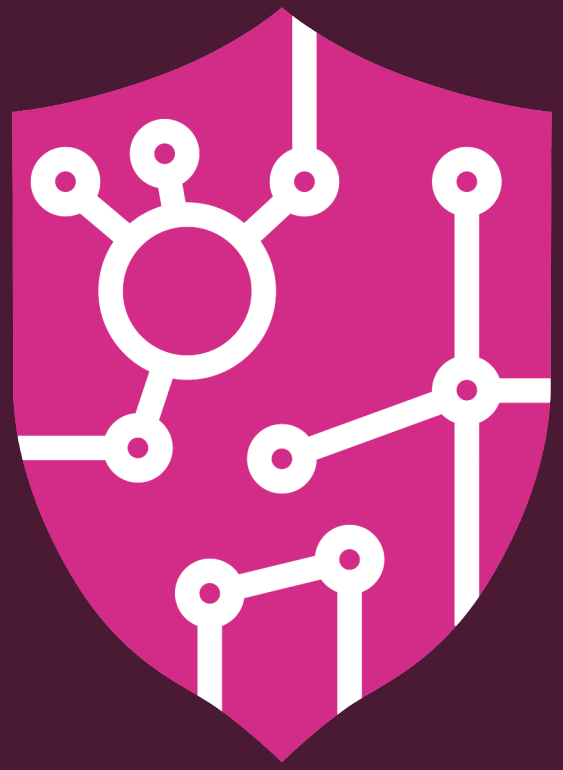


Tietoturvan perusasiat kuntoon järjestöissä!

Anu Laitila, KyberVPK

SOSTE 17.11.2020, #digiosaavatjärjestöt

Agenda

- Termit tutuiksi
- Miten parantaa järjestön tietoturvaa?
- Vinkkejä oman tietoturvan parantamiseen
- Yhteenveto ja aikaa kysymyksille

Tietoturva

- Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon
  - **Luottamuksellisuus (Confidentiality)** eli se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla,
  - **Eheys (Integrity)** eli se, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä
  - **Käytettävyys (Availability)** eli se, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.

Tietosuoja

- Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä
- Henkilötietojen käsittelyn on aina perustuttava lakiin
- Riippumaton viranomainen valvoo henkilötietojen suojaa koskevien säännösten noudattamista

Miten parantaa järjestön tietoturvaa?

Vastuut ja roolit

- Tietoturvan (ja –suojan) hoitamisessa on oltava vastuuhenkilö, joka seuraa ja tarkkailee tietoturvan tasoa sekä kehittää sitä jatkuvasti

Kybersää lokakuu 2020

Tietomurrot ja -vuodot

- Office 365 –tapauksista edelleen ilmoituksia
- Psykoterapiakeskus Vastaamoa ja sen asiakkaita kiristettiin tietovuodon uhalla. Potilas- sekä henkilötietoja vuodettiin
- https://tietovuotoapu.fi –sivustolle on koottu neuvoja.

Huijaukset ja kalastelut

- Office 365 -tunnuksia on kalasteltu erittäin uskottavilla Zoom-kokouskutsuilla.
- COVID19-teema on palannut pornokiristyksiin, lahjoitushuijauksiin, nigerialaiskirjeisiin ja monenlaisiin tietojenkalastelukampanjoihin.

Haittaohjelmat ja haavoittuvuudet

- Kiristyshaittaohjelmia on kohdennettu terveydenhuoltosektoriin
- Postin nimissä levitetään Android-haittaohjelmaa

Automaatio ja IoT

- Nokian julkaisemassa uhkaraportissa kolmasosa kaikista haittaohjelmahavainnoista kohdistui IoT-laitteisiin.
- Osuus nousi vuoden takaisesta 17 prosenttiyksiköllä, mikä kertoo IoT-laitteiden heikosta tietoturvatasosta ja määrän lisääntymisestä.

Verkkojen toimivuus

- Vain kolme merkittävää häiriötä kotimaisissa viestintäpalveluissa
- Microsoftin ja Slackin palveluissa maailmanlaajuisia häiriöitä
- Kyberturvallisuuskeskus sai ilmoituksia palvelunestohyökkäyksistä, joilla oli myös laajoja vaikutuksia palveluiden toimintaan.

Vakoilu

- Norja syyttää Venäjää maansa parlamenttiin aiemmin syksyllä kohdistuneesta kyberhyökkäyksestä.
- Suojelupoliisin mukaan koronaviruspandemia on kasvattanut kybervakoilun roolia suhteessa muuhun vakoiluun. Supon mukaan Suomi on erityisesti Venäjän ja Kiinan kiinnostuksenkohteena.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1 ↑

Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja 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.

