TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuuden ajankohtaisia älyliikenteen näkökulmasta

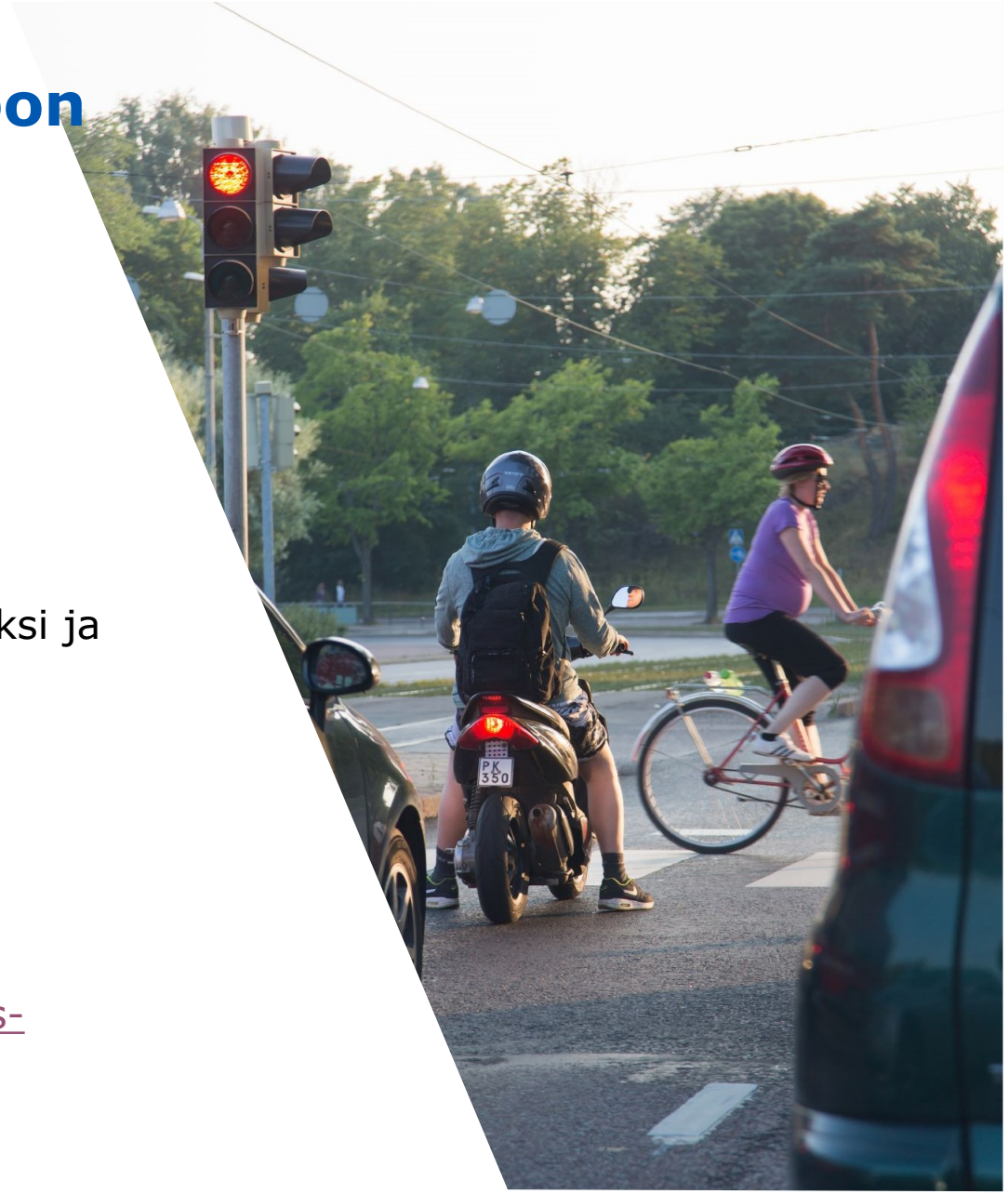
ITS Finlandin verkostopäivä

20.8.2020

Virpi Tuulaniemi
erityisasiantuntija
liikenteen kyberturvallisuuden koordinaattori

