TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuus-keskuksen ajankohtaiskatsaus

24.10.2023

TLP:CLEAR

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuus-keskuksen ajankohtaiskatsaus

24.10.2023

TLP:CLEAR

Varoitus 1/2023: Tietojenkalastelun seurauksena Microsoft 365 -tilien tietomurtoaalto (20.10.2023)

- Rikolliset kalastelevat väärennetyillä sähköpostiviesteillä Microsoft 365 -ympäristön salasanoja [1-3].
- Tietojenkalastelulla saatujen käyttäjätunnusten ja salasanojen avulla rikollisten on mahdollista murtautua M365-tilille.
- Viikolla 42/2023 kalasteluviestejä ja uusia tilimurtoja raportoitiin kymmenistä suomalaisista organisaatioista [1].
- Kalastelukampanja leviää organisaatiosta toiseen hyödyntämällä murrettujen käyttäjätilien yhteystietolistoja.
- Monissa kalasteluviesteissä on hyödynnetty turvapostiteemaa [2].
- Jos epäilet saamasi viestin aitoutta, älä vastaa viestiin vaan pyri varmistumaan jotain muuta reittiä pitkin.

TLP:CLEAR

Agenda

- Varoitus 1/2023
- Haemme teollisuusautomaation toimialavastaavaa Kyberturvallisuuskeskukseen
- Toimivaltaiset viranomaiset
- Kyberturvallisuuskeskus
- Nostoja Kybersäästä ja muut ajankohtaiset

Teollisuusautomaation toimialavastaava Kyberturvallisuuskeskukseen

- Kyberturvallisuuskeskus hakee vakituista erityisasiantuntijaa kasvattamaan Kyberturvallisuuskeskuksen osaamista teollisuusautomaation kyberturvallisuuskysymyksissä, sekä kehittämään prosessiteollisuuden ja automaatiota hyödyntävän teollisuuden kanssa tehtävää yhteistyötä.
- ID: 31-222-2023
- Hakuaika päättyy 31.10.2023 klo 16.15
- https://www.valtiolle.fi/fi-FI/ilmoitus?id=31-222-2023

VALTIOLLE.fi

TRAFICOM

TLP:CLEAR

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.

Toimivaltaiset viranomaiset

Poliisi

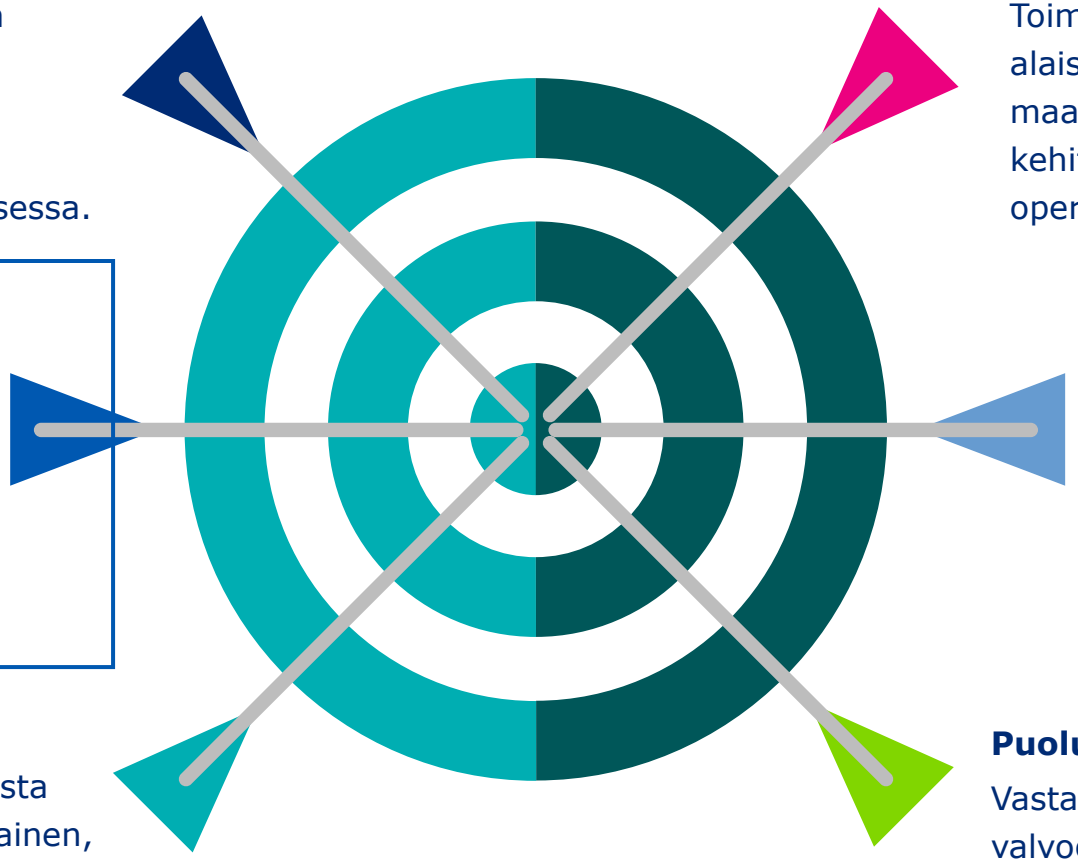
Toimivaltainen viranomainen rikosten selvittämisessä, esitutkinnan toteuttamisessa, syyteharkintaan saattamisessa, rikosten ennaltaehkäisemisessä ja paljastamisessa.

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.

