TLP:CLEAR

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Sähköverkkojen kyberturvallisuus-aspektit

SESKOn kevätseminaari 2023
30.3.2023

Yhteistyöryhmien tiedonvaihtokäytäntöjä - Traffic Light Protocol -käsittelyluokitus

- TLP:tä voidaan käyttää niin kokousten yhteydessä kuin yhteistyöryhmien välisessä tiedonvaihdossa ja viestinnässä.
- Käsittelyluokituksen toimivuuden kannalta on ensiarvoisen tärkeää, että tiedon vastaanottajat ymmärtävät tiedon käsittelylle asetetut reunaehdot ja toimivat osoitettujen ehtojen mukaisesti.
- Kyberturvallisuuskeskus noudattaa tiedonvaihdossaan Forum of Incident Response and Security Teams -yhteisön (FIRST) versio 2-määritelmää TLP:stä (FIRST Standards Definitions and Usage Guidance - Version 2.0) Käsittelyluokitusta käytetään useissa Kyberturvallisuuskeskuksen kansallisissa ja kansainvälisissä kyberturvallisuuden yhteistyöryhmissä.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/yhteistyoryhmien-tiedonvaihtokaytantoja

Jakelurajoitteen merkintä Traffic Light Protocolilla

- **TLP:CLEAR**: Ei jakelurajoitetta. Saa jakaa edelleen missä ja kenelle tahansa.
- **TLP:GREEN**: Yhteisön sisäinen jakelu. Ei saa laittaa julkisesti Internetiin.
- **TLP:AMBER**: Rajattu organisaation sisäinen ja sen välttämättömien sidosryhmien keskeinen jakelu. ”Perusteltu tarve tietää itsensä tai asiakkaansa suojaamiseksi”.
- **TLP:AMBER+STRICT**: Rajattu organisaation sisäinen jakelu. ”Perusteltu tarve tietää”.
- **TLP:RED**: Henkilökohtainen jakelu.

Kalvosetin jakelurajoite

TLP:CLEAR

- Tieto voidaan jakaa vapaasti.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/yhteistyoryhmien-tiedonvaihtokaytantoja

Joitakin sähköverkkojen kyberturvallisuusaspekteja

- Regulointi ja lainsäädäntö
- Standardisointi
- Viranomaiset
- Tietoturvallisuuden hallintajärjestelmät
- Kybermaturiteetin mittaus
- Uhkat
- Hyvät ja huonot käytännöt
- Varautumis- ja toipumissuunnitelmat
- Poikkeamanhallintaprosessit
- Omaisuudenhallinta
- Riskienhallinta
- Haavoittuvuuksienhallinta ja päivitykset
- Lokitus ja tietoturvamonitorointi
- Käyttäjienhallinta
- Etäyhteyksien turvaaminen
- Hyökkäyspinta-alan minimointi
- Järjestelmien eristäminen ja eriyttäminen
- Kustannustehokkaimmat kovennukset
- Tiedonvaihto ja yhteistyö
- Protokollien turvallisuus
- Tuotteiden elinkaaret
- ...

TLP:CLEAR

Kyberturvallisuuskeskus

TRAFICOM Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuus on...

- Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan
- Toimenpiteitä, joilla voidaan ennaltaehkäistä ja tarvittaessa sietää erilaisia kyberhäiriöitä ja niiden vaikutuksia
- Pitkälti tietoturvaa ja entistä enemmän myös tiedon luotettavuuden arviointia
- Digitaalisen ja fyysisen maailman hankauspinnassa
- Valtaosin ihmisten ohjaamaa toimintaa
  - Tilannekuva – missä olemme, mitä ympärillämme tapahtuu, minne olemme menossa

Kyberturvallisuuskeskus

- Olemme mukana rakentamassa maailman toimivinta ja turvallisinta digitaalista yhteiskuntaa.
- Huolehdimme, että suomalaisilla on käytössään toimintavarmat ja tietoturvalliset verkot ja palvelut.
- Turvaamme yhteiskunnan elintärkeitä toimintoja kyberturvallisuusuhkilta.
- Tarjoamme kansalaisille ja organisaatioille ajankohtaista ja luotettavaa tietoa kyberturvallisuudesta.
- Toimimme läheisessä yhteistyössä eri viranomaisten, yritysten, järjestöjen, kansainvälisten kumppanien kanssa ja oppilaitosten kanssa.

Kyberturvallisuuskeskus

- tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä
- ylläpitää kansallisen kyberturvallisuuden tilannekuvaa
- huolehtii viestintätoimialan varautumisesta normaaliolojen häiriötilanteisiin ja poikkeusoloihin
- edistää ja valvoo sähköisen viestinnän toimintavarmuutta
- tukee yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin
- toimii eurooppalaiseen Galileo-paikannusjärjestelmään liittyvän julkisesti säännellyn satelliittipalvelun (PRS) vastuuviranomaisena.

Palvelumme

- Tietoturvapalvelumme ovat pääsääntöisesti maksuttomia ja kuuluvat kaikille.
- Osa Kyberturvallisuuskeskuksen palveluista on suunnattu erityisesti tukemaan valtionhallinnon ja huoltovarmuuskriittisten organisaatioiden kyberturvallisuutta.
- Lisätietoa palveluistamme
  - kyberturvallisuuskeskus@traficom.fi
  - www.kyberturvallisuuskeskus.fi/fi/palvelumme

Tilannekuvatuotteita

- Haavoittuvuustiedotteet
- Haavoittuvuuskooste
- Kybersää
- News-uutiskirje
- Tietoturva Nyt! –julkaisut
- Toimialakohtainen tilannekuva ja tiedotteet
- Varoitukset
- Viikkoraportti
- Tietoturvan vuosi

- Saat tuotteet käyttöösi liittymällä toimialakohtaisille sähköpostilistoille.
  - Laita viestiä osoitteeseen kyberturvallisuuskeskus@traficom.fi
- Uutiskirjeen ja haavoittuvuuskoosteen voit tilata internet-sivuiltamme osoitteesta
  - www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

Toimialakohtaiset sähköpostilistamme

- Elintarvikeala
- Energia-ala
- Finanssiala
- ICT-ala
- Julkishallinto
- Kemia- ja prosessiteollisuus
- Kunnat
- Laite- ja tuotevalmistajat
- Logistiikka-ala
- Media-ala
- Puolustusteollisuus
- Teollisuusautomaatio
- Teollisuusyritykset
- Terveydenhuolto
- Tietoturvakonsultit ja -talot
- Tietoturvatutkijat
- Valtionhallinto
- Vesihuolto

Voit tiedustella listojen jäsenyyttä ja sisältöä sähköpostiosoitteesta: kyberturvallisuuskeskus@traficom.fi

Ohjeet ja suositukset

- Julkaisemme tietoturva-aiheisia ohjeita, oppaita ja vinkkejä niin organisaatioille, yksityishenkilöille kuin palveluiden ylläpitäjille.
  - Kyberturvallisuus ja yrityksen hallituksen vastuu
  - Pienyritysten kyberturvallisuusopas
  - Suojautuminen Microsoft Office 365 –tunnusten kalastelulta ja tietomurroilta
  - Näin suojaudut nettihuijaukselta
  - Turvallisesti netissä –opas lapsille
  - ... ja monia muita!
- Tutustu ohjeisiin ja oppaisiin osoitteessa
  - www.kyberturvallisuuskeskus.fi/fi/ohjeet

TLP:CLEAR

Haavoittuvuuskoordinaatio

- Autamme ohjelmistohaavoittuvuuden tai vakavan ohjelmistovirheen löytäjää tekemään yhteistyötä ohjelmistovalmistajan kanssa.
- Huolehdimme että tieto haavoittuvuudesta ja sen asianmukaisesta korjauksesta päätyy kaikille, myös tuotteen loppukäyttäjille.
- Käsitellemme löydöksiä vastuullisesti, koska niillä voi olla kauaskantoisia haittavaikutuksia ihmisten yksityisyyteen, omaisuuteen, liiketoimintaan ja jopa kansalliseen turvallisuuteen.
- Ota yhteyttä: vulncoord@traficom.fi

