Zero Trust OT-tietoverkoissa

Suojaa automaatio ilman oletuksia

Suomen Automaatioseura ry:n webinaari

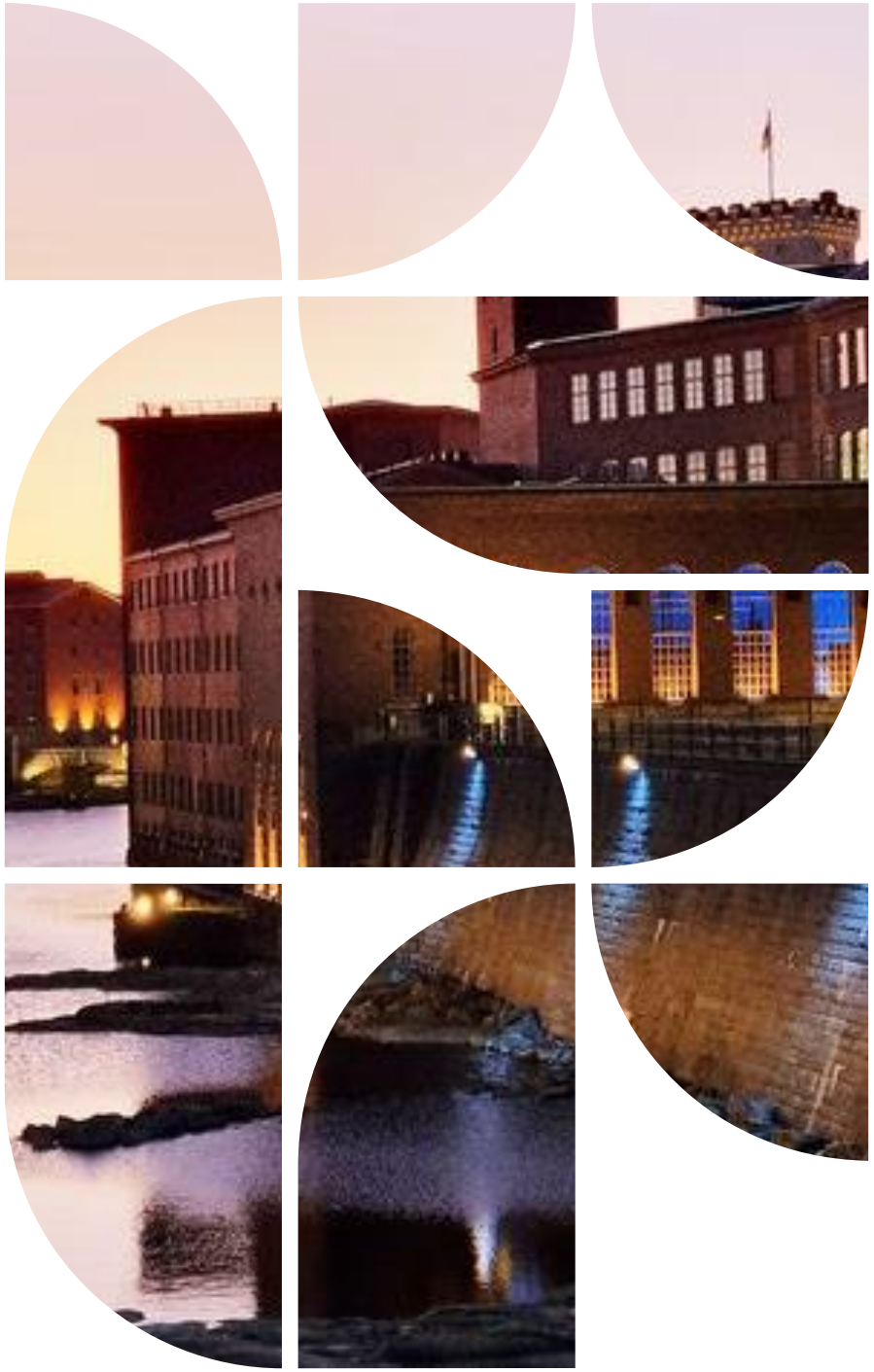
2024-10-23

Leo Mikonmaa

Tietoliikennearkkitehtina Tampereen Energiassa, entinen Tampereen Sähkölaitos

Vastaan konsernin tietoliikenteestä

leo.mikonmaa@tampereenenergia.fi



Sisältö

Zero Trust lyhyesti

Jatkuva varmentaminen

- Autentikoi ja valtuuta jokainen pääsypyyntö

Pienimmän mahdollisimman pääsyoikeuden periaate

- Anna käyttäjille ja laitteille vain ne vähimmäisoikeudet, joita heidän tehtävänsä edellyttävät

