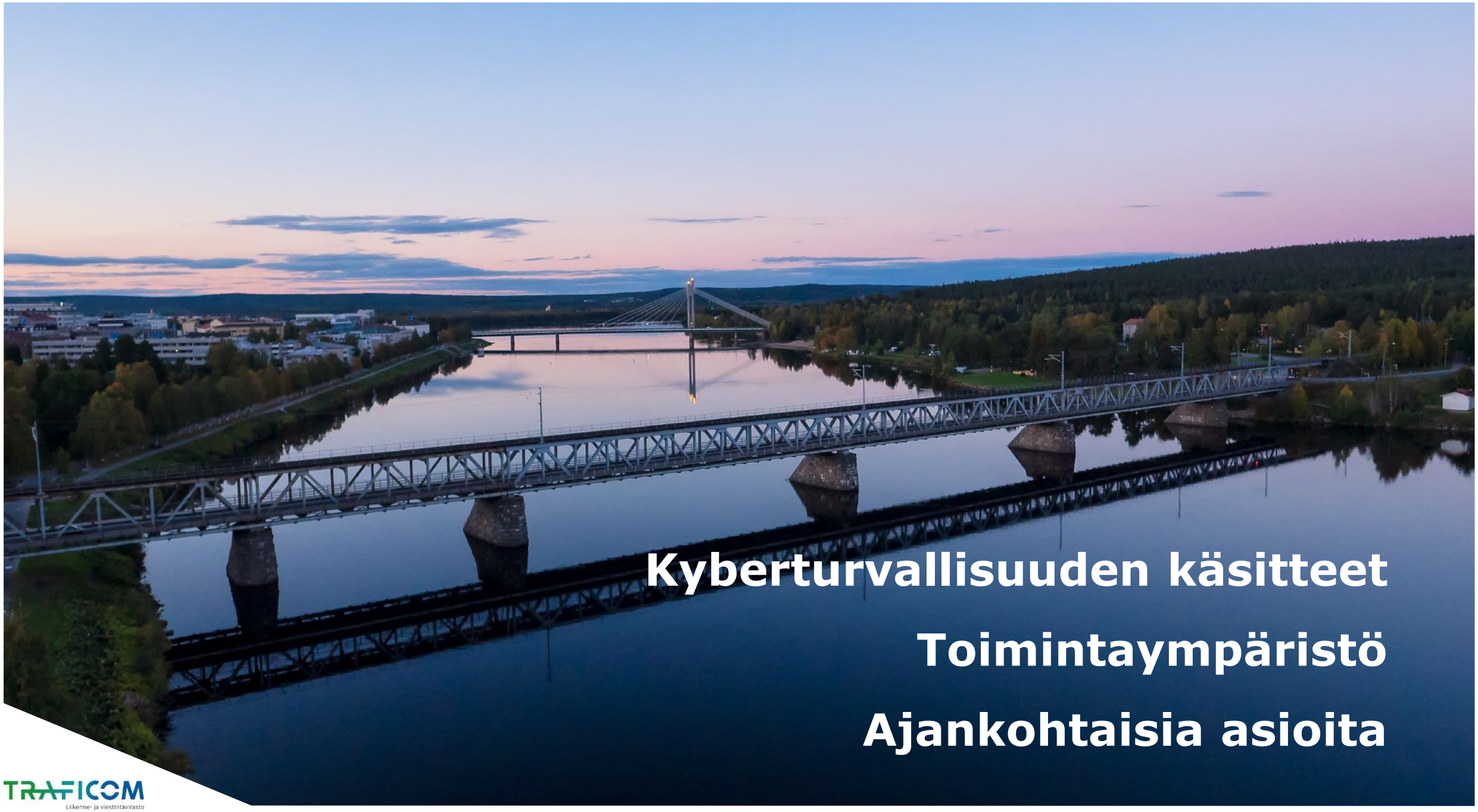
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuuskeskuksen tietoisku

Raideliikenteen kyberturvallisuuspäivä 11.3.2020

Virpi Tuulaniemi
erityisasiantuntija
liikenteen kyberturvallisuuden koordinaattori



Kyberturvallisuuden käsitteet

Toimintaympäristö

Ajankohtaisia asioita

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuus

- Kyberturvallisuudella ymmärretään tilaa, jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta on turvattu (Kyberturvallisuuden sanasto 2018).

