Kybersää ja OT-ajankohtaisnostot.

ASAF
28.5.2024

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kimmo Saarni
Teollisuusautomaation toimialavastaava. (OT / ICS)
Vesihuolto ja Kemian sektori.
Kyberturvallisuuskeskus

Traffic Light Protocol -käsittelyluokitus

TLP:RED - Vain vastaanottajalle

TLP:AMBER+STRICT - Vain vastaanottajan organisaatiolle "yksilöity tarve tietää" -periaatteella.

TLP:AMBER - Vain vastaanottajan organisaatiolle sekä organisaation asiakkaille "yksilöity tarve tietää" -periaatteella.

TLP:GREEN - Rajoitettu jakelu. Tieto voidaan jakaa vapaasti sen vastaanottajan edustaman organisaation sisällä, organisaation sidosryhmille, asiakkaille, sekä toimialalle/yhteisölle.

TLP:CLEAR - Tieto voidaan jakaa pakottavasta lainsäädännöstä johtuvat rajoitukset huomioiden vapaasti.

Lisätietoa tiedonvaihtokäytännöistä on ohjeessa https://www.kyberturvallisuuskeskus.fi/fi/yhteistyoryhmien-tiedonvaihtokaytantoja

TLP:AMBER

Agenda

- Kyberturvallisuuskeskuksen rooli viranomaiskentässä
- Kybersää ja muut ajankohtaiset kansallisesti
- Tiedonvaihto ja yhteistyö
- KV-katsaus
- Kyberturvallisuuskeskuksen palvelut
- Keskustelu

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Viranomaiskenttä

Kyberturvallisuuden viranomaiskenttä

Toimivaltaiset viranomaiset

Kyberturvallisuuskeskus

Toimivaltaiset viranomaiset

Poliisi

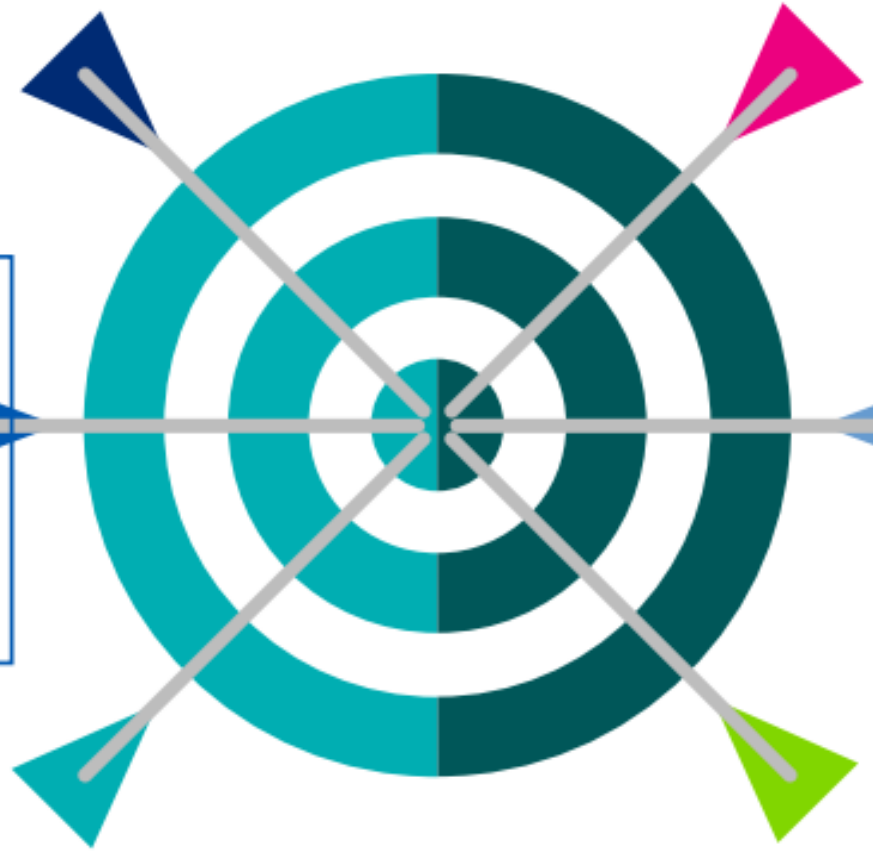
Toimivaltainen viranomainen rikosten selvittämisessä, esitutkinnan toteuttamisessa, syyteharkintaan saattamisessa, rikosten ennaltaehkäisemisessä ja paljastamisessa.