Mistä lähteä liikkeelle?

Selvitä organisaatiosi tietoturvan nykytila (1/2)

- Mitä tietoja pitää suojata eli mitkä ovat ns. kriittisiä tietoja?
- Mitä riskejä tunnistatte nykyisissä toimintatavoissa?
- Mikä on teknisen tietoturvan taso ja mistä organisaation mistä tietotekninen ympäristö käytännössä koostuu
  - mitä sovelluksia on käytössä ja mitkä järjestelmät ovat yhteydessä toisiinsa?
  - kuka omistaa minkäkin verkon tai palvelun ja miten vastuu on jakautunut (sopimukset)?
  - kenen laitteita ja ohjelmia organisaation työntekijät ja vapaa-ehtoiset käyttävät, miten ne on suojattu?
  - onko ohjelmisto, palomuurit ja suojaohjelmat yms. ajantasalla?
  - onko organisaation internetliikenne ja -yhteydet suojattu?
  - onko tietokoneiden kovalevyt ja sähköpostit salattu?

Selvitä organisaatiosi tietoturvan nykytila 2/2

- Onko henkilökunnalle ohjeistuksia esim. salasanoista ja kaksivaiheisesta tunnistautumisesta ja miten he toimivat, jos havaitsevat esim. tietojenkalasteluviestin?
- Mikä on fyysisen turvan taso:
  - Onko organisaation tiloissa hälytyslaitteet ja/tai valvontalaitteet?
  - Kenellä on tiloihin avaimet?
- Mitä tietoa säilytetään arkistossa esim. paperina?
- Miten organisaation on varautunut kyberturvaan liittyviin haasteisiin ja liiketoiminnan jatkuvuuteen häiriötilanteessa?
- Mitä kyberuhkia olette tunnistatte organisaation toiminnan jatkuvuudelle?
- Onko olemassa esim. toimialan vaatimuksia, joita organisaation tulee täyttää?
- Kuka vastaa tietoturvasta ja –tietosuojasta?

Mitä on organisaation toiminnan kannalta kriittistä tietoa?

- Selvitä, mikä on toiminnan kannalta kriittistä tietoa.
  - Mitä tietoja organisaatiossa säilytetään esim. henkilötietoja?
  - Kenellä on oikeus päästä organisaation käyttämissä järjestelmissä olevaan tietoon?
  - Miten tietoja säilytetään ja miten tiedot on suojattu?
  - Kuinka usein tiedoista otetaan varmuuskopiot?
  - Missä varmuuskopiot säilytetään??
  - Kuka varmuuskopiot tarvittaessa palauttaa?
  - Miten varmuuskopioiden palautus tehdään ja kuinka kauan siinä kestää?
  - Mikä on eri palveluiden/tietokantojen palautusten järjestys?

Henkilökunnan ohjeistukset ja koulutus

- Jokaisella työntekijällä ja vapaaehtoisella on tärkeä rooli organisaation tietoturvan edistämisessä
- Koulutuksien tavoitteena on lisätä henkilökunnan tietoturvaosaamista ja motivoida noudattamaan tietoturvallisia toimintatapoja

Mitä järjestelmiä organisaatioissa tulisi käyttää?

- Tutustu https://techsoup.fi/

Vinkkejä oman tietoturvan parantamiseen

Tietoturvavinkkejä

1

Pidä tietokoneen, tablettien ja puhelinten ohjel-mistot aina ajan tasalla

2

Valitse pitkät salasanat ja säilytä niitä huolellisesti ja valitse joka palveluun oma salasana. Ota kaksivaiheinen tunnistautuminen käyttöön

3

Käytä maalaisjärkeä ja mieti mitä julkaiset verkossa

4

Ennen kuin klikkaat ”mainosviesteihin” tai muihin tuntemattomiin linkkeihin tai liitteisiin, selvitä niiden alkuperä