- Kybertoimintaympäristö puolestaan voidaan käsittää samana kuin digitaalinen toimintaympäristö, joka kehittyy yhteiskunnan osana ja palveluina nopeasti.

https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

Muutamia kyberturvallisuuden käsitteitä

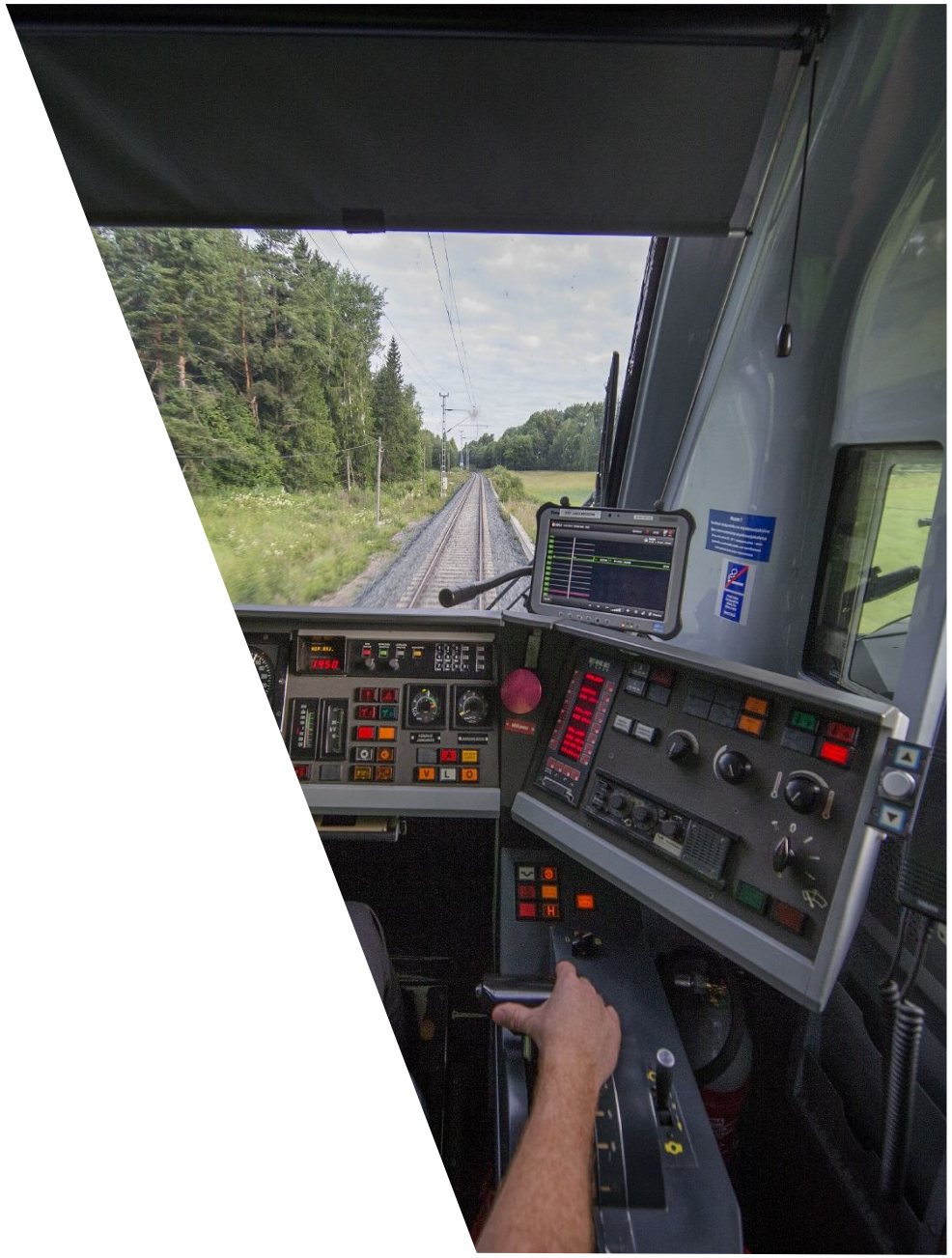
- **Riski** – yhdistelmä todennäköisyyttä, että uhka hyväksikäyttää olemassa olevaa haavoittuvuutta, ja kyseisen ei-toivotun tilanteen vaikutuksia
- **Uhka** – mikä tahansa olosuhde tai tapahtuma, jolla voi olla haitallisia vaikutuksia organisaation toimintaan tai henkilöt, jotka vastoin tietoturvapolitiikkaa estävät tahallisesti tai tahattomasti pääsyn tietoihin tai aiheuttavat tietojen tuhoamisen, paljastamisen tai muuttamisen
- **Haavoittuvuus** – heikkous tietojärjestelmässä, järjestelmän turvallisuusmenettelyissä, sisäisessä valvonnassa tai toteutuksessa, joita uhkalähde voi hyödyntää tai laukaista
- **Kyberresilienssi** – kyky ennakoida, kestää, toipua ja sopeutua kyberresursseihin kohdistuviin epäsuotuisiin olosuhteisiin, stressiin, hyökkäyksiin ja vaarantumisiin

