Sopimuspalokunnan kyberturvallisuus

Perttu Halonen

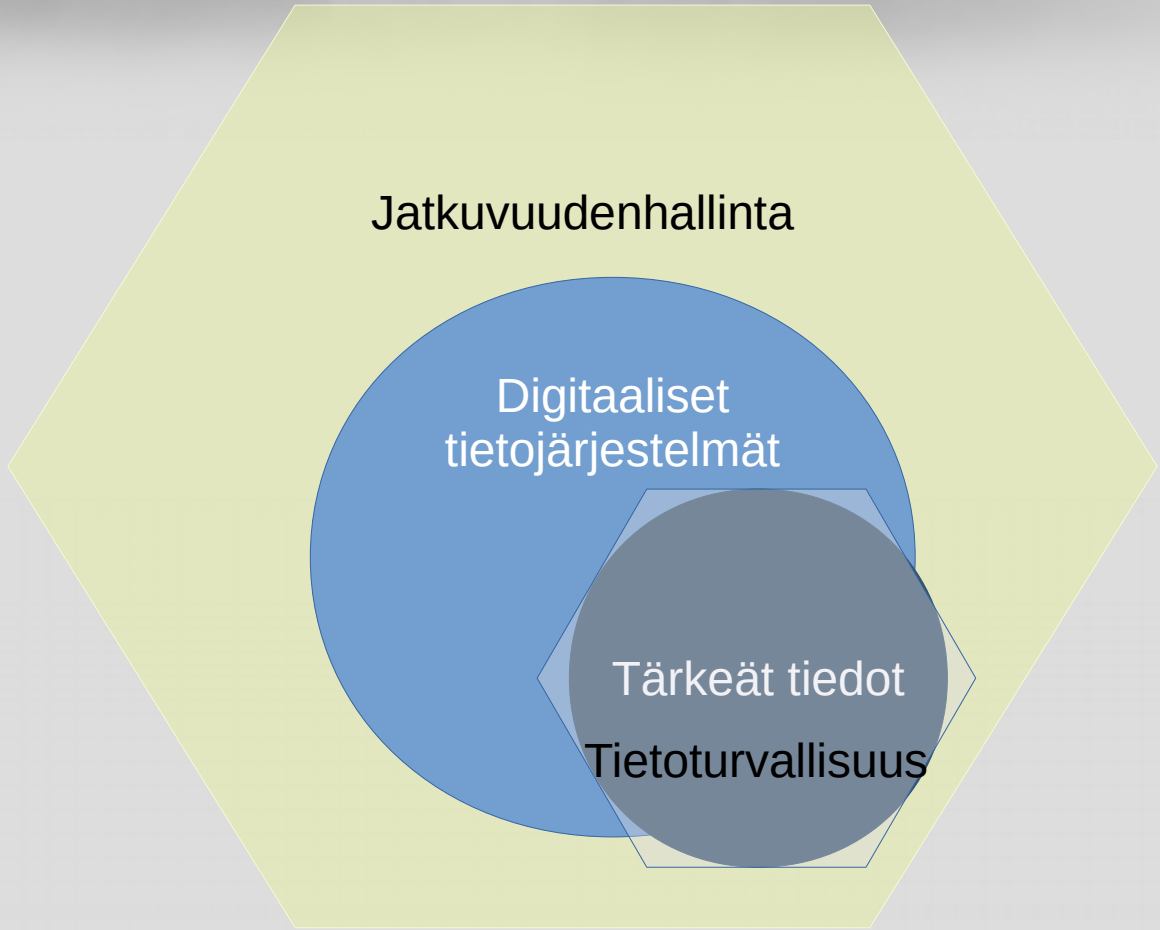
13.4.2023

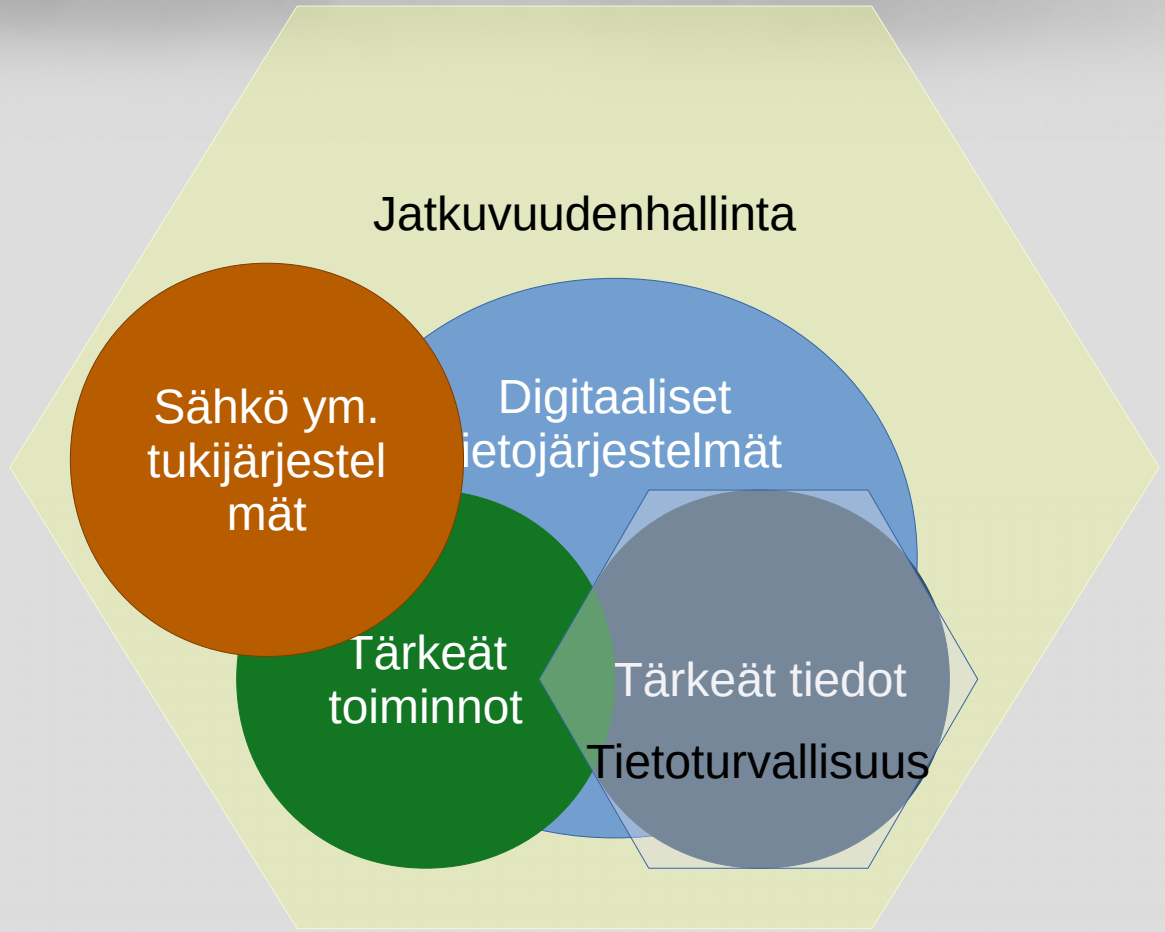
Sisältö

- Tietoturvallisuus, kyberturvallisuus ja tietosuoja
- Uhkia
- Puolustuskeinoja
- Vaatimuksia ja strategioita
- Hyviä tiedonlähteitä