TRAFICOM

TLP:CLEAR

Kyberturvallisuuskeskus

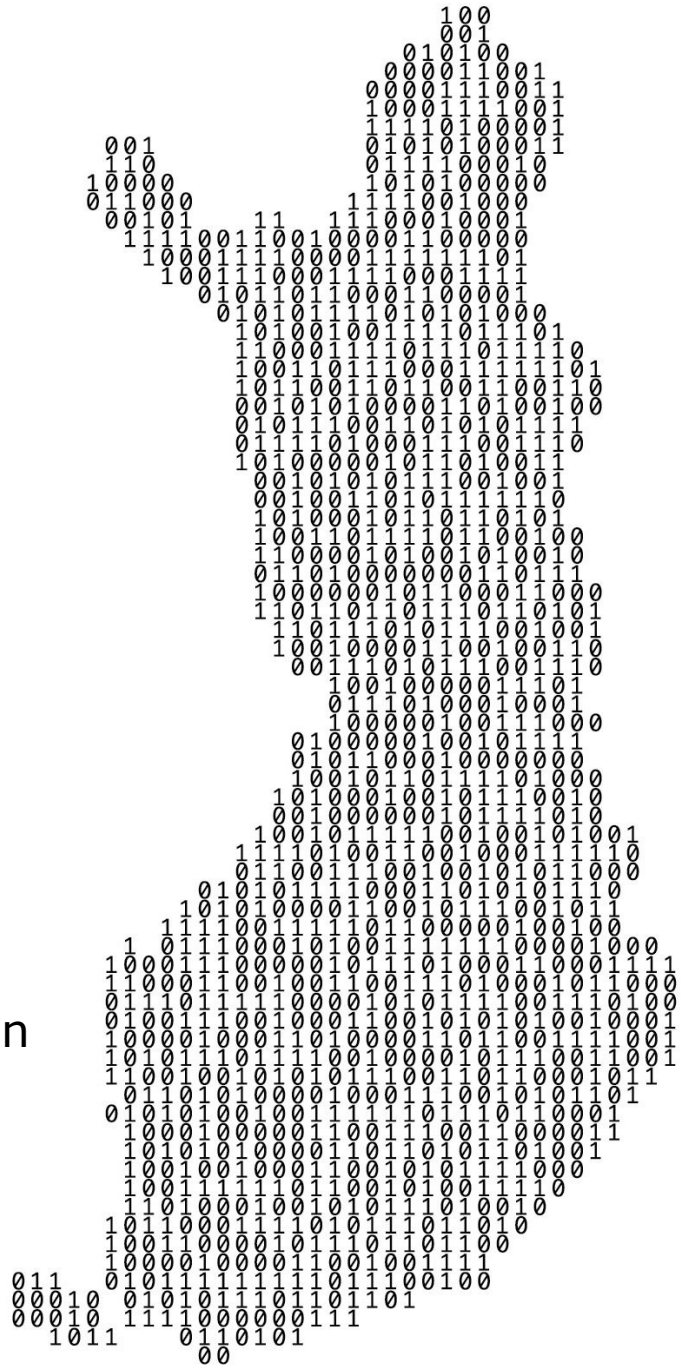
Kyberturvallisuuskeskus tukee Suomen kriittistä infrastruktuuria havainnoimalla uhkia sekä ylläpitämällä luottamuksellisia tiedonjakoryhmiä ja kansallista kyberturvallisuuden tilannekuvaa.

TRAFICOM

TLP:CLEAR

Kyberturvallisuuskeskuksen CERT-toiminto

- Computer Emergency Response Team
- CERT-toiminnon tehtävänä on
  - ennaltaehkäistä tietoturvaloukkauksia ja niiden uhkia
  - ylläpitää tilannekuvaa
  - tiedottaa tietoturva-asioista.
- CERT-toiminnan tavoitteena on
  - yleisten viestintäverkkojen ja viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistaminen
  - yhteiskunnan elintärkeiden toimintojen turvaaminen.
- CERT-palvelustamme saat apua tietoturva-asioissa. Yleisen tietoturvatietouden lisäksi voimme auttaa vakavien tietoturvaloukkausten teknisessä selvityksessä.
- Yhteydenotot kerryttävät tilannekuvaa, jonka perusteella voidaan tehdä viestintää ja pyrkiä estämään vastaavat vahingot muualla



TLP:CLEAR

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

Tietoturva Nyt! 21.04.2023

Kyberturvallisuuden uhkataso pysynyt kohonneena - kohdistettujen hyökkäysten määrä noussut

TRAFICOM Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TLP:CLEAR

Kybersää 01/2023

Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.

TRAFICOM Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TLP:CLEAR

Tärkein tietoturvateko on tiedostaa, mitkä ovat yrityksen tuotannolliset ‘kruununjalokivet’, mikä on niiden nykyinen tietoturvallisuuden taso ja mitä tulisi kehittää? Tämän jälkeen pitäisi myös viedä läpi tarvittavat kehitystoimet.

Kybermittari [4]

- 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.
- Ota yhteyttä: kybermittari@traficom.fi

TLP:CLEAR

Kybersää syyskuu 2023

Tietomurrot ja -vuodot

- Julkisuudessa olleen Essityn/Westlogin tietomurron seurauksena saimme ilmoituksia vuotaneista tiedoista.
- Sosiaalisen median tilimurroissa on nähty myös järjestelmiin tallennettujen luottokorttien väärinkäyttöjä esimerkiksi ostamalla mainoksia.

Automaatio ja IoT

- **NIST on päivittänyt teollisuusautomaatioympäristöjen suojaamiseen keskittyvän ohjeensa 800-82.[5]**
- Uudessa versiossa huomioidaan mm. muuttuneet tuotanto-ympäristöjen kyberturvallisuus-uhkat, suojaustyökalut, suositellut käytännöt sekä arkkitehtuurit.

Huijaukset ja kalastelut

- **Huijauspuheluita soitettiin väärennetyistä numeroista syyskuussa ennätysmäärä.**
- Pankkitunnusten kalastelu siirtyi taas tekstiviesteistä sähköpostiin.
- Laskutuspetoksilla yritettiin huijata organisaatioita kalastusseuroista kotiseutuyhdistykseen.

Verkkojen toimivuus

- Syyskuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä.
- **Haktivistit jatkavat palvelunestohyökkäyksiä ja kotimaiset organisaatiot ovat saaneet osansa hyökkäyksistä.**
- Palvelunestohyökkäyksillä ei ole ollut vakavia vaikutuksia palveluiden saatavuuteen.

Haittaohjelmat ja haavoittuvuudet

- Kriittinen ja etäkäytettävä haavoittuvuus libwebp-kirjastossa edellyttää välitöntä päivittämistä. Kirjasto on käytössä mm. useissa eri selaimissa.

Vakoilu

- Puolivuosittain julkaistava Microsoftin raportti kuvaa Itä-Aasian kyberoperaatioiden trendiä.
- Microsoftin raportti kertoo esimerkiksi Kiinaan liitettävästä kybervakoilusta ja vaikuttamisoperaatioista sekä Pohjois-Korean tietojenkeruusta ja kryptovaluuttojen hankinnasta.

TRAFICOM Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TLP:CLEAR

Kybersää syyskuu 2023

Tietomurrot ja -vuodot

- Julkisuudessa olleen Essityn/Westlogin tietomurron seurauksena saimme ilmoituksia vuotaneista tiedoista.
- Sosiaalisen median tilimurroissa on nähty myös järjestelmiin tallennettujen luottokorttien väärinkäyttöjä esimerkiksi ostamalla mainoksia.

Huijaukset ja kalastelut

- **Huijauspuheluita soitettiin väärennetyistä numeroista syyskuussa ennätysmäärä.**
- Pankkitunnusten kalastelu siirtyi taas tekstiviesteistä sähköpostiin.
- Laskutuspetoksilla yritettiin huijata organisaatioita kalastusseuroista kotiseutuyhdistykseen.

