Digitaalinen turvallisuus

Tietoturva, kyberturva

30.10.2024

Matkailu- ja tapahtumaturvallisuus

Helsingin kaupungin talon tapahtumatori

Mikael Inkinen, Turvallisuusjohtamisen maisteri, insinööri, JYEAT Cyber Master, AmO, Tekn.yo
Tietoturvapäällikkö - CISO
Helsingin kaupunki

Päivän teemat

- Uhkakenttä kybermaailmassa
- Mistä (digitaalinen) turvallisuus koostuu?
- Digitaalinen turvallisuus on yhteistyötä
- Yhteistyön toteuttaminen
- Tietoturvan kolmikanta
- Hybridivaikuttaminen
- Informaatiovaikuttaminen
- Narratiivin voima
- Kehityskulkuja ja vaaroja
- Miten tekoäly vaikuttaa tietoturvaan?
- Yhteenveto ja lisätiedot.

”Kun tunnet vastustajasi ja tunnet itsesi, et ole vaarassa sadassakaan taistelussa.

Jos et tunne vastustajaasi mutta tunnet itsesi, mahdollisuutesi voittoon tai tappioon ovat samat.

Jos et tunne vastustajaasi etkä itseäsi, olet jokaisessa taistelussa vaarassa.”

Sunzi: Sodankäynnin taito (n. 140 eaa)

Nämä täytyy tuntea

Näihin voidaan vaikuttaa

Uhkatoimijat

ATT&CK

Kiristyshaittaryhmät

Valtiolliset toimijat eli APT -ryhmät

Haktivistit ym.

Sisäiset toimijat, virheet, vahingot

Hyökkäys-menetelmät

ATT&CK

Palvelunesto, DDoS

Sosiaalinen hakkerointi, kuten kalastelu

Autentikoinnin ohitus ”Hackers don’t break in, they log in”

Monivaiheinen tunnistauminen

LISÄÄ KEKSITÄÄN KOKO AJAN !

Suojakontrollit

TUNNISTA

Riskienhallinta, Hyökkäyspinta-analyysi, Haavoittuvuusskannaus

SUOJAA

Pääsynhallinta, Antivirus, Harjoittelu, Tietoisuus

TARKKAILE

Anomaliat, SIEM, Verkon monitorointi, XDR

CSOC

Jatkuvuuden hallinta, Viestintä, Analysointi, Mitigointi, Jatkuva parantaminen

VASTAA

Toipumissuunnitelmat, Viestintä, Jatkuva parantaminen

TOIVU

NIST CSF

Suojattavat kohteet

Helsingin kaupungin arvo-omaisuus

M365., laitteet, Platta, Ahjo HR, Talous, Dokumentin hallinta, …

Kumppanit, sidosryhmät, virastot, liikelaitokset, osakeyhtiöt

Kehitysympäristöt

Toimialakohtainen digitaalinen arvo-omaisuus

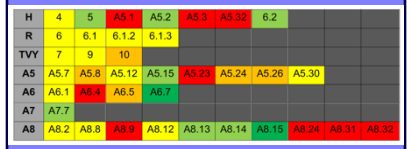
Muu digitaalinen arvo-omaisuus

Tunnistamattomia kohteita ei voi suojata!