Alankomaiden hakkerit löysivät helpon keinon vaikuttaa liikennevaloihin

- Tietoturvautkijat hyödynsivät pyöräilijöille suunnattuja sovelluksia, jotka jakavat ajajien sijaintitietoja liikennejärjestelmille ja joiden tarkoituksena on antaa pyöräilijälle vihreä valo tämän lähestyessä liikennevaloa.
- Tutkijat pystyivät **internetin kautta vaikuttamaan samanaikaisesti useisiin eri liikennevaloihin**.
- Tutkijat pystyivät väärennettyjä viestejä lähettämällä huijaamaan liikennevaloja vaihtumaan pyöräilijöille vihreäksi ja muille punaiseksi ilman, että risteyksessä oli pyöräilijöitä.
- Tällä tavoin voitaisiin aiheuttaa **keskeytyksiä liikennevirtoihin**.
- Älykkään liikenteen ratkaisuja rakennettaessa on otettava turvallisuus huomioon. Mitä jos kysymys olisi sadoista väärennetyistä rekoista?
- Lähde: https://www.wired.com/story/hacking-traffic-lights-netherlands/, 5.8.2020



Mercedes-Benz E-sarjan ajoneuvossa 19 haavoittuvuutta

- Tutkijat löysivät Mercedes-Benz E-sarjan ajoneuvosta 19 haavoittuvuutta. Haavoittuvuudet on korjattu.
- Löydettyjen haavoittuvuuksien avulla hyökkääjä olisi pystynyt mm. **etänä avaamaan ajoneuvon ovet ja käynnistämään moottorin**.
- Ajoneuvon connectivity-toiminnallisuuksien arkkitehtuurista löydettiin useita erilaisia haavoittuvuuksia.
- Head-Unit 1 haavoittuvuus, Telematics Control Unit (TCU) 6 haavoittuvuutta, ajoneuvon taustapalvelu 9 haavoittuvuutta ja ajoneuvon käyttöjärjestelmä 2 haavoittuvuutta
- Vaikutus: mahdollisesti yli 2 miljoonaa ajoneuvoa
- Lähde: https://threatpost.com/black-hat-19-flaws-connected-mercedes-benz-vehicles/158144/, 6.8.2020

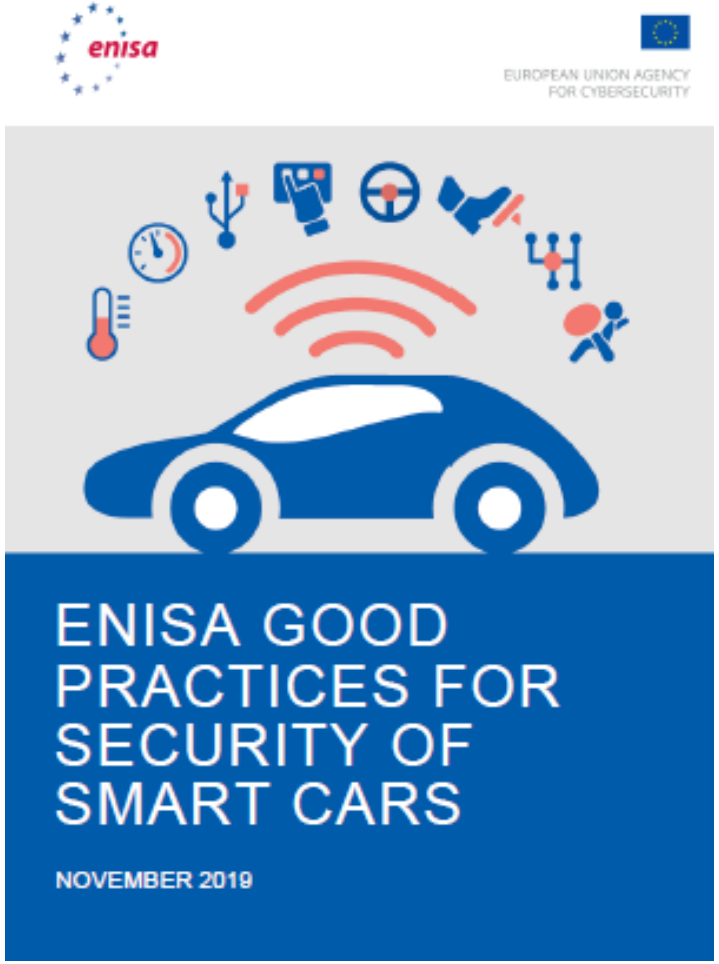
YK:n regulaatiot ajoneuvojen kyberturvallisuudesta ja ohjelmistopäivityksistä