Haittaohjelmat ja haavoittuvuudet

- Kriittinen ja etäkäytettävä haavoittuvuus libwebp-kirjastossa edellyttää välitöntä päivittämistä. Kirjasto on käytössä mm. useissa eri selaimissa.

Automaatio ja IoT

- **NIST on päivittänyt teollisuusautomaatioympäristöjen suojaamiseen keskittyvän ohjeensa 800-82.[5]**
- Uudessa versiossa huomioidaan mm. muuttuneet tuotanto-ympäristöjen kyberturvallisuus-uhkat, suojaustyökalut, suositellut käytännöt sekä arkkitehtuurit.

Verkkojen toimivuus

- Syyskuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä.
- **Haktivistit jatkavat palvelunestohyökkäyksiä ja kotimaiset organisaatiot ovat saaneet osansa hyökkäyksistä.**
- Palvelunestohyökkäyksillä ei ole ollut vakavia vaikutuksia palveluiden saatavuuteen.

Vakoilu

- Puolivuosittain julkaistava Microsoftin raportti kuvaa Itä-Aasian kyberoperaatioiden trendiä.
- Microsoftin raportti kertoo esimerkiksi Kiinaan liitettävästä kybervakoilusta ja vaikuttamisoperaatioista sekä Pohjois-Korean tietojenkeruusta ja kryptovaluuttojen hankinnasta.

TRAFICOM Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TLP:CLEAR

NIST SP 800-82 versio 3 ”Guide to Operational Technology (OT) Security” [5]

- NIST julkaisi uudistetun kolmannen version 800-82 -ohjeestaan, joka keskittyy tuotantoverkkojen ja teollisuusautomaatioympäristöjen suojaamiseen.
- Ohjeen edellinen versio julkaistiin vuonna 2015.
- Tämän jälkeen niin tuotantoympäristöjen kyberturvallisuusuhkat kuin suojaamiseen käytettävät työkalut, teknologiat, standardit sekä suositellut käytännöt sekä arkkitehtuurit ovat päivittyneet tai muuttuneet.
- Ohje on kattava ja monipuolinen – varaa siis sopivasti resursseja sen läpikäyntiin!

Nopeat vinkit (NIST) [6]

1. Vastuut: Nimeä vähintään yksi henkilö johtamaan tuotantoympäristöjen kyberturvallisuuteen liittyvä toimia.

2. Omaisuudenhallinta: Ymmärrä mitä järjestelmiä omistat, miten niitä käytetään ja mikä niiden kriittisyys on.

3. Yhteistyö: Muodosta yhteistyöverkostot oman sektorin toimijoiden, järjestelmätoimittajien sekä muiden tärkeiden yhteistyökumppaneiden kanssa.

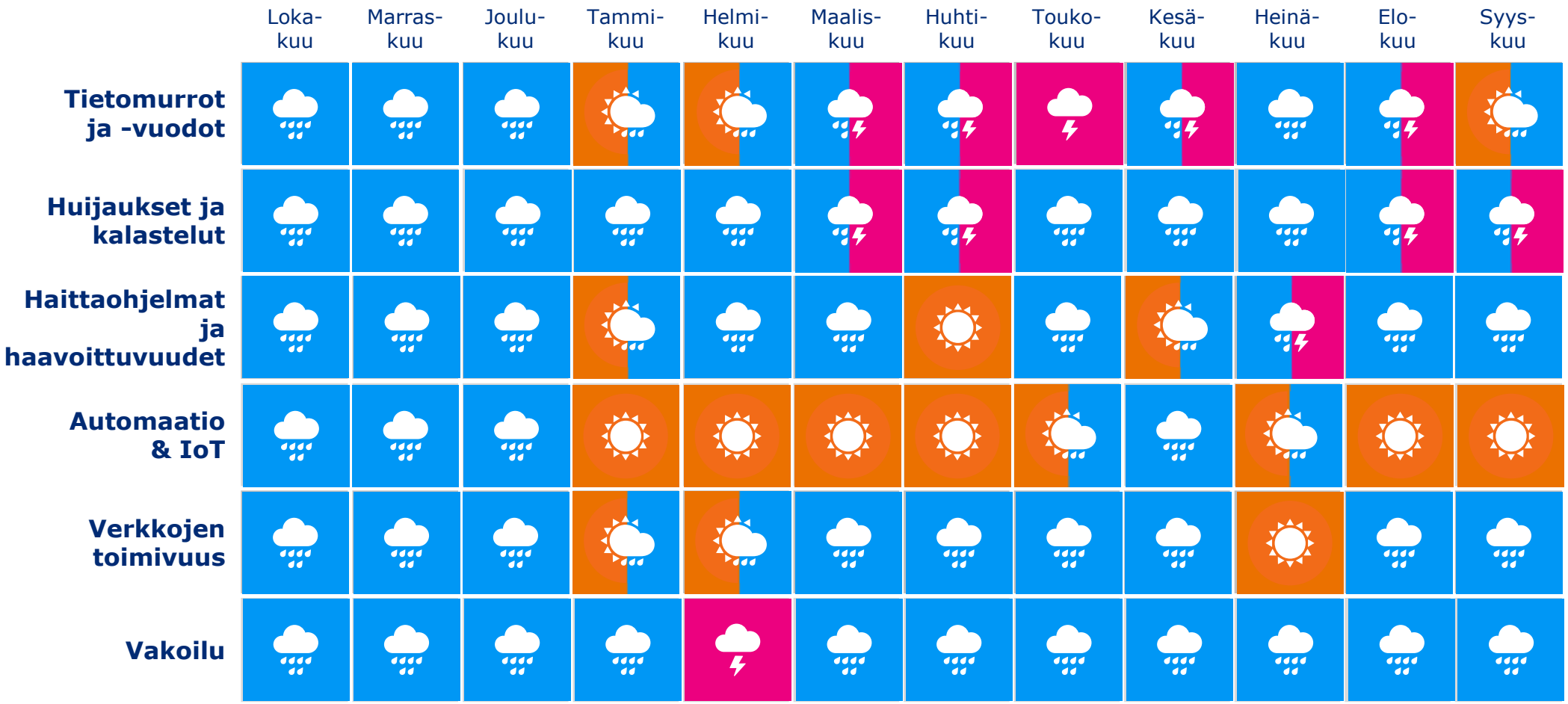
4. Salasanat: Vaihda oletussalasanat ja varmistu hyvästä salasanojen kyberhygieniasta.

