3.12.2024 Case-esimerkki: kyberhyökkäys Tyrskylään - miten tilannetta johdetaan ja hallitaan ja kuinka tilanteessa palaudutaan normaaliin?

DVV digiturvatiimi & muut asiantuntijat

DIGI- JA VÄESTÖTIETO-VIRASTO

Tilaisuuden tarkoitus

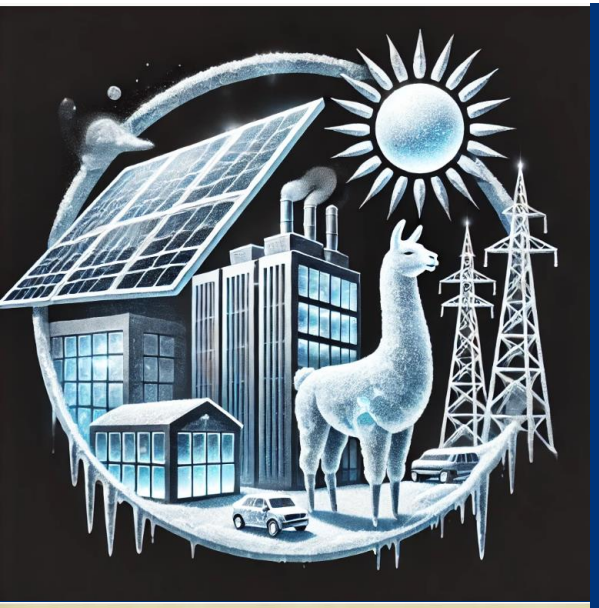
- Yhä useampi julkisen hallinnon organisaatio, kuten myös yritys on joutunut erilaisten kyberhyökkäysten tai niiden yritysten kohteeksi. Näiden hyökkäysten määrä ja kyvykkyys on kehittynyt vuosittain, joka näkyy myös viranomaisille tehtävinä ilmoituksina.

- Tässä tilaisuudessa käymme läpi yleisiä näihin hyökkäyksiin ja niiden hallintaan ja torjumiseen liittyviä havaintoja, vinkkejä ja hyviä käytäntöjä esimerkkien avulla.

- Käytämme tässä viitekehyksenä kuviteltua **Tyrskylän kuntaa**, johon jokainen puhujamme sijoittuu eri rooleissa.

- Materiaalin lopussa olevien keskusteluyhteenvetojen tuottamisessa on hyödynnetty ChatGPT-tekoälypalvelua, mutta kyseinen osuus on **myös luettu ja korjattu** asiantuntijoiden toimesta.

- Palaute: digiturva@dvv.fi



Tyrskylä

”Meillä toimii digi vuoden jokaisena päivänä”

DIGI- JA VÄESTÖTIETOVIRASTO

Tervetuloa Tyrskylään!

- **Yleiskatsaus:**
  - Tyrskylä on idyllinen ja elinvoimainen kunta, joka sijaitsee merenrannalla ja tarjoaa asukkailleen ja vierailijoilleen kauniita maisemia, monipuolisia palveluja ja yhteisöllisen ilmapiirin. Kuntamme on tunnettu puhtaasta luonnosta, ystävällisistä ihmisistä ja korkeasta elämänlaadusta ja teknologiasta.
- **Tyrskylä – digitalisaation kehto meille kaikille**
  - Tyrskylä sijaitsee Kaakkois-Suomessa meren rannalla. Tämä **5879 asukkaan kunta** pitää sisällään useampia korkean teknologian yrityksiä sekä myös sataman, jota kautta kulkee **2,42% Suomen meriliikenteen kautta tapahtuvasta ulkomaankaupasta.** Lisäksi kunta sisältää merkittävän energia-alan osaamis- ja tuotekehityskeskittymän, joka näkyy myös akkutehtaan ja merkittävän aurinkovoimalapuiston muodossa. Osin näiden takia kunnassa toimii myös kansainvälisen merkittävän **pilvipalvelutoimittajan nykyaikainen konesalikokonaisuus**, joka on erityisesti kehitetty kvanttilaskentaa- ja tekoälypalveluiden tuotekehittelyä varten. Konesali myös hyödyntää kunnan alueella tarjolla olevia kestävän kehityksen energiamuotoja.

Tervetuloa Tyrskylään!

- **Palvelut:**
- Tyrskylässä on laaja valikoima palveluja, jotka kattavat kaiken mitä tarvitset mukavaan ja vaivattomaan arkeen. Tarjolla on:
  - **Terveydenhuolto:** Moderni terveyskeskus ja hyvin varustellut apteekit takaavat, että saat tarvitsemasi hoidon ja lääkkeet helposti.
  - **Koulutus:** Kunnassamme on erinomaiset koulutusmahdollisuudet varhaiskasvatuksesta lukioon ja ammatillisiin oppilaitoksiin sekä yliopiston tutkimuskeskukseen.
  - **Liikunta ja vapaa-aika:** Useita liikuntahalleja, urheilukenttiä, kuntosaleja ja hyvin hoidettuja ulkoilureittejä.
  - **Luonto ja aktiviteetit:** Tyrskylä on täydellinen paikka luonnonystäville.

