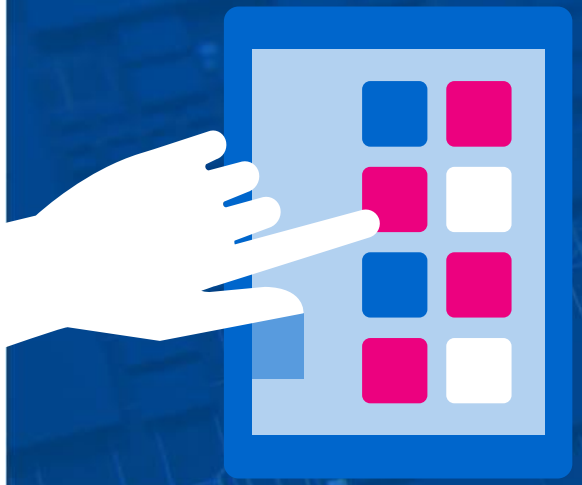
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuus raiteilla

29.10.2020

Virpi Tuulaniemi
Erityisasiantuntija
Liikenteen kyberturvallisuuden koordinaattori

Kyberturvallisuuskeskus – kansallinen tietoturvaviranomainen



Kerää tietoa tietoturvaloukkauksista ja niiden uhkista

Tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta

Selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia sekä niiden uhkia

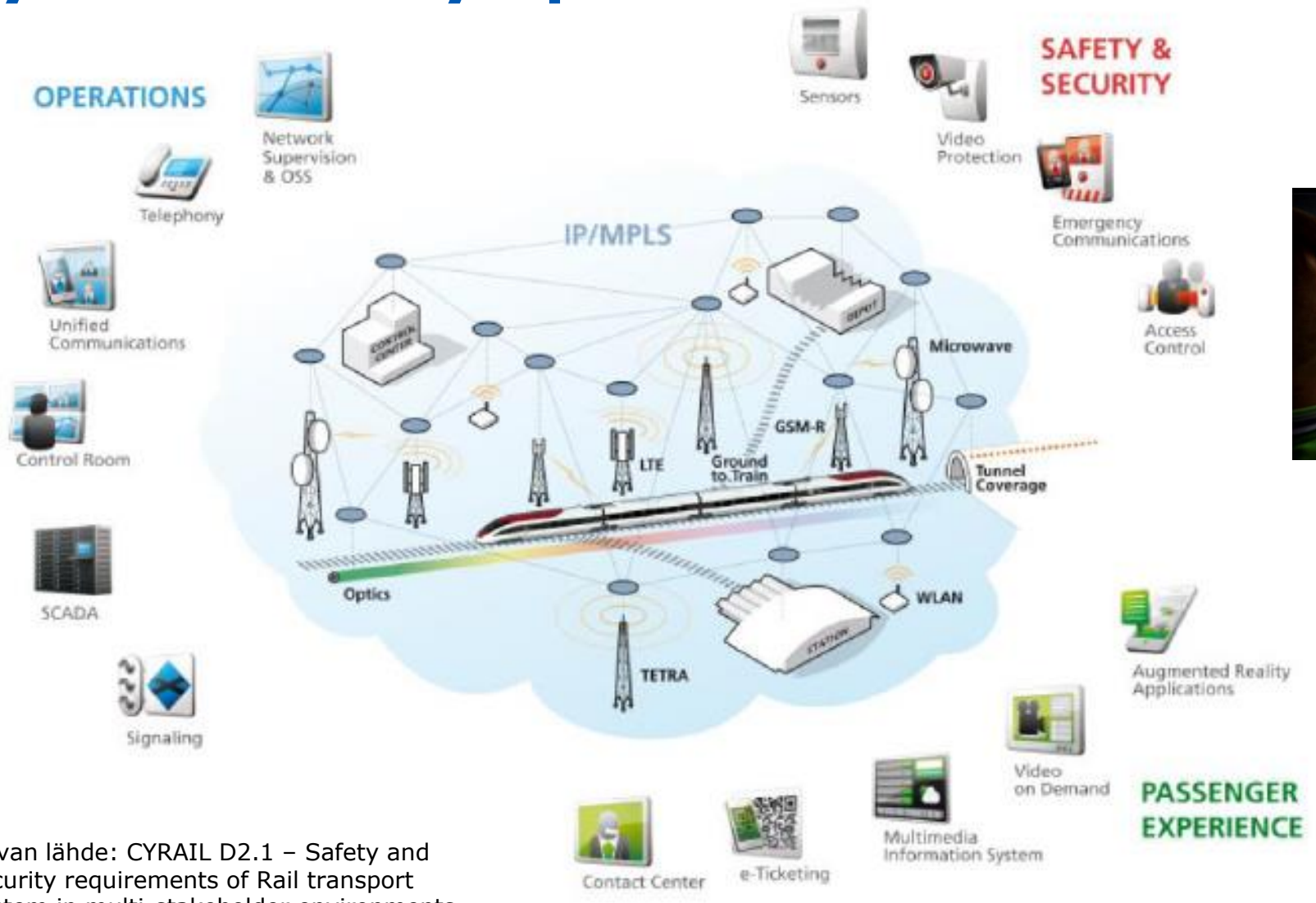
Arvioi ja hyväksyy järjestelmiä ja verkkoja