- Tieliikenteen ajoneuvojen kyberturvallisuuden ja ohjelmistopäivityksien regulaatiot on YK:ssa 24.6.2020 hyväksytty. Nämä ovat ensimmäiset kansainvälisesti yhdenmukaistetut ja sitovat normit tällä alueella.
- Regulaatiot astuvat voimaan tammikuussa 2021. EU:ssa Kyberturvallisuuden regulaatio tulee pakolliseksi uusille ajoneuvotyypeille heinäkuusta 2022 alkaen ja kaikille uusille ajoneuvoille heinäkuusta 2024 alkaen.
- Regulaatiot asettavat vaatimuksia ajoneuvovalmistajille:
  - Ajoneuvojen kyberturvallisuusriskien hallintaan
  - Ajoneuvojen turvalliseen suunnitteluun riskien mitigoimiseksi
  - Ajoneuvojen turvallisuustapahtumien havaitsemiseen ja niihin reagointiin
  - Tarjoamaan ohjelmistopäivitykset turvallisesti (safe and secure) varmistaen, että turvallisuus (safety) ei vaarannu
- Lisätietoa uutisesta: https://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html
- Ko. regulaatioiden tulkintadokumentit työn alla YK:n alaisessa alatyöryhmässä.

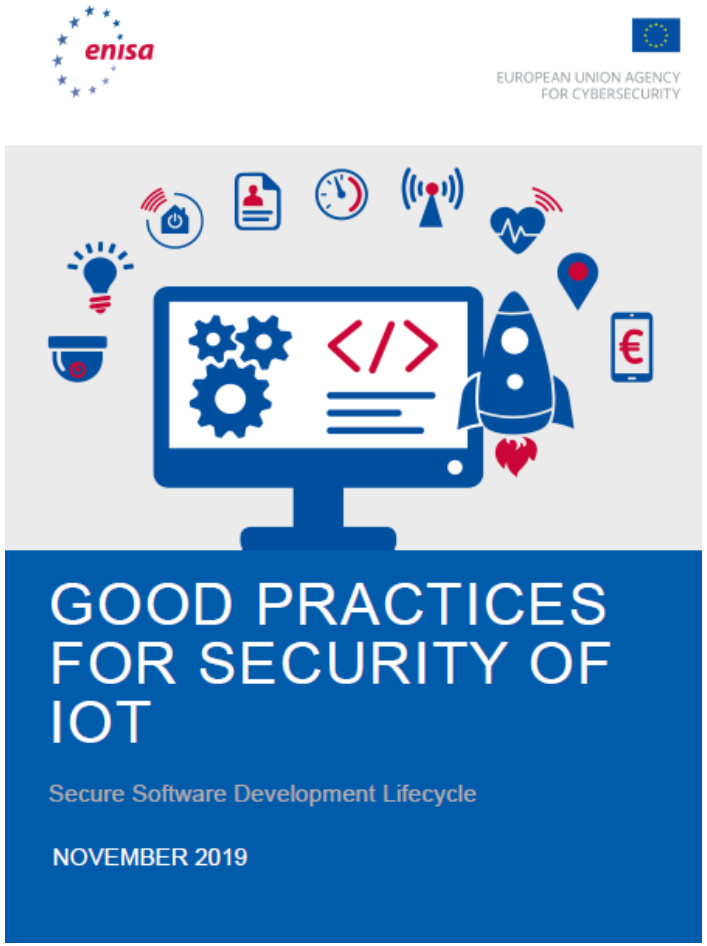
ISO/SAE DIS 21434 tieliikenteen ajoneuvojen kyberturvallisuusstandardi

- ISO/SAE DIS 21434 Road vehicles – Cybersecurity Engineering
  - Määrittelee vaatimukset kyberturvallisuusriskien hallinnalle tieliikenteen ajoneuvojen E/E-järjestelmille koko niiden elinkaaren ajalle (konseptivaiheesta käytöstä poistoon)
  - Sisältää vaatimukset kyberturvallisuusprosesseille ja yhteisen kielen kyberturvallisuusriskien kommunikointiin ja hallintaan
  - Ei määrittele kyberturvallisuuteen liittyviä teknologioita tai ratkaisuja
  - Aikataulu:
    - Standardiluonnos oli lausunnoilla keväällä 2020
    - Tullee loppuäänestykseen loppuvuodesta 2020 tai vuoden 2021 alussa
    - Standardi julkaistaan viimeistään heinäkuussa 2021