Voit nauttia:

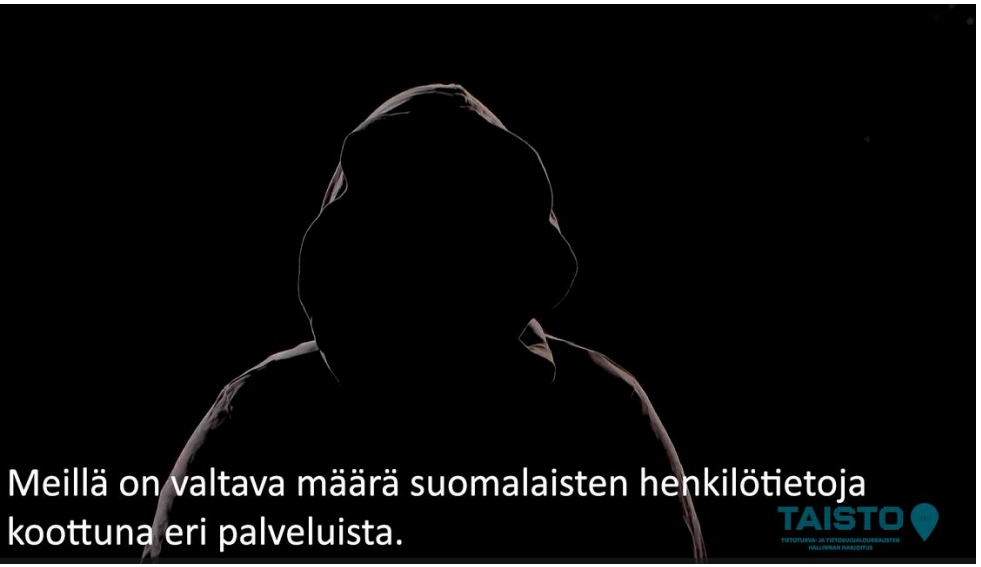
- **Merenranta:** Upeat hiekkarannat ja kivikkoiset poukamat tarjoavat loistavat mahdollisuudet uimiseen, auringonottoon ja kalastukseen.
- **Retkeily:** Lukuisat retkeilyreitit ja luonnonsuojelualueet kutsuvat seikkailuihin metsissä ja rannikoilla.
- **Vesistöt:** Melonta, purjehdus ja muut vesiharrastukset ovat suosittuja niin asukkaiden kuin vierailijoiden keskuudessa.

Tervetuloa Tyrskylään!

- **Yhteisöllisyys:**
- Tyrskylän yhteisöllisyys on vertaansa vailla. Kunta järjestää säännöllisesti tapahtumia ja juhlia, jotka kokoavat ihmiset yhteen. Voit osallistua:
  - Paikallisiin markkinoihin ja käsityöläistapahtumiin.
  - Kulttuuritapahtumiin, kuten konsertteihin ja teatteriesityksiin.
  - Urheiluturnauksiin ja yhteisiin liikuntatapahtumiin.
- **Asuminen:**
  - Tyrskylä tarjoaa monenlaisia asumisvaihtoehtoja viehättävistä omakotitaloista moderneihin kerrostaloasuntoihin. Asunnot ovat tilavia ja laadukkaita, ja monista avautuu upea merinäköala.

Tervetuloa tutustumaan Tyrskylään, jossa digi toimii vuoden jokaisena päivänä!

Ystävyyskunta Hyrzskylässä huolestuttavia ilmiöitä



LUPASIN 2018, ETTÄ PALAAN TAKAISIN

– nyt saatte maksaa kohtelustani korkojen kera

- Nyt myös geopoliittisesti **hieman epävakaassa** naapurivaltiossa toimivan ystävyyskunnan Hyrzskylän - Хюрзскюля tilanne myös huolestuttaa.
- Esimerkiksi siellä tapahtuu usein vakavia tietomurtoja sekä tiedetään, että ainakin yksi **rikollisorganisaatio** toimii sieltä aktiivisesti kohdistaen mm. **#palvelunestohyökkäyksiä**, **#informaatiovaikuttamista, lunnashaittaohjelmahyökkäyksiä ja #hybridivaikuttamista** Tyrskylän suuntaan.

  Eräs näiden operaatioiden taustalla oleva toimija on pahamainen Vuoden 2018 #TAISTO-harjoituksessa esiintynyt **#Tietovuoto-ryhmittymä**

MORE ☰ > MOST WANTED

ÄFBIIAI

Most Wanted

Ten Most Wanted Fugitives | Fugitives | Capitol Violence | Terrorism | Kidnappings/Missing Persons

Crimes Against Children | Murder | Additional Violent Crimes | Cyber | White Collar Crimes | Counteri

Cyber Crimes

Select the images of suspects to display more information.

Filter by: Filter by title, description, category...

Filter by Year

CHINESE PLA MEMBERS, 54th RESEARCH INSTITUTE

GRU 29155 CYBER ACTORS

THREE IRANIAN CYBER ACTORS

TIETOVUOTO, HYRSKYLA

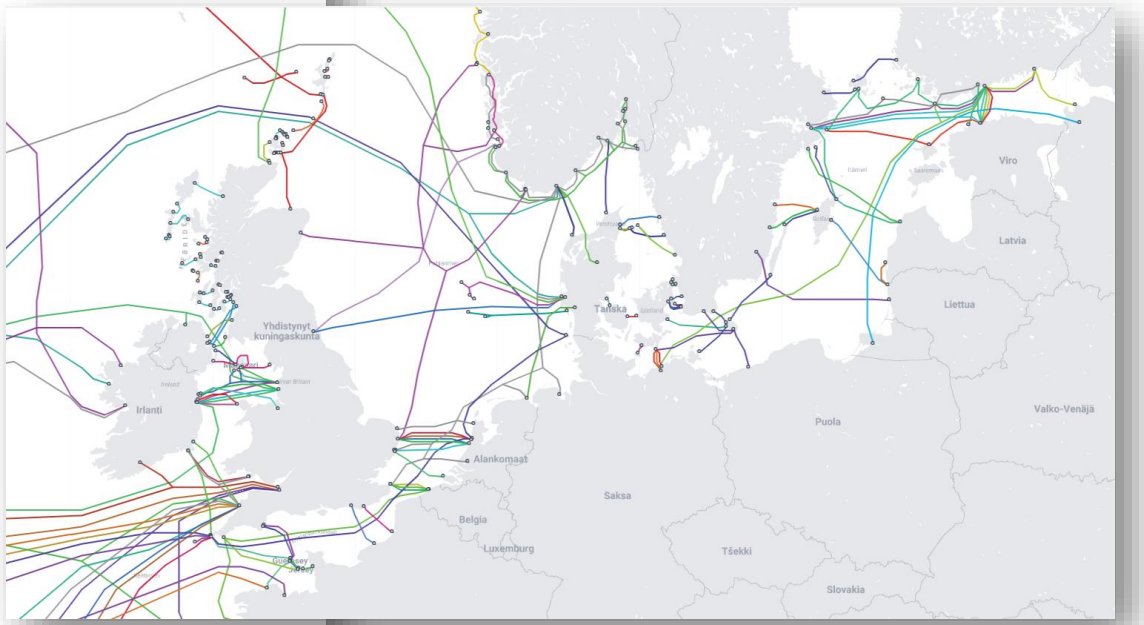
Myös Tyrskylästä on verkkokaapeli suoraan Eurooppaan