TRAFICOM

Harjoitustoiminta

- Tuemme yhteiskunnan toiminnan kannalta kriittisten yritysten kyberharjoittelua viranomaispalveluna.
- Harjoitustoimintaan liittyvät palvelumme:
  - Sopivan harjoitusyhteistyökumppanin löytäminen.
  - Ajankohtaiset tilannekuvapalvelut harjoituksen suunnittelun tueksi.
  - Tarkkailijan rooli harjoituksessa.
  - Avustaminen harjoituksen jälkianalyysissa.
- Lue lisää:
  - https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta
- Ota yhteyttä: kyberharjoitukset@traficom.fi

TLP:CLEAR

Kybermittari

- Kybermittari on organisaatioiden johdolle ja tietoturva-ammattilaisille suunnattu työkalu kyberturvallisuuden hallintaan.
- Arviointityökalun avulla organisaatio mittaa kypsyystasonsa kyberturvallisuuden hallinnan eri osa-alueilla. Kybermittari kertoo saavutetun kypsyystason ja esittää seuraavalle tasolle vaadittavat kehitysalueet.
- Organisaatio voi halutessaan jakaa mittaustuloksensa Kyberturvallisuuskeskukselle, joka anonymisoi tulokset ja tarjoaa organisaatiolle niiden pohjalta tuotettua toimialan vertailutietoa ja suosituksia.
- Tutustu kybermittariin: www.kybermittari.fi
- Ota yhteyttä: kybermittari@traficom.fi

TRAFICOM

TLP:CLEAR

HAVARO

- HAVARO–palvelu havainnoi suomalaisiin yrityksiin kohdistuvia vakavia tietoturvauhkia ja varoittaa niistä.
- Kyberturvallisuuskeskus tuottaa palvelun yhteistyössä valittujen palvelukeskuksien kanssa.
- Palvelu on ostettavissa palvelukeskuksilta.
- Palvelukokonaisuuden avulla organisaation verkkoliikenteestä havainnoidaan vakavia tietoturvauhkia, joilla on vaikutusta organisaation
  - kriittiseen tietoon
  - talouteen
  - liiketoiminnan jatkuvuuteen.
- Palvelu varoittaa asiakasta havaituista tietoturvaloukkauksista.
- Koostamme asiakkaalle varoituksia muualla havaituista uhkista sekä laadimme raportteja sen omasta ja toimialan tietoturvatilanteesta.
- Lue lisää: www.havaro.fi

TRAFICOM

TLP:CLEAR

Autoreporter

- Kyberturvallisuuskeskus ja teleyritykset torjuvat yhdessä haittaohjelmia Autoreporter-palvelun avulla.
- Järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta.
- Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen.

TRAFICOM

TLP:CLEAR

Tietoturvaneuvonta

- Valtionhallinnolle sekä huoltovarmuuskriittisille toimijoille tarkoitettu palvelu.
- Tietoturvaneuvontapalvelun tavoitteena on
  - varmistaa organisaatioiden tietoisuus kybertoimintaympäristön uhkista, sekä
  - tukea organisaatioita toimintansa ja järjestelmiensä turvallisuuden varmistamisessa.
  - tukea ja opastaa turvallisuusluokitellun aineiston suojaamiseen liittyvissä kysymyksissä.
- Ota yhteyttä: neuvontapalvelu@traficom.fi

TRAFICOM

Miten voisitte parantaa organisaationne tilannetta (tulosten pienentäminen ja havainnoista ilmoittamisen helpottaminen)?

TIETOTURVA NYT!

Noin 1000 automaatiolaitetta on yhä suojaamatta suomalaisissa verkoissa

Julkaistu 12.01.2021 13:13

Kartoitimme jälleen suomalaisten verkkojen turvallisuutta etsimällä verkosta suojaamattomia automaatiolaitteita. Vuonna 2020 havaitsimme niitä noin tuhat. Määrä ei juuri poikkea edellisvuoden tuloksista. Automaatiolaitteita ovat esimerkiksi automaation hallintajärjestelmät, erilaiset näyttöpaneelit ja kiinteistöjen hallintaan käytetyt järjestelmät.

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/noin-1000-automaatiolaitetta-yha-suojaamatta-suomalaisissa-verkoissa
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suojattomien-etatyopoyta-ja-verkkoyhteyspalveluiden-maara-kasvoi-maaliskuussa

RFC 9116 – auta valkohattuhakkereita ja viranomaisia raportoimaan haavoittuvuuksista!

- RFC 9116 julkaistiin huhtikuussa 2022.
- Verkkosivuston kansiorakenteesta löytyvä security.txt sisältää tiedot, henkilöt ja oikeat toimintatavat - linkit niihin haavoittuvuuksista ilmoittamiseen.
- Tiedosto löytyy yleensä lisäämällä verkkosivuston url-osoitteen perään: /security.txt
- Joissain tapauksissa saatetaan käyttää myös /.well-known/security.txt -rakennetta
  - esim. https://www.google.com/.well-known/security.txt

Lue lisää:

- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein
- https://www.ietf.org/rfc/rfc9116.txt

ISAC-tiedonvaihtoryhmät

- ISAC-tiedonvaihtoryhmät (Information Sharing and Analysis Centre) ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä.
- Ryhmät toimivat valtionhallinnon ja huoltovarmuuden kannalta kriittisten toimialojen parissa (mm. energia, SOTE ja finanssiala).
- Tiedonvaihtoryhmät mahdollistavat:
  - tietoturva-asioiden luottamuksellisen käsittelyn
  - organisaatioiden tietoturvaosaamisen lisäämisen
  - Kyberturvallisuuskeskuksen kokonaistilannekuvan kehittämisen
  - toimialan ja yhteiskunnan kyberturvallisuuden kehittämisen.
  - https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

ISAC-tiedonvaihtoryhmiä toimii seuraavilla toimialoilla

- Elintarviketuotanto ja -jakelu
- Energia-ala
- Finanssi
- HAVARO-käyttäjät
- ICT-toimiala
- Internet-palveluntarjoajat
- Kemia ja metsäteollisuus
- Logistiikka ja liikenne
- Media
- SOTE
- Valtionhallinto
- Vesihuolto

Kyber- ja informaatiovaikuttamisen suhde

- Kyberin ja informaatiovaikuttamisen keinoja käytetään myös samanaikaisesti vahvistamaan suunnitellun toimenpiteen vaikuttavuutta.
- Suomessa on pitkät perinteet laaja-alaisesta yhteistyöstä varauduttaessa kyberuhkiin. Huomattavan osan yhteiskunnan kriittisistä palveluista tuottavat erilaiset yritykset. Nämä tekevät yhteistyötä keskenään ja viranomaisten kanssa. Uhkiin varaudutaan ja niitä torjutaan joka päivä. Tarvittaessa otetaan käyttöön varajärjestelyjä.
- Samoin informaatiovaikuttamiseen vastaamisessa eri toimijat tekevät yhteistyötä ja erilaisiin uhkiin varaudutaan. Pohjana on kokonaisturvallisuuden yhteistoimintamalli. Yhteiskunnan turvallisuus kuuluu kaikille.

Kyber- ja informaatiovaikuttamisen suhde

- Lisää tietoa:
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyber-ja-informaatiovaikuttaminen-saman-kolikon-kaksi-puolta
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vinkkeja-informaatiovaikuttamisen-tunnistamiseksi-ole-tarkkana-ja-toimi
  - Informaatiovaikuttamiseen vastaaminen : Opas viestijöille https://julkaisut.valtioneuvosto.fi/handle/10024/161512
  - Kyber- ja informaatiovaikuttaminen - mitä minun on hyvä tietää? https://youtu.be/L5oW0MJNZeE
  - Traficom Live – info – ja kybervaikuttaminen https://youtu.be/rFs-gyjpnek

Tietoturvamerkki

- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen myöntämä Tietoturvamerkki kertoo siitä, että merkillä varustettu tuote tai palvelu on jo lähtökohtaisesti suunniteltu tietoturvalliseksi ja täyttää Traficomin asettamat tietoturvavaatimukset.
- Merkkiä käytetään älykkäissä kuluttajalaitteissa, jotka yhdistetään internetiin eli ns. IoT-laitteissa. Näitä laitteita ovat esimerkiksi älytelevisiot, älyrannekkeet ja kodin reitittimet.
- Tutustu Tietoturvamerkkiin: https://tietoturvamerkki.fi

Koordinointi ja avunanto tietoturvaloukkauksissa

- Tarjoamme apua tietoturvaloukkauksen selvittämiseen ja tutkimiseen sekä koordinoimme tarvittavia toimenpiteitä.
- Käsittelemme kaikki tapaukset luottamuksellisesti.
- Toimenpiteet voivat pitää sisällään
  - tiedon jakamista
  - yhteistyökumppanien ja -verkostojen kontaktointia
  - teknistä analyysiä
  - lainopillista neuvontaa.