ENISA (Euroopan unionin verkko- ja tietoturvavirasto) julkaisuja



https://www.enisa.europa.eu/publications/smart-cars



https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

Kyberturvallisuuskeskuksen ohjeita – Turvallinen tuotekehitys

TRAFICOM

TURVALLINEN TUOTEKEHITYS: KOHTI HYVÄKSYNTÄÄ

SECURE DEVELOPMENT – TOWARDS APPROVAL

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/turvallinen-tuotekehitys-kohti-hyvaksyntaa

SISÄLLYSLUETTELO

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Heinäkuu 2020

Poimintoja

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

Kybersää Heinäkuu 2020

Tietomurrot ja -vuodot

- Havaintoja suomalaisista murretuista PulseSecure- ja Netscaler-palvelimista ja haavoittuvista BIG-IP-palvelimista.
- Office 365 –tietomurtojen määrä jälleen nousussa kesän hiljaisemman ajan jälkeen.

Huijaukset ja kalastelut

- Tietojenkalastelu on ammattirikollisten aktiivisesti käyttämä työkalu, jonka merkitys verkkohuijauksissa on korostunut.
- Puhelinhuijaukset ovat palanneet karanteenitauon jälkeen. Suomeen tulee satojatuhansia huijauspuheluita.

Haittaohjelmat ja haavoittuvuudet

- Ransomware-toimijat huutokauppaavat varastettuja tietoja tavoitteenaan rahastaa tiedoilla.
- Heinäkuussa julkaistiin kriittisiä haavoittuvuuksia ja verkkolaitteisiin kohdistuneita haavoja käytettiin aktiivisesti hyväksi.

Automaatio

- Yhdysvaltain viranomaiset varoittivat lisääntyneestä kyberhyökkäysten uhkasta automaatiojärjestelmiä vastaan.
- Automaatiojärjestelmiä koskevia haavoittuvuuksia löytyy entistä useammin.

Verkkojen toimivuus

- Vain kolme merkittävää yleisten viestintäpalveluiden häiriötä.
- DigiCert mitätöi useita varmenteita 11.7., mikä vaikutti myös useiden suomalaisten palveluiden toimintaan.
- Heinäkuu oli palvelunestohyökkäysten osalta Suomessa rauhallinen.

Vakoilu

- EU on ryhtynyt ensimmäistä kertaa aktiivisiin vastatoimiin valtiollisia kyberhyökkäyksiä vastaan pakotteiden muodossa.
- Kohdistettujen hyökkäysten tavoitteena ei ole vain vakoilu, vaan myös vaikuttaminen ja ydinaseohjelman rahoittaminen.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1 ↑

Laajavaikutteiset kiristyshyökkäykset uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

2 ↓

Tietojenkalastelu on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdennetuissa hyökkäyksissä ja vakoilussa.

3 ↓

Haavoittuvuuksien hyväksikäyttö on nopeaa, mikä edellyttää nopeita päivityksiä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet sekä ylläpito ovat puutteellisia.

↑ *kohonnut*

↓ *laskenut*

→ *ennallaan*

Keltainen = uutta/ päivitettyä*

4 UUSI

Heikko kyberriskienhallinta ja palveluidenhallinnan epäselvä vastuunjako. Kyberuhkien vaikutuksia ei osata ennakoida ja epäselvyydet palveluiden hallinnan vastuunjaossa heikentävät tietoturvaa.

5 UUSI

Lokitietojen puutteellisuus on riski monessa organisaatiossa. Puutteellisen lokitietojen keruun, seuraamisen ja säilyttämisen takia poikkeamatilanteita ei kyetä havainnoimaan tai selvittämään.