STRATEGIC ANALYSIS AUSTRALIA

HOME ARTICLES ABOUT READING PODCASTS CONTACT

The internet relies on things: vulnerable undersea cables

Undersea cables carry almost all the world's internet traffic - and they are vulnerable to deliberate destruction as China has shown around Taiwan.



Tyrskylän ”who is who” asiantuntijamme

Jari Isokallio, Digi- ja väestötietovirasto – fasilitoivat Teams-keskustelua
Juha Malmivaara, Tampereen yliopisto
Kari Paara, Digi- ja väestötietovirasto
Tuomas Pelttari, Digi- ja väestötietovirasto – fasilitoivat Teams-keskustelua
Antti Pirinen, Deloitte ja Tietoturva ry
Juha Tretjakov, Kyberturvallisuuskeskus
Tatu Vehmas, Tyrskylän vastavalittu tietoturvapäällikkö – tervetuloa! – myös Tietoturva ry
Lea Viljanen, HackrFi

Tilaisuuden tarkkailijoina toimii **Juha Kirves** Digi- ja väestötietovirastosta. Tilaisuuden moderoivat **Tapani Rinne** ja **Kimmo Rousku**, Digi- ja väestötietovirasto.

Mitä tapahtuu kun, häiriö – hyökkäys tai loukkaus käynnistyy?

… tai sähkökatko, salama, tykkylumi, tulva tai pandemia …

DIGI- JA VÄESTÖTIETOVIRASTO

Mikä hyökkäyksen käynnistää?

- **Meidän ihmisten toiminta.**

- Me ihmiset toimimme digimaailmassa esimerkiksi ns. **loppukäyttäjinä**, **IT-järjestelmien ylläpitäjinä, hallinnollisina asiantuntijoina** tai **pääkäyttäjinä** (administrator) ja **sovelluskehittäjinä**.

  - **Muista!** Kotona ja vapaa-ajalla olemme itse asiassa kaikki oman kodin it-infran ylläpitäjiä ja pääkäyttäjiä

  - Jokaisen meidän toiminnalla on merkitys, kukaan ei varmaan halua olla haavoittuvuuksien aiheuttaja tai se henkilö, jota kautta tietomurto tai muu onnistunut kyberhyökkäys käynnistyy? **Me ihmiset olemme keskiössä.**

  - Tämä ei onnistu, mikäli näistä asioista ei keskustella avoimesta, ohjeisteta ja kouluteta sitä mukaan, kun meidän toimintaympäristössä tapahtuu muutoksia myös uhkien ja riskien osalta

Toimenpiteitä, jotka voivat aiheuttaa organisaatioon tietomurron

a) Henkilöstön toimenpiteet ja virheet

1.Kalasteluviesteihin (phishing) lankeaminen: Luottamuksellisten tietojen, kuten kirjautumistietojen, luovuttaminen huijaussivustoille.

2.Heikko salasanakäytäntö: Helppojen tai uudelleen käytettyjen salasanojen käyttö.

3.Tietoturvaohjeiden noudattamatta jättäminen: Esimerkiksi työskentely suojaamattomilla laitteilla tai julkisilla Wi-Fi-verkoilla.

4.Tiedostojen lataaminen tuntemattomista lähteistä: Haittaohjelmien tai virusten asentaminen vahingossa.

5.Tiedon jakaminen väärille vastaanottajille: Sähköpostien tai asiakirjojen lähettäminen vahingossa ulkopuolisille.

6.USB-tikkujen tai muiden laitteiden käyttö ilman tarkastusta: Epäilyttävän tai haitallisen median käyttö.

7.Tietojen säilyttäminen epävarmoissa paikoissa: Esimerkiksi pilvipalveluissa, joita ei ole hyväksytty organisaation käyttöön.

b) IT-asiantuntijan toimenpiteet ja virheet

1.Päivitysten laiminlyönti: Palvelimien, ohjelmistojen ja käyttöjärjestelmien vanhentuneiden versioiden käyttö.

2.Huolimattomuus pääkäyttäjäoikeuksien hallinnassa: Liian laajojen käyttöoikeuksien myöntäminen henkilöstölle.

3.Väärin konfiguroidut järjestelmät: Esimerkiksi palomuurien tai tietokantapalvelinten virheellinen asennus.

4.Lokien ja valvonnan laiminlyönti: Järjestelmäpoikkeamien ja tietoturvauhkien havaitsematta jääminen.

5.Epävarmojen kolmannen osapuolen ohjelmistojen käyttö: Ilman riittävää arviointia käyttöön otetut ohjelmistot.