Ohjaa ja valvoo

- teleyritysten tietoturvallisuutta ja varautumista
- sähköisen viestinnän luottamuksellisuuden suojaa ja
- vahvojen sähköisten tunnistus- ja luottamuspalvelujen tietoturvaa

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybertoimintaympäristö



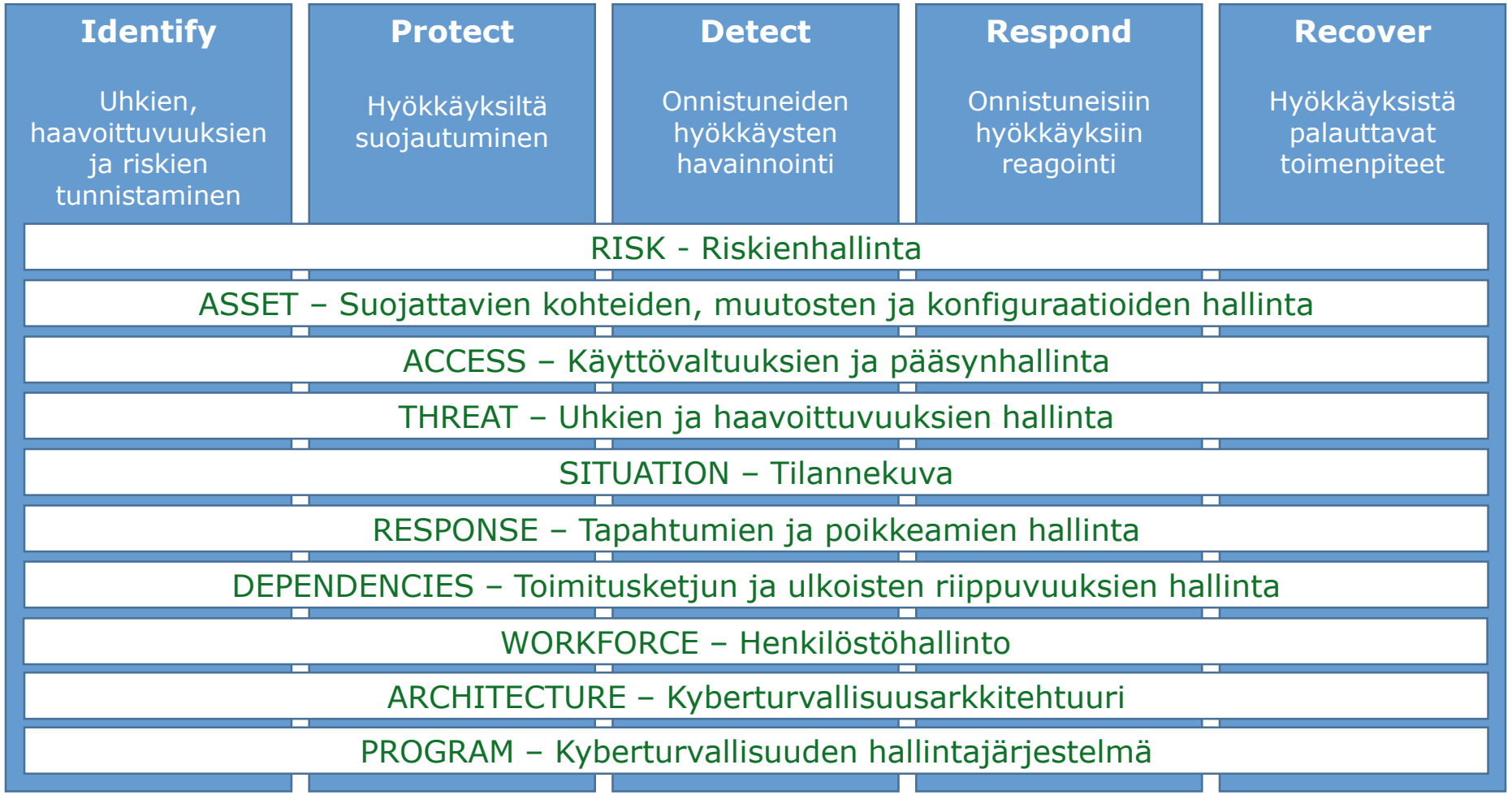
Kuvan lähde: CYRAIL D2.1 – Safety and security requirements of Rail transport system in multi-stakeholder environments