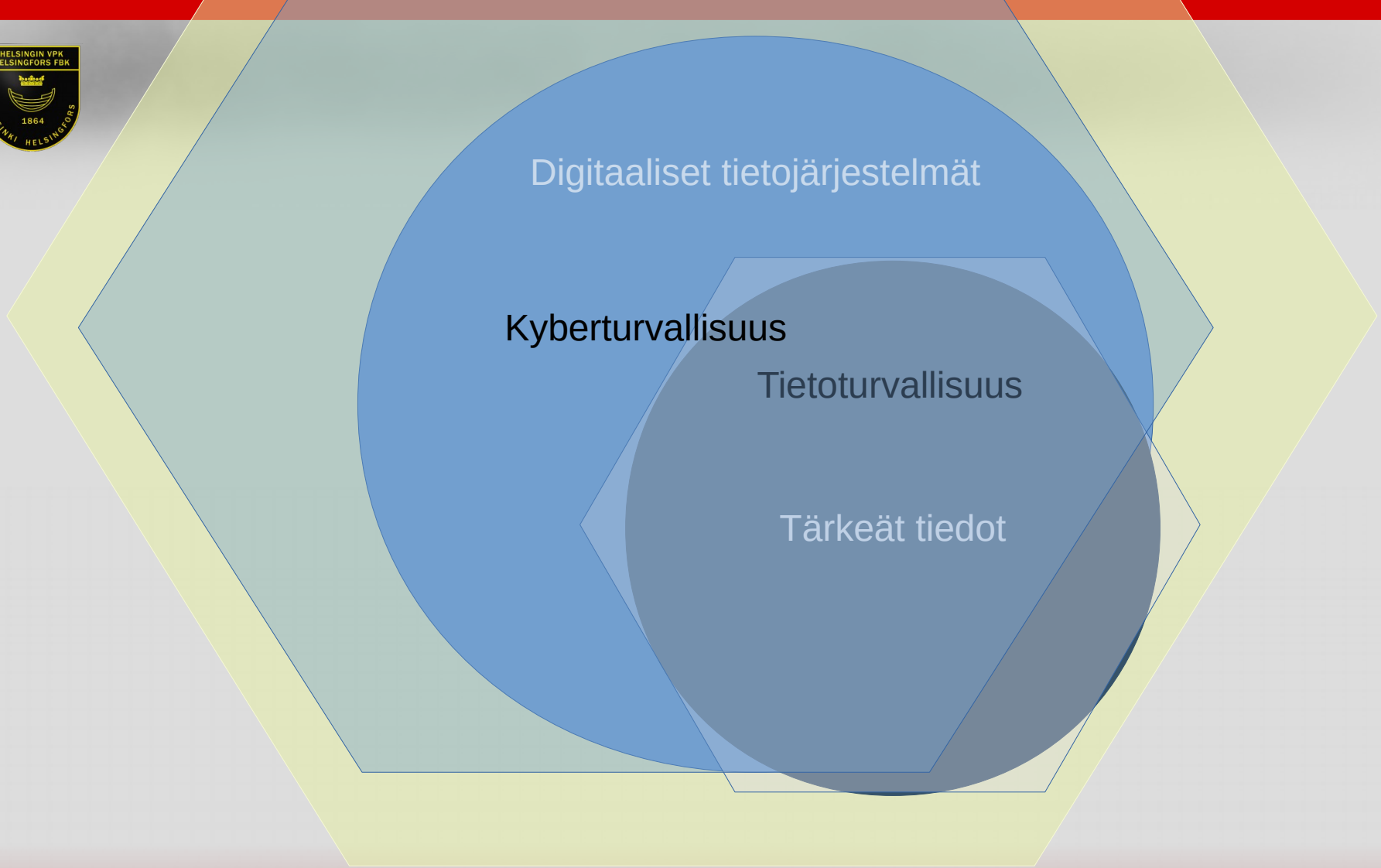
Tietoturvallisuus, kyberturvallisuus ja tietosuoja