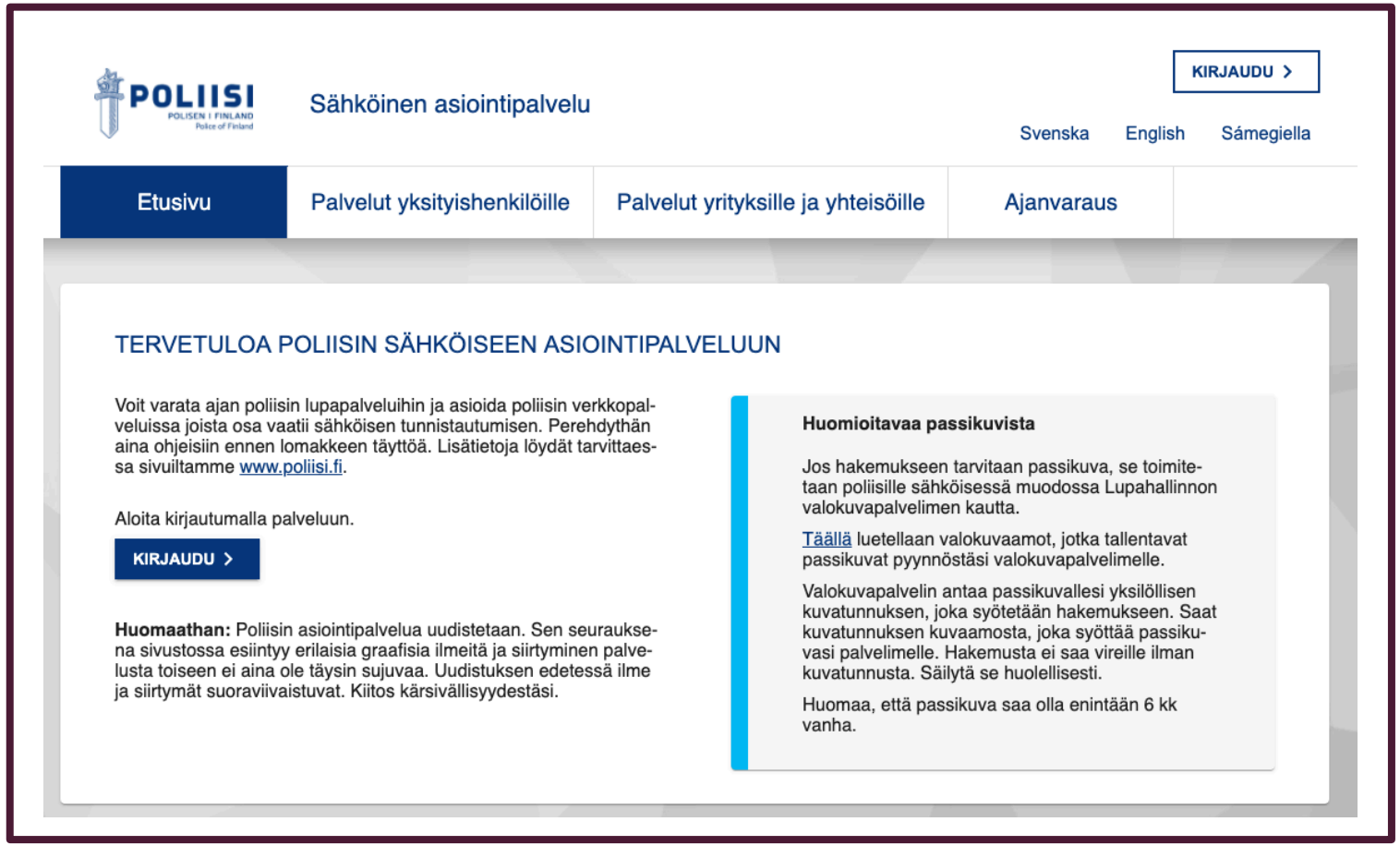
Mihin voi raportoida tietoturvapoikkeamasta?

Organisaation oma vastuuhenkilö

- IT
- toiminnanjohtaja
- toimitusjohtaja
- pääsihteeri
- Joku muu?

KyberVPK

Jos epäilet rikosta, tee rikosilmoitus https://asiointi.poliisi.fi/#main



KyberVPK

Vinkkaa asiasta myös Kyberturvallisuuskeskukselle https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Hae sivustolta

Suomi

ETUSIVU | AJANKOHTAISTA | PALVELUMME | TOIMINTAMME | OTA YHTEYTTÄ | Ilmoita tietoturvaloukkauksesta

Ota yhteyttä > Ilmoita meille

Ilmoita meille

Yksityiset henkilöt, yritykset ja organisaatiot voivat ilmoittaa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle niihin kohdistuneista tietoturvaloukkauksista, kuten tietojen kalastelusta tai palvelunestohyökkäyksistä, sekä näiden loukkausten yrityksistä.

Yhteydenottojen perusteella Kyberturvallisuuskeskus selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia, kerää tietoa näistä tapahtumista ja tiedottaa tietoturva-asioista. Kyberturvallisuuskeskus myös auttaa tietoturva-asioissa. Yleisen tietoturvatietouden lisäksi apu voi olla luonteeltaan teknistä.