5. Laitteiden suojaus: Eristä ja suojaa laitteet fyysisesti sekä estä niiden luvaton ohjelmointi.

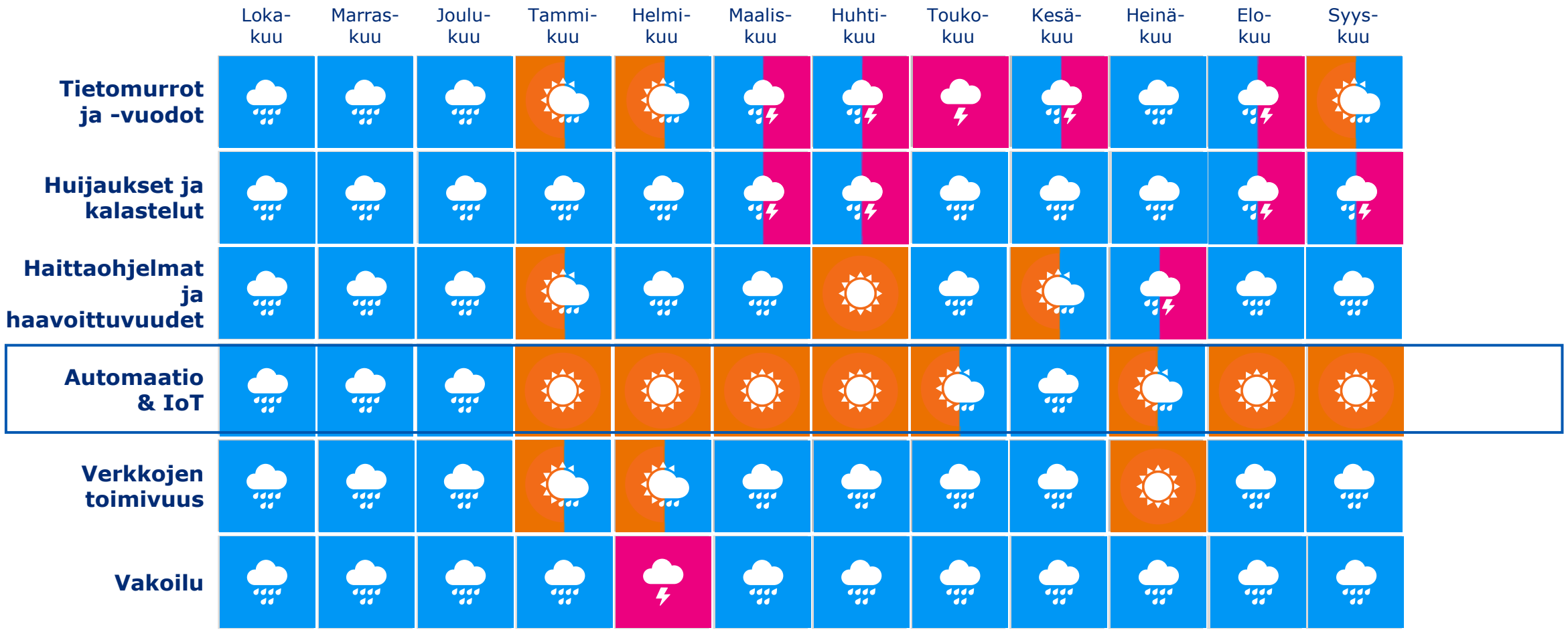
Lisävinkit (NIST) [6]

1. Varmistu henkilöstön kyberkoulutuksesta ja –harjoittelusta.
2. Varmistu käyttäjien- ja pääsynhallinnan toimivuudesta ja tietojen ajantasaisuudesta.
3. Eristä ja eriytä verkot, todenna käyttäjät monivaiheisesti ja anna heille vain tarvittavat oikeudet.
4. Hallitse haavoittuvuuksia riskiperustaisesti.
5. Salli vain hyväksyttyjen sovellusten ajaminen.
6. Varaudu poikkeamista palautumiseen tekemällä ja **testaamalla** palautumissuunnitelma.
7. Monitoroi jatkuvasti järjestelmiä sekä ulos ja sisään tulevaa verkkoliikennettä.

Kyberturvallisuuden trendit
kulunut 12 kk



Kyberturvallisuuden trendit
kulunut 12 kk



Toimialakohtaiset havainnot 06/2023

	Trendi **3kk**	Edeltävä **3kk**	
Elintarvike			Havaittu tietojenkalastelukampanjoita.
Energia			Tuleva sääntely (NIS2, CER, CRA, NCCS) yrittää päästää sadepilvien läpi joitakin auringonpilkahduksia. Sateisuutta aiheuttaa Suomen kyberturvallisuuden noussut uhkataso sekä sektorin toimijoiden, järjestelmätoimittajien ja yhteistyökumppaneiden ympäristöihin tehdyt tietomurrot.
Finanssi			Pankkitunnusten kalastelu jatkuu tasaisen voimakkaana. QR-koodin sisältävä tietojenkalasteluviesti levinnyt laajasti myös finanssialalle.
Teollisuus			Tietomurtoja tai niiden yrityksiä sekä myös kirityshaittaohjelmatapauksia. Erilaisia huijaus- ja tietojenkalasteluyrityksiä kohdistuen teollisuusyrityksiin sekä myös näiden toimitusketjuihin.
Logistiikka ja liikenne			Havaittu satamiin kohdistettuja palvelunestohyökkäyksiä.
Valtionhallinto			Havaittu useita tietojenkalastelukampanjoita, joista osassa hyödynnettiin ns. turvapostiteemaa.
Media			Yksittäisiä tietojenkalasteluyrityksiä.
SOTE			Sote-alalta ilmoitettujen kyberturvallisuuden poikkeamien määrä kasvoi ensimmäiseen vuosineljännekseen verrattuna. Erityisesti kasvoi tietomurtojen ja kalastelun määrä.
Vesihuolto			Havaittu huijaus- ja tietojenkalasteluyrityksiä.
Kunnat			Aktiiviset tietojenkalastelu- ja huijauskampanjat kuntaorganisaatioita kohtaan johtivat lukuisiin onnistuneisiin tilimurtoihin ja tekivät säästä sateisen.