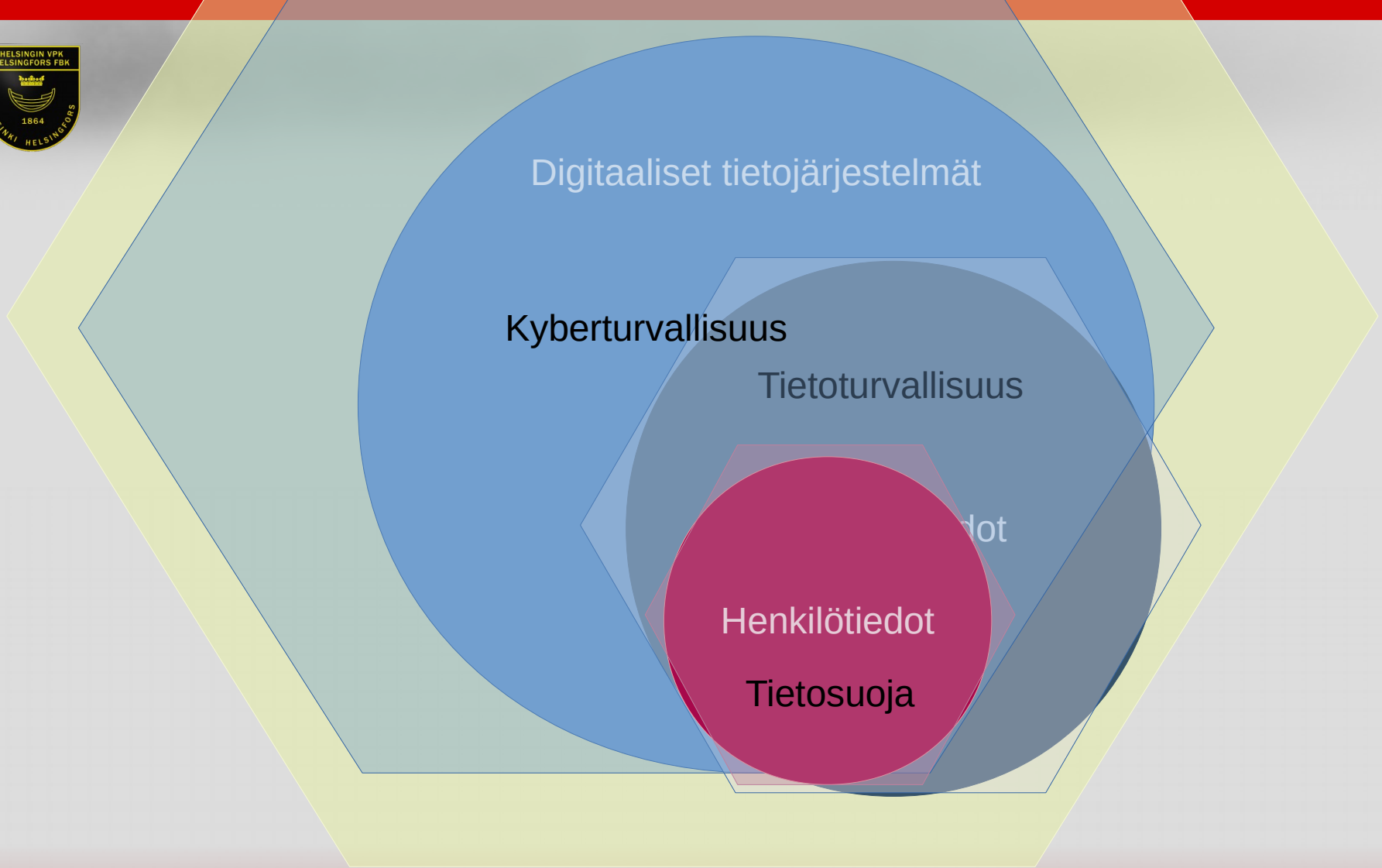

Jatkuvuudenhallinta
Digitaaliset tietojärjestelmät


Jatkuvuudenhallinta
Digitaaliset tietojärjestelmät
Tärkeät tiedot
Tietoturvallisuus