Tunnistetut riskit

	Riskien tunnistaminen				Riskianalyysi		Riskin merkityksen arviointi		
	Riskin tunniste	Riskiluokka	Riski (riskin nimi)	Riskin kuvaus (mistä riski johtuu, mitä voi tapahtua toteutuessa):	Todennäköisyys	Vaikutus	Riskin suuruus (T x V)	Toimenpidetarpeet riskin käsittelylle (vakavuus/sietokyky)	Toimenpide-ehdotukset riskin käsittelylle
1	UVP-001	2 Operatiivinen	Kirjautuminen ilman vahvaa tunnistautumista	Vahva tunnistaminen edellyttää käyttäjän tunnistamista vähintään kahdella eri menetelmällä. Ilman tätä, asiaton kirjautuminen on todennäköisempää. Murtautuja pääsee käsiksi käyttäjän näkemiin viesteihin ja muihin sovelluksiin pilvimpäristössä.	2 Mahdollinen	1 Vähäinen	2 Ei riskiä	3 Huomioitava riski	2 Seurattava riskin kehittymistä
2	UVP-002	2 Operatiivinen	Kirjautuminen ilman vahvaa tunnistautumista pääkäyttäjä tilille	Edellinen, mutta murtautujelle suuremmat käyttöoikeudet	2 Mahdollinen	2 Kohtalainen	4 Huomioitava riski	3 Huomioitava riski	2 Seurattava riskin kehittymistä
3	UVP-003	2 Operatiivinen	Ympäristössä käsitellään luottamuksellisia aineistoja	Käyttäjä voi käsitellä osana keskustelua luottamuksellisia aineistoja	2 Mahdollinen	2 Kohtalainen	4 Huomioitava riski	2 Ei riskiä	1 Ei vaadi akuuttoja toimenpiteitä
4	UVP-004	2 Operatiivinen	Azure AD:n kautta hyökkäys THL:lle AD	Azure AD:n kautta hyökkääjä voi vaikuttaa THL:n käyttäjähakemiston sisältöön	1 Epätodennäköinen	3 Merkittävä	3 Huomioitava riski	2 Ei riskiä	2 Seurattava riskin kehittymistä
5	UVP-005	1 Strateginen	Azure AD:n suhde Valtorin tuotteistettuihin palveluihin	Azure AD on asiakaskohtainen ratkaisu. Tämä rajaa THL:n mahdollisuuksia Valtorin palveluiden käyttöönotoissa moduulivaittiin (suvanto-projekti) tai asiakaskohtaiseen windows 10 ympäristöön	3 Todennäköinen	1 Vähäinen	3 Huomioitava riski	2 Ei riskiä	2 Seurattava riskin kehittymistä
6	UVP-006	2 Operatiivinen	Teams ja Skype for Business yhteentoimivuus	Teams-sovelluksen jakelu GPO kautta johtaa Skype for Business sovelluksen asennusten konvaantumiseen, mikä estää kokousvanausten tekemisen Skype for Business varauksina, mikä estää Valtorin videosillan käytön.	4 Lähes varma	2 Kohtalainen	8 Merkittävä riski	3 Huomioitava riski	3 Luotava suunnitelma pienentämiseksi
7	UVP-007	3 Taloudellinen	Lisenssikustannukset	Lisenssikustannukset ovat osa THL:n Microsoft M365 E3 +YOPO:ta	1 Epätodennäköinen	1 Vähäinen	1 Ei riskiä	1 Ei riskiä	1 Ei vaadi akuuttoja toimenpiteitä

Kirjatut poikkeamat



H	4	5	A5.1	A5.2	A5.3	A5.32	6.2				
R	6	6.1	6.1.2	6.1.3							
TVY	7	9	10								
A5	A5.7	A5.8	A5.12	A5.15	A5.23	A5.24	A5.26	A5.30			
A6	A6.1	A6.4	A6.5	A6.7							
A7	A7.7										
A8	A8.2	A8.8	A8.9	A8.12	A8.13	A8.14	A8.15	A8.24	A8.31	A8.32	

NIST CSF = National Institute of Standard and Technology Cyber Security Framework

Kuvan lähde: metropolia.fi

Digitaalinen turvallisuus luodaan yhteistyöllä

Turvallisuus-kulttuuri

Esimerkin voima

Digitaalisen turvallisuuden viitekehys

Riskienhallinta
Riskienhallinta ja sisäinen valvonta

Toiminnan jatkuvuuden hallinta ja varautuminen
Turvallisuus- ja valmiustiimi

Tietoturvallisuus
Tietoturvapäälliköt

Tietosuoja
Tietosuojavastaavat

Kyberturvallisuus

Kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Kybertoiminta- ympäristön synonyyminä voidaan käyttää termiä digitaalinen toimintaympäristö

Organisaatio-turvallisuus

Fyysiset suojaukset

Muokattu lähteestä:
https://www.kuntaliitto.fi/kehittaminen-ja-digitalisaatio/digiosaaminen/digitaalinen-turvallisuus

Digitaalinen turvallisuus vastaa kolmeen kysymykseen

Mikä?