Tietoturvallisuus ja kyberturvallisuus

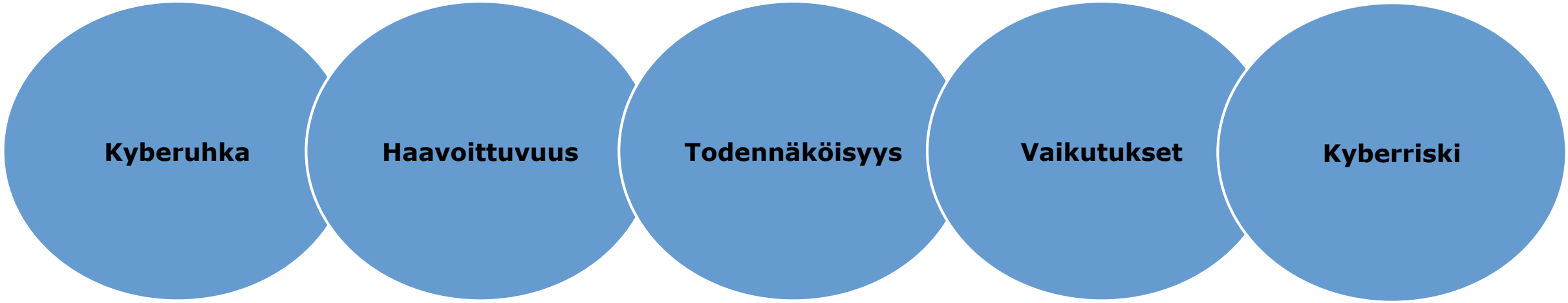
Käsite	Määritelmä
Tietoturvallisuus	Tietoturvallisuudella tarkoitetaan **järjestelyjä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus**. Saatavuus tarkoittaa, että tieto on **hyödynnettävissä haluttuna aikana**. Eheys tarkoittaa **tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa** ja luottamuksellisuus sitä, **ettei kukaan sivullinen saa tietoa.** Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa myös oloja, joissa tietoturvariskit ovat hallinnassa.
Kyberturvallisuus	Kyberturvallisuus on **tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan**. Kyberturvallisuuteen kuuluvat **toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia**. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä **tietoturva on keskeinen tekijä**. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on **turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot**. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa **digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin**.

Lähde: Kyberturvallisuuden sanasto, Turvallisuuskomitea 2018

NIST- ja C2M2-dimensiot (v2 mukaan)



Kyberuhka, haavoittuvuus, kyberriski



- Haitallinen tapahtuma tai kehityskulku
- Kohdistuu kybertoimintaympäristöön
- Voi vaarantaa kybertoimintaympäristöstä riippuvaisen toiminnon

- Heikkous
  - Järjestelmissä (IT ja OT)
  - Prosesseissa
  - Ihmisen toiminnassa

- **Todennäköisyys** sille, että **uhka** hyödyntää **haavoittuvuutta** sekä niitä **vaikutuksia**, joita tämä haitallinen tapahtuma toteutuessaan organisaatiolle aiheuttaa.

IT- ja OT-järjestelmät

Toimintaympäristö	Ominaispiirteet	Esimerkit
Informaatiojärjestelmät (**IT,** information technology)	Liiketoimintaa tukevat IT-järjestelmät sekä IT-järjestelmät, jotka tukevat operatiivisia järjestelmiä ja tarjoavat liittymän operatiivisiin järjestelmiin.	Matkustajainformaatio, kuljettajan päätelaitesovellukset, kuljetusten seurantajärjestelmät, liikenteenohjauksen hallintajärjestelmät, yleisesti käytössä olevat tiedonsiirtotavat (esim. WLAN-verkko) sekä tieto- ja viestintäjärjestelmät
Operatiiviset järjestelmät (**OT**, operational technology)	Operatiiviset järjestelmät, joilla hallitaan liikenneverkkoinfrastruktuuria ja liikkuvaa kalustoa, kuten liikennöintiä, merkinantoa, voimanlähteitä, viestintää ja asemien hallintaa.	ERTMS, JKV, kauko-ohjaus, asetinlaitteet, sähkörata ja sen ohjausjärjestelmät, operatiivisten järjestelmien virransyöttö, kuumakäynti- ja lovipyöräilmaisinjärjestelmät

Kybersää syyskuu 2020

Tietomurrot ja -vuodot

- Olemme vastaanottaneet tavallista enemmän ilmoituksia murretuista kotimaisista sivustoista
- Maailmalla on paljon havaintoja terveysalan toimijoihin kohdistuneista kiristyshaittaohjelmista
- Office 365 –tietomurrot jatkuvat

Huijaukset ja kalastelut

- Postin nimissä on lähetelty tuhansia tekstiviestejä, jotka johtavat sekä tilausansaan, tietojenkalasteluun että haittaohjelmaan.
- Paljastuneen kalastelusivun takaa löytyi kymmenien uhrien tiedot, joiden avulla tietomurrot saatiin katkaistua.

Haittaohjelmat ja haavoittuvuudet

- Emotet leviää aktiivisesti sähköpostien liitetiedostojen avulla myös Suomessa.
- Zerologon-haavoittuvuutta hyväksikäytetään aktiivisesti. Varmista, että kaikki toimialueen ohjauskoneet on päivitetty.

Automaatio

- Microsoftin tutkimuksessa havaittiin haavoittuvuuksia 71% tutkituista automaatiojärjestelmäverkoista.
- Kasperskyn mukaan vuoden 2020 ensimmäisellä puoliskolla, vähiten hyökkäyksiä tehtiin pohjoiseurooppalaisia automaatiojärjestelmiä vastaan.