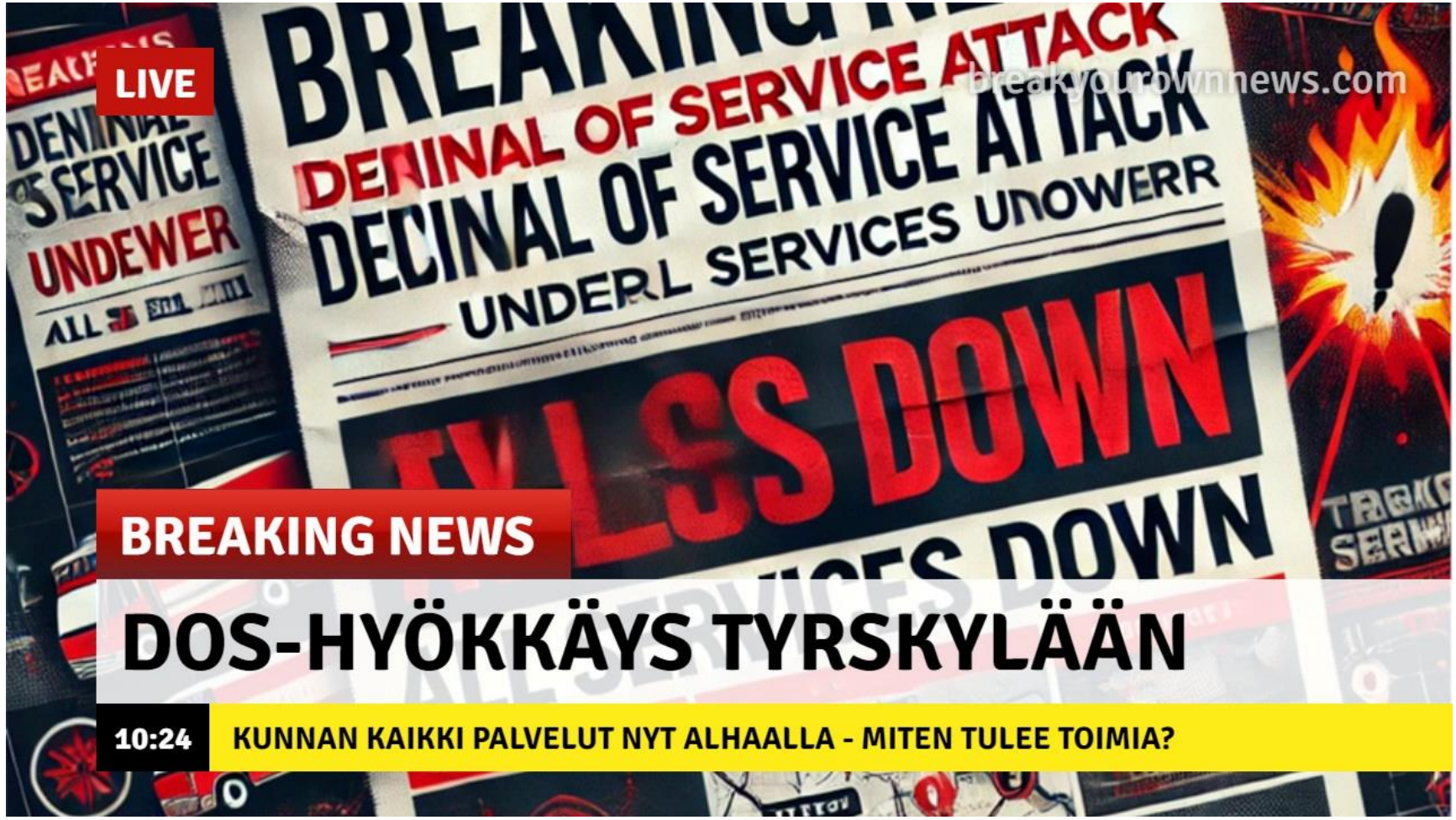
6.Varmuuskopioinnin puutteet: Varmuuskopiointien ja niiden palautustoimintojen testaamisen unohtaminen.

7.Monivaiheisen tunnistautumisen (MFA) käyttöönoton laiminlyönti: Pääsynhallinnan heikkoudet.

c) Sovelluskehittäjän toimenpiteet ja virheet

1. **Tietoturvaheikkoudet koodissa:** Esimerkiksi SQL-injektion, XSS-hyökkäysten tai heikon autentikoinnin mahdollistaminen.
2. **Puutteellinen koodin testaus:** Koodin testaamisen laiminlyönti, mikä jättää ohjelmistoon avoimia haavoittuvuuksia.
3. **Kolmannen osapuolen kirjastoihin luottaminen ilman tarkastusta:** Epäluotettavat tai haavoittuvat kirjastot voivat olla hyökkäyksen väylä.
4. **Tietojen salaamatta jättäminen:** Herkät tiedot, kuten käyttäjätiedot, tallennetaan salaamattomana.
5. **Väärin konfiguroitu API:** Rajapinnat, jotka ovat avoimia ulkopuolisille hyökkäyksille.
6. **Testiympäristön käyttö tuotannossa:** Testitietokantojen ja -järjestelmien käyttö ilman asianmukaisia tietoturvatoimia.
7. **Tietoturvakäytäntöjen ohittaminen:** Esimerkiksi suora pääsy tietokantoihin ilman turvamekanismeja tai varmuuskopioita.

Millaisiin hyökkäyksiin Tyrskylän kannattaa varautua?



Millaisiin hyökkäyksiin Tyrskylän kannattaa varautua?

Millaisiin hyökkäyksiin Tyrskylän kannattaa varautua?

Uusi Tyrskylän kunnan palvelu – Tyrskyläinen-kuntalaispalvelu on otettu käyttöön – rekisteröidy!

Arvoisa kuntalainen,

Helpotamme sähköistä asioi

123 ensimmäistä palve talaista saa ainutkertaisen, arvokk a kullatun Tyrskylä-ämpärin!

Kirjaudu: https://ty talainen

Karoliina Kunnanjohtaja
Tyrskylän kunta
kunnanjohtaja@tyrskyla.fi

Ensimmäinen teema – mitenTyrskylän kannattaisi kehittää omaa tietoturvallisuutta ja varautumista – ennakoivasti?

- Jotta tällaista tilannetta ei pääsisi syntymään, mitkä ovat tärkeimmät asiat, jotka pitäisi olla Tyrskylässä kunnossa?
  - Millaisia virheitä olette tunnistaneet

Kun jokin edellä olevista käynnistyi eli DoS | tietomurto | kalastelukampanja

Mitä pitää tehdä ensimmäiseksi? Entä seuraavaksi?