Kaupunkistrategia

Digitaalisen turvallisuuden toteuttaminen

- Strategia linjaa digitaalisten palveluiden toteuttamisesta turvallisesti
- Kaupunginkanslia yhdessä hallinto-osaston kanssa varmistaa vastuut ja roolit sekä riittävät toimintamallit
- Digitaalinen johtoryhmä ohjaa digitaalisen turvallisuuden toteuttamista
- Kaupungin tietoturvapäällikkö johtaa ja koordinoi digitaalisen turvallisuuden toteuttamista kaupunkitasoisesti
- Digitaalisen turvallisuuden ryhmä (digiturvaryhmä) koordinoi turvallisuustyötä toimialoilla ja liikelaitoksissa
- Toimialojen, virastojen ja liikelaitosten tietoturvapäälliköt ja –asiantuntijat toteuttavat digitaalista turvallisuutta vastuualueillaan

Kenelle?

Vaikutus eri asiakasryhmille

- **Kaupunkilaiset ja yritykset** voivat luottaa siihen, että kaupungin tarjoamat digitaaliset palvelut ovat turvallisia.
- **Työntekijät** ymmärtävät omaan työhönsä liittyvät riskit ja osaavat toimia niin, ettei nämä riskit toteudu tai ovat muuten hallinnassa.
- **Johdolla** on käytössään ajantasainen digitaalisen turvallisuuden tilannekuva ja ennustemalleja päätöksenteon tukena. Toiminnan vaikutuksia voidaan ennustaa datan avulla ja resursseja kohdentaa tarkemmin tiedon avulla.
- **Yhteistyökumppanit** saavat toimintamallit siihen, miten omassa palvelutuotannossa digitaalinen turvallisuus tulee ottaa huomioon, jotta se täyttää kaupungin sille asettamat vaatimukset
- **Digitaalisen turvallisuuden ammattilaiset** haluavat olla osana Helsingin kaupungin toimintaympäristöä ja tuoda oman osaamisensa siihen.

Miten?

Digitaalisen turvallisuuden jalkauttaminen

- Lakiin ja määräyksiin perustuvat toimintamallit
- Tietoturvalinjaukset ja tietoturvakäsikirja (2024)
- Onnistumisen mittarit (Julkri, kybermittari)
- Ohjeet ja käytänteet (omat ja julkisen hallinnon yleiset)
- Koulutus ja oman osaamisen kehittäminen
- Harjoittelu ja opastus (mm. perehdytys)
- Kokeilut (saa myös epäonnistua)

Mahdollistajat eli onnistumisen edellytykset

- Jatkuvasti kehittyvä toimintamalli ja ohjaavat standardit sekä julkisen hallinnon ohjeet, oppaat ja hyvät käytänteet
- Teknisen digitaalisen turvallisuuden toteuttaminen yhdessä digitalisaatioyksikön kanssa
- Teknologian hyödyntäminen tarkoituksenmukaisesti
- Riskilähtöinen lähestymistapa ja ajantasainen tilannekuva
- Toimiva digitaalinen perusta (perustietotekniikka ja fyysinen turvallisuus kaikissa toimipisteissä
- Muutoskyvykkyys (resilienssi) – kyky reagoida muuttuvaan ympäristöön
- Osaamisen kehittäminen
- Määräysten- ja säädöstenmukaisuus (Compliance)
- Yhteistyö julkisen hallinnon kesken ja kokemusten hyödyntäminen

Digitaalisen turvallisuuden kolmikanta

RESILIENSSI

RESILIENSSI

Tietoturvan hallintamalli

2023-2024

- ISO 27001 ja ISO 27002 standardien mukainen malli, joka määrittelee tietoturvan johtamisen, ylläpitämisen, kehittämisen ja jatkuvan parantamisen menetelmät kaksivuotisessa projektissa (2023-2024)
- Tunnistettu 38 kehittämisen kohdetta, joita edistetään vielä vuoden 2024 aikana
- Sertifikaatti ei ole tavoitteena, mutta tarkastellaan tilannetta tämän vuoden jälkeen.

Väliraportti 2023 tehty

Digiturva-ryhmä

Uudistetaan 2025 alkaen - Kyberturvaryhmä

Tietoturvalinjaukset

Syksy 2024

- Tiietoturvallisuuden periaatteet (”tietoturvapolitiikka”)
- Alkuperäiset vuodelta 2020 valmisteltu laajassa yhteistyössä
- 14 linjausta -> 10 linjausta
- Uudistus tehty kevyemällä menettelyllä
- Uudistuksen tarkoituksena oli parantaa luettavuutta, selkeyttää vastuita ja päivittää vastaamaan nykypäivän digitaalista ympäristöä
- Linjauksia on yhdistetty ja lisätty linjaus tekoälystä
- Esitelty digiturvaryhmässä ja digijoryssa
- Esittely jatkuu ja hyväksyntä KP:lle syksyn aikana yhdessä ICT-uudistuksen kanssa (Hannu Heikkinen).