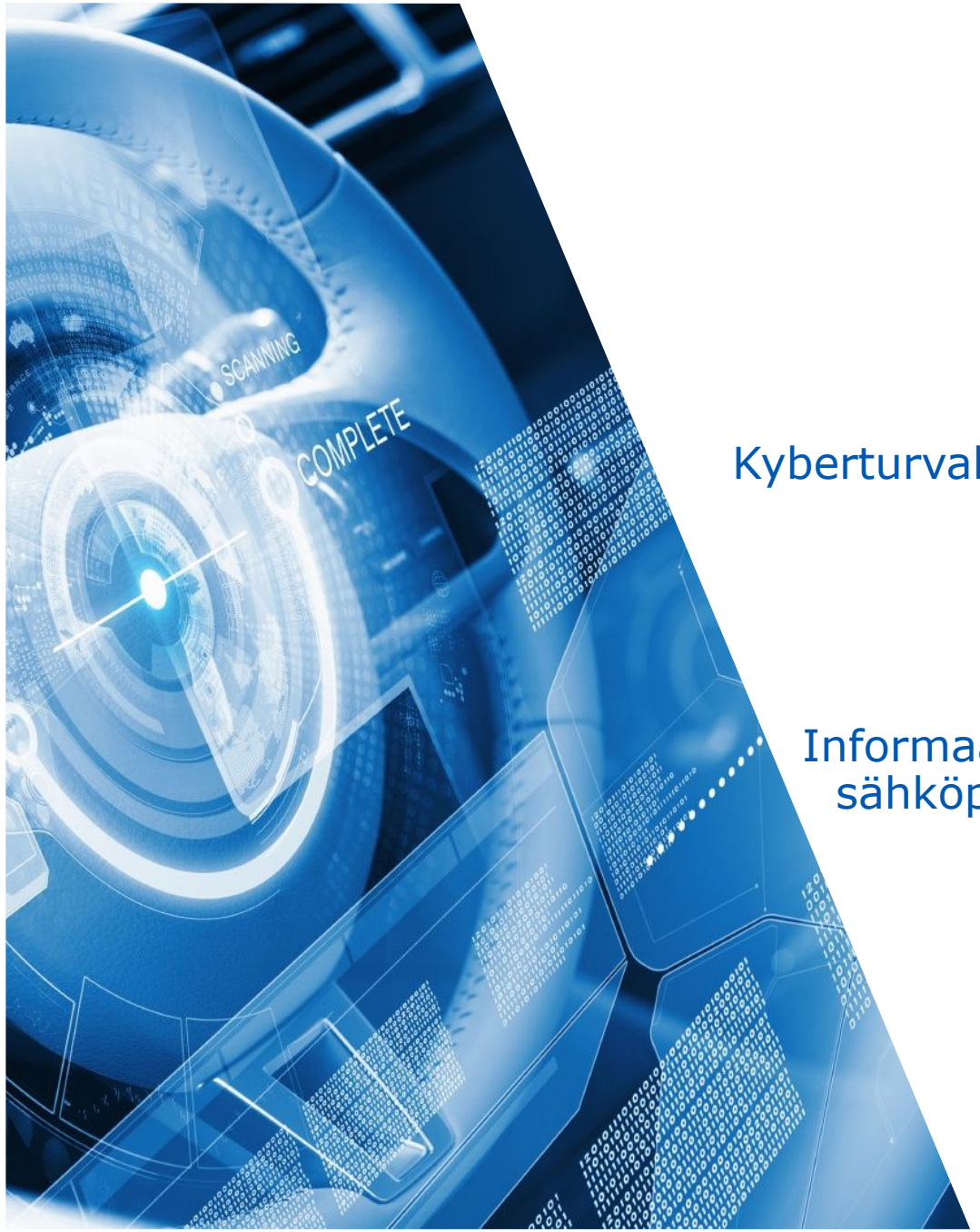
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