- Vinkkejä ja kokemuksia Tyrskylästä pohjautuen aikaisempiin tapauksiin:
  - Miten tilannetta **tulee johtaa**?
  - Missä vaiheessa ja kenelle tehdään **viranomaisilmoitukset?**
- Mitä **EI KANNATA** tehdä?
  - Mikä tässä kohtaa on **viestinnän rooli?**
    - Millaisia virheitä tai haasteita olette tunnistaneet esimerkiksi Tyrskylän naapurikuntien kriisiviestinnässä?

Miten palaudutaan normaaliin?

Tilannekuvan ja tutkinnan merkitys, tiekartta palautumiseen?

DIGI- JA VÄESTÖTIETOVIRASTO

Hutkitaanko teillä vai tutkitaanko huolella?

1) Tietoturvapoikkeamien tunnistaminen ja tutkiminen
- Selvitetään, mitä on tapahtunut, miten hyökkäys tapahtui ja mihin se on vaikuttanut.

2) Tietojen kerääminen ja analysointi
- Kerätään ja tutkitaan digitaalisia todisteita hyökkäyksen jäljittämiseksi ja syiden ymmärtämiseksi. Miten teidän lokitus voi? Mitä te muuten lokitatte? Onko pituus 24h – 1 – 2 – 5 – 10 v vai emme tiedä? Onko lokien hallinta (keskitetty)? Oletteko harjoitelleet lokien hyödyntämistä?

3) Tilanteen hallinta ja eristäminen
- Rajoitetaan hyökkäyksen vaikutuksia estämällä sen leviäminen ja poistamalla haittaohjelmat ja muut hyökkäysvektorit. Missä kaikessa voitte käyttää maantieteellistä geoblocking? Takaportteja EI SAA jäädä.

4) Palautuminen ja vahinkojen korjaaminen
- Palautetaan järjestelmät toimintakuntoon, varmistetaan palveluiden turvallisuus ja tietojen eheys. Mites ne backupit voi? Onko niitä? Testattuna?

5) Oppiminen ja raportointi
- Dokumentoidaan tapauksen kulku ja parannetaan organisaation tietoturvaa tulevien hyökkäysten estämiseksi. Takaisinkytkentä riskienhallintaan? Haluatteko kertoa kaikille avoimesti?

Esimerkkejä avoimesta tiedottamisesta ja oppien jakamisesta

- https://dvv.fi/digiturvatilaisuudet

Kyberhyökkäysten opit-videot

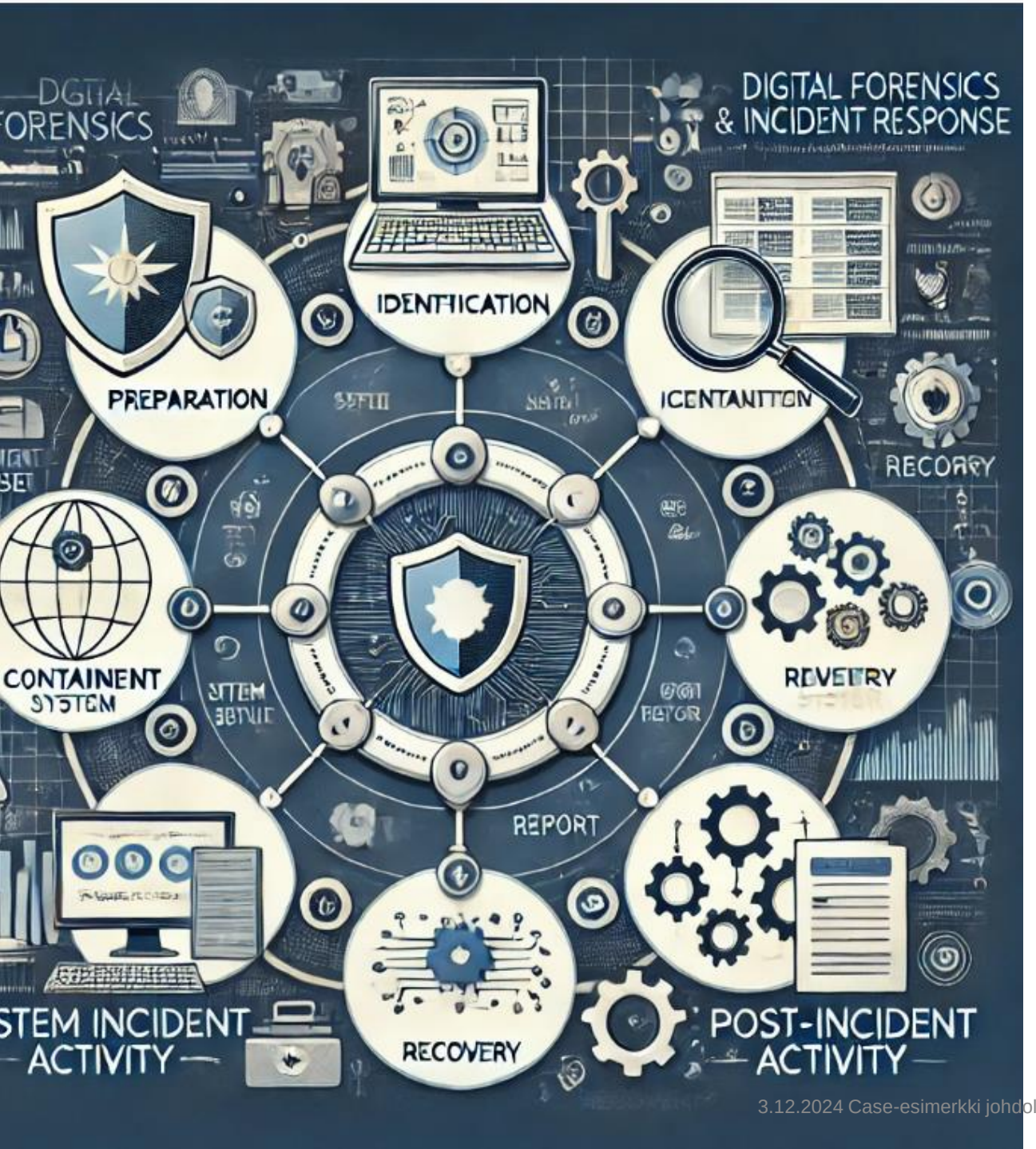
Alapuolelle on koottu ne julkiset videot, joissa eri toimijat ovat käsitelleet heihin kohdistuneen kyberhyökkäyksen vaikutusta ja oppeja. Jokainen näistä toimijoista on saanut myös aikanaan VAHTI-tunnustuksen tästä esimerkillisestä avoimuudesta ja oppien jakamisessa muille.