Toimialakohtaiset havainnot 06/2023

	Trendi **3kk**	Edeltävä **3kk**	
Elintarvike			Havaittu tietojenkalastelukampanjoita.
Energia			Tuleva sääntely (NIS2, CER, CRA, NCCS) yrittää päästää sadepilvien läpi joitakin auringonpilkahduksia. Sateisuutta aiheuttaa Suomen kyberturvallisuuden noussut uhkataso sekä sektorin toimijoiden, järjestelmätoimittajien ja yhteistyökumppaneiden ympäristöihin tehdyt tietomurrot.
Finanssi			Pankkitunnusten kalastelu jatkuu tasaisen voimakkaana. QR-koodin sisältävä tietojenkalasteluviesti levinnyt laajasti myös finanssialalle.
Teollisuus			Tietomurtoja tai niiden yrityksiä sekä myös kirityshaittaohjelmatapauksia. Erilaisia huijaus- ja tietojenkalasteluyrityksiä kohdistuen teollisuusyrityksiin sekä myös näiden toimitusketjuihin.
Logistiikka ja liikenne			Havaittu satamiin kohdistettuja palvelunestohyökkäyksiä.
Valtionhallinto			Havaittu useita tietojenkalastelukampanjoita, joista osassa hyödynnettiin ns. turvapostiteemaa.
Media			Yksittäisiä tietojenkalasteluyrityksiä.
SOTE			Sote-alalta ilmoitettujen kyberturvallisuuden poikkeamien määrä kasvoi ensimmäiseen vuosineljännekseen verrattuna. Erityisesti kasvoi tietomurtojen ja kalastelun määrä.
Vesihuolto			Havaittu huijaus- ja tietojenkalasteluyrityksiä.
Kunnat			Aktiiviset tietojenkalastelu- ja huijauskampanjat kuntaorganisaatioita kohtaan johtivat lukuisiin onnistuneisiin tilimurtoihin ja tekivät säästä sateisen.

Toimialakohtaiset havainnot 09/2023

	Trendi **3kk**	Edeltävä **3kk**	
Elintarvike			Ilmoitettujen poikkeamien määrä on laskenut. Moni yritys valmistautuu NIS2-direktiivin toimeenpanoon kehittämällä tietoturvallisuuden hallintajärjestelmäänsä.
Energia			Ilmoitettujen poikkeamien määrässä ei merkittäviä muutoksia. Onnistuneiden tietomurtojen tai niiden yritysten määrät lisääntyivät. Kyberturvallisuuden uhkataso on yhä koholla.
Finanssi			Pankkitunnusten kalastelu jatkuu eri muodoissaan. Pankkeihin kohdistuneet palvelunestohyökkäykset eivät aiheuttaneet häiriöitä palveluihin.
Teollisuus			Ilmoitettujen poikkeamien määrä on laskenut etenkin puolustus-, metsä-, ja kemianteollisuudessa. Erityisesti tietomurtojen määrät vähenivät ja ne kohdistuivat lähinnä sähköpostitileihin.
Logistiikka ja liikenne			Toimialaan kohdistunut palvelunestohyökkäyksiä.
Valtionhallinto			Jo vuoden ajan koholla ollut uhkataso näkyy edelleen valtionhallinnossa mm. erilaisina tietojenkalastelukampanjoina ja ajoittaisina palvelunestohyökkäyksinä eri organisaatioihin.
Media			Muutamaan media-alan yritykseen kohdistui palvelunestohyökkäyksiä, joilla ei ollut mainittavia vaikutuksia palveluihin.
SOTE			Ilmoitettujen poikkeamien määrä on laskenut; erityisesti tietomurrot ovat vähentyneet. Euroopassa esiintynyt entistä enemmän sote-palveluihin kohdennettuja kiristyshyökkäyksiä.
Vesihuolto			Ilmoitettujen poikkeamien määrässä ei juurikaan muutoksia; kalastelu- ja huijausyritykset jatkuvat välillä valitettavasti onnistuen.
Kunnat			Hyvin toteutettujen huijausviestien avulla onnistuneita tilimurtoja sekä teknisen tuen nimissä soitettuja huijauspuheluita, joiden yhteydessä saatu pääsy käyttäjän työasemalle. Palvelunestohyökkäyksiä.

Toimialakohtaiset havainnot 09/2023

	Trendi **3kk**	Edeltävä **3kk**	
Elintarvike			Ilmoitettujen poikkeamien määrä on laskenut. Moni yritys valmistautuu NIS2-direktiivin toimeenpanoon kehittämällä tietoturvallisuuden hallintajärjestelmäänsä.
Energia			Ilmoitettujen poikkeamien määrässä ei merkittäviä muutoksia. Onnistuneiden tietomurtojen tai niiden yritysten määrät lisääntyivät. Kyberturvallisuuden uhkataso on yhä koholla.
Finanssi			Pankkitunnusten kalastelu jatkuu eri muodoissaan. Pankkeihin kohdistuneet palvelunestohyökkäykset eivät aiheuttaneet häiriöitä palveluihin.
Teollisuus			Ilmoitettujen poikkeamien määrä on laskenut etenkin puolustus-, metsä-, ja kemianteollisuudessa. Erityisesti tietomurtojen määrät vähenivät ja ne kohdistuivat lähinnä sähköpostitileihin.
Logistiikka ja liikenne			Toimialaan kohdistunut palvelunestohyökkäyksiä.
Valtionhallinto			Jo vuoden ajan koholla ollut uhkataso näkyy edelleen valtionhallinnossa mm. erilaisina tietojenkalastelukampanjoina ja ajoittaisina palvelunestohyökkäyksinä eri organisaatioihin.
Media			Muutamaan media-alan yritykseen kohdistui palvelunestohyökkäyksiä, joilla ei ollut mainittavia vaikutuksia palveluihin.
SOTE			Ilmoitettujen poikkeamien määrä on laskenut; erityisesti tietomurrot ovat vähentyneet. Euroopassa esiintynyt entistä enemmän sote-palveluihin kohdennettuja kiristyshyökkäyksiä.
Vesihuolto			Ilmoitettujen poikkeamien määrässä ei juurikaan muutoksia; kalastelu- ja huijausyritykset jatkuvat välillä valitettavasti onnistuen.
Kunnat			Hyvin toteutettujen huijausviestien avulla onnistuneita tilimurtoja sekä teknisen tuen nimissä soitettuja huijauspuheluita, joiden yhteydessä saatu pääsy käyttäjän työasemalle. Palvelunestohyökkäyksiä.