Tietoturvakäsikirja

Syksy 2024

- Kokoaa yhteen tietoturvan ohjeet, määräykset ja käytänteet
- Sisältää myös sanastoja, termien määrittelyn, lakikatsaukset sekä linkkejä tietoturvaan liittyvään julkisen hallinnon materiaaliin (DVV, KTK, VM, TiHLK, …)
- Tiedonhallintalain soveltaminen ja mittarointi
- Toteutettu intraan, jossa helppo muokata ja kehittää käsikirjaa jatkuvasti

- ***Ennen julkaisua esitellään eri ryhmille ja toivotaan parannuksia***

Riskienhallinta, varautuminen, jatkuvuus, tilannekuva, valvonta, teknologia, harjoittelu, koulutus, yhteistyö, …

Helsinki

Tietoturvalinjaukset 2024 tavoitteet

Helsingin kaupunki on linjannut kaupunkistrategiassaan (2021–2025) yhdeksi painopistealueeksi

Älykästä Helsinkiä johdetaan tiedolla ja digitalisaatiota hyödyntäen

Helsingin kaupungin Organisaatioturvallisuuden linjausten luvun 2.7 mukaan tietoturva on osa kaupungin organisaatioturvallisuuden kokonaisuutta.
Organisaatioturvallisuuden linjausten mukaisesti tietoturvallisuuden tavoitteena on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että niiden

- luottamuksellisuuteen (tietojen suojaaminen luvattomalta käytöltä)
- eheyteen (tietojen vääristämisen estäminen)
- saatavuuteen (tietojen käytön mahdollistaminen niitä tarvittaessa)

liittyvät riskit otetaan huomioon.

UUDET TIETOTURVALINJAUKSET JULKAISTAAN LOKAKUUSSA 2024

- Kaupunkilaiset voivat luottaa Helsingin kaupungin digitaalisiin palveluihin
- Digitaalisten palveluiden turvallisuus on vahva
- Digitaaliset palvelut toimivat myös häiriötilanteissa ja palautuvat niistä nopeasti
- Henkilöstön digitaalista turvallisuutta kehitetään määrätietoisesti
- Uudet teknologiat ovat suunniteltu turvallisiksi ja ne tukevat kaupungin digitaalista turvallisuutta
- Helsingin kaupungin digitaalista turvallisuutta johdetaan tiedolla ja osaamista kohdentamalla.

Tietoturvalinjaukset 2024

Tietoturvalinjaukset on ylimmän johdon hyväksymät linjaukset

1. Tiedon tunnistamisesta ja luokittelusta
2. Tietoturvariskien tunnistamisesta ja hallinnasta
3. Riittävän tietoturvatason noudattamisesta
4. Käyttäjän tunnistamisesta ja käyttöoikeuksien hallinnasta rooliperusteisesti
5. Henkilöstön tietoturvaosaamisen ja -ymmärryksen kehittämisestä
6. Lokitietojen keräämisestä
7. Digitaalisten palveluiden jatkuvuuden turvaamisesta
8. Tietoturvan tilannekuvan seurannasta ja raportoinnista
9. Tietoturvan huomioimisesta hankinnoissa
10. Tekoälyn käytöstä työtehtävissä tietoturvan näkökulmasta.

Kirjattuna tietoturvan vastuut ja velvoitteet koko henkilöstölle organisaatioittain

Tietoturvalinjaukset on **ylimmän johdon** tahtotila siitä, että me osaamme tunnistaa ja luokitella meidän hallussa olevat tiedot ja ymmärrämme niihin kohdistuvat riskit, jotta kykenemme niitä hallitsemaan.
Kouluksella varmistetaan, että **jokainen** osaa noudattaa työssään vaadittavaa tietoturvan tasoa. Henkilö tulee teknisesti tunnistaa ja antaa hänelle rooliinsa liittyvät käyttöoikeudet, jotka ovat voimassa vain kyseisen roolin ajan. Jotta osaamme toimia tietoturvallisesti on jokaisen velvollisuus kehittää omaa ymmärrystä tietoturvasta.
Tietoturvan ammattilaiset huolehtivat lokitietojen keräämisestä, jotta voidaan jäljittää viat ja erilaiset tapahtumat myös jälkeenpäin. He myös varmistavat, että digitaaliset palvelut toipuvat häiriöistä ja seuraavat tietoturvan tilannekuvaa. **Hankinta-asiantuntijat** varmistavat tietoturvan noudattamisen hankinnoissa.
Tekoäly tulee kaikkialle ja sen käytössä **jokaisen** on huomioitava tietoturvallinen käyttö.