https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf

Raideliikenteen kybertoimintaympäristö

- Hyökkääjillä on melko helppo fyysinen pääsy
- Monipuolinen ja maantieteellisesti hajautunut ekosysteemi
- Ekosysteemissä sekä turvallisuuskriittisiä, että ei-turvallisuuskriittisiä järjestelmiä (tässä: turvallisuus = safety)
- Pitkän elinkaaren omaavaa legacya
- Kyberturvallisuuden yhteistyöprojekteja:

CYRAIL 4SECURail



Kaiken digitalisoituminen ja verkottuminen

Laskentateho
Supertietokoneet
Yhteiskunnalliset taidot
6G
Tekoäly
IoT
VR&AR
Kyberturvallisuus
ja **luottamus**
Kvanttiteknologia
5G

Ulko- ja turvallisuus politiikka

BBC: Venäjä kertoo testanneensa onnistuneesti maan sisäistä tietoverkkoa

25.12.2019 YLE

Supo: 5g-verkkotoimijat arvioitava ja poliittinen keskustelu käytävä

20.12.2019 DigiToday

Valuutanvaihtoyhtiö Travelex joutui kyberhyökkäyksen kohteeksi, hakkerit vaativat yhtiöltä 5,3 miljoonan euron lunnaita

7.1.2020 Helsingin Sanomat

Perinteinen tietoturva

Kunnilla heikkoja salasanoja ja huteria palomuureja – Lahti maksoi kyberhyökkäyksen torjunnasta liki miljoonan ja jakaa nyt oppeja muillekin

27.12.2019 YLE

Uutinen

Windowsissa ”poikkeuksellisen pelottava” haavoittuvuus – turvallisuusvirasto löysi aukon

15.1.2020 Tekniikka & Talous

Kiristyshaittaohjelmatapauksia liikennesektorilla

- Liikenne ja logistiikkasektori ovat erityisen houkuttelevia kohteita kiristyshaittaohjelmatoimijoille
- Onnistuneita hyökkäyksiä on ollut usein
- Liikennesektorin
  - organisaatiot voivat olla kohde siinä missä mikä tahansa organisaatio millä tahansa sektorilla
  - infrastruktuuri on osa kriittistä infrastruktuuria ja on siksi ollut valtiollisten toimijoiden kiristyshaittaohjelmahyökkäyksien kohteina. Ko. hyökkäyksien tavoitteena on aiheuttaa vieraalle valtiolle sekasortoa ja kaaosta.
- Big game hunting (BGH) –taktiikan hyödyntäminen, joissa yhdistetään kohdistettu hyökkäys ja kiristyshaittaohjelma, on lisääntynyt. BGH-hyökkäyksien tavoitteena on saada rahaa. Niiden kohteena on tyypillisesti organisaatiot, joilla ei ole varaa häiriöihin.
- Hyökkääjien kiinnostuksen kohteena ovat todennäköisimmin ilmailun lennonjohdon järjestelmät, rahtiprosessit ja lentokoneet sekä merenkulun isot infrastruktuurit kuten satamat.
- CERT-EU:n muistio: https://media.cert.europa.eu/static/MEMO/2020/TLP-WHITE-CERT-EU-THREAT-MEMO-200121.pdf

Raideliikenteen tapahtumia

UK rail network attacked by Hackers four time in a year

Independent 13.6.2016

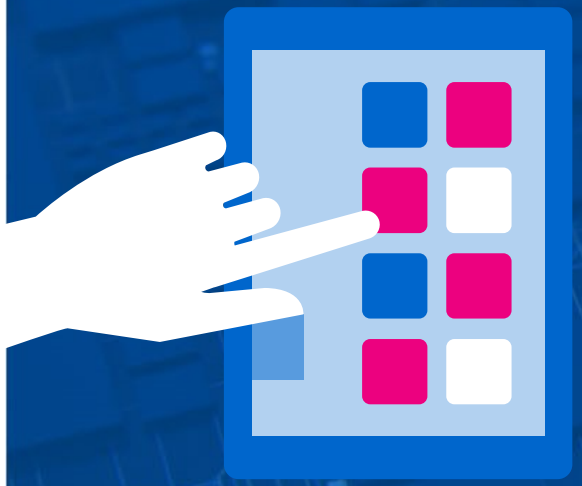
DDoS Attacks Cause Train Delays Across Sweden