Verkkojen toimivuus

- Yhdeksän merkittävää toimivuushäiriötä, joista kolme johtui Aila-myrskystä. Muiden häiriöiden syynä useimmiten sähkönsyötön vika tai ylläpitotöissä tehty virhe.
- Palvelunestohyökkäysten osalta kohtuullisen rauhallista Suomessa, mutta hyökkäyksillä uhkailu nousussa.

Vakoilu

- Microsoft kertoi APT28-ryhmän kampanjasta, jonka pyrkimyksenä on ollut kerätä lukuisten organisaatioiden työntekijöiden salasanoja.
- Erilaisia ilmaisia tai kokeilujaksollisia palveluita voidaan hyödyntää komentokanavina haitallisen liikenteen piilottamiseksi.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Varoitus 1/2020 Emotet-haittaohjelmaa levitetään aktiivisesti Suomessa

- Emotet-haittaohjelmaa levitetään sähköpostitse suomalaisten organisaatioiden nimissä.
- Hyökkäyskampanja on näkynyt aktiivisena 17.8.2020 alkaen ja se on jatkunut myös syyskuussa.
- Keltainen varoituksemme kertoo tilanteesta, jossa käyttäjien ja ylläpitäjien on noudatettava yleistä varovaisuutta tai valmistauduttava mahdollisiin korjaaviin toimiin.
- Lue koko varoitus: https://www.kyberturvallisuuskeskus.fi/fi/emotet-haittaohjelmaa-levitetaan-aktiivisesti-suomessa

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

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

5

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

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Merenkulun kyberhyökkäyksiä

Kyberhyökkäyksiä varustamojätteihin

- Kaikki neljä suurinta varustamoa ovat kärsineet valtavia tuhoja kyberhyökkäyksistä
- Kohteena maapuolen IT-järjestelmät
- Maersk kesäkuussa 2017
  - Joutuivat uusimaan koko IT-järjestelmänsä
- Cosco heinäkuussa 2018
  - IT-palvelut sekaisin viikkojen ajan
- Mediterranean Shipping Company (MSC) huhtikuussa 2020
  - Geneven pääkonttori ja sen datakeskuksen IT-palvelut kiinni muutaman päivän ajan
- CMA CGM syyskuussa 2020
  - Toimistot Shanghaissa, Shenzenissä ja Guangzhoussa kiinni

https://www.tivi.fi/uutiset/tama-alaa-vetaa-kyberrikollisia-nelja-suurinta-yritysta-iskujen-kohteina/fb8d2af5-1da5-41de-91c0-fc5e9efe3d8e

Kyberhyökkäys Antwerpenin satamaan

- 2011 - 2013
- Kohdennettu hyökkäys
- Huumeiden salakuljettajat rekrytoivat hakkereita hyökkäämään IT-järjestelmiin, jotka kontrolloivat konttien liikkeitä ja sijaintia
- Tietojen avulla huumeiden salakuljettajat pystyivät varastamaan lastin ennen lastin oikeiden omistajien saapumista

https://www.bbc.com/news/world-europe-24539417

Raidesektorin kyberhyökkäyksistä

- **Tietovuoto UK:ssa**
  - Rautatieasemien ilmaista Wi-Fi:ä käyttäneiden n. 10 000 henkilön sähköpostiosoitteita ja matkustustietoja oli ollut avoimesti internetissä saatavilla.
  - Tietoturvatutkija oli löytänyt avoimena internetistä 146 milj. tietueen tietokannan, jossa henkilöiden yhteystietoja ja syntymäaikoja.
  - https://www.bbc.com/news/technology-51682280, 2.3.2020
- **Kyberhyökkäys ja kiristys Sveitsissä**
  - Rautatiekalustovalmistajalta kyberhyökkäyksessä varastettuja luottamuksellisia dokumentteja oli julkaistu internetissä, kun valmistaja oli kieltäytynyt maksamasta lunnaita.
  - https://www.railjournal.com/technology/internal-documents-published-after-stadler-refuses-us-6m-ransom/, 29.5.2020
- **Kiristyshaittaohjelma Espanjassa**
  - Infrastruktuurin haltijaan oli kohdistunut kiristyshaittaohjelmahyökkäys, jossa hyökkääjä väitti saaneensa 800 GB tietoa ja kiristi tietojen julkaisulla ja uusilla hyökkäyksillä.
  - https://www.railjournal.com/technology/adif-hit-by-cyberattack/, 23.7.2020

Raidesektorin kyberturvallisuushaasteita

- Sektorin digitaalinen kulttuuri ja kyberturvallisuuskulttuuri sekä niihin liittyvä tietoisuus
- Vahvat riippuvuudet toimitusketjuista teknisissä ja kyberturvallisuuden standardeissa ja vaatimuksissa
- Sektorin erityispiirteet: hajautettu infrastruktuuri, vanhat legacy-järjestelmät
- Vaikeus sovittaa turvallisuus (safety) ja kyberturvallisuus (akkreditiointi, kulttuuri, lainsäädäntö)
- Kustannukset: turvallisuus (security) vs kilpailukyky ja toiminnallinen tehokkuus
- Sääntelyekosysteemin monimutkaisuus: Erot NIS-direktiivin (verkko- ja tietoturvadirektiivin) kansallisessa täytäntöönpanossa