Tietoturvakäsikirja

- Toteutettu intraan, mahdollistaa sujuvan uudistamisen
- Tulee intran tietoturvasivulle
- Sisältää mm. tietoturvan johtamisen periaaatteet, tietoturvallisen toiminnan työtehtävissä ohjeet, tietoturvan hallintakeinoja ja toimintaohjeet tietoturvan vaarantuessa.
- Lisäksi sanasto, käsitteitä ja lähteitä oman tietoturvatietoisuuden kehittämiseksi.
- Julkaistaan lokakuussa 2024.
- Löytyy intrasta haulla ”tietoturvakäsikirja”
- https://helsinginkaupunki.sharepoint.com/sites/Intra-Tietoturva/SitePages/Tietoturvakasikirja.aspx?web=1

Taulukko sisältää lyhyen kuvauksen kunkin sivun sisällöstä sekä pikalinkin kyseiseen sivuun

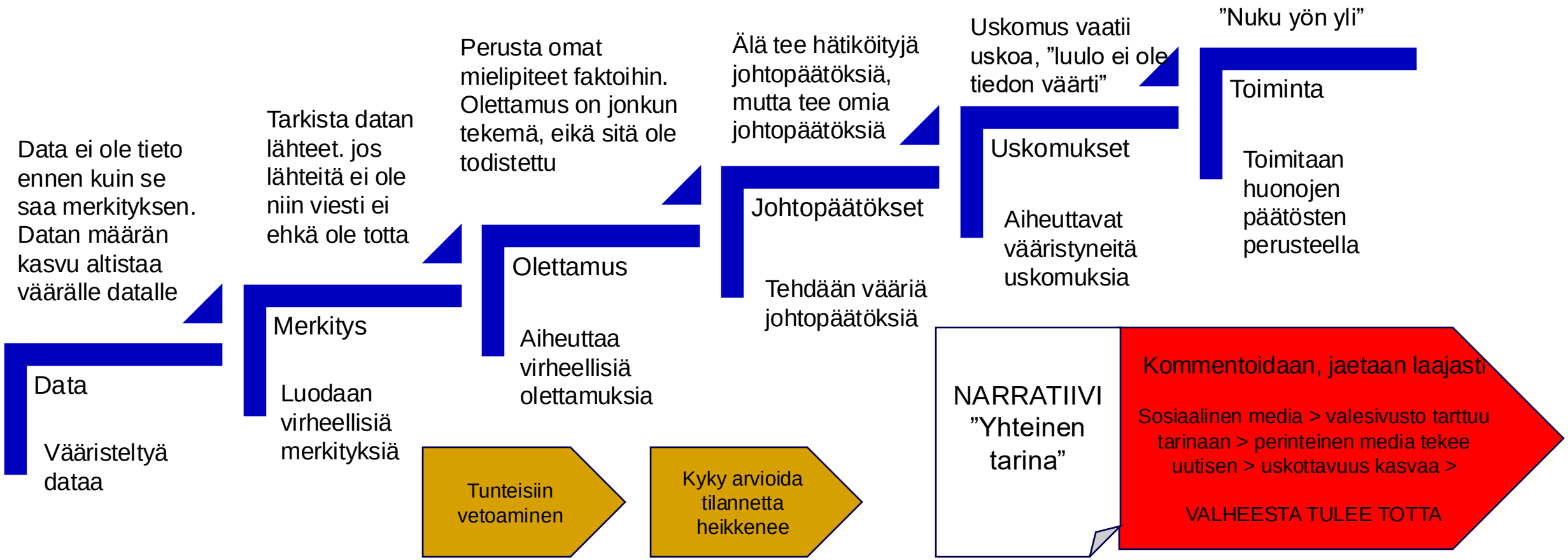
Sivun nimi	Sivun sisältö tiivistettynä
Helsingin kaupungin tietoturvalinjaukset	Tietoturvatyötä ohjaavat säännöt ja linjaukset. Tietoturvalinjaukset on uudistettu vuonna 2024, mutta ovat vielä hyväksymättä.
Toimintaympäristö ja sidosryhmät	Sisäinen ja ulkoinen toimintaympäristö sekä sidosryhmät ovat osa tietoturvallisuuden kokonaishallintaa ja siksi ne tulee olla tunnistettu ja niihin tulee kohdistaa
Tietoturvan johtaminen	Tietoturvan johtaminen on osa kaupungin johtamista ja kytkeytyy strategiseen ja operatiiviseen johtamiseen hallintosäännön ja toimintasääntöjen kautta. Myös tietoturvalinjaukset ovat osa tätä kokonaisuutta. Tietoturvan toteuttamisesta vastaa omalta osaltaan esihenkilöt, toimialojen johto, DigiHelsinki Oy sekä jokainen kaupungin työntekijä.
Tietoturvan suunnittelu	Tietoturvan suunnittelulla varmistetaan tietoturvariskien hallinta. Tietoturvan riskienhallinta perustuu standardien määrittelemiin kontrolleihin, joiden avulla tunnistetaan ja hallitaan koko tietoturvallisuuden kokonaisuutta.
Tietoturvaan liittyvät mahdollistavat toiminnot	Tietoturva on yhteispeliä. Tarvitaan erilaisia toimijoita joiden yhteistyöllä Helsingin kaupungin tietoturvallisuus voidaan pitää hyväksyttävällä tasolla. Sisäisiä yhteistyökumppaneita ovat mm. henkilöstöhallinto, DigiHelsinki Oy, Stadin Helpdesk, viestintä sekä sisäinen valvonta ja riskienhallinta.
Tietoturvallinen toiminta työtehtävissä	**Tämä koskee ihan jokaista.** Jokainen on oman työnsä paras asiantuntija ja paras tunnistamaan siihen liittyvät riskit. Tällä sivulla on ohjeita toimintaan kun havaitaan erilaisia poikkeamia normaalissa toiminnassa tai kun haluaa kehittää omaa tietoturvaosaamistaan.