Bleeping Computer 13.10.2017

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuuskeskus turvaa digitaalista yhteiskuntaa

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 ja .fi-verkkotunnusvälittäjien tietoturvallisuutta ja varautumista
- sähköisen viestinnän yksityisyydensuojaan liittyvien velvoitteiden

ja vahvojen sähköisten tunnistamis- ja luottamuspalveluja

Kyberturvallisuuskeskuksen palvelut

1 Tilannekuva ja verkostojohtaminen

2 Havainnointi ja avunanto

3 Muut viranomaispalvelut

1 Tilannekuva ja verkostojohtaminen

- Tilannekuva
- Ohjeet ja suositukset
- Haavoittuvuuskoordinaatio
- Yhteistyöverkostot
- Harjoitustoiminta

Tilannekuva

Tilannekuvatuotteet antavat ajantasaista tietoa kyberturvallisuuteen vaikuttavista tapahtumista ja ilmiöistä.

Tilannekuvatuotteitamme ovat:

- Varoitukset
- Toimialakohtainen tilannekuva ja tiedotteet
- Haavoittuvuustiedotteet
- Tietoturva Nyt -julkaisut
- Viikkoraportti
- Kybersää
- Uutiskirje
- Haavoittuvuuskooste

- Saat tuotteet käyttöösi liittymällä toimialakohtaisille sähköpostilistoille.
- Uutiskirjeen ja haavoittuvuuskoosteen voit tilata internet-sivuiltamme osoitteesta:
- www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

Ohjeet ja suositukset

www.kyberturvallisuuskeskus.fi/fi/ohjeet

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberharjoittelu

Kyberturvallisuuskeskuksen palvelut

kyberharjoitukset@traficom.fi

Kyberharjoitus

- Simuloitu (vakava) tietoturvaloukkaustilanne.
- Harjoituksessa mallinnetaan uhka- tai poikkeustilanne ja reagoidaan siihen asianmukaisin keinoin.
- Harjoituksen aika, sisältö ja laajuus on vapaasti määriteltävissä.
- Opit helposti analysoitavissa ja jalkautettavissa käytäntöön

Harjoitus on (lähes) ilmainen hallittu kriisitilanne!

Harjoittelun edut

- Vahvistaa käsitystä kyberongelmien laajoista vaikutuksista.
- Kehittää toimintatapoja ja prosesseja.
- Paljastaa puutteita varautumisessa.
- Kehittää kriisiviestintäkykyä.

Parantaa toimintakykyä kriisitilanteessa ja nopeutta toipumista.

Kyberturvallisuuden arviointimalli -hankkeen esittely

kybermittari@traficom.fi

Hankkeen tarkoitus

Tarkoituksena on toimijakohtaisesti kartoittaa suomalaisen kriittisen infrastruktuurin osalta liiketoimintakriittisten järjestelmien

- keskeisimmät kyberriskit,
- toimijoiden riskinottohalukkuus
- kyberriskien hallintaan kohdistettujen resurssien ja kontrollien taso suhteutettuna eri viiteryhmiin.