Teollisuuden järjestelmätoimittajaan kohdistunut tietomurto edellyttää myös sen asiakkailta ripeitä toimenpiteitä

- Organisaatioiden varautumisen tulee kattaa myös toimittajiin kohdistuvat poikkeamat.
- Euroopassa viimeaikaisten kiristyshaittaohjelmatapauksiin johtaneiden tietomurtojen uhrien joukossa on ollut myös sellaisia suuryrityksiä, jotka toimivat kriittisen infrastruktuurin sekä teollisuuden tuotantoautomaatiojärjestelmien toimittajina.
- Organisaation tulisikin varmistaa jo etukäteen, että sillä on
- tiedossa mitä kaikkea tuotantoympäristöjen suojattavaa tietoa sen palvelutuottajilla on hallussaan, sekä millaisen riskin tämän tiedon mahdollinen vuotaminen muodostaa organisaatiolle itselleen.
- tekniset valmiudet sekä ennalta määritellyt toimintamallit kyseiselle palvelutuottajalle avattujen etähuoltoyhteyksien estämiseksi. Tässä yhteydessä ei tule luottaa tietomurron uhriksi joutuneen toimittajan omaan ilmoitukseen näiden yhteyksien katkaisemisesta, vaan estää ne myös omin toimenpitein.
- valmiudet estää (esim. käyttäjätunnukset lukitsemalla) kyseisen toimittajan henkilöiden pääsy kaikkiin organisaation omiin palveluihin, kuten yhteisiin työtiloihin tai dokumentinhallintajärjestelmiin.
- kyvykkyys valvoa ja havaita poikkeamia myös tuotantoympäristöihin suuntautuvien huoltoyhteyksien osalta.

Syyskuun 2023 kyberturvallisuuden yleiskuva

- **Syyskuun alkupuolella haktivistiryhmä ilmoitti hyökänneensä useita eurooppalaisia kyberturvallisuusviranomaistahoja kohtaan.**
  - Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus oli yksi ilmoitetuista kohteista.
  - Palvelunestohyökkäysten vaikutus palveluiden toimintaan on yleensä tilapäinen. Niitä on usein rinnastettu verkossa toteutettuun ruuhkaan tai mielenilmaukseen, joiden tavoitteena onkin saada aikaan uutisointia.
  - Palvelunestohyökkäyksistä voi lukea lisää mm. viikkojen 38 ja 41 viikkokatsauksista [7, 8].
- Ilmoituksia väärennetyistä numeroista saapuvista huijauspuheluista tuli syyskuussa suuri määrä. **Lokakuun alussa astui voimaan Traficomin määräys, joka velvoittaa teleoperaattorit torjumaan ulkomailta saapuvia suomalaisiksi numeroiksi väärennettyjä puheluita myös mobiilinumeroiden osalta [9].**
- Syyskuun aikana Kyberturvallisuuskeskukselle tulleet ilmoitusmäärät tietomurroista, tietomurron yrityksistä ja tietovuodoista ovat vähentyneet.

Ketjutonttu-kampanja tunnisti ja korjasi toimitusketjuihin liittyviä kyberriskejä [10]

- Kyberturvallisuuskeskuksen Ketjutonttu-kampanja paransi suomalaisen yrityskentän tietoturvaa tunnistamalla ja korjaamalla riskejä niiden toimitusketjuissa.
- Ketjutonttu on viimeisin Kyberturvallisuuskeskuksen toteutettavuustutkimuskampanjoiden sarjassa. Kampanjoiden tarkoituksena on selvittää, miten yritysten turvallisuutta voidaan parantaa kevyillä menetelmillä. Ketjutontussa palvelun toimitti suomalainen Badrap Oy.
- Kampanja osoitti, että kyberturvallisuutta voidaan parantaa keveilläkin menetelmillä. Kampanjaan osallistuneiden organisaatioiden toimittajat saivat maksuttoman, avoimiin tietolähteisiin perustuvan tietoturvan tarkastuksen ja lisäksi apua korjausten tekemiseen.
- Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -ohjelmasta rahoitettuun kampanjaan osallistui 150 organisaatiota ja yritystä.

Kotiverkon ja reitittimen tietoturva [11]

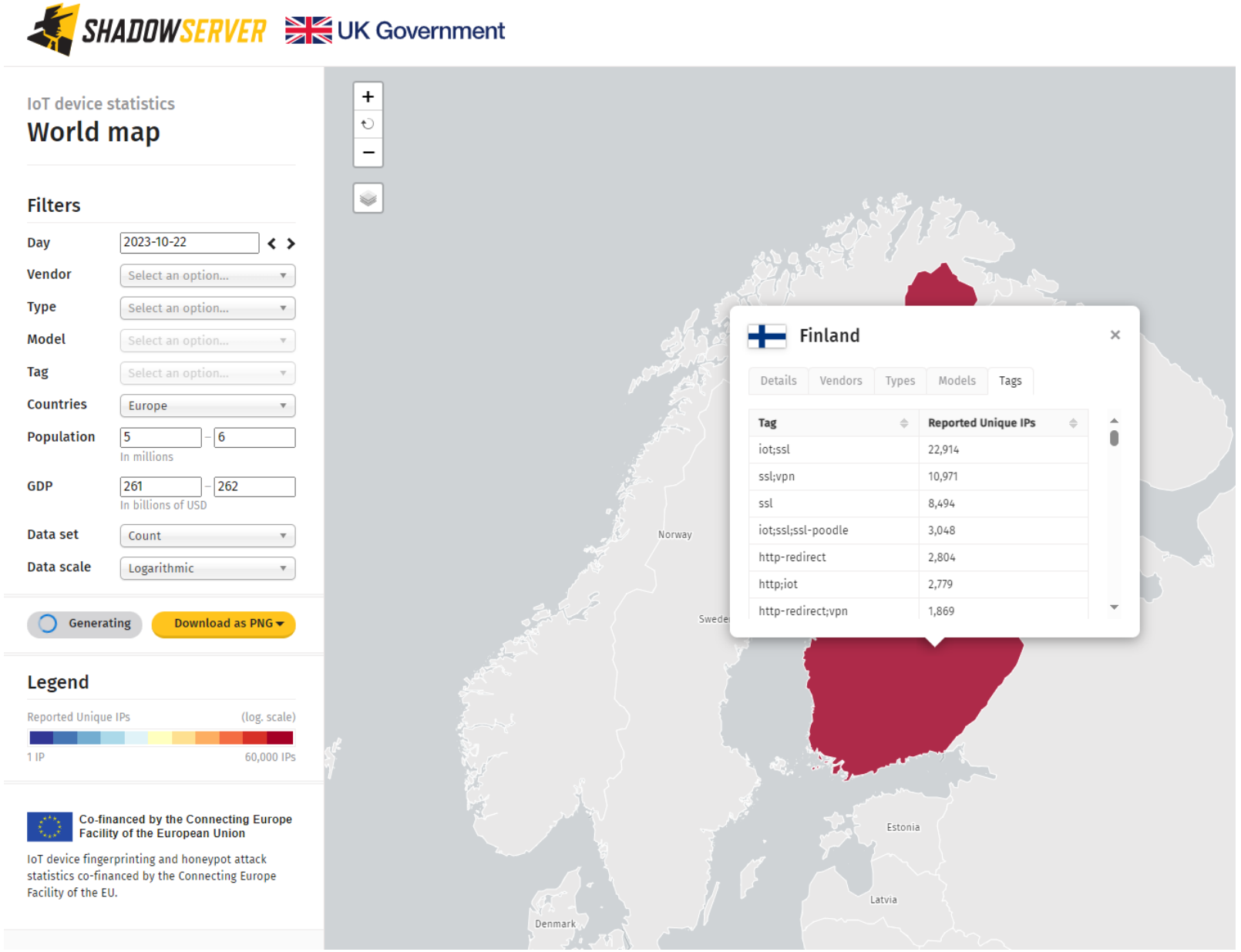
- Modeemi tai reititin on portti kotiverkkoomme, ja sen turvallisuus on avainasemassa.
- Laitteet voivat olla joko erilliset, tai sama laite voi toimia niin modeemina kuin reitittimenäkin.
- Rikolliset etsivät käsin tai automatisoidusti verkosta haavoittuvuuksia. Kaapattuja verkkolaitteita käytetään esimerkiksi palvelunestohyökkäysten tekemiseen.
- Hajautetut palvelunestohyökkäykset (DDoS, Distributed Denial of Service) ovat usein toteutettu kaapatuilla laitteilla näitä ohjaamalla.
- Verkkolaitteet ovat myös tapa peitellä omia jälkiä, tai hyökätä kohdemaan lähdeosoitteen avulla.