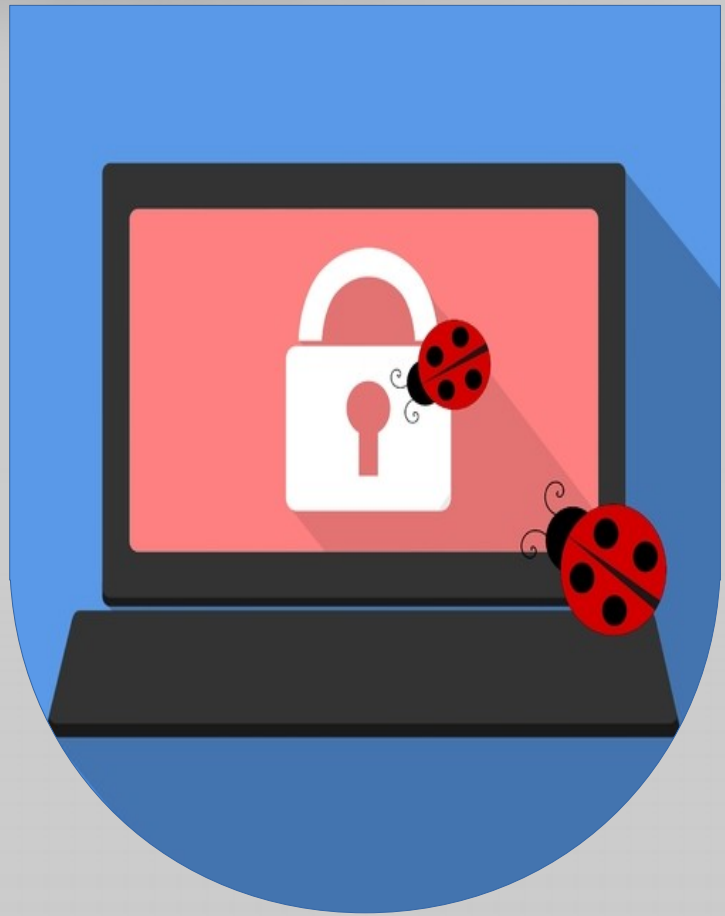

Jatkuvuudenhallinta
Sähkö ym. tukijärjestelmät
Digitaaliset tietojärjestelmät
Tärkeät toiminnot
Tärkeät tiedot
Tietoturvallisuus


Jatkuvuudenhallinta
Sähkö ym. tukijärjestelmät
Digitaaliset tietojärjestelmät
Kyberturvallisuus
Tärkeät toiminnot
Tärkeät tiedot
Tietoturvallisuus


Digitaaliset tietojärjestelmät
Kyberturvallisuus
Tietoturvallisuus
Tärkeät tiedot


Digitaaliset tietojärjestelmät
Kyberturvallisuus
Tietoturvallisuus
dot
Henkilötiedot
Tietosuoja

Uhkia



Kyberuhkien yleiskuva

- Uhkatoimijoita ja motiiveita
- Tekniikoita ja taktiikoita
  - Luonto vaikuttaa tietojärjestelmiin
  - Inhimillinen virhe tietojärjestelmien käytössä
  - Organisaation toiminta mahdollistaa kyberuhkia
  - Ihmisten manipulointi (social engineering)
  - Pahantahtoinen sisäpiiriläinen
  - Ohjelmistohaavoittuvuus
  - Tietomurto

Uhkatoimijoita ja motiiveita

uhka	motivaatio
Organisaation jäsen	Vahinko, välinpitämättömyys, kosto
Organisaatio itse	Johtajuuden puute, hallinnon puute
Kyberrikollinen	Raha
Aatteellinen hakkeri	Kosto, maine, terrorismi
Luonto	Sattuma, luonnonlait
Vakoilija	Tiedonsaanti, asenteisiin vaikuttaminen, sabotaasi

Luonto

- Sähkökatkos estää tietojärjestelmän käytön
- Tuli, vesi, sähkö tai eläin vahingoittaa tietojärjestelmää ja tuhoaa tietoja
- Tietokone hajoaa vanhuuttaan eikä sillä olevia tietoja päästä käyttämään

Inhimillinen virhe

- Suojattavia tietoja paljastuu, koska käyttäjä asettaa tietojärjestelmään väärät käyttöoikeudet
- Sivullinen näkee salassa pidettäviä tietoja käyttäjän näyttöruudulta
- Suojattavia tietoja tuhoutuu huonosti suunnitellun tai toteutetun tietojärjestelmän toiminnan vuoksi
- Pääsy suojattaviin tietoihin estyy, koska käyttäjä unohti salasanan