Kartoituksen lopputuloksena syntyy tarkka kuva

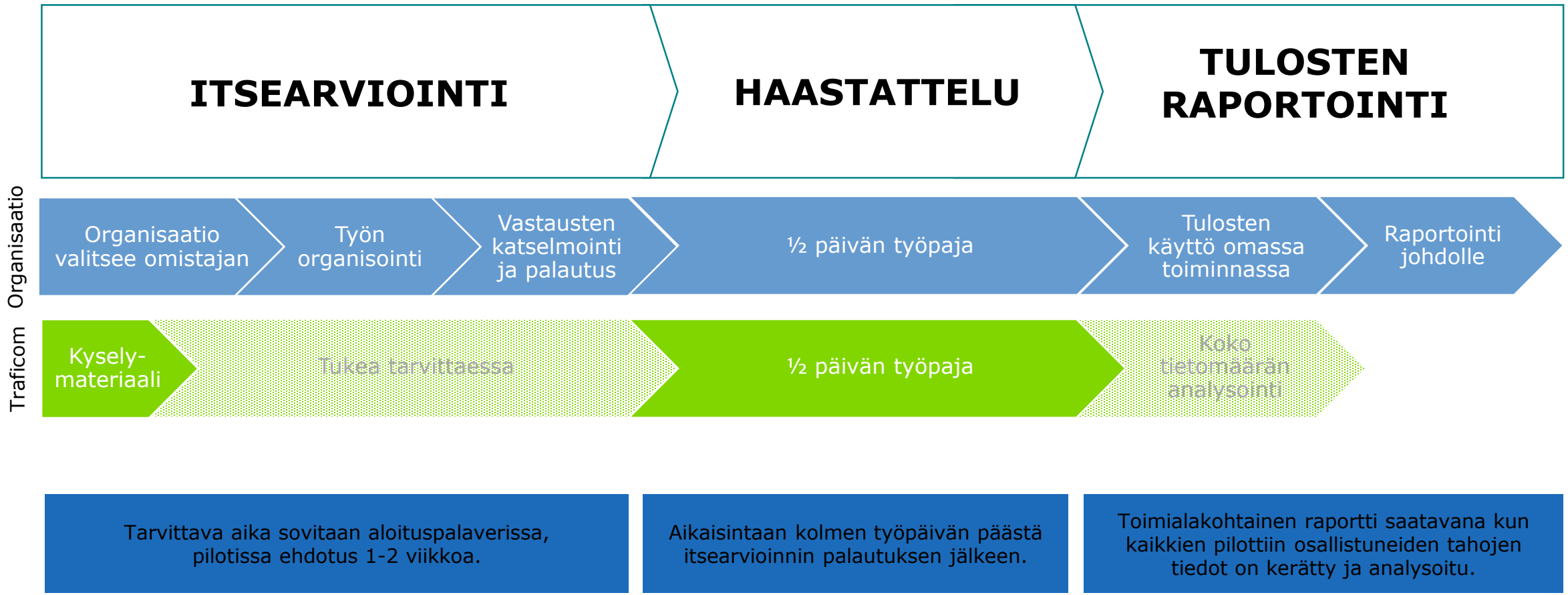
- koko sektorin halukkuudesta ja kyvykkyydestä vastata kyberriskeihin
- käytännön toimenpidesuositukset kyberturvallisuuden parantamiseksi.

Tärkeimpinä sidosryhminä ovat huoltovarmuuskriittiset yhtiöt, Huoltovarmuuskeskus sekä Kyberturvallisuuskeskus.