Tietoturvassa onnistumisen arviointi	Tietoturvaakin voidaan mitata. Erilaisten mittarien avulla voidaan todeta Helsingin kaupungin tietoturvan taso ja tunnistaa kehitettäviä kohteita.
Tietoturvatoiminnan kehittäminen	**Tietoturvan kehittäminen on jatkuva prosessi, joka vaatii koko henkilöstön osallistumista.** Jatkuvaan kehittämiseen kuuluu niin teknologia, koulutus, harjoittelu kuin tapahtumista oppiminenkin. Sisältää taulukon kehitteillä olevista parannuksista kaupungin digitaaliseen turvallisuuteen.
Tietoturvan hallintakeinot ja tietoturvajärjestelyt	Tietoturva koostuu erilaisista hallintakeinoista kuten hallinnollisista ja teknisistä ratkaisuista ja päätöksistä, kokonaisarkkitehtuurista, fyysisestä turvallisuudesta (seinät, ovet, ikkunat, kulunvalvonta jne.) sekä ohjelmistokehityksen tietoturvallisesta hallinnasta ja henkilöstön osaamisesta.
Toimitusketjuihin liittyvä riskienhallinta ja tietoturva	Ketju on yhtä vahva kuin sen heikoin lenkki. Tietoturvassa pitää pitää huolta koko toimitusketjusta alihankkijan alihankkijasta aina kaupungin oman organisaation turvallisuuteen ja jatkuvaan parantamiseen.
Uusiin teknologioihin liittyvät erityiset huomiot tietoturvasta	Digitaalinen maailma kehittyy jatkuvasti ja muutokset vaikuttavat myös tietoturvallisuuteen. Uusissa teknologioissa on sekä mahdollisuuksia, että uhkia. Nämä täytyy tunnistaa ja huomioida sekä tietoturvan suunnittelussa ja hallinnassa, että jokapäiväisessä toiminnassa.
TOIMINTAOHJEET tietoturvan vaarantuessa	**Jokaisen henkilöstössä tulee osata toimia poikkeustilanteissa.** Tällä sivulla on ohjeita ilmoitusten tekemiseen, kun havaitsee jotain poikkeavaa.
Tietoturvaan liittyvä lainsäädäntö	Tietoturvaan liittyy sääntöjen, ohjeiden ja käytänteiden lisäksi myös lainsäädännöstä tulevia velvoitteita. Sivulle on kasattu tärkeimpiä tietoturvaan liittyviä lakeja ja asetuksia.
Verkkolähteistä, sanastoja ja käsitteitä	Täältä löydät lisätietoa ja tietoturvaan liittyvistä Helsingin kaupungin ulkopuolisista verkkolähteistä, sanastoista ja käsitteistä. **Sivulla on myös vinkkejä itseopiskeluun.**