27.9.2023 Teemakeskustelu - Miten kyberhyökkäys muutti toimintaamme?
Säkylän kunnan ja Keudan ohella sisältää myös HSL:ään kohdistuneen palveluestohyökkäysten tarinan.

15.3.2023 Keuda - kyberhyökkäyksen opit
Noin 10 minuutin kohdalta.

2.3.2023 Säkylän kunta - kyberhyökkäyksen opit

11.10.2022 Savonia - kyberhyökkäyksen opit
Noin 59 minuutin kohdalta.

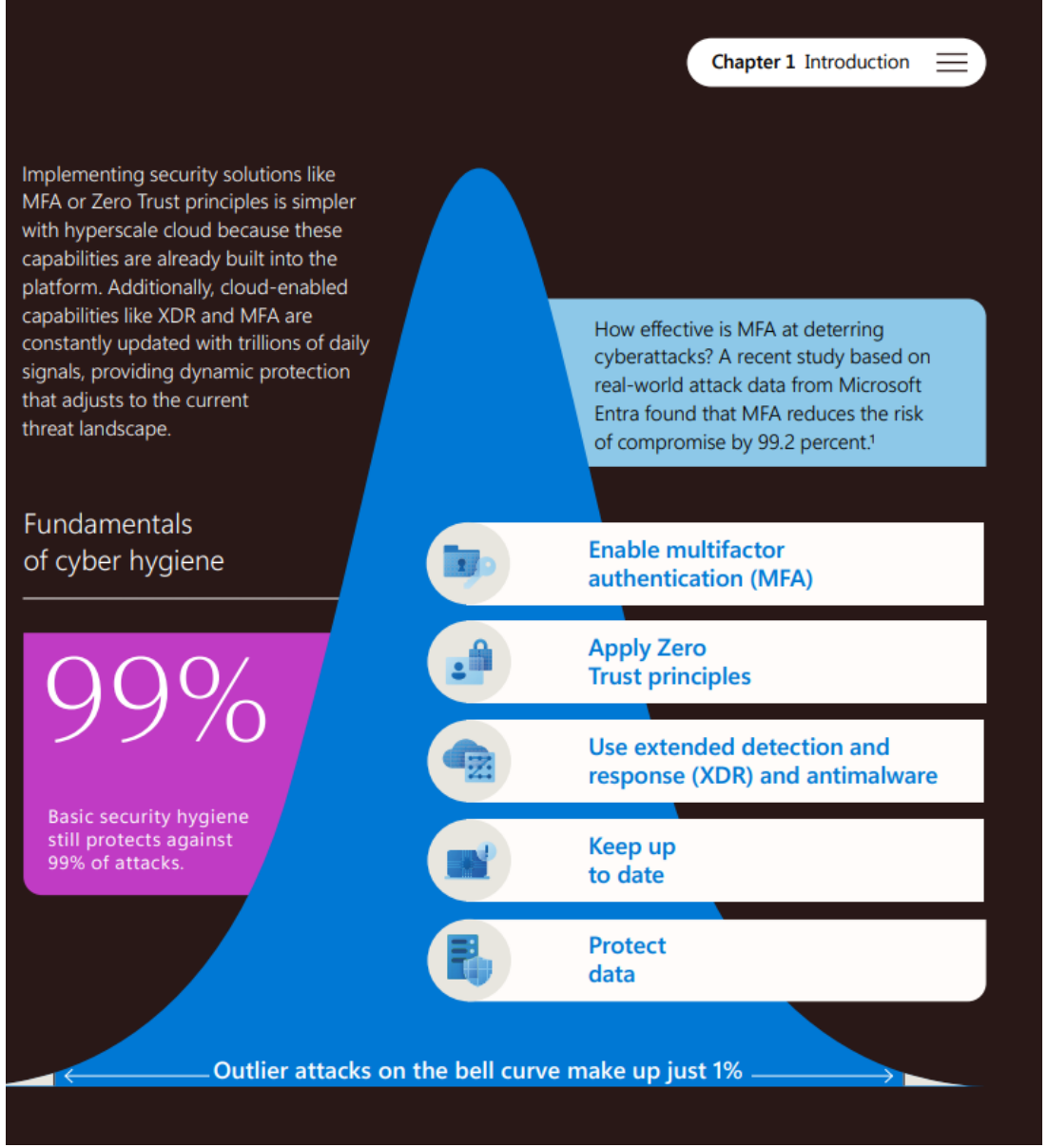


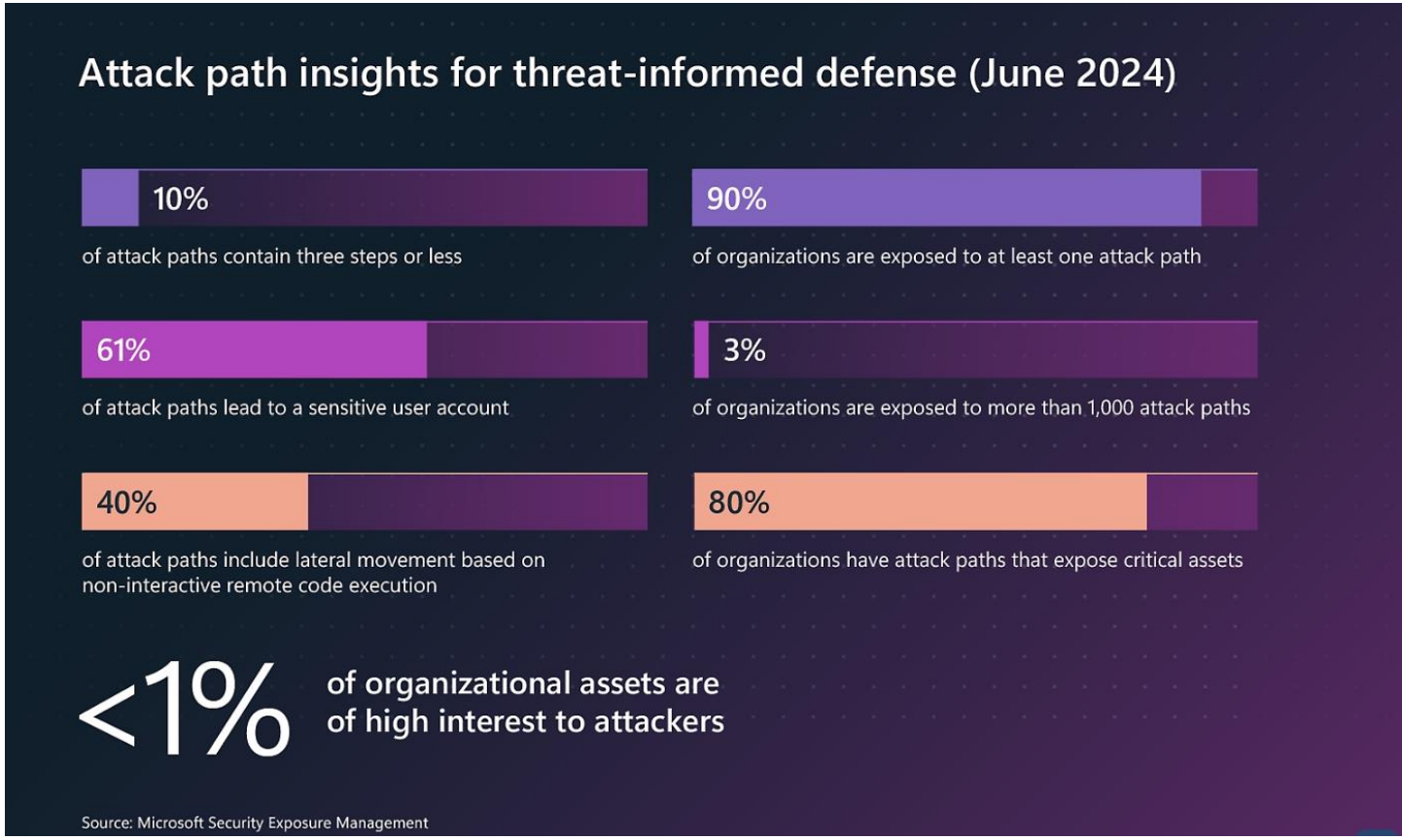
Kertaus - tilannekuvan ja tutkinnan merkitys, tiekartta palautumiseen?

- Mistä saadaan apua ja millaisia resursseja tilanteen tutkiminen, häiriötilanteen tai hyökkäyksen rajaaminen ja ”tuhojen” korjaaminen eli **palautuminen normaaliin tilanteeseen edellyttää**?
  - Millaisia eroja tilanteen hallinnassa erilaisten hyökkäysten osalta on tunnistettavissa?
  - Mitkä ovat Tyrskylässä koettuja käytännön kokemuksia erilaisten hyökkäysten, loukkausten ja murtojen osalta palautumiseen liittyen?
  - Millaisia ongelmia olette kuulleet naapurikunnan kollegoilta, **millaisia virheitä** siellä on tehty palautumisen osalta?

Miten voit pienentää riskiä, että organisaatio joutuu tietomurron tai onnistuneen kyberhyökkäyksen tai muun merkittävän uhan tai riskin kohteeksi sekä kuinka organisaatio voi nopeuttaa tällaisessa tilanteessa palautumista normaaliin?

DIGI- JA VÄESTÖTIETOVIRASTO


Chapter 1 Introduction
Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.
How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.[1]
Fundamentals of cyber hygiene
99%
Basic security hygiene still protects against 99% of attacks.
Enable multifactor authentication (MFA)
Apply Zero Trust principles
Use extended detection and response (XDR) and antimalware
Keep up to date