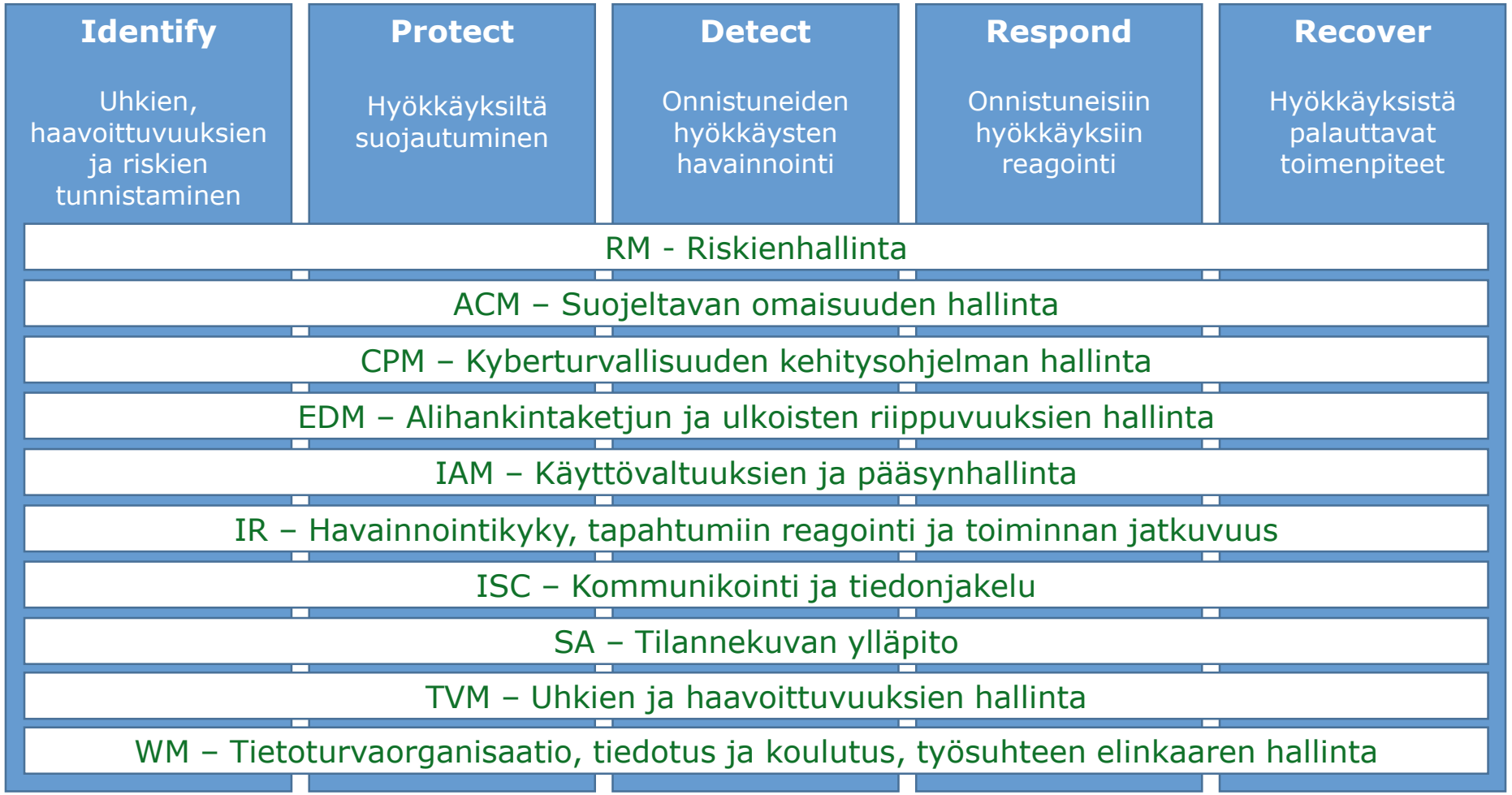
Kartoituksen sisältö

- Kartoitus kattaa yleisimmät kyberturvallisuuden riskienhallinnan osa-alueet
- Erityisenä fokuksena on liiketoiminnalle ja yhteiskunnalle kriittiset toiminnot ja niiden jatkuvuus häiriö- ja poikkeustilanteissa
- Kartoitus kattaa myös kyberturvallisuuden kehittämiseen ja ylläpitämiseen tarkoitetut investoinnit ja niiden kohdistuminen
- Tuloksena tuotetaan viitekehyksen perusteella mitattu organisaation kyberturvallisuuden kypsyystaso eri osa-alueilla (tasot 0-3)
- Malli pitää sisällään työkalun sovellusohjeen ja mittauksen sekä kartoitukseen käytettävän työkalun

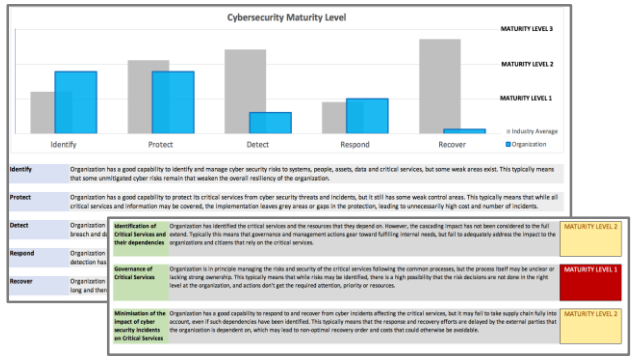
Arviointiprosessi

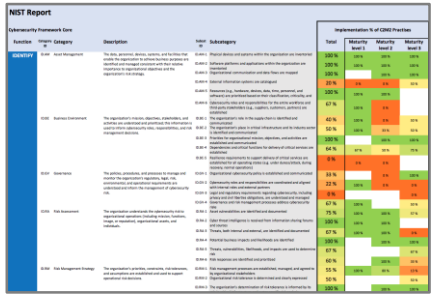


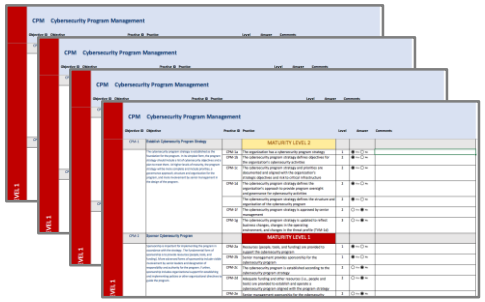
NIST- ja C2M2-dimensiot



Raportit







CIO/CISO/CSO
Prosessien omistajat
Yksityiskohtien tarkastelu prosessien näkökulmasta

Vastaukset

Ylin johto

- Yleinen maturiteetti ja kyvykkyys
  - Uhkien, haavoittuvuuksien ja riskien tunnistaminen (identify)
  - Hyökkäyksiltä suojautuminen (protect)
  - Onnistuneiden hyökkäysten havainnointi (detect)
  - Onnistuneisiin hyökkäyksiin reagointi (respond)
  - Hyökkäyksistä palauttavat toimenpiteet (recover)
- Vertailu omaan toimialaan
- Kriittisten palveluiden suojaaminen