TLP:CLEAR

Kybersää helmikuu 2023

Tietomurrot ja -vuodot

- PowerApps-pohjaiset kalastelut aiheuttivat edelleen merkittäviä määriä tietomurtoja. MFA:lla on helppo suojautua ilmiöltä.
- Rikolliset seuraavat julkaistuja haavoittuvuusilmoituksia aktiivisesti, ja pyrkivät hyödyntämään haavoittuvuuksia tehdäkseen tietomurtoja.

Huijaukset ja kalastelut

- Vuokranmaksuhuijauksilla yritettiin saada maksamaan vuokra huijarin tilille.
- Finanssiala kertoo, että vuonna 2022 pankkitunnuskalastelulla suomalaisilta huijattiin 10 miljoonaa euroa.

Haittaohjelmat ja haavoittuvuudet

- Helmikuun alussa maailmalla levisi aggressiivisesti VMWare ESXi -ohjelmiston haavoittuvuutta hyödyntävä kiristyshaittaohjelmakampanja.
- Päivitystiistai toi korjauksia lukuisiin haavoittuvuuksiin, joukossa oli myös nollapäivähaavoittuvuuksia.

Automaatio ja IoT

- Julkaisimme ohjeen teollisuusautomaation tärkeimmistä kyberturvallisuuskontrolleista.

Verkkojen toimivuus

- Helmikuussa yleisissä viestintäpalveluissa oli yksi merkittävä toimivuushäiriö.
- Ilmoitettujen palvelunestohyökkäysten määrä on laskenut selvästi loppuvuodesta.
- Osa hyökkäyksistä aiheutti lieviä vaikutuksia palveluiden saatavuuteen.

Vakoilu

- Euroopan unionin kyberturvallisuusvirasto (ENISA) ja CERT-EU julkaisivat yhdessä raportin varoittaakseen tiettyjen uhkatoimijoiden jatkuvasta toiminnasta.
- ENISA ja CERT-EU kannustavat voimakkaasti kaikkia julkisen ja yksityisen sektorin organisaatioita EU:ssa soveltamaan julkaisussa lueteltuja suosituksia.

TRAFICOM Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TLP:CLEAR

Esimerkkejä

TLP:CLEAR

Automaatio (Kybersää 04/2022)

- Kriittisen infrastruktuurin käyttämiin automaatiolaitteisiin suoraan kohdistettuja haittaohjelmia on havaittu vuoden 2010 Stuxnet-tapauksen jälkeen verrattain vähän.
- Tuoreiden havaintojen perusteella suoraan automaatiojärjestelmiin suunnatut kyberuhat olisivat kuitenkin lisääntymässä.
  - FBI varoitti aiemmin keväällä, että kyberrikolliset kehittävät suoraan automaatioympäristöihin suunnattuja haittaohjelmia.
  - Ukraina ilmoitti torjuneensa maassa kahden miljoonan ihmisen sähkönjakeluun kohdistetun automaatiohyökkäyksen, jossa yritettiin käyttää Industroyer.v2 -haittaohjelmaa.
  - Tietoturvayritykset ilmoittivat löytäneensä joukon työkaluja, jotka helpottavat kyberoperaatioita eri valmistajien automaatioympäristöissä. Ne mahdollistavat myös näiden ympäristöjen turvajärjestelmiin vaikuttamisen vaarantaen siten pahimmillaan myös ihmisten turvallisuuden.

Analyysi

- Aiemmin myös kriittisen infrastruktuurin organisaatioiden tietoturvapoikkeamat ovat lähes poikkeuksetta kohdistuneet näiden perustietotekniikkaan.
- Automaatioympäristöjen monimutkaisuus ja yksilölliset ratkaisut ovat saattaneet suojata niitä, koska kyberrikolliset ovat saaneet saman tuoton helpommin toimistoympäristöistä.
- Tilanteessa on nähtävissä nyt muutoksen merkkejä kriittisen infrastruktuurin merkityksen korostuessa geopoliittisten jännitteiden lisääntymisen myötä.
- Eri maiden asevoimat panostavat nyt myös voimakkaasti kriittiseen infrastruktuuriin suunnattujen kyberaseiden kehittämiseen.

TRAFICOM

IoT (Kybersää 11/2022)

- Vanhoja haavoittuvuuksia lymyää IoT-laitteissa.
  - IoT-laitteiden yhteydessä valmistajat suhtautuvat välinpitämättömästi tietoturvapäivityksiin. Kriittisiä haavoittuvuuksia sisältävä laite muodostaa aina riskin esimerkiksi yrityksen verkkoympäristölle.
  - Tästä ongelmasta saatiin ennätyksiä hipova esimerkki, kun Microsoft nosti raportissaan esille monissa IoT-laitteissa sisäisesti hyödynnetyn ”Boa” web-palvelimen. Sen kehitys on lopetettu vuonna 2005 eikä siihen ole julkaistu tietoturvapäivityksiä sen jälkeen.
    - Raportin mukaan esimerkiksi siruvalmistaja Realtek on paketoinut tämän vanhan ja erittäin haavoittuvan sovelluksen IoT-laitteita valmistaville asiakkailleen suunnatun sovelluskehitysalustan sisään.
    - Laaja haavoittuvien laitteiden määrä tekee niistä houkuttelevan kohteen esimerkiksi bottiverkkoja operoiville kyberrikollisille.
    - Intialaiseen Tata Power energiayhtiöön tehtiin lokakuussa tietomurto näitä haavoittuvuuksia hyödyntäen.

Analyysi

- Mikä tahansa haavoittuva sekä tavalla tai toisella julkisesta verkosta tavoitettavissa oleva IoT-laite nostaa tietomurron riskiä.
  - IoT-laitteet ovat nykyään täysiverisiä tietokoneita, joihin päässyt rikollinen voi hyödyntää niitä monella tavalla. Rikollinen voi esimerkiksi valjastaa laitteen palvelunestohyökkäyksiä tekevän bottiverkon osaksi. Toisen rikollisen tavoitteena saattaakin olla IoT-laitteen hyödyntäminen lopulta kiristyshaittaohjelmaan päätyvässä tietomurrossa.
- Kaikkien IoT-laitteita hankkivien tahojen tulisi aina arvioida myös niiden tietoturvaa ennen ostopäätöstä. Suhtautuuko valmistaja vakavasti tietoturvaan? Onko tietoturvapäivityksiä saatavilla?
- Kyberturvallisuuskeskuksen Tietoturvamerkki kertoo siitä, että valmistaja on sitoutunut varmistamaan tuotteen tietoturvallisuuden ja tarjoamaan siihen tietoturvapäivityksiä merkin voimassaoloajan.

TLP:CLEAR

Top 5 uhat lähitulevaisuudessa
(6kk–2v)

1.

Talouden ja politiikan ilmiöt heijastuvat myös kyber-turvallisuuteen.

Ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia kyberturvallisuudessa.

2.

Suomeen kohdistunut kyberympäristön uhkataso on edelleen kohonneella tasolla.

Kohonneen uhkatason vuoksi organisaatioiden varautumisen merkitys korostuu.

3.

Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.

Esimerkiksi käyttäjäoikeuksien hallinta, ohjelmistojen ajantasaisuuden ylläpito ja hyvä tietoturvakulttuuri ovat kyberturvallisuuden kivijalkaa.

Uusi

Päivitetty

Symbolit

4.

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä.

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

5.

Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Tarve kyberturvallisuuden osaajille monipuolistuu. Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta osaajille.

TRAFICOM Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TLP:CLEAR

1. Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen

Muutokset kansainvälisessä turvallisuustilanteessa on huomioitava organisaatioiden jatkuvuuden- ja riskienhallinnassa. Riskienhallinnan ja jatkuvuussuunnittelun tulee reagoida turvallisuusympäristön muutoksiin.