Informaatio-vaikuttaminen

Hybridivaikuttaminen

Disinformaatio	Misinformaatio	Malinformaatio	Muut keinot
Käytännössä valhetta. Disinformaatioon liittyy usein joku tosiasia, jonka avulla vastaanottajalle syötetään pajunköyttä	Tarkoittaa valheellisen tai vääristellyn tiedon TAHATONTA levittämistä. Jokin tunteisin vetoava tai hätkähdyttävä ”uutinen”, joka halutaan heti jakaa seuraajilleen. ”Hyväuskoinen hölmö” on informaatiovaikuttajan oiva apulainen.	Oikean mutta (esim.) luvattomasti hankitun, henkilön yksityisyyteen liittyvän tiedon levittämistä. Tietoa käytetään vahingoittamaan tietoisesti kohdetta. Esim. terveystiedot, seksuaalinen suuntautuminen, rikosrekisteri tms.	Maalittaminen Informaation pesu Osoita ja hätkähdä Vesittäminen Botit

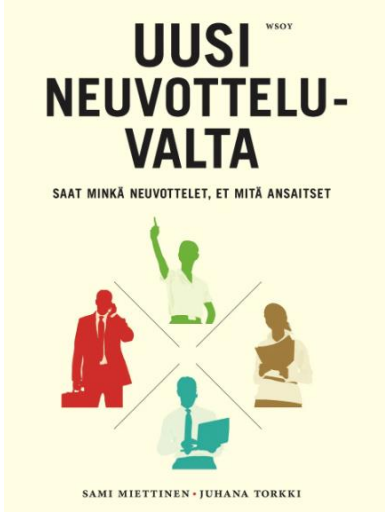
Informaatiovaikuttamisen portaat



Mikä on informaatiovaikuttamisen tavoite?

Miksi valheelliset Narratiivit uskotaan?

- Sivullisuuden tunne on tragedia yksilölle ja ase informaatiovaikuttajalle.
- Lähiverkoston puute tai heikkous lisää vaikuttamisalttiutta.
- Tiedon puute tai virheelliset tiedot ovat informaatiovaikuttajalle raaka-ainetta.
- Päättäjien ja vastuullisten toimintakyvyttömyys ja haluttomuus kompromisseihin ovat yhteiskunnan heikkous. *”Elämä on neuvottelua”.*
- Vaikutusmahdollisuuksien puute tai tunne siitä irrottavat kansalaisia yhteisestä päätöksenteosta, mikä heikentää päättäjien demokraattista katetta.



Mitä pitäisi tehdä?

- Kansalaisia pitää kohdella aikuisina.
- Ongelmista on puhuttava.
- Turhien kierteiden laittaminen (spinnaaminen) käsiteltävään asiaan tai refleksinomainen **pöyristyminen** tavalliseen elämään kuuluvista asioista erkaannuttavat kansalaisia päätöksentekijöistä.

Kehityskulkuja ja vaaroja

- Deepfake-videoita käytetään yhä enemmän poliittisessa propagandassa ja uutisissa.
- Sosiaalisen median algoritmit antavat yhä räätälöidymmän mahdollisuuden tarjota ja vahvistaa henkilöillä jo olevaa näkemystä. (Kuplaantuminen)
- Suuret yhdistävät tarinat heikkenevät ja yhteiskunta alkaa pirstoutua heimoihin.
- Kyberhyökkäykset yleistyvät, ja niiden kohteena ovat valtiot, yritykset ja jopa yksittäiset kansalaiset.
- Disinformaatio-operaatiot yleistyvät ja niitä käytetään usein vaikuttamaan poliittisiin vaaleihin tai muihin yhteiskunnallisiin tapahtumiin. Onnistuminen voi vääristää vaalituloksen ja jopa estää kansan todellisen tahdon toteutumisen.
- Tekoälyllä luodaan suuria määriä valeuutisia tai deepfake-videoita. Luottamus päättäjiin heikkenee ja informaatiokenttä myrkyttyy. Kukaan ei tiedä mihin uskoa ja mikä on totta. *”Totuuden jälkeinen aika”.*