Protect data
Outlier attacks on the bell curve make up just 1%


Attack path insights for threat-informed defense (June 2024)
10%
of attack paths contain three steps or less
90%
of organizations are exposed to at least one attack path
61%
of attack paths lead to a sensitive user account
3%
of organizations are exposed to more than 1,000 attack paths
40%
of attack paths include lateral movement based on non-interactive remote code execution
80%
of organizations have attack paths that expose critical assets
<1%
of organizational assets are of high interest to attackers
Source: Microsoft Security Exposure Management

Mitkä ovat 12+ keskeistä kyber- ja digiturvaan liittyvää asiaa Tyrskylässä, joiden toiminta kannattaa ehdottomasti varmistaa?

- Olemme koonneet tähän eri VAHTI-asiantuntijoiden esille nostamia asioita, joita he ovat nostaneet esille oman organisaationsa näiden osa-alueiden kehittämisessä.
- **Seuraavan sivun lista on koottu VAHTI-verkostolle saadun ennakkokyselyn perusteella – otamme sen pohjaksi keskusteluun**

Ennakolta - oman organisaation toiminnan turvaaminen

1. **Henkilöstön koulutus ja tietoisuus**
   - Jatkuva koulutus työntekijöille tunnistamaan hyökkäykset ja vaaran paikat.
   - Tietoisuuden ylläpitäminen ja matalan kynnyksen raportointimahdollisuudet poikkeamatilanteissa.
   - Johdon säännöllinen viestintä ja henkilöstön ajantasalla pitäminen.

2. **Tekniset toimenpiteet**
   - Kaksivaiheinen tunnistautuminen (MFA) ja käyttövaltuuksien hallinta ("admin-right are not human rights").
   - Järjestelmien ja tiedostojen pääsyn rajoittaminen luotetuille laitteille.
   - Immutable-varmuuskopiointi, M365-varmuuskopiot ja tiedonvalvonta (DLP).