Puutteellinen rakennusautomaatiolaitteiden suojaus verkossa altistaa kyberuhille [12]

- Suojaamattomana internetissä oleva laite on houkutteleva kohde verkkorikollisille. Laitteen voi valjastaa esimerkiksi osallistumaan palvelunestohyökkäyksiin, lähettämään roskapostia tai laite voi tarjota helpon pääsyn rakennusautomaatiojärjestelmään sekä rakennuksen sisäverkkoon.
- Rikolliset etsivät verkosta pääsyä automaatiojärjestelmiin automaattisilla menetelmillä ja myös manuaalisesti. Heidän käytettävissään on sekä valmiita automatisoituja työkaluja että omia ohjelmiaan, koneille asennettavia haavoittuvuusskannereita ja julkisia skannauspalveluita kuin perinteisiä hakukoneita. He saattavat käyttää löytämiään järjestelmiä väärin joko itse tai myymällä tiedot eteenpäin.

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.



Lähde: Shadow Server (24.10.2023 klo 10:20) [14]

TRAFICOM

TLP:CLEAR

Shadow Server - Tilastoja (2023-10-22)

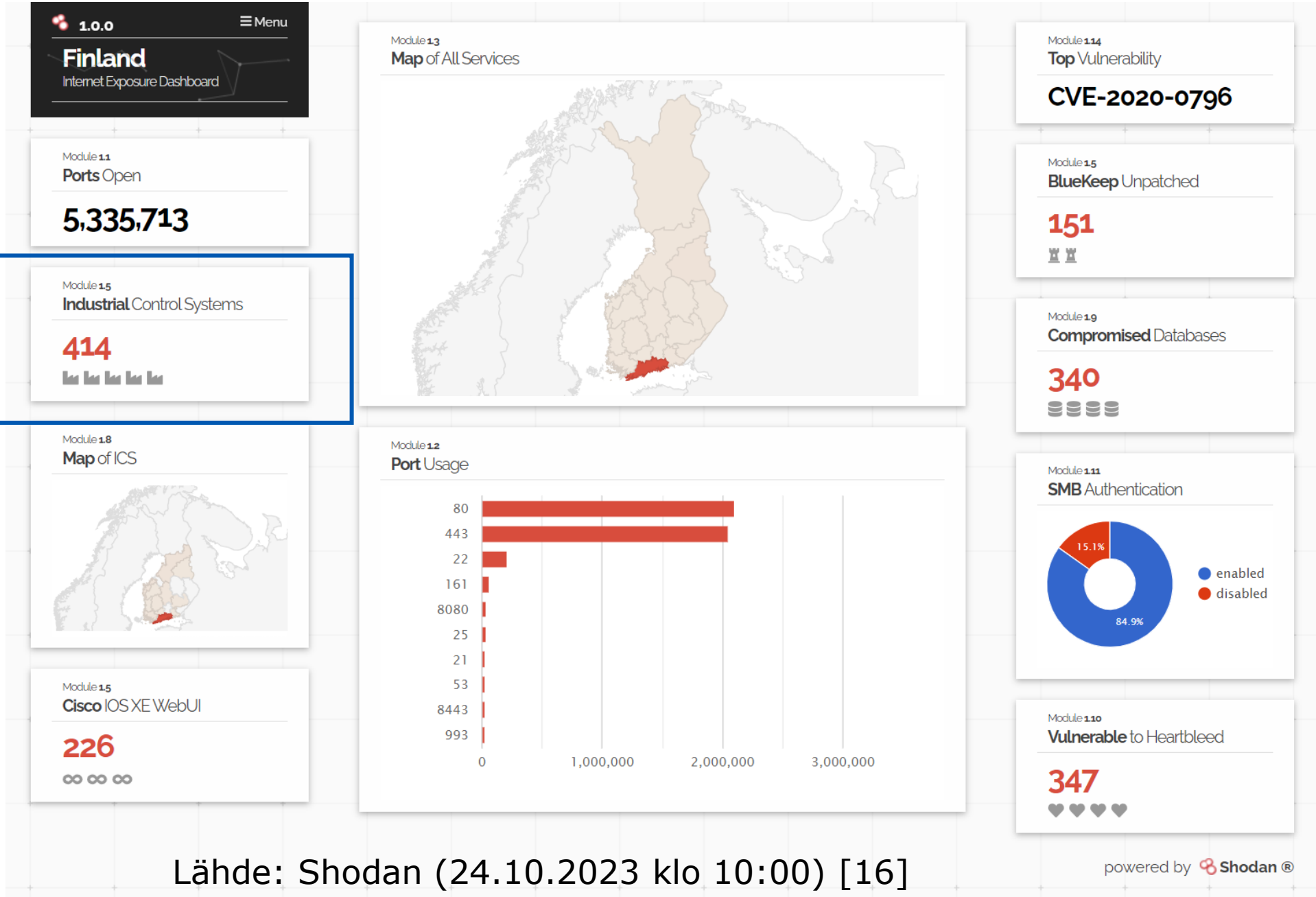
- IoT-karttanäkymä ->
  - Type: embedded-system: 491 kpl
  - Type: plc: 20 kpl
  - Type: power-device: 105 kpl
  - Type: printer: 248 kpl
  - Type: smart-building-management: 208 kpl
  - Type: smart-home-management: 760 kpl
  - Type: smart-alarm: 6 kpl
- Yleinen karttanäkymä -> Sources: ics: 144 kpl
  - Tag: bacnet: 54 kpl
  - Tag: codesys: 3 kpl
  - Tag: fox: 24 kpl
  - Tag: iec-60870-5-104: 2 kpl
  - Tag: modbus: 33 kpl
  - Tag: opc-ua-binary: 26 kpl
  - Tag: S7: 7 kpl