Lähde: Marianthi Theocharidou, ENISA, Addressing the cyber-security risks for rail –webinaarissa 30.6.2020, https://www.globalrailwayreview.com/webinar/101253/webinar-addressing-cyber-security-rail/

Verkko- ja tietoturvadirektiivi (NIS-direktiivi)

- **N**etwork and **I**nformation systems **S**ecurity
- Yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi Euroopan unionin kaikissa jäsenmaissa yhteiskunnan kriittisille sektoreille ja toimijoille.
- Ensimmäinen laatuaan, ollut voimassa 5/2018 lähtien
  - Nyt uudelleenarvioitavana
- Suomessa 13 eri kansallista sektorikohtaista lakia, mm. raideliikennelaki
  - Implementointityössä (2016-2018) muutettiin 9 lakia
    - Myös rautatielakia, 41a § > raideliikennelaki 169 §

NIS-direktiivin päätavoite

- Määritetty yhteiskunnalle kriittiset sektorit ja toimijat
- Vähimmäisvaatimukset tietoturvalle
  - Riskienhallinta
  - Varautuminen
- Ilmoitusvelvollisuus
- Yhteistyö (kotimaassa ja EU-tasolla)
- Määritetty valvovat sektoriviranomaiset

Tiedonjako ja Tilannekuva

NIS-direktiivi - sektorit, toimijat ja valvovat viranomaiset

- Sähkönjakeluverkon ja suurjännitteisen jakeluverkon haltijat
- Sähkön kantaverkonhaltija: Fingrid
- Maakaasun siirtoverkonhaltija: Gasum

n. 90 toimijaa

Energia
Energiavirasto

- Sosiaali- ja terveyspalvelujen antajat
- Lääkinnällisten laitteiden valmistajat
- SOTE-tietojärjestelmien valmistajat

n. 350 + 100 toimijaa

Terveydenhuolto
Valvira

- Pankit
- Pankkien keskusyksiköt
- EU-pankkien sivuliikkeet

n. 320 toimijaa

Finanssiala
Finassivalvonta

- Pörssi: Nasdaq

1 toimija

Finanssialan infrastruktuuri
Finanssivalvonta

- Ilmailu:
  Air Navigation Services Finland, Finavia Helsinki-Vantaa lentokenttä
- Merenkulku:
  Vessel Traffic Services Finland Oy, Turun, Naantalin, HaminaKotkan ja Helsingin satamat
- Rautatieliikenne:
  Väylävirasto rataverkon haltijana, Finrail Oy
- Maantieliikenne:
  Intelligent Traffic Management Finland Oy

10 toimijaa

Liikenne
Traficom

- Vesilaitokset:
  jotka toimittavat/vastaanottavat yli 5000 m3/vrk vettä

n. 60 toimijaa

Vesihuolto
Maa- ja metsätalousministeriö
ELY-keskukset

- Teleyritykset (DNS)
- Yhdysliikennepisteet (IXP)
- DNS nimipalveluiden tarjoajat
- .FI maatunnusrekisteri

n. 100 toimijaa

Digi-infrastruktuuri
Traficom, Kyberturvallisuuskeskus

- Pilvipalvelut
- Hakukoneet
- Verkon keskitetyt markkinapaikat

Ei koske pieniä-/mikroyrityksiä

Digitaaliset palvelut
Traficom, Kyberturvallisuuskeskus

Traficomin raideliikenteen kyberturvallisuussuositus

- Suositus on ensimmäinen askel kyberturvallisuustietoisuuden lisäämisessä
- Suositus sisältää yleistä tietoa kyberturvallisuudesta raideliikenteessä sekä toimenpideosion, jonka tarkoituksena on ohjata tärkeiden kyberturvallisuus-kysymysten pariin.
  - Suosituksessa toivotaan, että toimijat käsittelisivät toimenpideosion seuraavat asiakokonaisuudet 1.6.2021 mennessä:
    - Kyberturvallisuus osana turvallisuusjohtamista ja turvallisuuskulttuuria
    - Osaaminen ja pätevyydenhallinta
    - Kyberturvallisuusuhkien seuranta ja niihin varautuminen
    - Riskienhallinnan hyödyntäminen
    - Yhteistyön lisääminen
    - Kyberturvallisuuden ohjauksen kehittäminen
  - https://www.traficom.fi/fi/ajankohtaista/traficom-antoi-raideliikenteelle-kyberturvallisuussuosituksen
  - Suora linkki suositukseen: https://www.traficom.fi/sites/default/files/media/regulation/Suositus%20kyberturvallisuuden%20edist%C3%A4misest%C3%A4%20raideliikenteess%C3%A4.pdf