Mikrosegmentointi

- Jaa verkot pienempiin osiin laitteiden välisen kommunikaation rajoittamiseksi

Monivaiheinen todennus

- Vaatia useita todennusmenetelmiä käyttäjien ja ylläpitäjien kirjautumiseen

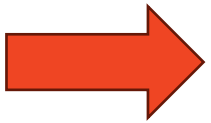
Valvo

- Seuraa ja analysoi jatkuvasti käyttäjien, ylläpitäjien ja laitteiden toimintaa

Miksi?

- Koska se, että sinulla ei ole ”yhteyttä” hyökkääjään, ei tarkoita etteikö hyökkääjä voisi aiheuttaa sinulle tai yhteiskunnallesi haittaa *(1,2)*
    - Verkosta erottaminen ei riitä

”At best, an air gap is a high-latency connection” –Ed Skoudis – DerbyCon 3.0



Eli joka tapauksessa pitää olla muita kontrolleja, kuin internetistä erotus.

Tarinan pihvi elikkä mitä olemme tekemässä

Kasvattaa hyökkäyksen kustannuksia hyökkääjälle. Vähentää suojauksen kustannuksia puolustajalle.

OT-Ympäristön ominaispiirteet

- Ympäristön ja järjestelmien saatavuus on ensisijaista, kaikki muu suojaaminen on toissijaista
- Tutut perusasiat
    - Pitkät elinkaaret verrattuna muuhun tietotekniikkaan
    - Erilaiset protokollat kuin muualla
    - Suljetut ympäristöt
    - Muutosnopeus pieni
    - Sovelluskoodi on vanhaa
    - Käyttöjärjestelmät ja kirjastot vielä vanhempia
    - OT järjestelmän suunnittelun lähtökohdat aivan jossain muualla
    - Toimittajariippuvuus
    - Käynnissäpidon tarpeet

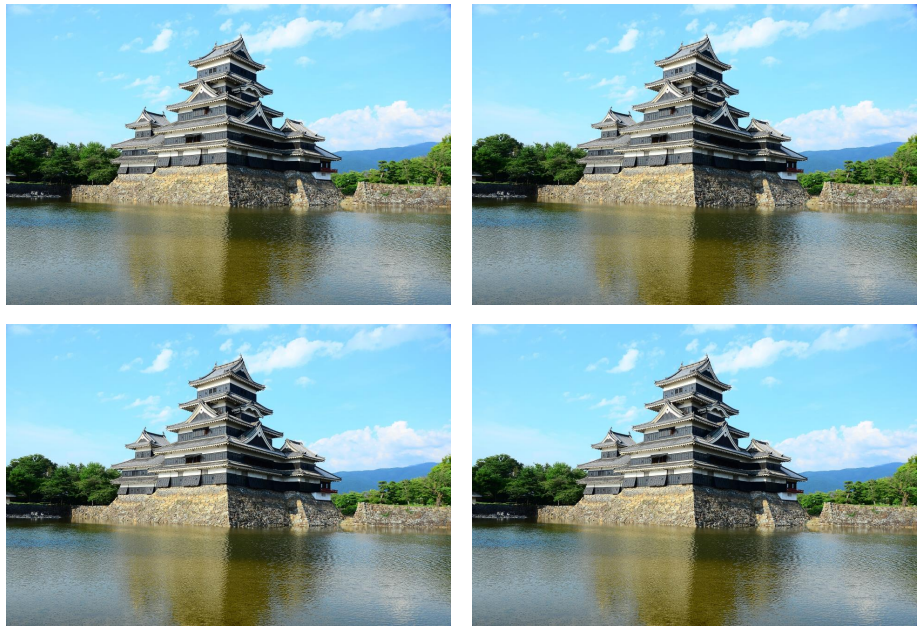
Varmentaminen

- Onko toiminto, jonka henkilö teki, oikeasti hänen tekemänsä?
- Toimintokohtaisesti, eli saako henkilö kirjoittaa tiedoston tiedostojakoon X
- Onko tietovuo sallittu?

Pienin mahdollinen pääsyoikeus

- Jokainen käyttäjä tai toiminto saa vain sen käyttöoikeuden jonka hän minimissään vaatii
- Pääkäyttäjäoikeuksien rajoittaminen
- Prosessinvalvonnan ja käyttötoiminnan oikeuksien rajaaminen järkeviksi
- Järjestelmien RBAC käyttöön

Segmentointi



- Siirtymä yhdestä todella vahvasta suojauksesta kohti hajautettua suojausta

Matsumoto niminen linna ja sen vallihauta
https://en.wikipedia.org/wiki/Moat#/media/File:Matsumoto_castle_3.jpg

Todentaminen

- Käyttötoiminta tai käynnissäpitotoiminnan toimenpiteiden vahva tunnistus
    - Käytännössä MFA lisäys kirjautumiseen
    - Huom! Ks. Haasteet
- MFA ylläpitotoiminnalle
- MFA toimittajayhteyksille

Valvonta

- Zero Trust valvonta tarkoittaa hallintakeinojen toiminnan todentamista
- Valvo siis
    - Pääsypyyntöjä
    - Pääsyoikeuksia
    - Segmenttien välistä liikennettä
    - Todentamisen toteutumista
    - Valvontaa

Zero Trust Mallin haasteet

- Saatavuus
  - PKI ja AAA tuovat uusia järjestelmiä, lisää järjestelmiä, jotka voivat pettää
- Kasvanut kompleksisuus
- Tarve koulutukselle kasvaa
- Pienet kohteet ja isot kohteet
  - Voimalaitos vs. pumppaamo
  - Sähköasema vs. muuntamo
- Huoltovarmuus ja vara-osien saatavuus
  - Jos kyseessä on
- Käyttö ja käynnissäpitotoiminnan haasteet
  - Vuoronvaihto?

Käytäntö 1 – Reitityksen suojaus

- Suojaaminen reitityksen keinoilla
  - Kun olet segmentoinut, reititä vain ne reitit jotka oikeasti tarvitset segmenttien välillä
    - Ei koskaan
      - ::/0
      - 0.0.0.0/0
- Eriytä eri verkot VRF:llä
  - Vaikka et käyttäisi MPLS verkkoja, reititystaulujen erotus suojaa virheiltä
  - Front-door VRF suojaa reitittimen ulkopintaa (WAN, VPN ja LAN eriytys)
  - Erillinen hallintaverkko = eri VRF
- Suojaa dynaaminen reititys, aina
- Myös NAT on reititystä, jos teet NAT:a, tee se defensiivisesti, ajattele hyökkääjää verkossa

Käytäntö 2 – Lähiverkon suojaus

- Perustoimenpiteet
    - Suojaa kytkimet itsessään
    - Valvo kytkimiä
    - Poista tarpeettomat portit pois käytöstä
    - Suojaa paikalliset konsolit yms.
    - Reititä jo lähiverkon kytkimellä jos mahdollista
    - Eriytä liikenne VLAN:lla, jos et voi reitittää
    - Älä koskaan levitä L2 Broadcast domaineja jos sinun ei tarvitse, etenkään toimintojen välillä
    - Vain 1 aliverkko per 1 VLAN ja vain 1 VLAN per 1 aliverkko
    - Dokumentoi portit myös konfiguraatioon
- Edistyneet toimenpiteet
    - Kerää Netflow dataa kytkimiltä
    - Tunnista liikenne
    - Hälytä muutoksista porteissa

Käytäntö 3 – Peruspalveluiden suojaus

- Suojaaminen DNS keinoilla
    - Ei koskaan DNS:ää, jos et tarvitse sitä
    - Jos tarvitset, split-brain ja vain tarpeellinen
    - Segmentoi DNS alueet. Esimerkiksi eri palvelimilla, jos palvelu ei tue split-brain toiminnallisuutta

- Pidä DHCP, DHCP-PD ja RA (ipv6) päällä, vaikka käyttäisit staattisia osoitteita
- Suojaa myös ipv6, sillä vain hyvin harvassa verkossa ei ole ipv6 liikennettä nykypäivänä, myös OT ympäristöissä on tämä tilanne
- NTP voi olla jo hyökkäysvektori, Zero Trustin myötä se on vielä suurempi riski
    - Toteuta luotettava aikasynkronointi joka perustuu useisiin lähteisiin ja teknologioihin
    - Valvo NTP laatua ja poikkeamia
    - Protokollasidonnaiset aikasynkronoinnit

Käytäntö 4 – Palomuuri

- Suojaaminen palomuurilla
  - Kaikki oletuksena estetty
  - Vai tunnettu, tunnistettu ja tiedetty liikenne sallittu
    - Vaadi toimittajaa selittämään jokainen portti ja protokolla
  - Selkeä sääntöpolitiikka, jossa on kommentit, aikaleimat ja selkeät liiketoimintatarpeet kuvattuna
- Suojaa muuri myös itsessään
- Valvo muuria, etenkin jos sinulla on enemmän kuin 1 muuri
- Jos et voi muurata, panosta IPS/IDS tuotteisiin, mutta yleensä hyöty-panos suhde voi olla pieni vs. palomuuri

Käytäntö 5 – Hallintayhteydet

- Hallitse
  - Toimittajayhteydet
  - Oman väen yhteydet
  - Paikalliset yhteydet (Engineering asemat yms.)
- Estä hyppiminen, vähintään hälytä
  - Arvioi hyöty poikkeustilanteissa
- Käytä SSH, RDP ja VNC yhteyksiin vähintään hyppypalvelinta/PAM ratkaisua
- Arvioi Hyppypalvelimen/PAM suojaaminen toisella kerroksella, esim. VPN:llä
- S2S/L2L VPN yhteydet tulee päättää DMZ:lle ja niiden lisäksi tulee käyttää hyppypalvelinta
- Estä suorat salaamattomat yhteydet, asenna hallintasovellukset/ylläpitotyökalut erilliselle palvelimelle

Käytäntö 6 – Linux suojaus

- Zero Trust periaatteet pätevät
    - Eriytä palvelut eri käyttäjätunnuksille
    - Varmista tiedostojen oikeudet
    - SELinux päällä ja enforcing tilassa, mielellään vielä oikeat politiikat käytössä
    - IPTables/IPFW päällä ja säännöt/chainit selkeinä, dokumentoituina ja vakioituina
    - Jos teet reititys/yms. suojausta itse palvelimella, vakioi ja dokumentoi
    - Ei koskaan root oikeuksin hallintaa, vain sudo ja vain PAM kautta
    - Käytä sertifikaatteja kirjautumiseen
    - Kerää syslog tietoa, hälytä poikkeamista
    - Älä asenna turhia asioita, vältä graafista ympäristöä, jos et tarvitse sitä
- Pidä myös ajan tasalla
- Vasta näiden jälkeen ala hienostella MDR/XDR tuotteilla ja muilla vastaavilla

Ajatuksia

- Kaikilla on testiympäristö, joillakin on onni omistaa erillinen tuotantoympäristö
    - @stahma, 2015 (4)
- Tietoturvan perusperiaatteet pätevät edelleen, valtaosa hyökkäyksistä perinteisiä (3)
- Suojaus paperilla on vain suojaus paperilla, vielä täysin tekemättä
- Tee suunnitelma ja lähde toteuttamaan sitä. Keskity olennaiseen määrittämällä olennainen ja sen jälkeen suojaamalla ensin se, sitten vasta muu
    - Liiketoimintamerkitys ja/tai eurot voivat olla hyvä lähtökohta (esim. KAH)
- Päivä kerrallaan, osa-alue tai toiminnallisuus kerrallaan. Ei kaikkea kerralla. (7)

Lähteet

1. https://www.welivesecurity.com/en/eset-research/mind-air-gap-goldenjackal-gooses-government-guardrails/
2. https://www.welivesecurity.com/2021/12/01/jumping-air-gap-15-years-nation-state-effort/
3. https://www.bleepingcomputer.com/news/security/cisa-hackers-target-industrial-systems-using-unsophisticated-methods/
4. https://x.com/stahnma/status/1348493763434291 20
5. https://www.opengroup.org/forum/security/Zerotrust
6. https://hub.dragos.com/hubfs/116-Whitepapers/ZeroTrust_OT_Environments_final.pdf?hsLang=en
7. https://media.defense.gov/2024/Mar/05/2003405462/-1/-1/0/CSI-ZERO-TRUST-NETWORK-ENVIRONMENT-PILLAR.PDF

Lopetus

Kiitos mielenkiinnosta!

Kysymyksiä? Kommentteja?

Kysyä voi myös jälkikäteen:
leo.mikonmaa@tampereenenergia.fi

Määritelmät eli termien merkitys