KyberVPK

Ilmoitus tietosuojaloukkauksesta Tietosuojavaltuutetun toimistolle (72 h)

Ilmoitus tietosuojavaltuutetulle

Kun on kyse omista oikeuksistasi

Tietosuojaoikeudet auttavat sinua hallitsemaan omia tietojasi. Jos haluat käyttää oikeuksiasi, ole aina ensin yhteydessä henkilötietojasi käsittelevään yritykseen tai organisaatioon eli rekisterinpitäjään.

Jos rekisterinpitäjä kieltäytyy pyynnöstäsi eikä kieltäytymiselle ole mielestäsi perusteita, voit ottaa yhteyttä tietosuojavaltuutettuun. Tietosuojavaltuutettu voi joissakin tapauksissa määrätä rekisterinpitäjän toteuttamaan pyyntösi.

Lue lisää: Onko tietosuojaoikeuksiasi loukattu?

Kun on kyse muusta epäkohdasta henkilötietojen käsittelyssä

Voit ilmoittaa tietosuojavaltuutetulle, jos epäilet, että jokin organisaatio tai henkilö käsittelee henkilötietoja tietosuojasäännösten vastaisesti.

Epäkohta voi tarkoittaa esimerkiksi, että henkilötietojen käsittelylle ei ole lainmukaista perustetta tai että henkilötietoja käsitellään liian laajasti käsittelyn tarkoitukseen nähden.

Lue lisää: Havaitsitko epäkohdan henkilötietojen käsittelyssä?