CIO/CISO/CSO
Tietoturva-arkkitehti
Yksityiskohtien tarkastelu identify/protect/detect/respond/recover

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Tammikuu 2020

Poimintoja

Kybersää tammikuu 2020

Tietomurrot ja -vuodot

- Tietomurtoja käytetään kiristyshaittaohjelmien asentamiseen
- Office 365 –tietomurrot jatkuvat entiseen tapaan

Huijaukset ja kalastelut

- Organisaatioihin kohdistuvat laskutushuijaukset ovat aiheuttaneet tuntuvia rahan menetyksiä
- Henkilökunnan kouluttaminen auttaa suojautumaan huijauksia vastaan

Haittaohjelmat ja haavoittuvuudet

- Kriittisten päivitysten laiminlyönti vaarantaa yritystoiminnan jatkuvuuden

Automaatio

- Tutkimuksen mukaan eri valtiolliset toimijat ovat aktivoituneet energiasektorilla Yhdysvalloissa viime aikoina

Verkkojen toimivuus

- Palvelunestohyökkäyksillä ei ollut merkittäviä vaikutuksia palveluiden toimintaan
- Määräys teletoiminnan häiriötilanteista uudistettiin

Vakoilu

- Vakoilu kohdistuu valtioiden lisäksi myös yrityksiin

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

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

2

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

3

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

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Puutteet lokien tarkkailussa vaikeuttavat uhkien havaitsemista.

5

Organisaatiot eivät osaa hallita kyberriskejään. Uhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Palautumissuunnitelmissa on puutteita.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

1

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

- Rikolliset kehittävät hyväksikäyttömenetelmiä nopeasti heti ohjelmistopäivitysten ilmestyttyä ja iskevät kohteisiin, joita ei ole päivitetty. Erityisesti tietoturvatuotteissa olevat haavoittuvuudet ovat vakavia, sillä ne on yleensä sijoitettu muutenkin hyökkäyksille alttiisiin tietojärjestelmien kohtiin.
- Hyökkäyksissä käytetyt järjestelmähaavoittuvuudet ovat usein olleet 2-6 kk vanhoja haavoittuvuuksia, joihin on korjaus ollut saatavilla jo pitkään, mutta syystä tai toisesta haavoittuvuutta ei ole korjattu.
- Mitä pidempään haavoittuvuuden korjaamisessa kestää tai korjausta siirretään myöhemmäksi, sitä korkeammaksi hyväksikäyttämisen riski kasvaa.

CASE

Pulse Secure VPN:stä korjattiin kriittinen haavoittuvuus huhtikuussa 2019. Haavoittuvuuden hyväksikäyttömenetelmä julkaistiin elokuussa, jonka jälkeen hyväksikäyttöyrityksiä alettiin näkemään. Silti vielä tammikuussa 2020 haavoittuvuus on useissa kohteissa päivittämättä, ja sitä hyödynnetään yhä mm. laajavaikutteisissa kiristyshyökkäyksissä.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

2

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

- Tietojenkalastelu on ollut hyvin yleistä pidemmän aikavälin tarkastelulla. Tyypillisesti rikolliset kalastelevat suomalaisilta käyttäjätunnuksia ja salasanoja Office 365 -tuotteisiin ja sähköpostiin.
- Typosquatting / domainsquatting liittyvät myös ilmiöön: kirjoitusvirheillä höystetyillä verkkotunnuksilla voidaan tehostaa huijauksen vaikuttavuutta.
- Henkilökunnan koulutuksella on suuri merkitys. Tutkimusten mukaan tietojenkalastelua opitaan tunnistamaan koulutuksen avulla ja tämä auttaa siihen, että tietojenkalastelu jää vain yritykseksi.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

3

Laajavaikutteiset kiristyshyökkäykset (Big Game Hunting) uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

- Tapauksia myös Suomessa. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan seurauksena.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja. Jos rikolliset havaitsevat huonosti suojatun ympäristön kiristämisen arvoiseksi, siihen saatetaan kohdistaa Big Game Hunting –toimintaa.
- Yhdysvalloissa tilannetta voi kuvata jo epidemiaksi. Uusia ilmoituksia laajoista kiristyshaittaohjelmatartunnoista tulee kansainvälisesti viikoittain.

CASE

Norjassa Norsk Hydroon kohdennettu kiristyshaittaohjelma pääsi leviämään tuotantojärjestelmään asti. Toimintahäiriöt kestivät kuukausia ja kosketti yrityksen useita eri toimipisteitä.