- Venäjän hyökkäys Ukrainaan heijastuu myös kyberturvallisuuteen. Esimerkiksi sodan aiheuttamat muutokset talouteen, energian hinnan nopea nousu ja informaatioympäristön herkkyys näkyvät vaikeasti ennakoitavina kehityskulkuina, jotka ulottuvat myös digitaaliseen maailmaan.
- Valtioiden ja organisaatioiden päätökset altistavat entistä helpommin vaikuttamiselle, kuten mielenilmauksena tehdyille palvelunestohyökkäyksille.
- Energiamarkkinoiden häiriöt voivat vaikuttaa myös kyberturvallisuuteen. Kriittiseen infrastruktuuriin vaikuttaminen voi näkyä myös kyberympäristön häiriöinä Euroopassa.
- Organisaatioiden on tärkeää tunnistaa oman toimintaympäristönsä riskitekijät. Niillä voi olla isoja vaikutuksia organisaatioiden päivittäiseen toimintaan. Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön muutokset ja sen aiheuttamat uhkat kriittisille prosesseille.

TLP:CLEAR

1. Case: Palvelunestohyökkäykset lisääntyivät merkittävästi vuonna 2022

Palvelunestohyökkäysten määrä lisääntyi niin Suomessa kuin Euroopassakin vuonna 2022. Myös niiden käyttötapa poliittisena mielenilmauksena korostui.

Palvelunestohyökkäyksiä tekevien tahojen motiivit ja kyvyt vaihtelevat runsaasti. Suurimmassa osassa palvelunestohyökkäyksiä vaikutukset ovat olleet pieniä, ja hyökkäyksiä käytetäänkin paljolti mielenilmauksena esimerkiksi valtion tai muun tahon päätösten vuoksi. Palvelunestohyökkäysten taustalla on yhä useammin erilaisia haktivistiryhmiä, jotka toimivat ilman selkeää keskitettyä ohjausta.

Palvelunestohyökkäysten lisääntynyt trendi tulee todennäköisesti jatkumaan, eikä ilmiötä lieventäviä tekijöitä ole nähtävissä. Organisaatioiden riskienhallinta, varautuminen ja harjoittelu ovat avainasemassa uhkiin varautumisessa. Kyberturvallisuuskeskus tarjoaa varautumiseen useita ohjeita.

TLP:CLEAR

2. Suomeen kohdistunut kyberympäristön uhkataso on edelleen kohonneella tasolla.

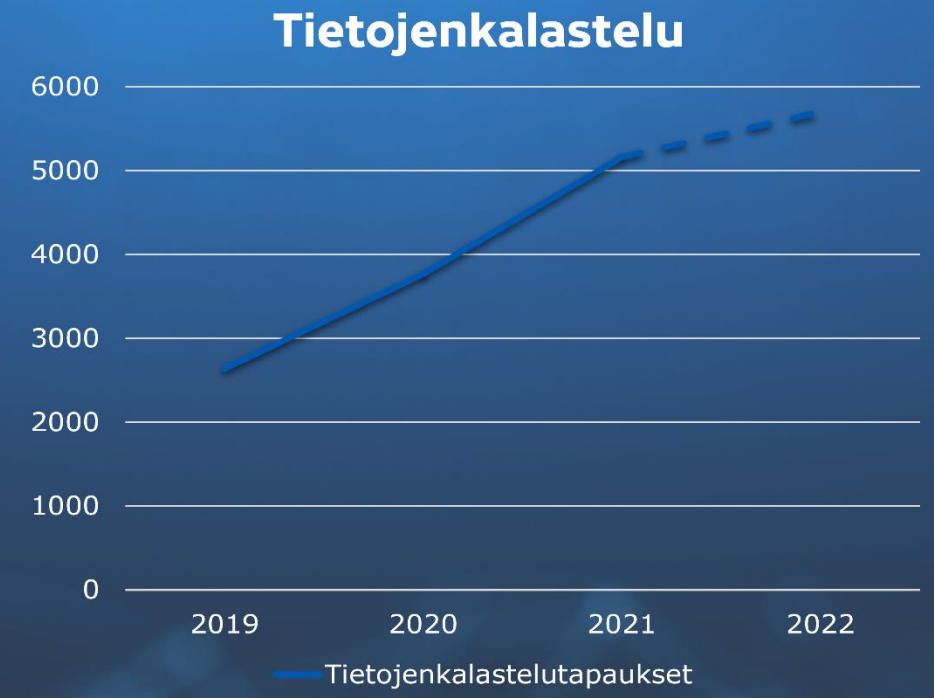
Kyberhyökkäykset ovat lisääntyneet maailmanlaajuisesti vuoden 2022 aikana, ja Suomessa havaitut ilmiöt noudattelevat kansainvälisiä trendejä.

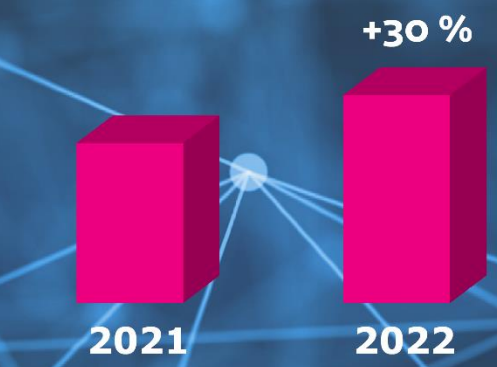
- Merkittävä uhka organisaatioille ovat kiristyshaittaohjelmat, joiden määrä kasvaa jatkuvasti. Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi.
- Erityisesti huoltovarmuuskriittisten organisaation joutuessa kiristyshaittaohjelman uhriksi yhteiskunnan elintärkeät toiminnot voivat vaarantua.
- Suojelupoliisi on todennut kansallisen turvallisuuden katsauksessaan kriittiseen infrastruktuuriin kohdistuvan tiedustelun ja vaikuttamisen uhkan pysyvän kohonneena lähitulevaisuudessa.
- Vaikka tavanomaisten kyberhyökkäysten määrä on kokonaisuudessaan kasvanut, myös mm. kohdennetut tietojenkalasteluviestit ja murtautumisyritykset ovat lisääntyneet.
- Tutustu Kyberturvallisuuskeskuksen tiedotteeseen kohonneesta kyberuhkatasosta.

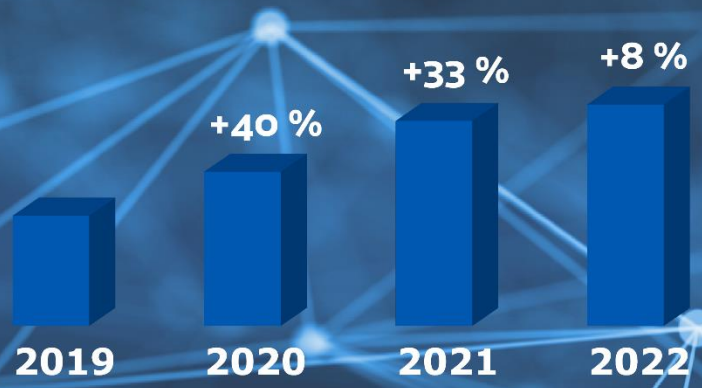
TLP:CLEAR

Tapausten luonne vaikuttaa uhkatason nousuun

- Tietojen kalastelu kasvaa selvästi vuosittain.
- Vuonna 2021 kalasteluviestien määrä kasvoi 33% vuodesta 2020.
- Vuonna 2022 kasvun lisäksi kalastelut ovat olleet kohdennetumpia ja kohdistuneet kriittiseen infrastruktuuriin.
- Kiristyshaittaohjelmahyökkäysten määrät liikkuvat muutamissa kymmenissä tapauksissa vuosittain. Määrä on kasvanut noin 30% viime vuoden vastaavaan ajankohtaan verrattuna.
- Hyökkäykset ovat olleet aiempaa räätälöidympiä ja tarkoituksella kohdistettu tiettyyn suomalaiseen organisaatioon.







TRAFICOM
Liikenne- ja viestintävirasto
Transport- och kommunikationsverket
Finnish Transport and Communications Agency

https://www.traficom.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

3. Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.