Mikä on infovaikuttajan tavoite

- **Identiteetin muuttaminen** – Henkilöön vaikuttaminen
- **Todenmukaisen Narratiivin vääristäminen** – Ihmisryhmään vaikuttaminen
- **Yhteisen kulttuurin muuttaminen** – Päättäjiin vaikuttaminen
- **Kansallisen narratiivin tuhoaminen** – Kansakuntaan vaikuttaminen

Informaatiovaikuttaminen uhkaa vapaata mediaa

Mediatalot ovat havahtuneet uuteen uhkaan, kun toimittajat ovat joutuneet informaatiosodan kohteeksi. Informaatiovaikuttaminen on usein huomaamatonta.

HUOLTOVARMUUS, HYBRIDISOTA, INFORMAATIOSOTA

| 14.5.2018

TEKSTI JUKKA NORTIO ,
KUVAT VESA LAITINEN, ISTOCK, YLEISRADIO, JYVÄSKYLÄN YLIOPISTO

Valeuutiset, informaatiovaikuttaminen, kyberhyökkäykset, vihapuhe ja hybridisodankäynti koskettavat toimittajia sekä uutisaiheina että henkilökohtaisesti. Toimittajien kyky välittää kansalaisille luotettavaa ja faktoihin perustuvaa tietoa korostuu epävakauden aikoina. Siksi toimittajien työn turvaaminen ja valmiuksien kehittäminen on otettu vakavasti mediataloissa.

Tietoturva ja tekoäly

Hyökkäys tekoälyn avulla

- Hyökkäysten automatisointi on yksi tekoälyn tuomista mahdollisuuksista
  - Kohdennetut kalasteluhyökkäykset
  - Haavoittuvuuksien etsiminen
  - Sosiaalinen manipulointi ja imitoiminen videoiden ja äänen avulla (deepfake, syväväärennös).
- Tekoälyn käyttäminen myös ”perinteisten” hyökkäysten apuna ja tehostamisessa (DDoS, kiristyshaitta, tiedonkeruu, käyttäjämanipulointi, …).
- Tekoälyteknologia muuttuu nopeasti ja uhat sen myötä.

Puolustus tekoälyn avulla

- Hyökkäyksen havainnointi ja puolustuksen automatisointi; nopea ja oikea reagointi.
- Hyökkäysten ymmärtäminen ja tekoälyn kehityksessä mukana pysyminen.
  - Teknologiset ratkaisut
  - Koulutus, blogit, kirjallisuus, podcastit, luennot, tapahtumat, kokeilu ja oma uteliaisuus
- Yhteistyön tiivistäminen. Opi muilta ja opi muiden kanssa.
- Tekoäly on hyvä seulomaan tietomassoja (lokit), etsimään poikkeavuuksia (verkot) ja etsimään tietoa (SOC).
- Ihmiselle tiekoäly on hyvä renki.
  - Ohjeet, koulutus, havainnot, visualisointi, …

Yhteenveto ja lisätiedot

- Tietoturvaa johdetaan kaupunginkansliasta ja digiturvaryhmä on koordinoinnin väline (ydinryhmä + laajennettu ryhmä).
- Toimialoilla on omat tietoturvapäälliköt, jotka kuuluvat digiturvaryhmään.
- Tietoturvan hallintamalli perustuu standardiin.
- Tietoturvallisuus on jokaisen vastuulla ja siitä ohjeistetaan tietoturvalinjauksissa.
- Muuta ohjeistusta löytyy Tietoturvan intrasta ja Ohje-sovelluksesta – Tietoturvakäsikirja kokoaa kaiken tiedon yhteen (2024).
- Apua saa oman toimialan tietoturvavastaavalta erityisesti viranomaisyhteistyössä (Kyberturvallisuuskeskus (mm. ISAC-ryhmä), poliisi, tietoturvasuojavaltuutettu).
- Tiedonhallintalautakunta ja Digi- ja väestötietovirasto (DVV) tekee hyviä ohjeita ja suosituksia, joita kannattaa seurata.

Kiitos !

Kysymyksiä, kommentteja, keskustelua

Mikael Inkinen
Tietoturvapäällikkö - CISO
Helsingin kaupunki