Norsk Hydro arvioi omilla sivuillaan kiristyshaittaohjelman kokonaiskustannukseksi noin kuusikymmentä miljoonaa euroa.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Puutteet lokien tarkkailussa vaikeuttavat uhkien havaitsemista.

- Epäselvä vastuunjako ICT-palveluiden hankinnassa ja tuotannossa heikentää tietoturvan hallintaa. Tämä pätee myös organisaatioiden sisällä, jos tietoturvariskien omistajuus ja tietoturvavastuut eivät ole selkeästi määriteltyjä.
- Yleinen puute on jättää keräämättä ja tarkkailematta tietoturvalokeja. Lokien jatkuvan tarkkailun avulla tietojärjestelmän omistaja voi havaita lievät tietoturvaloukkaukset ja järjestelmän heikkoudet ennen kuin kukaan ehtii käyttää niitä suurempaan vahingontekoon. Lokeja tarvitaan myös loukkausten selvittämiseen jälkikäteen.
- Lisäksi käytöstä poistuvien palveluiden alasajo tulee tehdä huolella. Jos alasajotoimenpiteitä ei tehdä johdonmukaisesti loppuun asti, voi taustalle jäädä pyörimään käyttämättömiä palveluita, jotka voivat aiheuttaa merkittäviä tietoturvariskejä organisaatiolle.

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kaytosta-poistuvien-palveluiden-alasajo-tulee-tehda-huolella

OHJE

Top 5 kyberuhat – merkittävät pitkän aikavälin ilmiöt

5

Organisaatiot eivät osaa hallita kyberriskejään. Uhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Palautumissuunnitelmissa on puutteita.

- Tietoturvaloukkauksista toipumista ei usein suunnitella huolellisesti ennakkoon. Suunnitelmat ovat vain luokkaa "palautetaan tiedot varmuuskopioista". Palautumisen tärkeysjärjestyksiä ja resursseja ja aikajänteitä ei mietitä ennakkoon.
- Häiriön iskiessä palautumisen monimutkaisuus ja työläys yllättävät. Jos palautuminen olisi suunniteltu ennakolta paremmin, myös varautuminen häiriöihin ja niiden ennaltaehkäisyyn olisi parempaa.
- Kyberturvallisuuskeskus on julkaissut yritysten hallituksille suunnatun kyberturvallisuutta käsittelevän oppaan. Kyberturvallisuus ja yrityksen hallituksen vastuu -opas antaa työkaluja ja tukea organisaation kyberturvallisuuden parantamiseen.
  - https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas

Organisaatioiden kyvyssä hallita kyberriskejään on selviä puutteita. Tyypillisesti organisaatiot eivät osaa ennalta arvioida kyberuhkien toteutumisen vaikutuksia niiden päivittäiseen toimintaan, tai arvioivat vaikutukset selvästi todellista lievemmiksi. Tämän seurauksena on, että kyberriskit aliarvioidaan eikä niiden hallintaan osoiteta riittävästi resursseja.

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)

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tietoturvan vuosi 2019

- Kyberturvallisuuskeskuksen vuosikatsaus
  - Poimintoja

10 tietoturvanäkymää vuodelle 2020

1. Automatisoidut ja tekoälyä hyödyntävät tietoturvaratkaisut kehittyvät
2. Palveluja tuotetaan monikerroksisissa ja -kansallisissa alihankinta-ketjuissa
3. Kyberturvalli-suuden vaikutus liiketoimintaan huomioidaan aiempaa paremmin
4. Suojautuminen ontuu, koska kyberrikollisuuden luonnetta ei tunneta riittävästi
5. Kyber-turvallisuuden harjoittelu lisääntyy
6. Löydettyjä tietoturva-aukkoja hyödynnetään yhä nopeammin
7. Monipuolisten tietoturvaosaajien tarve kasvaa
8. Pilveen siirtyy tietojen lisäksi toiminta
9. Tietoturva-arviointien suosio lisääntyy tietoisuuden noustessa
10. Tietoturvan taso on sidoksissa henkilöstön valveutu-neisuuteen

TOP 3: uhat ja ratkaisut organisaatioille

UHAT

- Tietojen kalastelu ja huijaukset
- Uusia haavoittuvuuksia nopeasti hyödyntävät hyökkäykset
- Palvelujen keskittäminen ja ulkoistaminen ilman suunnittelua ja vastuuttamista

RATKAISUT

- Juurruta kyberturvallisuus riskienhallintaanne
- Harjoittele häiriö- ja poikkeamatilanteissa toimimista
- Vastuuta toimittajat ja selvitä palveluidenne liitännäisyydet

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos!

virpi.tuulaniemi@traficom.fi

https://www.kyberturvallisuuskeskus.fi