Organisaation toiminta

- Johtajuuden ja taidon puute
  - Kyberturvallisuuteen ei osoiteta riittävästi resursseja
  - Uhkien toteutumiseen ei varauduta ja tilanteet yllättävät organisaation ”housut kintuissa”.
- Heikko riskienhallinta
  - Hallintakeinoja kohdennetaan väärin
- Huono turvallisuuskulttuuri
  - Ongelmien peittely johtaa niiden pahenemiseen
- Laiton toiminta; esim. ohjelmistojen lisenssiehtojen rikkominen

Ihmisiä manipuloiva hyökkääjä

- Käyttäjätunnusten kalastelu johtaa suojattavan tiedon paljastumiseen → Tietomurto
- Käyttäjien houkuttelu avaamaan linkkejä tai liitetiedostoja → Haittaohjelmatartunta
- Väärennetty sähköpostiviesti saa käyttäjän siirtämään rahaa rikolliselle

Pahantahtoinen sisäpiiriläinen

- Suuttunut jäsen tuhoaa tietoja
- Utelias jäsen tutkii enemmän tietoja kuin mihin hänellä on lupa, koska kiinni jäämisen riski on pieni
- Siivooja varastaa tietokoneen, mikä estää koneen ja sillä olevien tietojen käyttämisen

Ohjelmistohaavoittuvuus

- Organisaation kyvyttömyys asentaa korjaavia ohjelmistopäivityksiä mahdollistaa muita kyberuhkia
- Ohjelmistohaavoittuvuus mahdollistaa haittaohjelman suorittamisen → Tietomurto, tietovuoto, tietojen tuhoutuminen
- Ohjelmistohaavoittuvuus mahdollistaa tietojärjestelmän toiminnan estämisen

Tietomurto

- Paljastunut tai arvattava salasana johtaa tietomurtoon, jonka myötä hyökkääjä voi tehdä kohteessa mitä tahansa
- Tietomurron selvittäminen ja pääsyn estäminen hyökkääjältä edellyttää tietojärjestelmän sulkemista, mikä haittaa puolustavan organisaation toimintaa.

Palvelunestohyökkäys

- Yleensä webbipalvelimen kuormittamista
- Roskaposti mm. webbisivujen lomakkeen kautta
- Itse aiheutettu sivuosuma: esim. hyökkäys webbipalvelinta kohtaan kaataa samassa tietokoneessa olevan sähköpostipalvelimen
- Ennakoimaton sivuosuma: esim. koko palvelinhotelli kyykkää

Puolustuskeinoja

Puolustuskeinojen yleiskuva

- Suunnitelmallisuus
- Hallinnolliset keinot
- Toiminnalliset keinot
- Tekniset keinot

Suunnitelmallinen puolustus

- Kuinka ehkäiset turvallisuuspoikkeamia?
- Kuinka varaudut ja valmistaudut poikkeamiin?
- Kuinka reagoit poikkeaman tullen?
- Kuinka palaudut normaalitilaan?
- Jatkuva parantaminen
- Kyberturvallisuus on erottamaton osa organisaation yleistä riskienhallintaa!

Hallinnollisia keinoja

- Riskien ja tietojen omistajuus
- Kirjalliset suunnitelmat ja toimintaohjeet
- Valvonta- ja toteutusvastuista sopiminen
- Suojattavan toiminnan ja kohteiden prioriteetit
- Vähimmän käyttöoikeuden periaate
- Käyttöoikeuksien muuttaminen henkilön tehtävien muuttuessa
- Noudata ohjelmistolisenssejä
- Tuhoa salassapidettävät tiedot hallitusti
  - Esimerkiksi pelastustoiminnan hälytysviestit
- Pidä ymmärryksesi uhista ja suojauskeinoista ajan tasalla