Raideliikenteen kyberturvallisuutta kehitetään kansainvälisesti

- Raideliikenteen kyberturvallisuus nousemassa mukaan myös standardeihin
  - Mm. CENELEC:in raideliikennettä koskeva kyberturvallisuusstandardi TS50701 ”Railway Application – Cybersecurity” työn alla
    - Tulossa äänestykseen marraskuussa (SESKO) ja julkaisuun 2021
- Kyberturvallisuutta kehitetään yhteistyöprojekteissa
  - Mm. Shift2Rail:in X2RAIL-1, CYRAIL, X2RAIL-3, 4SECURAIL -projektit https://projects.shift2rail.org/s2r_ip_TD_r.aspx?ip=2&td=1bccaf76-7915-4283-8b52-36afdb1bdf42
- ENISA:n ja ER-ISAC:in raidesektorin/rautatiesektorin tutkimus
  - Tutkimuksessa arvioidaan raidesektorin/rautatiesektorin kyberturvallisuuden tasoa ja tuodaan esille nykyiset käytännöt ja tärkeimmät kyberturvallisuushaasteet
  - Tulossa julkaisuun lokakuussa 2020. Tutkimus julkaistaan ENISA:n sivuilla https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0

Kyberturvallisuuden nykytila eri toimialoilla

- Huoltovarmuusorganisaation Digipoolin teettämä Kyberturvallisuus eri toimialoilla –kartoitus, jossa mukana 12 toimialaa, yli 100 suomalaisyritystä
- Johdon sitoutuminen ja ohjaus ratkaisevat yrityksen kyberkestävyyden ja sitä kautta liiketoiminnan jatkuvuuden

KEHITYSKOHTEET

Merkittävimmät yhteiset huoltovarmuusnäkökulmasta

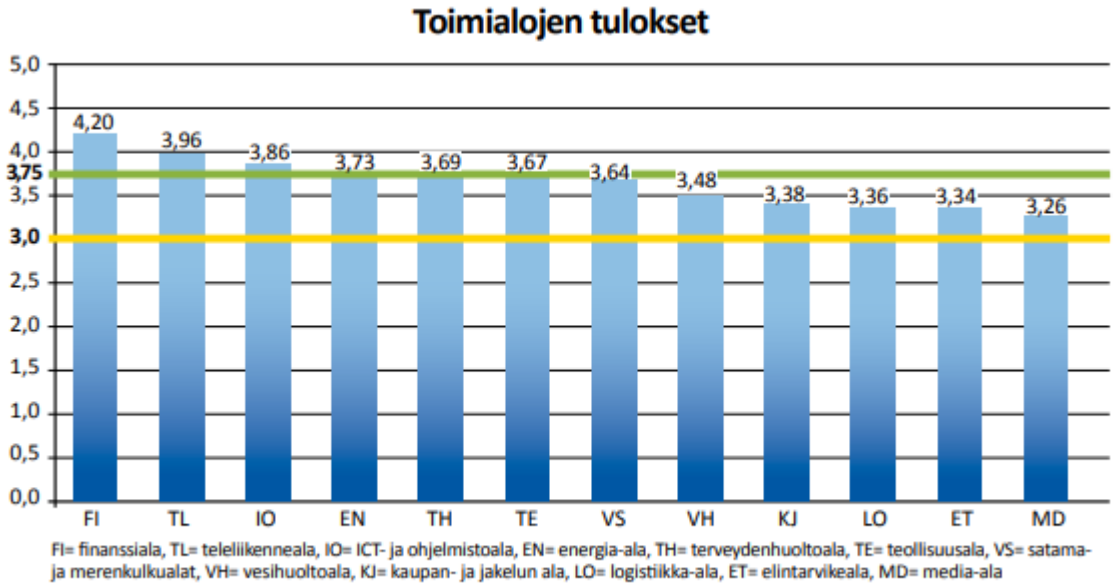
1. Yhteinen tilannekuva
2. Turvallinen ohjelmistokehitys
3. Henkilöstön osaaminen

Tärkeimmät yhtenevät yritysten liiketoiminnan näkökulmasta

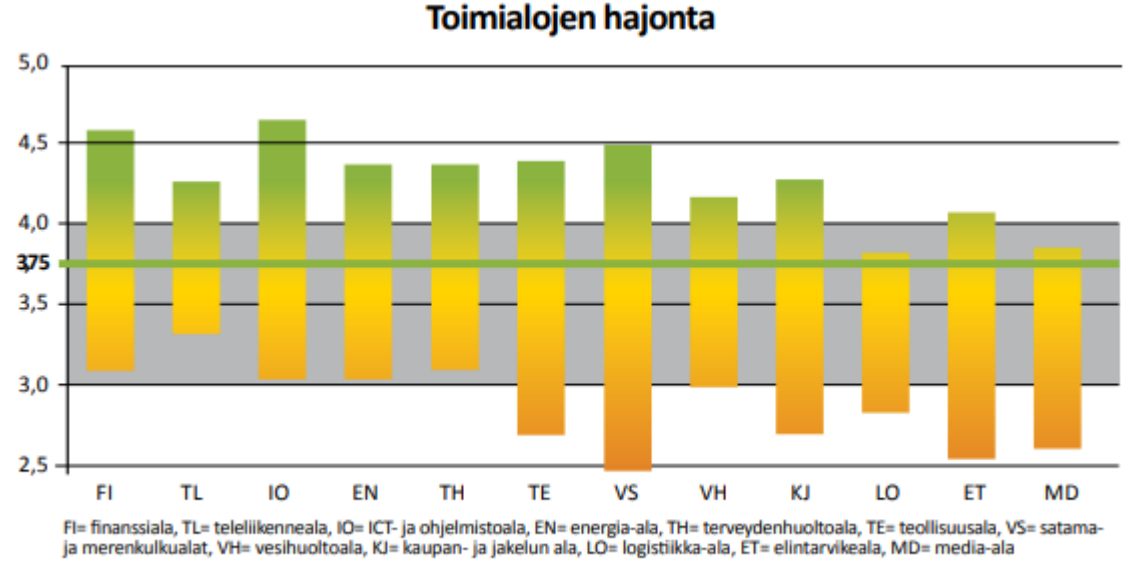
1. Yrityksen kyberturvallisuus-strategia
2. Kyberturvallisuusarkkitehtuuri
3. Tekninen jäljitettävyys

https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/10/07170555/Kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