Lähde: Shadow Server (24.10.2023 klo 10:20) [14]

Censys - Tilastoja

- Censys haku
  - `labels=`scada` AND location.country_code=FI`
  - Tulos ilman päällekkäisten laitteiden tarkastusta:
    - 326 SCADA laitetta (label=scada), joihin 94 pääsee mahdollisesti etänä (label=remote-access)
    - palveluina mm.
      - BACNET: 100 kpl
      - Modbus: 161 kpl
      - FOX: 32 kpl
      - S7: 30 kpl
      - MQTT: 9 kpl

Lähde: Censys (24.10.2023 klo 9:45) [15]



Lähde: Shodan (24.10.2023 klo 10:00) [16]

TRAFICOM

TLP:CLEAR

Miten teidän organisaatiolle voi ilmoittaa ongelmista tai haavoittuvuuksista? [17-19]

- Yleisimmät haasteet tietoturvailmoitusten tekemisessä liittyvät yrityksen saavutettavuuteen ja viestintään. Tärkeintä olisikin, että yrityksen yhteystiedot löytyisivät helposti – myös englanniksi.
- Saamme Kyberturvallisuuskeskukseen toisinaan esimerkiksi ulkomaisia yhteydenottoja, joissa kysellään, mitä tarkoittaa yrityksen verkkosivuilla mainittu "etunimi piste sukunimi".
- Organisaatiot voivat edistää yhteystietojensa ja käytäntöjensä löytymistä julkaisemalla ne aina samassa paikassa ja muodossa. Tästä on hyötyä erityisesti tilanteessa, jossa suomalaisesta palvelusta haavoittuvuuden löytänyt tietoturvatutkija on kotoisin toisesta maasta.
- RFC 9116:ssa on kuvattu tekninen määritelmä, joka esittää tiedoille yhtenäistä, koneluettavaa sijaintia verkkopalvelimilla.

Materiaaleja kriittisen infran turvaamiseen [20]

- Olemme koonneet sivuillemme yhteen eri hankkeissa toteutettuja julkisia työkaluja, dokumentteja sekä tarkastuslistoja, joita voi hyödyntää niin energia-alalla kuin muillakin kriittisen infran sektoreilla tietoturvan sekä -suojan parantamiseksi.
- Ohjeet sekä tietoturva- ja tietosuojavaatimusten listat ovat luonteeltaan kriittistä infrastruktuuria turvaavien kyberturvallisuuden ja tietosuojan asiantuntijoiden käsityksiä hyvistä käytännöistä, mutta ne eivät ole virallisia ohjeita tai suosituksia.
- Epävarmoissa tilanteissa varmista dokumenttien lisenssit ja käyttöehdot suoraan niiden julkaisijoilta.

Toimialakohtaiset sähköpostilistamme [21]

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

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

Kaikki liikkeessä 2030 -virtuaalitapahtuma 2023 9.11.2023 klo 9-12 [22]

- Mukana Robert M. Lee, Dragos Inc. ”Tietoturvan uhkamaisema: strategioita kriittistä infrastruktuuria puolustaville johtajille” (englanniksi)

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)

Yhteiskunnan kannalta kriittisten organisaatioiden ilmoituslomake: https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx

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

Lähdeluettelo

[1] Varoitus 1/2023 https://www.kyberturvallisuuskeskus.fi/fi/tietomurtoaalto-leviaa-organisaatiosta-toiseen-katkaise-tietojenkalastelu

[2] Turvapostiteemaiset kalasteluviestit https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turvapostiteemaiset-kalasteluviestit-johtavat-sahkopostitilimurtoihin

[3] Ohje M365-tilien murtoihin https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/toimi-nain-microsoft-365-tilin-tietomurron-sattuessa

[4] Kybermittari https://kybermittari.fi

[5] Guide to Operational Technology (OT) Security https://csrc.nist.gov/pubs/sp/800/82/r3/final

[6] NIST:n vinkkejä tuotantoympäristöjen suojaamiseen https://csrc.nist.gov/CSRC/media/Projects/operational-technology-security/documents/NIST_Control_Systems_Tips_and_Tactics_Infographic.pdf

[7] Viikkokatsaus 38/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-382023

[8] Viikkokatsaus 41/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-412023

Lähdeluettelo

[9] Traficomin määräys lopettaa suomalaisiksi naamioidut valepuhelut lähes kokonaan https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficomin-maarays-lopettaa-suomalaisiksi-naamioidut-valepuhelut-lahes-kokonaan

[10] Ketjutonttu-kampanja https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kampanja-tunnisti-ja-korjasi-toimitusketjuihin-liittyvia-kyberriskeja

[11] Kotireitittimien tietoturva https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kotiverkon-ja-reitittimen-tietoturva

[12] Rakennusautomaatiolaitteiden suojaus https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kuka-sammutti-valot-puutteellinen-rakennusautomaatiolaitteiden-suojaus-verkossa

[13] HYÖKY https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/hyoky

[14] Shadow Serverin IoT-järjestelmien karttanäkymä https://dashboard.shadowserver.org/statistics/iot-devices/map/ ja yleinen karttanäkymä https://dashboard.shadowserver.org/statistics/combined/map/

[15] Censys https://search.censys.io/

[16] Shodanin maanäkymä https://exposure.shodan.io/

Lähdeluettelo

[17] Miten vastaanottaa valkohattujen yhteydenottoja https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palveluistanne-loytyi-tietoturva-aukko

[18] Miten ilmoittaa haavoittuvuuksista https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein

[19] Tutkimus RFC 9116:n hyödyntämisestä Suomessa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuuksien-ilmoittamista-helpottavaa-kaytantoa-ei-viela-taysin-hyodynneta

[20] Materiaaleja kriittisen infran turvaamiseen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/materiaaleja-kriittisen-infran-turvaamiseen

[21] Toimialakohtainen tilannekuva ja tiedotteet https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/tilannekuva?toggle=Toimialakohtainen%20tilannekuva%20ja%20tiedotteet

[22] Kaikki liikkeessä 2023 –virtuaalitapahtuma https://www.traficom.fi/fi/ajankohtaista/tilaisuudet/kaikki-liikkeessa-2030-virtuaalitapahtuma-2023-ohjelma