Kyberturvallisuuskeskus

Kansallinen tietoturvaviranomainen, joka kerää tietoa tietoturvaloukkauksista ja niiden uhkista, käsittelee tapaukset luottamuksella, auttaa tarvittaessa selvittämisessä, tutkinnassa ja koordinoinnissa.

Tietosuojavaltuutetun toimisto

Tietosuojalainsäädännön toimeenpanosta vastaava kansallinen valvontaviranomainen, joka käsittelee henkilötietojen tietoturvaloukkaukset.



Huoltovarmuuskeskus ja poolit

Toimivat työ- ja elinkeinoministeriön alaisuudessa ja tehtävänä on huolehtia maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvästä suunnittelusta ja operatiivisesta toiminnasta.

Suojelupoliisi

Sisäministeriön alaisuudessa toimiva siviilitiedusteluorganisaatio, joka tiedustelee ja estää ennalta kansalliseen turvallisuuteen kohdistuvia uhkia, myös kybertoimintaympäristössä.

Puolustusvoimat

Vastaa maan sotilaallisesta puolustamisesta, valvoo maa- ja vesialuetta sekä ilmatilaa. Tehtävänä turvata maan sotilaallinen koskemattomuus ja itsenäisyyden säilyminen.

Kyberturvallisuuskeskus

Kyberturvallisuuskeskus tukee Suomen kriittistä infrastruktuuria havainnoimalla uhkia sekä ylläpitämällä luottamuksellisia tiedonjakoryhmiä ja kansallista kyberturvallisuuden tilannekuvaa.

Palvelulupaus tietoturvaloukkauksissa

Neuvomme
vahinkojen rajoittamisessa

Autamme
loukkauksen analysoinnissa

Tuemme
palautumis-toimenpiteissä

Keräämme
lisätietoja Suomesta ja maailmalta

Varoitamme
muita mahdollisia uhreja

Koordinoimme
haavoittuvuuksien korjaamista

Luottamuksellisesti ja maksutta

TRAFICOM

TLP:CLEAR

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Kybersää huhtikuu 2024

Tietomurrot ja -vuodot

- Palo Alton kriittinen haavoittuvuus (CVE-2024-3400) johti useisiin tietomurtoihin ja tietomurron yrityksiin. Saimme n.15 ilmoitusta, joiden perusteella vakavilta vahingoilta kuitenkin vältyttiin.
- Huhtikuussa M365-käyttäjätilejä murrettiin DropBox-teemaisilla kalasteluviesteillä. Osassa murroista käytettiin AiTM-tekniikkaa.

Huijaukset ja kalastelut

- Android-puhelimiin levitetään haittaohjelmaa huijausviesteillä perintäyhtiön nimissä. Kredinorin lähettämiltä näyttävät tekstiviestit ja puhelinsoitot ohjaavat asentamaan puhelimeen "virustorjuntaohjelmiston", joka onkin pankkitietoja varastava haittaohjelma.
- Huijaussivustoja on väärennetty myös .fi-päätteisiin verkko-osoitteisiin mm. PRH:n nimissä.

Haittaohjelmat ja haavoittuvuudet

- Varoitus 1/2024: Organisaatioissa laajasti käytetyn Palo Alto GlobalProtect-tuotteen haavoittuvuutta (CVE-2024-3400) käytettiin aktiivisesti hyväksi.
- Kyberturvallisuuskeskukselle tehtyjen ilmoitusmäärien vähennettyä päätettiin poistaa Varoitus 7.5.2024.

Automaatio ja IoT

- Kuluttajatuotteissa on ollut merkittäviä kyberturvallisuus-ongelmia. Osassa niistä viestintä on herättänyt tyytymättömyyttä kuluttajissa. Huono kriisiviestintä on yritykselle merkittävä maine- ja liiketoimintariski.[4, 5]
- Kriisiviestinnän suunnittelu ja harjoittelu on jatkuvuudenhallinnan ydintä.