3. **Varautuminen ja harjoittelu**
   - Dokumentoitujen toimintasuunnitelmien luominen ja niiden säännöllinen harjoittelu.
   - Organisaation kriittisten toimintojen tunnistaminen ja varautuminen niiden kautta.
   - Häiriötilanteiden valmiuden ja osaamisen kehittäminen.

4. **Ulkoisten resurssien hyödyntäminen**
   - Ulkopuolisen avun hankkiminen viestintään ja tietoturvaan, jos organisaatiolla ei ole riittäviä resursseja.
   - Ulkoistusten ja toimitusketjujen hallinta varmistaen, että kumppanit täyttävät tietoturvavaatimukset.

5. **Hallinnolliset ja prosessien parannukset**
   - Tietoturva- ja tietosuoja-asioiden pitäminen ajan tasalla.
   - Selkeät ohjeet ja turvatoimet langenneille käyttäjille, ja niiden julkinen saatavuus ilman kirjautumista.
   - Rooliin perustuvat käyttöoikeudet ja kirjautumisen hallinta.

Tärkeimmät vinkit johtaminen ja hallinta

1. **Ennakointi ja valmistautuminen**
   - Laadi selkeät toimintasuunnitelmat ja vastuut jo normaalioloissa.
   - Sopikaa roolit ja vastuut tietoturvahäiriöiden hallinnassa, mukaan lukien järjestelmän toimittajat ja kumppanit.
   -Tuota jatkuvaa tilannekuvaa läpinäkyvästi ja avoimesti organisaatiossa.
   - Harjoittele säännöllisesti: realistiset skenaariot ja johdon osallistuminen ovat avainasemassa.

2. **Toiminta hyökkäyksen | häiriön | loukkauksen aikana**
   - Pysy rauhallisena ja keskity tilanteen selvittämiseen.
   - Ota yhteyttä tarvittaviin viranomaisiin mahdollisimman aikaisessa vaiheessa.
   - Viesti selkeästi ja rehellisesti niin organisaation sisällä kuin ulkopuolelle.
   - Käytä dokumentoituja toimintamalleja | prosesseja, jotta kaikki tietävät tehtävänsä.

3. **Tekninen valmius ja riskienhallinta**
   - Paranna teknisiä järjestelmiä ja kovennuksia, sillä ne toimivat tehokkaammin kuin pelkät dokumentit.
   - Pidä käytössä "pienimmän käyttöoikeuden periaate" ja varmista jatkuvuus- ja palautumissuunnitelmien toimivuus (DRP).
   - Tarvittaessa käytä SOC-kumppania riskien hallintaan ja hyökkäysten torjuntaan.

4. **Viestinnän merkitys**
   - Selkeä ja rehellinen viestintä korostuu nopeasti muuttuvassa tilanteessa.
   - Laadi etukäteen viestintäsuunnitelma, joka kattaa sisäisen ja ulkoisen tiedottamisen.
   - Käytä myös offline-viestintävälineitä, kuten poissa verkosta olevia puhelimia ja tulostimia.

5. **Jälkiselvittely ja jatkuva parantaminen**
   - Tallenna ja kirjaa selvitysten vaiheet, kuten kuvakaappaukset ja kommentit, dokumentiksi.
   - Analysoi tapahtuma jälkikäteen ja päivitä prosessit sekä toimintasuunnitelmat.
   - Jatkuva harjoittelu ja prosessien kehittäminen ovat välttämättömiä organisaation resilienssin vahvistamiseksi

Bonusosio

Voit lisäksi hyödyntää seuraavia materiaaleja, ennen kaikkea Poliisin tuottamaa ”Alkutoimiohjeet asianomistajaorganisaatiolle tietoverkkorikostapauksessa”

DIGI- JA VÄESTÖTIETOVIRASTO

1. Tiedonhallinta

- Lakisääteisten ja muiden kokonaisuuteen liittyvien velvoitteiden tunnistaminen
- Eri tiedonhallinta | turvallisuus | IT-arkkitehtuurien huomioiminen organisaation toiminnan kehittämisessä
- Tiedonhallintamalli ja siihen liittyvät ohjeet
- Tietojen elinkaarenhallintamalli toteuttaminen tiedon syntymästä => arkistointi / hävittämiseen
- Tietojen varmuuskopiointi ja eheyden varmistaminen
  - Teknisesti toteutettava muusta IT-infrasta erillisenä, muistettava myös suojakopiot
- Henkilöstön perehdytys, ohjeistus ja koulutus **– tämä koskee KAIKKIA osa-alueita**

2. Riskienhallinta

- Politiikka ja ohjeistus organisaation toiminnan eri tasoille
- Prosessimalli, jonka mukaan toimitaan
- Säännöllinen organisaation eri tasoille ulottuva raportointi
  - Ja DVV:n kokonaiskuvapalvelun hyödyntäminen omassa toiminnassa
- Häiriöistä, poikkeamista, hyökkäyksistä ja loukkauksista oppiminen eli kytkentä toiminnan jatkuvuuteen
- Henkilöstön motivoiminen ilmoittamaan pienemmistäkin epäilyistä tai risahduksista
- Henkilöstön (ja siihen kuuluu myös ylin johto) turvallisuus ja digiturvakävelyt

3. Toiminnan jatkuvuus ja varautuminen

- Palveluiden kriittisyyden vuosittainen tai sen roolin muuttumisen myötä tehtävä kriittisyys/tärkeysarviointi
- Organisaation kriittisten palveluiden, toimijoiden ja toimitusketjujen ja alihankintaverkoston tunnistaminen ja niiden turvallisuuden varmistaminen
- Tarvittavat suunnitelmat
- Säännöllinen harjoittelu - #Taisto
- Jatkuvuuden hallinnan huomioiminen kaikissa palvelusopimuksissa

4. Tietosuoja

- