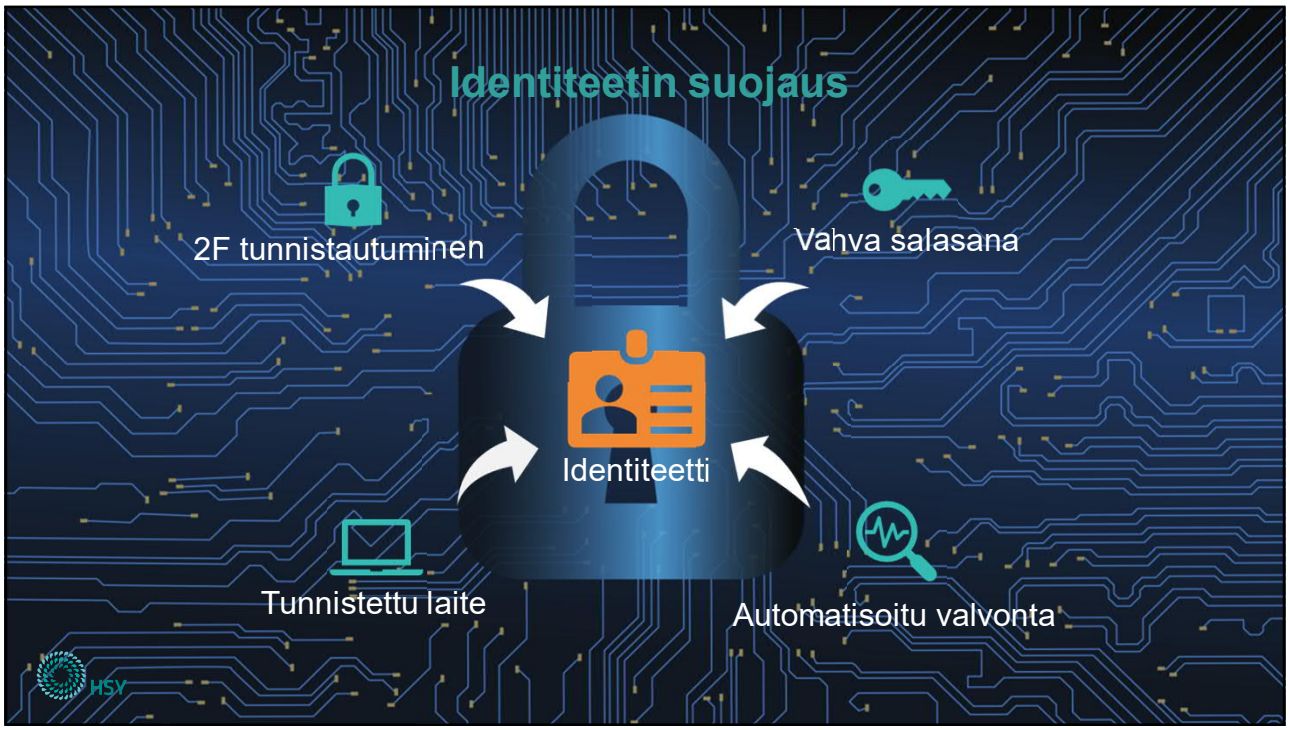
- Palomuuri
- Teknologiaratkaisut
- Käyttäjäkoulutus
- ***Identiteetin suojaus***

Identiteetin suojaus

Digitalisaation ajama kehitys on siirtänyt tietoturvan painotuksen pois perinteisistä tietoturvaratkaisuista kuten palomuurista ja virustorunnasta käyttäjän identitettiin.

Käyttäjän identiteetillä tarkoitetaan käyttäjän henkilöllisyyttä järjestelmissä, joka on perinteisesti nojannut käyttäjätunnukseen ja salasanaan. Nykyään kuitenkin pelkästään näihin nojaava tunnistautuminen on hyvin murtoaltis.

Nykyään suojaukseen kannattaa käyttää useaa identiteettiä vahvistavaa tekijää.



Kuinka toimia tietoturvariskin tapahtuessa?

Tietoturvariskeihin varautumisessa ehkä tärkeimpänä osana on varautua siihen KUN, ei jos, riski toteutuu. Nykyään riskin toteutumisen todennäköisyys vuoden sisällä on todennäköisempi kuin mitään ei tulisi tapahtumaan. Tämän vuoksi organisaatioiden tulisi omata suunnitelma kuinka toimia yleisellä tasolla riskin luonteesta huolimatta.