Verkkojen toimivuus

- Huhtikuussa yleisissä viestintäpalveluissa oli 9 toimivuushäiriötä.
- Haktivistien palvelunestohyökkäykset eivät kohdistuneet huhtikuun aikana Suomeen.
- Muilla palvelunestohyökkäyksillä ei raportoitu olleen merkittäviä vaikutuksia.

Vakoilu

- Sandwormiin liitetyt havainnot nousivat esiin useissa julkaisuissa.
- Toimijan takaovena käyttämää haittaohjelmaa havaittiin mm. Ukrainassa ja Virossa.[6, 7, 8]
- Ukrainassa toimijan raportoitiin valmistelleen hyökkäyksiä paikallista energia-, vesi- ja lämmöntuotantoa vastaan.

Huhtikuun kyberturvallisuuden yleiskuva

- Julkaisimme 18.4.2024 Varoituksen 1/2024 Palo Alto GlobalProtect-tuotteisiin kohdistuneisiin tietomurtoihin liittyen.[2]
  - Palo Alto GlobalProtect Gateway ja sen hallintaan käytetty GlobalProtect Portal ovat tuotteita, joita organisaatiot käyttävät esimerkiksi turvallisiin VPN-etätyöratkaisuihin.
  - Tilanne oli lopulta rauhallisempi kuin ennakoitiin, ja Varoitus poistettiin 7.5.2024.[3]
- Fitsec on julkaissut keinon Akira-haittaohjelman tekemän salauksen purkamiseen ja tarjoaa apuaan Akira:n uhreille sivuillaan.[10]

Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

Suomeen kohdistunut kyberympäristön uhkataso on pysynyt kohonneena.

Kohdistettujen hyökkäysten määrä on noussut. Kohonneen uhkatason vuoksi organisaatioiden varautumisen merkitys korostuu.

2.

Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

Haavoittuvuuden korjaavan päivityksen asentamisen lisäksi on usein tarpeen tutkia, onko haavoittuvuutta hyödynnetty jo ennen päivityksen asentamista.

3.

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.

Symbolit

Uusi

Päivitetty

4.

Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa.

Organisaatioiden olisi hyvä tunnistaa tekoälyn tuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään.

5.

Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta erilaisille osaajille. Myös riskienhallinnan ja jatkuvuuden näkökulmasta riittävän osaamisen varmistaminen kaikkina vuodenaikoina on organisaatioille tärkeää.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

CASE Helsingin kaupunki

Helsingin kaupungin tietomurto

-Helsingin kaupunki on kertonut, että kaupungin kasvatuksen ja koulutuksen toimialaan kohdistuneessa tietomurrossa vuoti jopa 120 000:n oppijan, huoltajan sekä henkilökunnan tietoja. Osa tiedoista oli arkaluonteisia.

-Tietomurrossa käytetty hyväksi etäyhteyspalvelinta

-Tietomurto olisi voitu välttää tietoturvapäivityksellä

(YLE 13.5.2024)

Tutkinnan yleisjohtaja, Keskusrikospoliisin (KRP) rikosylikomisario Marko Leponen vahvistaa, että Suomessa ei ole tiedossa suurempaa tietovuotoa. Vastaamon tietomurrossa varastettiin noin 30 000 ihmisen tiedot.

Helsinkiin kohdistuneessa murrossa ovat vaarantuneet 150 000 nykyisen ja entisen oppijan tiedot. Sama koskee Helsingin kaupungin 38 000 hengen henkilökuntaa. Vaarantua ovat voineet myös oppilaiden huoltajien tiedot

Jos jokaisella oppijalla on keskimäärin hieman alle kaksi huoltajaa, lukumäärä voi IS:n laskutoimituksen mukaan teoriassa nousta lähelle puolta miljoonaa.

Eli toisin sanoen voidaan puhua Suomen suurimmasta tietovuodosta?

– Kyllä. Kyllä me voimme puhua, Leponen vahvistaa.