KyberVPK

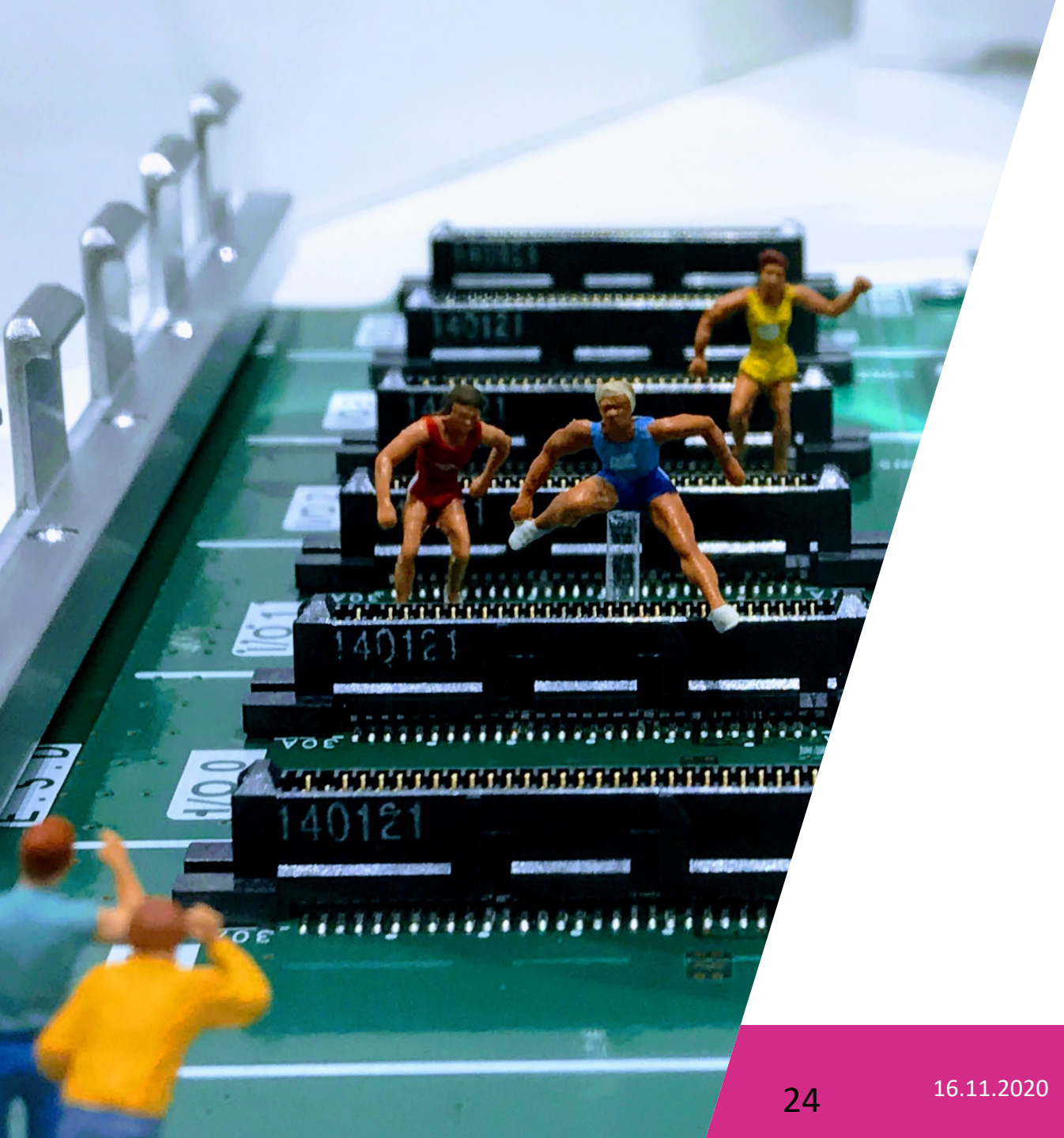
KyberVPK
COMMUNITY CYBER
RESPONSE FORCE

nixu
cybersecurity.

https://www.nixu.com/fi/palvelut/tietoturvaloukkaus

Avunpyynnöt ja yleiset tiedustelut:
contact@kybervpk.fi

Yhteenveto



Vinkkilista

- Vastuut ja roolit
- Kartoita nykytila
- Selvitä mitä pitää suojata ja mitkä ovat kriittisiä tietoja
- Tee tarvittavia teknisiä ja hallinnollisia toimenpiteitä tietoturvan varmistamiseksi
- Henkilökunnan ohjeistukset ja koulutus
- Muista jatkuvuus

Kenelle ilmoittaa tietoturvapoikkea masta?

- Oman organisaation vastuuhenkilöt
- Viranomaiset
- Kaupalliset toimijat
- KyberVPK

Ole utelias ja opi uutta!

- .. koskaan ei ole liian myöhäistä!

Linkkejä itseopiskeluun

Tutustu oppaisiin

- https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

- https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

KyberVPK

Lukemista - Kyberturvallisuuskeskukselta

- **Kybersää** https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa
- **Tietoturva nyt! –artikkelit** https://www.kyberturvallisuuskeskus.fi/fi/tietoturva-nyt?limit=20&offset=0&query=&sort=updated
- **Ohjeet ja oppaat** https://www.kyberturvallisuuskeskus.fi/fi/ohjeet
- **Tietoturvamerkki** https://tietoturvamerkki.fi/
- **Turvalistit** https://turvalistit.fi/

Lukemista

- **Yhteiskunnan turvallisuus strategia** https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/
- **Suomen kyberturvallisuusstrategia** https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/
- **Kyberin taskutieto** https://mpk.fi/wp-content/uploads/2019/04/MPK-JY-Kyberopas_2018-issuu.pdf
- **Kilpailu- ja kuluttajavirasto** https://www.kkv.fi/Tietoa-ja-ohjeita/viittomakieli/tunnista-verkkohuijaus/ ja https://www.kkv.fi/kuluttajakasvatus/alykoti/ (sivustolta löytyy useita muitakin eri aiheita digitaalisuuteen liittyen)
- **Kyberturvallisuuden nykytila** https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/10/07170555/Kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf
- **Katso myös muut Huoltovarmuuskeskuksen julkaisut** https://www.huoltovarmuuskeskus.fi/julkaisut/

Lukemista

- **Ylen toimittaja testasi tärkeiden yritysten ja laitosten tilaturvallisuutta: Lähes kaikilla puutteita kulunvalvonnassa** https://yle.fi/uutiset/3-10320853
- **Ylen digitreenit** https://yle.fi/aihe/digitreenit
- **Missä mun data** https://www.sitra.fi/tapahtumat/missa-mun-data-kansalaisen-digijalki/
- **Digibarometri 2020: Kyberturvallisuuden tilannekuva** https://www.etla.fi/julkaisut/digibarometri-2020-kyberturvan-tilannekuva-suomessa/
- **Sitra: digijälkitesti** https://www.sitra.fi/hankkeet/digijalki/
- **Yle: salasanakone** https://yle.fi/aihe/artikkeli/2017/02/01/digitreenit-17-salasanakone-testaa-kuinka-nopeasti-salasana-murretaan
- **Tietosuojasta lisätietoja** www.tietosuoja.fi
- **Kodin kyberopas** https://turvallisuuskomitea.fi/wp-content/uploads/2017/04/Kodin_kyberopas_TK_2017_verkkojulkaisu.pdf

Anu Laitila

+358 40 84 55 021

anu.laitila@kybervpk

www.nixu.com

@anujanina
@kybervpk

www.linkedin.com/in/anulaitila
company/kybervpk

KyberVPK

COMMUNITY CYBER
RESPONSE FORCE