Toiminnallisia keinoja

- Myönteinen turvallisuuskulttuuri
- Vaihda tehtaalla asetetut salasanat
- Lue tietokoneen näyttämät ilmoitukset
- Harkitse, mitä klikkaat
- Henkilökohtaiset käyttäjätunnukset
- Lukitse istuntosi tietokoneella aina kun poistut sen äärestä: ⊞ + L
- Eri salasana joka järjestelmässä
- Fyysinen kulunhallinta ja -valvonta
- Harjoittele poikkeamien hallintaa
  - Esimerkiksi kokeile palauttaa varmuuskopiot tai harjoittele päätöksentekoa kyberuhkatilanteessa

Teknisiä keinoja

- Automatisoi puolustuskeinot
- Pidä ohjelmistot päivitettyinä
- Käytä laitteiden ja ohjelmistojen turvaominaisuuksia
- Monivaiheinen tunnistautuminen (MFA, 2FA) verkkopalveluihin
- Käytä salasanojen hallintasovellusta
- Ota varmuuskopioita
- Kerroksellinen suojaus, verkkojen ja päätelaitteiden eriyttäminen käyttötarkoituksen mukaan

Pelastuslaitosten kumppanuusverkosto

Toiminta poikkeustilanteissa

1) Älä hätiköi, pysy rauhallisena. Kaikki järjestyy.
2) Päätelaitetta tai auki olevia ohjelmia ei saa sammuttaa - tällöin aktiivisen haittaohjelman tiedot katoavat ja tapahtuman tutkinta vaikeutuu. Jätä siis näppäimistö ja hiiri rauhaan.
3) Irrota verkkokaapeli tai kytke langattomat yhteydet pois päältä. Tällä estät haittaohjelman leviämisen muihin verkossa oleviin laitteisiin.
4) Kirjoita ylös, mitä mahdollisessa varoituksessa tai ilmoituksessa luki. Jos näytöllä näkyy ilmoitus, älä sulje sitä. Tiedoista voi olla hyötyä asian tutkinnassa
5) Ilmoita asiasta tietohallinnolle oman organisaatiosi ohjeiden mukaan.
6) Auta tietohallintoa - kerro avoimesti mitä tiedät ja mitä olit tekemässä, ennen kun kone alkoi toimia oudosti.
7) Noudata saamiasi ohjeita.

Vaatimuksia ja strategioita

Lakeja

- **Pelastuslaki**: **vaitiolovelvollisuus**, virkavastuu
- **Julkisuuslaki**: viranomaisen julkisuusperiaate ja salassapitovelvollisuudet
- **EU:n yleinen tietosuoja-asetus (GDPR), tietosuojalaki**: henkilötietojen suojaaminen
- **Yhdistyslaki**: vastuuhenkilöiden vahingonkorvausvelvollisuus, hallituksen velvollisuus auttaa toiminnantarkastuksessa
- **Tilintarkastuslaki**: hallituksen velvollisuus auttaa tilintarkastuksessa
- **Työterveyslaki**: työntekijöiden terveydentilan ja toimintakyvyn seuranta, tietojen säilyttäminen ja antaminen työstä aiheutuvan terveydellisen vaaran tai haitan arvioimiseksi ja selvittämiseksi, salassapito
- ...