Kyberturvallisuuden nykytila eri toimialoilla – tuloksia



Kuva 1. ***Kaikki toimialat ylittivät arvion keskinkertainen.***



Kuva 2. ***Hajonta on laajaa useilla toimialoilla yritysten välillä.***

Kybermittari

- Kybermittari on avoin kyberkyvykkyyden mittaamisen ja jatkuvan parantamisen ohjauksen mahdollistava kansallinen konsepti, joka auttaa
  - kriittisten palveluiden ja riskien tunnistamisessa,
  - organisaation ja toimialan tilannekuvan muodostamisessa,
  - vertailussa toimialatuloksiin ja parhaisiin käytäntöihin sekä
  - kehitysalueiden tunnistamisessa ja toimien kohdistamisessa.
- Yhteinen tilannekuva tukee myös yhteiskunnan ja viranomaisten varautumiskyvyn ja huoltovarmuuden parantamista.

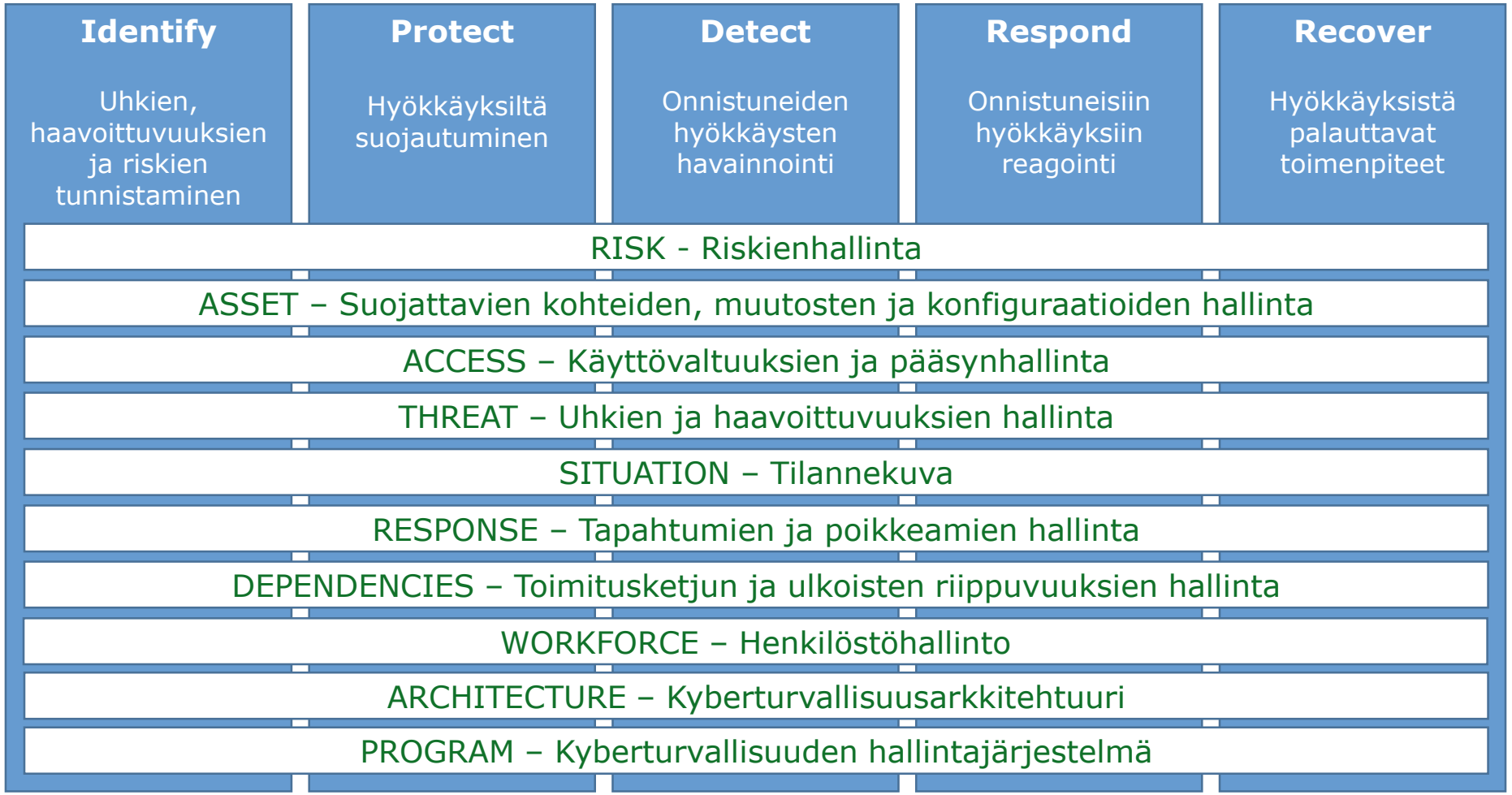
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