(Ilta-Sanomat 22.5.2024)

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tiedonvaihto ja yhteistyö

Tiedonvaihto ja yhteistyö

ISAC-tiedonvaihtoryhmät

Kansallinen yhteistyö tulevaisuudessa OT-sektorilla

ISAC-tiedonvaihtoryhmän tarkoitus

Jakaa luottamuksellisesti tietoa uhkista, tietoturvapoikkeamista ja ilmiöistä

Analysoida vaikutuksia ja suojautumiskeinoja organisaatio- ja toimialatasolla

Ylläpitää häiriötilanteiden hallinnassa tarvittavia operatiivisia **yhteistyörakenteita**

Toimia tarvittaessa hankkeiden, harjoitusten ja muiden toimialan **kyberturvallisuutta edistävien toimenpiteiden toteuttajina**, ohjaajina ja seuraajina

Information
Security &
Analysis
Centre

Tietoa käytetään Kyberturvallisuuskeskuksen tilannekuvan tuottamiseen.

TLP:CLEAR

ISAC-tiedonvaihtoryhmät

Noin

300

organisaatiota

TLP:CLEAR

ISAC-tiedonvaihtoryhmä

Toimintaan osallistuvat organisaatiot pääosin yhteiskunnan elintärkeiden toimintojen kannalta **kriittisiä organisaatioita**.

Osallistujat tietoturvan, yritysturvallisuuden ja riskienhallinnan parissa työskenteleviä henkilöitä.

Ryhmät määrittävät itse toimintatapansa ja tavoitteensa.
Kyberturvallisuuskeskus toimii ryhmien sihteerinä.

Ryhmässä
10-20
aktiivista
osallistujaa

Kokouksia yleensä
3-6
kertaa vuodessa

TLP:CLEAR

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

KV-katsaus

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuus keskuksen palvelut


TRAFICOM
HYÖKY
Kansallinen hyökkäyspinnan kartoitus
hyöky.fi | hyoky@traficom.fi
HARJOITUS-TOIMINTA
kyberharjoitukset.fi
kyberharjoitukset@traficom.fi
Tunnistaminen
Suojautuminen
Havainnointi
Vaste
Palautuminen
Kyber-turvallisuuden hallinta
KYBER-MITTARI
kybermittari.fi
kybermittari@traficom.fi
HAVARO
Vakavien tietoturvauhkien kansallinen havainnointipalvelu
havaro.fi | info@havaro.fi
Riskienhallinnan palvelut organisaatioille

Kybermittari

- Kansallinen kyberkyvykkyyksien **kypsyystason arviointi- ja kehittämismalli**
- Kybermittari **auttaa organisaatioita arvioimaan ja kehittämään kyvykkyyttään** suojautua kyberuhilta ja varmistamaan toimintanne **jatkuvuus** häiriötilanteissa?
- Kybermittari antaa **vertailutietoa ja helpottaa yhteistyötä sekä tiedonjakoa** organisaation sisällä ja verkostoissa.
- Tietoturvastandardit edellyttävät että tietoturvan kehittymistä **mitataan**. Kybermittari hoitaa tämä osan riippumatta käytössä olevasta viitekehyksestä ja auttaa asettamaan tavoitetason.
- Kerätty vertailutieto auttaa **kansallisen tilannekuvan muodostamisessa** ja investointien kohdentamisessa