Organisaation kyberturvallisuuden kivijalka rakennetaan arkisilla kyberturvallisuuden toiminnoilla. Suurin osa tietoturvapoikkeamista olisi vältettävissä tavanomaisilla keinoilla, kuten ohjelmistopäivityksillä, hyvillä salasanakäytänteillä ja tietoturvakulttuurilla.

- Käyttöoikeuksien kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi.
- Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon saatetaan jättää auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu.
- Tietojen kalastelu on edelleen helppo ja yleinen tapa rikolliselle pyrkiä organisaatioon sisälle. Tietoisuuden lisääminen organisaatiossa auttaa tunnistamaan epäilyttävän toiminnan.
- Suurin osa loppuvuonna 2022 tapahtuneista tietoturvapoikkeamista olisi ollut estettävissä hyvin arkisella kyberturvallisuuden hallinnan ylläpidolla.
- Kyberturvallisuuskeskus tarjoaa organisaatioille runsaasti käytännön ohjeita kyberturvallisuuden parantamiseksi.

4. Toimitus- ja palveluketjujen tietoturva ja jatkuvuus on yhä kriittisempää.

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

- Organisaatioiden on keskeistä ymmärtää omat alihankkijaketjunsa. On tärkeä selvittää kolmannen osapuolen tietoturvan taso ja ulottaa tietoturvallisuuden hallinta myös palveluihin. Esimerkiksi:
  - Konsultit ja heidän oman organisaation sisäiset järjestelmät.
  - Laitteistot ja palvelut joita voidaan käyttää joko osana omaa tuotetta tai palvelukokonaisuutena, tai ostettuna palveluna.
  - Organisaation tulee ymmärtää alihankinnanketju, koska myös alihankkija voi hankkia tuotteen/palvelun seuraavalta ketjussa olevalta palveluntarjoajalta.
- Organisaation tulisi kartoittaa, mistä osista sen eri palvelut muodostuvat, jotta ison kokonaisuuden voi hahmottaa. Esimerkiksi pilvipohjaista palvelua hankkiessa tällaisen tekeminen on oleellista.
- On hyvä ymmärtää, että käytettävien palvelujen kautta voidaan murtautua organisaation, jos kyberturvallisuutta ei ole huomioitu.

TLP:CLEAR

5. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta erilaisille osaajille.

- Yritykset eivät etsi pelkkiä koodareita. Tulevaisuudessa laaja-alaisemmalle digitalisaation, kyberturvallisuuden ja datan osaamiselle on entistä enemmän kysyntää.
- Osaamisen saaminen riittävälle tasolle kestää vielä pitkään. Organisaatioiden kyberturvallisuus vaarantuu, mikäli osaavaa henkilöstöä ei ole tarpeeksi saatavilla.
- Arviomme mukaan lyhyen aikavälillä tarvitaan erityisesti teknisiä osaajia, jotka osallistuvat tietoturvatutkintaan sekä ennaltaehkäisevään työhön.
- Pitkällä aikavälillä osaajatarve monipuolistuu ja esimerkiksi hallinnollisia osaajia tarvitaan lisää.
- Osaajapula ei ole kiinni määrästä vaan laadusta! Osaaminen ei saisi henkilöityä liikaa, jotta jatkuvuus voidaan turvata kaikissa tilanteissa. Organisaation tietoturvan hallinta tulee osallistaa ja kouluttaa osaksi kaikkien työntekijöiden päivittäistä toimintaa.
- Johdon tulee ymmärtää ja varmistaa riittävä osaaminen organisaatiossa kyberturvallisuusosaajien kysynnän kasvaessa. On tärkeää miettiä, millaista asiantuntemusta tarvitaan nyt ja tulevaisuudessa, sekä miten se hankitaan.

TLP:CLEAR

Kiristyshaittaohjelmat

Kiristyshaittaohjelmat

- Erityisen merkittävä uhka on kiristyshaittaohjelmahyökkäykset, joiden kohteeksi voi joutua kuka tahansa pienestä konepajasta kansainväliseen high tech -jättiin.
  - Hyökkäyksessä kohdetta kiristetään tietojen salaamisella. Salauksen purkamisesta vaaditaan lunnasmaksu.
  - Lisäksi voidaan kiristää lisäksi hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse.
- Varmuuskopiot, päivitykset!
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/edistyneet-kiristyshyokkaykset-yleistyvat-varo-joutumasta-saaliiksi

```
1  All of your files are currently encrypted by CONTI ransomware.
2  If you try to use any additional recovery software - the files might be damaged or lost.
3
4  To make sure that we REALLY CAN recover data - we offer you to decrypt samples.
5
6  You can contact us for further instructions through our website :
7
8  TOR VERSION :
9  (you should download and install TOR browser first https://torproject.org)
10
11 http://[redacted].onion
12
13 HTTPS VERSION :
14 https://contirecovery.info
15
16 YOU SHOULD BE AWARE!
17 Just in case, if you try to ignore us. We've downloaded your data and are ready
18  to publish it on out news website if you do not respond. So it will be better
19  for both sides if you contact us ASAP.
20
21 ---BEGIN ID---
22 7c85vpfYlRYHIA03SjFhX3oDfk2uTNlCQ8IROOMM33gL1FASiKPeodbG1K5YULtD
23 ---END ID---
```

Kuva: https://blog.malwarebytes.com/detections/ransom-conti

Esimerkki kiristyshaittaohjelmahyökkäyksestä

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Johdon_kiristyshaittaohjelmaohje.pdf

TLP:CLEAR

Ratkaisut

Ulkoisten kyberuhkien olemassaololle emme voi oikeastaan mitään.

- Johtamisessa huomio tulisi kiinnittää **kaikkien liiketoimintojen tarvitsemien digitaalisten palveluiden** suojaamiseen sekä niiden kyberhäiriöiden sietokyvyn parantamiseen.
- Toteutunut tietomurto aiheuttaa liiketoimintatappioita, mainehaittaa, tietoturvakonsulttien palkkioita ja muita toipumiskustannuksia sekä mahdollisia sanktioita. **Ennaltaehkäisyyn panostaminen kannattaa!**

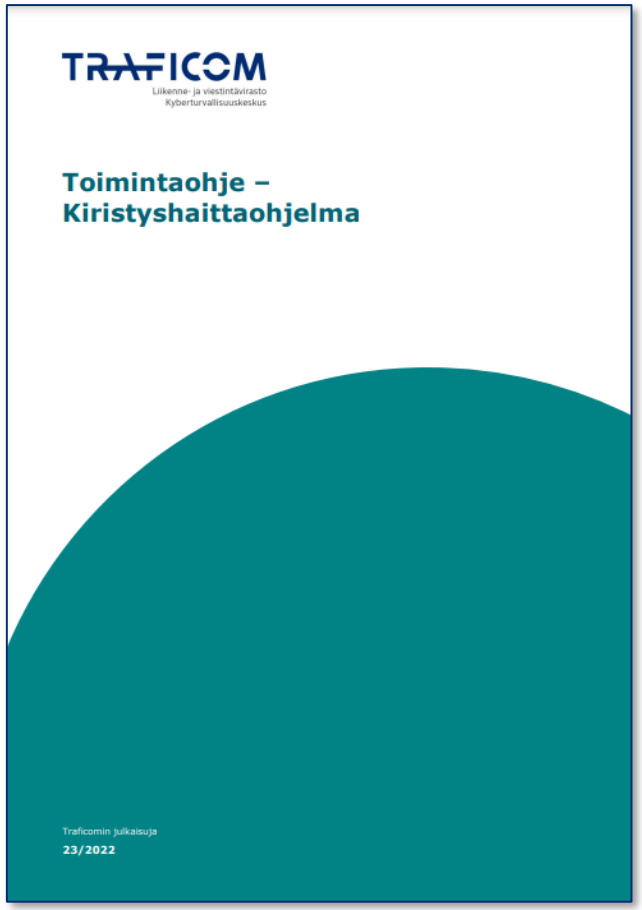
Toiminta kiristyshaittaohjelmatilanteessa – johdon ohje

- Riski kiristyshaittaohjelman kohteeksi joutumisesta on kasvanut viime vuosina merkittävästi. Uusi ohjeemme antaa neuvoja tilanteessa, jossa kiristyshaittaohjelma uhkaa organisaation toimintaa.
- Ohjeen tavoitteena on antaa organisaatioiden ylimmälle johdolle opastusta kiristyshaittaohjelmatilanteessa toimimiselle.
- Ohjeessa keskitytään erityisesti toimintaan kiristyshaittaohjelman aiheuttaman kyberhyökkäyksen tapahtuessa, mutta siinä käsitellään myös tärkeimpiä varautumistoimenpiteitä ja tilanteen jälkeen tehtäviä jälkitoimia.
- Ohje on tarkoitettu kaikille suomalaisille organisaatioille kyberturvallisuuden vahvistamiseen riippumatta organisaation koosta, tai siitä millä tasolla niiden oma varautuminen on.
- Ohjeen valmistelussa on tehty yhteistyötä poliisin kanssa.