VAROITUS 1/2020
Emotet-haittaohjelmaa levitetään aktiivisesti Suomessa

- Emotet-haittaohjelmaa levitetään sähköpostitse suomalaisten organisaatioiden nimissä. Hyökkäyskampanja on näkynyt aktiivisena 17.8. alkaen.
- Emotet-haittaohjelmahyökkäyksen tavoitteena on varastaa organisaatioiden tietoja, tunkeutua verkkoon syvemmälle ja käynnistää esimerkiksi kiristyshaittaohjelmahyökkäys.
- Emotet-haittaohjelma hyödyntää varastamiaan tietoja leviämiseen. Se väärentää uuden sähköpostin vastaukseksi jo olemassaolevaan sähköpostiketjuun. Väärennetyssä viestissä on haitallinen liite. Viestin otsikko ja sisältö voivat olla mitä vain, sillä ne on kopioitu oikeasta viestistä.
- Henkilökunnan tiedottaminen on tärkeä keino haitallisia liitteitä vastaan. Työntekijöitä on syytä ohjeistaa olemaan avaamatta epäilyttäviä liitteitä, mutta tässä tapauksessa liitteelliset viestit voivat olla hyvinkin uskottavia. Henkilökuntaa on hyvä kouluttaa tunnistamaan väärennettyjä lähettäjätietoja. Virustorjuntaohjelmistojen tietokannat on päivitettävä ajan tasalle ja organisaation sähköpostiliitteiden välityspolitiikkaa kannattaa kiristää tiukaksi.
- Ilmoita Emotet-havainnosta
  - Ota yhteyttä Kyberturvallisuuskeskukseen, jos teillä on havaintoja Emotet-haittaohjelman leviämisestä tai tartunnoista. Yhteydenottoon voit käyttää Ilmoita meille -lomaketta (https://www.kyberturvallisuuskeskus.fi/fi/ilmoita) tai lähettää sähköpostin osoitteeseen cert@traficom.fi.
- Lisätietoa: https://www.kyberturvallisuuskeskus.fi/fi/emotet-haittaohjelmaa-levitetaan-aktiivisesti-suomessa

Kyberturvallisuuskeskuksesta ajankohtaista kyberturvallisuustietoa logistiikkatoimialan organisaatioille

- **Kyberturvallisuuskeskuksen tilannekuvatuotteet** tarjoavat ajankohtaista tietoa kyberturvallisuuteen vaikuttavista tapahtumista ja ilmiöistä.
  - **Viikkoraporttiin** koostamme viikon merkittävimmät tapahtumat ja uutisnostot. Viikkoraportti lähetetään kaikille toimialakohtaisten sähköpostilistojen tilaajillemme.
  - **Tietoturva Nyt!** -julkaisut käsittelevät kyberturvallisuuden ajankohtaisia ilmiöitä ja tapahtumia. Julkaisut lähetetään automaattisesti kaikille toimialakohtaisten sähköpostilistojen tilaajillemme ja lisäksi ne julkaistaan kyberturvallisuuskeskuksen verkkosivuilla.
  - **Kybersää** on kuukausittain ilmestyvä säätiedote, joka antaa kattavan kuvan edellisen kuun kybertapahtumista. Kybersää on ensisijaisesti kohdennettu tietoturvasta vastaaville henkilöille. Liittymällä toimialalistalle, saat uusimman kybersään myös sähköpostiisi.
  - **Varoitukset**-osiossa julkaistaan varoituksia merkittävistä tietoturvauhkista. Varoituksen väri on ilmoitettu julkaisussa. Kun punainen varoitus julkaistaan, sekä käyttäjien että palvelujen ylläpitäjien on ryhdyttävä korjaaviin toimiin välittömästi. Keltainen varoitus puolestaan kertoo tilanteesta, jossa käyttäjien ja ylläpitäjien on noudatettava yleistä varovaisuutta tai valmistauduttava mahdollisiin korjaaviin toimiin.
  - **Haavoittuvuustiedotteiden** avulla välitämme tietoa merkittävimmistä tietoomme tulleista ohjelmistohaavoittuvuuksia.
- Tilannekuvatuotteet saa käyttöönsä liittymällä logistiikkatoimialan organisaatioille tarkoitetulle toimialakohtaiselle sähköpostilistalle.
- Toimialakohtaiselle sähköpostilistalle lähetetään myös tietoa **logistiikkatoimialan kyberturvallisuuteen** liittyvistä muista ajankohtaisista aiheista.
- Toimialakohtaiselle sähköpostilistalle liittymistä voi tiedustella lähettämällä viesti sähköpostiosoitteeseen cert@traficom.fi.
- Lisätietoa tilannekuvatuotteista osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen.



TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuuden huomiointi tulevissa hankkeissa oleellista!

Millaisia kokemuksia kyberturvallisuuden huomioimisesta on saatu?

Informaatiota ja kysymyksiä otetaan mielellään vastaan sähköpostitse osoitteella virpi.tuulaniemi@traficom.fi

Kiitos!

https://www.kyberturvallisuuskeskus.fi/