- **Havainnointokyky**
  - **Yleiseen kyberturvallisuuden ja tämän poikkeuksien monitorointiin ja havaintokykyyn tulee panostaa. Päämääränä on saada parempi näkyvyys ympäristön digitaalisiin toimintoihin.**
- **Viestintä**
  - **Organisaatiolla tulisi olla viestintäsuunnitelma ja pohjat sisäiseen (Esim. työntekijät, johto ja viestintäyksikkö) ja ulkoiseen viestintään (Esim. Media ja/tai viranomaiset). Tämän lisäksi toimittajien kanssa tulee sopia yhteydenotosta kyberturvallisuuteen liittyen etukäteen!**
- **Minimoi haitat**
  - **Arvioi jokaisen järjestelmän kohdalla onko tämä mahdollista eristää tai sulkea väliaikaisesti.**
- **Palauta normaalitoiminta**
  - **Kun tapaus on ratkaistu ja haavoittuvaisuus paikattu, tulee järjestelmien toiminta palauttaa. Järjestelmiä varten tulisi olla luotuna palautussuunnitelma yleisellä tasolla. Helpoin tapa toimia on palauttaa järjestelmä aiempaan, hyökkäystä edeltävään versioon.**

HSY

Käyttäjien osallistaminen

Käyttäjiä normaalisti käsitellään organisaation heikoimpana lenkkinä. Tämä ”klisee” ajattelumalli on itseasiassa organisaatiolle haitallista. Työntekijät pitäisi osallistaa ja kannustaa kyberturvalliseen työskentelemiseen pelottelun sijaan. Nykypäivänä digitaalisissa palveluissa tietoturvaa ei voida koskaan täysin järjestää ja ylläpitää käyttäjän puolesta.

- Kommunikointi
  - Työntekijöille tulee kommunikoida selvästi riskeistä ja haasteista tietoturvaan liittyen.
- Koulutus
  - Työntekijöitä tulee kouluttaa säännöllisesti niin perusteiden kuin uusien ominaisuuksien sekä nykyisiin uhkiin liittyen.
- Työntekijöitä ei tule syyllistää
  - Kyberhyökkäyksen tai huijauksen kohteeksi voi joutua ketä tahansa. Työntekijöitä ei tule syyllistää tästä vaan organisaatioiden kannattaa yrittää luoda avoin ja kannustava työkulttuuri, joka edistää sisäistä viestintää.

HSY

Yhteenveto

HSY

Myyttejä kyberturvallisuudesta

Kyberturvallisuudessa on vielä nykyäänkin monia ”myyttejä”, jotka hidastavat kyberturvallisuuden kehittymistä.

- **Meillä ei ole tietoa, jota kukaan haluaisi varastaa tai millä kukaan tekisi mitään.**
  - **Digiaikakautena kaikki data on arvokasta ja hyödynnettävissä. Jos datasi lukitaan miten organisaatiosi jatkaa toimintaa?**
- **Suomessa ei ole vakavaa kyberturvariskiä poliittisista ja maantieteellisistä syistä.**
  - **Suomi ei ole ollut pitkään aikaan ”lintukoto” ja kielimuuri ei enää suojaa meitä. Myös automaatioympäristön kannalta on yhden tekevää missä päin maailmaa tämä sijaitsee. Onnistuneella kyberhyökkäyksellä on aina hintansa uhrille ja rahallinen hyöty hyökkääjälle.**
- **Meidän yrityksen kyberturvallisuus ei ole yhtä tärkeää kuin muiden. Jos muut pitävät tästä huolta, meidän ei tarvitse panostaa tähän niin paljon.**
  - **Kysymys ei ole koskaan vain yhden organisaation kyberturvasta, tällä on aina vaikutus organisaation kanssa yhteistyössä oleviin organisaatioihin. Kyseisen ajatuksen logiikka on myös hyvin virheellinen.**
- **Kyberturvan mahdollisista tai tapahtuneista riskeistä ei kannata puhua julkisesti.**
  - **Kaikki tutkimukset ja tapaukset ovat osoittaneet, että tapauksista kannattaa puhua ja tietoa jakaa eteenpäin. Asiakkaat, yhteistyökumppanit ja organisaation omat työntekijät arvostavat avoimuutta ja mitä aktiivisemmin asioista keskustellaan, sitä paremmin näihin saa tukea.**

HSY

Puhtaasti parempaa arkea | En rent bättre vardag | Purely better, every day

Joonas Väyrynen
Tietoturva-asiantuntija
+358-504728540
joonas.s.vayrynen@hsy.fi

Helsingin seudun ympäristöpalvelut -kuntayhtymä
Samkommunen Helsingforsregionens miljötjänster
Helsinki Region Environmental Services Authority