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Johdon_kiristyshaittaohjelmaohje.pdf
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusi-ohje-auttaa-kiristyshaittaohjelman-kohteeksi-joutunutta-organisaatiota
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/toiminta-kiristyshaittaohjelmatilanteessa-johdon-ohje

Toimintaohje - kiristyshaittaohjelma

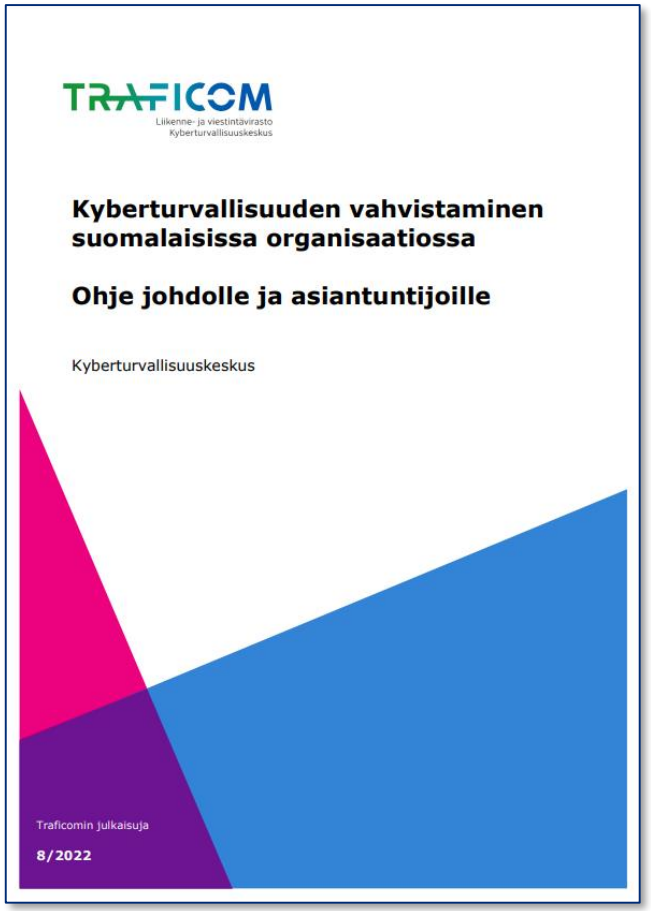
- Ohjeen tarkoituksena on neuvoa organisaatioita tilanteissa, joissa epäillään kiristyshaittaohjelman aiheuttamaa hyökkäystä tai kiristyshaittaohjelma estää normaalin toiminnan.
- Ohje keskittyy tämän tietoturvallisuuden poikkeamatyypin erityispiirteiden käsittelyyn.
- Tilanteen ratkaisemiseksi kokonaisuudessaan organisaation on hyvä ylläpitää ja noudattaa laatimaansa hallintasuunnitelmaa tietoturvapoikkeamatilanteita varten (engl. Incident Response Plan).
- Ohje opastaa yleisellä tasolla tietoturvaloukkaustilanteessa toimimista ja siitä toipumista.
- On suositeltavaa, että organisaatio laatii itselleen erillisen oppaan, joka huomioi sen oman teknisen ja toiminnallisen ympäristön tarkemmalla tasolla. Projektin on rahoittanut Huoltovarmuuskeskus.



https://www.kyberturvallisuuskeskus.fi/fi/ohjeet
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/KiristyshaittaohjelmaToimintaohje.pdf

Kyberturvallisuuden varautuminen tehdään hyvän sään aikaan - ohje organisaatioille

- Ohje keskittyy kolmeen osa-alueeseen:
  - Kyberturvallisuuden johtaminen
  - Kyberturvallisuuden kontrollit
  - Havainnointi, reagointi ja toiminnan jatkuvuus



Varaudu kyberturvallisuuden poikkeamia varten

- Varautumisen ohjenuoraksi tarvitaan määritelty, ylläpidetty, dokumentoitu ja harjoiteltu **poikkeamanhallintaprosessi**.
- Käytännössä tämä tarkoittaa sitä, miten tuotantoympäristöjen **kyberpoikkeamia** pystytään **havaitsemaan**, **analysoimaan**, miten niihin **vastataan** ja miten poikkeamista **palaudutaan**.
- Havaitsemisen kannalta olennaista on kyky **analysoida tietoliikennettä**.
- Poikkeamien **juurisyy** pitäisi pystyä aina löytämään.
- **Lokit** on kerättävä kattavasti. Lokitiedot on hyvä kerätä keskitettyyn paikkaan, jotta havaintoja voidaan korreloida ja aggregoida.
- Kyberturvallisuuskeskuksen kehittämä Kybermittari auttaa yritystä hahmottamaan kykyään torjua kyberuhkia.

Suunnitelkaa järjestelmäarkkitehtuurit puolustuskyvyn ehdoilla

- **Pienentäkää** riskien **todennäköisyyttä**.
- **Pienentäkää** riskien **vaikuttavuutta**.
- **Helpottakaa** järjestelmien **puolustamista**.
- Suojaavien tietoturvakontrollien käyttöönottamista ja hallintaa on hyvä tukea jo **arkkitehtuurin suunnitteluvaiheessa**.
- Tärkeitä tuettavia tietoturvakontrolleja ovat mm. **lokien kerääminen**, **näkyvyys** ja fyysiset tai loogiset **aliverkot**.
- Hyvin tehty verkkoympäristöjen **eriyttäminen** ja **eristäminen** toisistaan helpottaa ympäristön suojaamista, estää rikollisten vapaata liikkumista tietomurron jälkeen ja tarjoaa paremman mahdollisuuden valvoa ympäristöihin tulevaa ja niistä lähtevää liikennettä kuten myös tuotantoympäristöjen sisäistä liikennettä.

Hankkikaa näkyvyys sähköverkkoihin

- **Puutteellinen näkyvyys** tuotantoympäristöjen tietoliikenteeseen ja laitteisiin aiheuttaa haasteita havaita ja tutkia poikkeamia, saati ylläpitää tarkkaa omaisuusluetteloa.
- **Omaisuusluettelon** puute vastaavasti tekee riskienhallinnasta vaikeaa, ellei mahdotonta.
- Näkyvyyden varmistaminen rikkomatta verkkojen eristämistä toisistaan vaatii erityistä huolellisuutta.
- Näkyvyyttä voidaan saada mm. verkkoliikennettä, komentoja ja lokeja monitoroimalla.
- Kyberturvallisuuskeskuksen Lauttatonttu-projektissa vuonna 2021 mm. kartoitettiin verkon suojattavia kohteita ja hälytettiin havaituista odottamattomista suojaamattomista kohteista.
- Suosittelemme seuraamaan tulevia Tonttu-projekteja aiheeseen liittyen!

Hallitkaa haavoittuvuuksia riskiperustaisesti

- **Riskiperustainen** haavoittuvuuksien hallinta vaatii ajantasaisen **omaisuusluettelon** ja kyvyn **priorisoida** haavoittuvuudet ja järjestelmät.
- Hyödyntäkää **ohjelmistolistausta** (SBOM), mikäli se on saatavilla laite- ja järjestelmävalmistajannne tuotteista.
- Voitte arvioida **Kybermittari**-työkalulla organisaationne kykyä kyberuhkien ja -haavoittuvuuksien hallintaan suhteessa organisaatioon kohdistuviin riskeihin ja organisaation tavoitteisiin.
- Automaatiojärjestelmien valmistajat ilmoittavat valitettavan harvoin haavoittuvuustiedotteissaan muita hallintakeinoja kuin haavoittuvan ohjelmiston päivittämisen.
- Ohjelmistopäivitykset voivat olla mahdollisia vain tuotannon seisokin aikana.
  - Riskejä pitäisi pystyä jotenkin pienentämään jo haavoittuvuustiedotteen julkaisun ja seisokin välisenä aikana.
- Monissa tuotantoympäristöissä haavoittuvien järjestelmien päivitykset voi tehdä vain järjestelmätoimittajan henkilökunta, minkä takia järjestetään etäyhteydet.

Asentakaa tietoturvapäivitykset viipymättä julkisesti tavoitettavissa oleviin palveluihin

- **Tietoturvapäivitykset tulee asentaa viipymättä** erityisesti kaikkiin **julkisesta** verkosta tavoitettavissa oleviin digitaalisiin palveluihin.
- Rikolliset pyrkivät yleisesti hyödyntämään **myös päätelaitteiden** haavoittuvuuksia. Siksi erityisesti käytössä olevien laitteiden **käyttöjärjestelmät, toimisto-ohjelmistot sekä selaimet tulisi aina päivittää viipymättä**.
- Kaikkein suositeltavinta on ottaa käyttöön automaattiset päivitykset, mikäli se on vain mahdollista.
- Kartoittamalla julkiseen verkkoon näkyvät palvelut, pitämällä ne ajan tasalla ja rajoittamalla niihin pääsyä, **hyökkäyspinta-alaa saadaan pienennettyä** merkittävästi.

Varmistakaa etäkäytön turvallisuus

- Turvallisen etäkäytön avulla **vain tunnistetut ja hyväksytyt käyttäjät** pääsevät ottamaan **sallitulla tavalla** yhteyksiä tuotantoympäristöihin.
- Älkää käyttäkö samoja käyttäjätunnuksia tietotekniikka- (IT) ja tuotantotekniikkapuolella (OT). Käyttäkää vahvoja salasanoja.
- Monivaiheista todentamista (MFA) voidaan soveltaa turvallisesti useimmissa tuotantoympäristöissä.
- Hyödyntäkää **sessiopohjaisia kirjautumia**. Määrittäkää etäyhteyden pituudelle ja järjestelmien käytölle aikarajat.
- Sopikaa kommunikoinnille luotetut tavat.
- Turvatkaa yhteydet hyödyntämällä SSH:ää **avaimilla**, VPN:ää tai vastaavia tietoturvaratkaisuja mahdollisuuksien mukaan. Muistakaa **hyppykoneet**.
- Käyttäkää palomuureja eriyttämään verkot, järjestelmiin ei saa olla pääsyä suoraan Internetistä. Muistakaa **Purdue–malli**.
- Kyberturvallisuuskeskuksen havaintojen mukaan turvaton etäkäyttö liittyy toisinaan ongelmiin verkkojen eristämisessä.
- **Virheet palomuurisääntöjen suunnittelussa ja muokkaamisessa** saattavat tarjota suojatuiksi tarkoitettuja etäkäyttöpalveluita tai erilaisia laitteiden ja palveluiden kirjautumisikkunoita näkyville julkisesti Internetiin.
- Varmistukaa myös **varayhteyksistä**.

Vaihtakaa vakiosalasanat ja ottakaa käyttöön monivaiheinen tunnistautuminen

- Salasanat voivat joutua **monin** eri tavoin rikollisten haltuun.
- Etenkin ulkoisista verkoista tavoitettavien järjestelmien vakiosalasanat pitää vaihtaa.
- Kaikissa julkisesta verkosta tavoitettavissa ja kirjautumista vaativissa organisaation digitaalisissa palveluissa tulee aina olla käytössä **monivaiheinen tunnistautuminen** (MFA, 2FA).
- Mikäli monivaiheinen tunnistautuminen ei ole jostain syystä mahdollista, tulee kyseinen järjestelmä suojata jotenkin muuten estämällä sen suora käyttö julkisesta verkosta.

Varmistukaa johtamisesta, viestinnästä ja resursoinnista

- Varatkaa riittävät **resurssit** kyberturvallisuuden varmistamiseksi ja tarvittavien toimenpiteiden toteuttamiseksi.
- Huomioikaa **johdon tavoitettavuus** kriittisten päätösten tekemiseksi.
- Henkilöstölle tulee antaa **koulutuksen** ja **viestinnän** keinoin riittävät valmiudet arkipäiväisten kyberturvallisuusuhkien kohtaamiseen.
- Viestikää selkeästi henkilöstölle **kyberturvallisuuden merkityksen** organisaation toiminnalle sekä johdon ehdoton sitoutumisen asiaan.
- Järjestäkää henkilöstölle säännöllisesti sen työtehtävien kannalta riittävää **tietoturvakoulutusta**, jotta se kykenee toimimaan turvallisesti huomioiden yleisimmät työssään kohtaaman.
- Järjestäkää henkilöstölle kanava, jonka kautta se voi **ilmoittaa** havaitsemistaan **tietoturvapoikkeamista** tai niiden **epäilyistä**.

Huolehtikaa varmuuskopioista

- **Kaikista toiminnan kannalta tärkeistä tiedoista tulee ottaa säännöllisesti varmuuskopiot**.
  - Varmuuskopioihin tulee sisällyttää liiketoimintatiedon lisäksi **myös erilaiset järjestelmäasetukset.**
- **Varmuuskopioiden suojaamiseen tulee kiinnittää myös huomiota**. Ympäristöön tunkeutunut taho ei saa päästä turmelemaan varmuuskopioita tai varastamaan tietoa salaamattomien varmuuskopioiden avulla.
- Varmuuskopioiden **palauttamista tulee testata säännöllisesti.**
- Lisäksi testatkaa ja opetelkaa tekemään laiteohjelmistojen päivitykset ja asetuksien palautukset.
  - Päivityksien teko voi vaatia erilliset ohjelmistot ja laitteet.

Testatkaa ja simuloikaa järjestelmiä

- Suomesta löytyy energiasektorin järjestelmiin keskittyviä laboratorioita ja tutkimusalustoja, tutustukaa näihin!
  - TEM (2022): Selvitys akkuklusterin tutkimus – infrastruktuureista (2022), https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163941/TEM_2022_25.pdf
- Monia asioita on turvallisempaa ja helpompaa kokeilla tutkimusympäristöissä.
  - ICS-protokollissa voi olla tarjolla tiettyjä ei oletuksena käytössä olevia tietoturvaominaisuuksia.
  - Lisäksi on erilaisia tietoturvalisäyksiä, kuten IEC TS 60870-5-7
  - Hyökkäyksiä ei kannata testata tuotantoympäristössä.
- Sähköverkkojen kyberturvallisuuden suhteen on tehty tutkimusta. Myös lopputöitä löytyy esimerkiksi sähköverkkojen protokollien väärinkäytöksiin liittyen.

Toimintaohjeita kyberhyökkäystilanteista toipumiseen

- Uudet ohjeemme antavat neuvoja tilanteessa, jossa kyberhyökkäys häiritsee organisaation toimintaa. Ohjeet neuvovat teknisellä tasolla miten hyökkäys pysäytetään, hyökkäyksen laajuus selvitetään, ympäristöt puhdistetaan ja palautuminen voidaan aloittaa. Ohjeita on laadittu viiteen eri tyyppiseen kyberhyökkäystilanteeseen (tietomurto, vuotaneet käyttäjätunnukset, palvelunestohyökkäys, kiristyshaittaohjelma ja toimitusketjuhyökkäys). Kukin ohje keskittyy yhden hyökkäystyypin vaatimiin toimenpiteisiin ja sisältää neuvoja toimenpiteistä tilanteen selvityksen eri vaiheissa.
- Ohjeet on suunnattu organisaatioiden asiantuntijoille, joiden tehtävänä on suorittaa hyökkäyksen torjunta- ja palautumistoimet. Toimintaohjeiden tarkoituksena on toimia käsikirjana kriisitilanteessa. Akuuttien toimenpiteiden lisäksi niissä käsitellään myös varautumista sekä tilanteen jälkeen tehtävää jälkiselvitystä. Ohjeiden avulla voi myös helposti harjoitella toipumista häiriötilanteista.