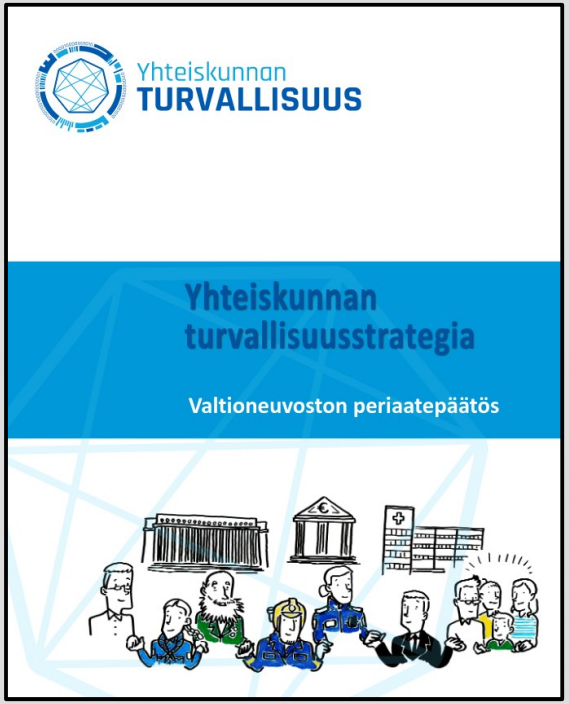
Sopimuksia

- Palokuntasopimus: palokunnan raportointivastuu pelastuslaitokselle
- Palokunnan sopimukset sen käyttämistä ICT-palveluista (Google Workplace, Microsoft Office, Facebook, …)
- ...

Ohjeita

- Pelastuslaitoksen ohjeet: digitaalisten kuvien käsittely
- Sopimuspalokuntien tietoturvakurssi Koulumaalissa
- Pronton käyttöohjeet ja -säännöt
- Johtamissovellusten käyttöohjeet ja -säännöt
- ICT-palveluiden tietoturvaohjeet (Microsoft, Google jne.)

Strategisia tavoitteita



- ”Turvallisuustoimijoita ovat kaikki johdettuun tai sitä kiinteästi tukevaan turvallisuustoimintaan osallistuvat tahot. Myös yksittäisillä kansalaisilla on tärkeä rooli omatoimisessa varautumisessa ja yhteiskunnan kriisinkestokyvyn vahvistamisessa.”
- Viittaukset Suomen Kyberturvallisuusstrategiaan ja kansalliseen riskiarvioon

Strategisia tavoitteita

- ”Kyberturvallisuus tulee nähdä luonnollisena osana jokaisen organisaation ja yksilöiden yhteiskuntavastuuta. Kyberturvallisuus on keskeinen osa yhteiskunnan häiriötöntä toimintaa.”

Strategisia tavoitteita

- ”Jokainen yksilö on siten tärkeä kyberturvallisuustoimija, joka omilla arjen kyberturvallisuutta parantavilla teoilla voi vaikuttaa omaan ja muiden kyberturvallisuuteen. Kansallisesti on varmistettava, että jokaisella on riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä.”

Hyviä tiedonlähteitä

Kuva: Traficomin Kyberturvallisuuskeskus

Traficomin Kyberturvallisuuskeskus

- Internetin ”hätäkeskus ja palokunta”
- Verkkosivut https://www.kyberturvallisuuskeskus.fi/
- Viikkokatsaus, Kybersää
- Twitter: @CERTFI. Facebook: NCSC-FI
- Sopimuspalokunnille erityisen hyvä ohje on ”Pienyritysten kyberturvallisuusopas”
- Tutustu harjoitusskenaarioihin
- Ilmoita kyberturvallisuuden poikkeamista!

Poliisi

- Tietoa kyberrikoksista https://poliisi.fi/kyberrikokset
- Twitter: . Facebook: Suomenpoliisi
  - Ole #ennakoija, vältä #digihuijaus
- Jätä vihje – tarvittaessa anonyymisti https://poliisi.fi/jata-vihje
- Jos epäilet kyberrikosta, ilmoita poliisille

Maanpuolustuskoulutus ry

- Kyber- ja informaatioturvallisuuden koulutusta https://mpk.fi/koulutukset/kyber-ja-informaatioturvallisuus/
- Opas ”Kyberin taskutieto maatiloille” sopii hyvin sopimuspalokuntienkin sovellettavaksi

Tietosuojavaltuutetun toimisto

- Organisaation velvollisuudet https://tietosuoja.fi/organisaatiot
- Tietoturvaloukkaukset https://tietosuoja.fi/tietoturvaloukkaukset
- Myös palokunnilla on velvollisuus ilmoittaa henkilötietoja koskevista tietoturvaloukkauksista

Kiitos mielenkiinnosta!

Lähetä palautetta:
perttu.halonen@helsinginvpk.fi