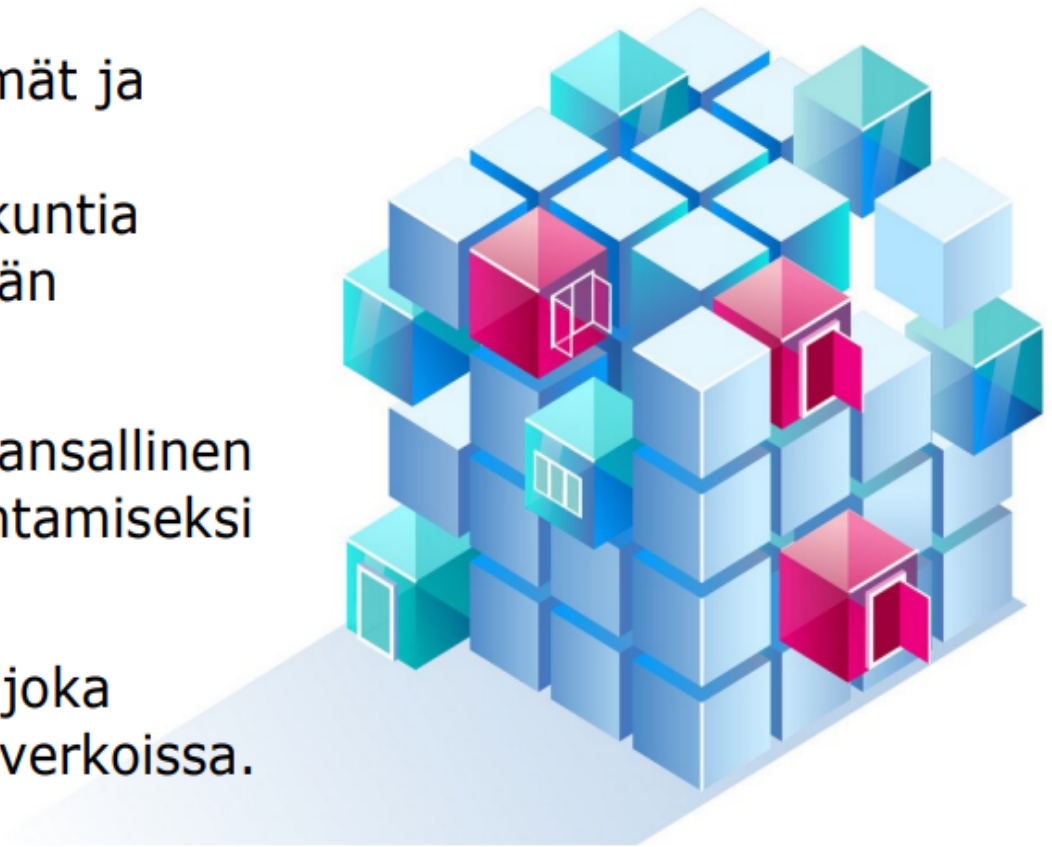
Harjoitustoimintatiimiltä saatava tuki

Tehtävänä on yhteiskunnan toiminnan kannalta kriittisten organisaatioiden kyberharjoittelun tukeminen ilman markkinahäiriön aiheuttamista. Lähtökohtaisesti emme fasilitoi tai järjestä harjoituksia organisaatioille.

- **Konsultaatio ja neuvonta.** Organisaatioiden opastaminen kyberharjoitteluun ja harjoitusten suunnitteluun liittyen.
- **Harjoituksiin osallistuminen.** Harjoitusten tukeminen tuomalla KTK harjoitukseen omassa roolissa.
- **Tukimateriaali.** Kyberharjoittelun helpottaminen tuottamalla harjoitteluun liittyvää materiaalia ja työkaluja
  - https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/-

Kansallinen Hyökkäyspintakartoitus kyberturvallisuuden parantamiseksi kunnissa [13]

- Hyökkäyspintaa lisäävät muun muassa avoimet tietoliikenneportit, suojaamattomat tietojärjestelmät ja verkkopalveluissa olevat haavoittuvuudet. Tieto hyökkäyspinnasta tehdyistä havainnoista auttaa kuntia kohdentamaan korjaustoimenpiteitä ja kehittämään ennakoivasti palveluidensa turvallisuutta.
- Hyöky on Kyberturvallisuuskeskuksen tuottama kansallinen hyökkäyspintakartoitus kyberturvallisuuden parantamiseksi kunnissa.
- Hyöky on maksuton ja helppokäyttöinen palvelu, joka kartoittaa kunnan hyökkäyspinnan julkisissa tietoverkoissa. Tieto havainnoista auttaa kuntaa suojaamaan toimintakykyään sekä kansalaisille tarjottavien palveluiden turvallisuutta ja toimintavarmuutta.



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Mitä NIS2-direktiivissä esitetyt kyberhygieniakäytännöt ovat?

Keskustelua kysymyksiä kommentteja ?