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toimintaohjeita-kyberhyokkaystilanteista-toipumiseen
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

Materiaaleja kriittisen infran turvaamiseen

- Olemme koonneet yhteen eri hankkeissa toteutettuja julkisia työkaluja, dokumentteja sekä tarkastuslistoja, joita voi hyödyntää niin energia-alalla kuin muillakin kriittisen infran sektoreilla tietoturvan sekä -suojan parantamiseksi.
- Listat ja ohjeet ovat luonteeltaan kriittistä infrastruktuuria turvaavien kyberturvallisuuden ja tietosuojan asiantuntijoiden käsityksiä hyvistä käytännöistä.
- Mikäli toimit kriittisen infrastruktuurin parissa energiasektorilla ja haluat tutustua dokumentteihin, jotka eivät ole saatavilla julkisesti, voit kysyä niitä Kyberturvallisuuskeskuksesta tai Huoltovarmuuskeskuksesta.
- Epävarmoissa tilanteissa varmista dokumenttien lisenssit ja käyttöehdot suoraan niiden julkaisijoilta!
- Suomen automaatioseura on julkaissut ”Automaation tietoturva – Kriittisen tuotannon turvaaminen” –kirjaan täydentävää lisämateriaalia.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/materiaaleja-kriittisen-infran-turvaamiseen

Turvatkaa toimitusketjut

- Toimitusketjun turvaaminen on tärkeää, sillä vakavimman uhkan aiheuttavat uhkatoimijat käyttävät hyväksi organisaatioiden luottamusta toimittajiinsa.
- Kyberturvallisuuskeskuksen Ketjutonttu-hankkeen tavoite on auttaa suomalaisia yrityksiä ja niiden toimittajia hallitsemaan toimitusketjuihin liittyviä kyberriskejä.
  - Kampanjaan osallistuvien organisaatioiden toimittajat saavat maksuttoman, avoimiin tietolähteisiin perustuvan tietoturvan tarkastuksen. Tämän lisäksi toimittajat saavat apua korjausten tekemiseen.
  - https://www.kyberturvallisuuskeskus.fi/fi/tonttu
  - https://onboard.badrap.io/ketjutonttustart
- Kybermittari-työkalulla voidaan arvioida organisaation kykyä tunnistaa ja hallita toimitusketjuihin ja kolmansiin osapuoliin liittyviä riskejä.

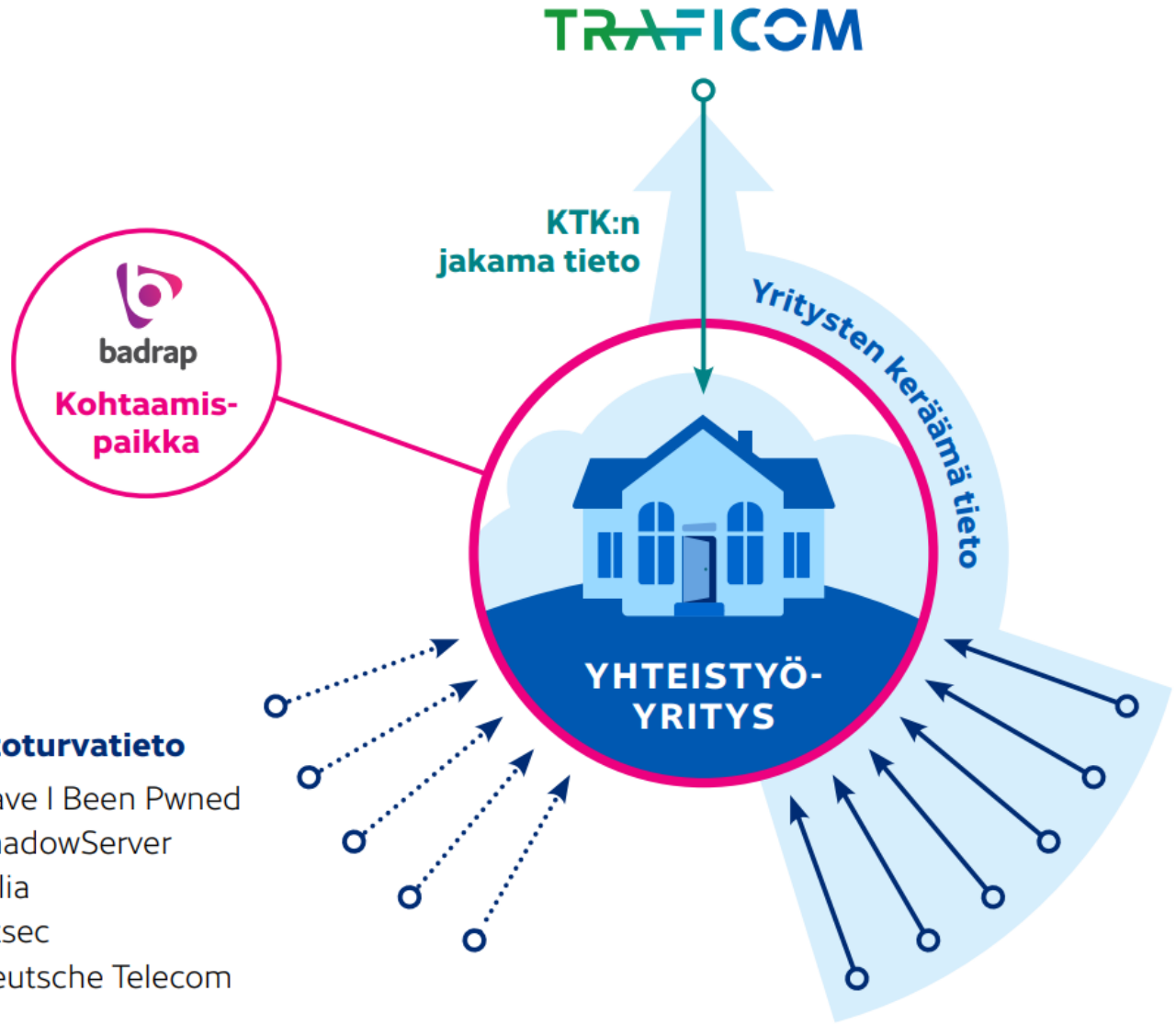
Tonttu-hankkeet

- Tonttu on kokeilumalli, jossa on useita erilaisia pilotteja.
- Pilottien avulla esimerkiksi testataan kevyitä ja skaalautuvia menetelmiä organisaatioiden suojattavien kohteiden tunnistamiseksi, niihin liittyvän tietoturvatiedon jakamiseksi, ja erityissuojattavien verkkojen eristyksen testaamiseksi.
- Seuraa sivuja:
  - https://www.kyberturvallisuuskeskus.fi/fi/tonttu

Tonttu-hankkeet

- Testattuja tietoturvamenetelmiä ovat tähän mennessä olleet mm.
  - Suojattavien kohteiden tunnistaminen
  - Suojattavien kohteiden tietoturvatiedon jakaminen
  - Internettiin näkyvien avointen palvelujen valvonta, kuten tiedostojaot tai tietokannat
  - Honeypot- kyvykkyys sisäverkon lateraaliliikkeen havaitsemiseen
  - Sisäverkon avointen palveluiden muutosten valvonta
  - Kohdennetut haavatarkistukset
  - Verkon suojattavien kohteiden kartoitus ja odottamattomista suojaamattomista kohteista hälyttäminen
  - Reaaliaikainen tietoturvamonitorointi (network security monitor, NSM)
  - Erityissuojattavien verkkojen eristyksen testaaminen

TLP:CLEAR



Tietoturvatieto

- Have I Been Pwned
- ShadowServer
- Telia
- Fitsec
- Deutsche Telecom

Suojattavat kohteet

- SensorFu Beacon
- Microsoft O365
- Microsoft Azure
- Amazon AWS
- Google Workplace
- Google Cloud Platform

Kuva: SensorFu Beaconit testaavat ja hälyttävät eristettyjen verkojen vuodoista.

https://www.kyberturvallisuuskeskus.fi/fi/tonttu

TRAFICOM

TLP:CLEAR

Epäiletkö tietoturvaloukkausta?

Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä meihin.

- Sähköinen lomake: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi
- Puhelin: 0295 345 630 (arkisin klo 9-15)

Muissa asioissa voitte olla meihin yhteydessä osoitteessa kyberturvallisuuskeskus@traficom.fi

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot

TLP:CLEAR

Kiitos!

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

VALTIOLLE.fi