Kybermittarin sisältö

- Kybermittari perustuu mm. kansainvälisiin C2M2- ja NIST CSF kybermaturiteettimalleihin, joiden kehityksen mukana työkalu tulee kehittymään tulevaisuudessa.
  - Sovellusohje (fi, se, en)
  - Itsearviointityökalu (excel-pohjainen), tuottaa myös raportit (fi, se, en)
  - Esimerkki- ja koulutusmateriaaleja
  - Vertailutietoa
  - Tapahtumia
  - Verkostoitumisen tukitoimia
- Kyberturvallisuuskeskus toimii kansallisena luottamuspisteenä anonyymin vertailutiedon keräämisessä, säilyttämisessä ja jakamisessa
- Saatavilla vapaasti
- Julkaistu 27.10.2020
- www.kybermittari.fi, kybermittari@traficom.fi

NIST- ja C2M2-dimensiot (v2 mukaan)



Kyberturvallisuuskeskuksen harjoitustoiminta

Harjoitustoiminnan avulla **kehitetään organisaatioiden reagointikykyä kyberhäiriötilanteisiin** sekä lyhennetään ja pienennetään tietoturvapoikkeamien vaikutuksia.

- Tuemme huoltovarmuuskriittisten yritysten kyberturvallisuuteen liittyvää harjoitustoimintaa.
- Tarjoamme asiantuntijatukea ja materiaalia harjoitusten järjestämiseen ja realististen, tosielämän tietoturvaloukkauksiin perustuvien harjoitusskenaarioiden suunnitteluun.
- Lisätietoa https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta, kyberharjoitukset@traficom.fi

Tilaa ajantasaista tietoa kyberturvallisuudesta!

- Ajankohtaista tietoa kyberturvallisuuteen vaikuttavista tapahtumista ja ilmiöistä
  - Viikkoraportti
  - Tietoturva Nyt!
  - Kybersää
  - Varoitukset
  - Haavoittuvuustiedotteet
  - Toimialakohtaista kyberturvallisuustietoa
- Tietoa voi tilata liittymällä Kyberturvallisuuskeskuksen logistiikka-alan toimialakohtaiselle sähköpostilistalle
- Liittymistä voi tiedustella osoitteesta cert@traficom.fi
- Lisätietoa https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen

Kyberturvallisuuskeskuksesta ohjeita ja oppaita

https://www.kyberturvallisuuskeskus.fi/fi/ohjeet

Organisaation tilanteen selvittäminen

- Selvittäkää tärkeimmät asiat esim.
  - Organisaation hallussa olevat henkilötiedot
  - Organisaation immateriaalioikeudet
  - Julkinen verkkosivusto
  - Teollisuuden ohjausjärjestelmät
  - Sisäverkon käyttäjien ja pääsynhallinnan järjestelmä
- Lähtötilanteen määrittely
  - Mitkä järjestelmät ovat yhteydessä toisiinsa
  - Kenellä on pääsy tiettyihin tietoihin
  - Kuka omistaa minkäkin verkon tai palvelun
- Kriittisten tietoteknisten resurssien määrittely
- Yhteistyö palveluntarjoajien ja kumppanien kanssa

Kysymyksiä pohdittavaksi

- Ymmärrämmekö organisaationa, miten tekniset järjestelmät, prosessit tai resurssit edistävät tavoitteidemme saavuttamista?
  - Mitkä ovat organisaatiomme kriittiset tietotekniset resurssit, joita ilman organisaatiomme ei selviäisi?
  - Mitä vaatimuksia meidän on täytettävä (esimerkiksi oikeudelliset vaatimukset tai sopimusvelvoitteet)?
  - Mitä emme halua tapahtuvan ja miten se voisi tapahtua?
  - Onko organisaatiollamme prosessi tärkeiden järjestelmien, tietojen ja palvelujen tunnistamiseen sekä näiden toimivuuden ja turvallisuuden seuraamiseen.
- Onko organisaatiossa viestitty selkeästi organisaation tärkeimmistä tavoitteista ja varmistettu, että nämä prioriteetit ohjaavat myös kyberturvallisuustoimenpiteitä?
  - Kyberturvallisuuden tulee tukea organisaation strategiaa. Kyberturvallisuutta ohjaavien dokumenttien, kuten kyberturvallisuusstrategian tai -politiikan, on suojattava organisaation strategisia tavoitteita.

Riskienhallinta ja kyberturvallisuus

- Sisällyttäkää kyberturvallisuus organisaation riskienhallintaprosesseihin
- Älkää mitatko onnistumista riskitason pienentymisellä
- Kyberriskejä tulee arvioida useammin kuin muita riskejä

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

Kiitos!

virpi.tuulaniemi@traficom.fi

kyberturvallisuuskeskus.fi

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus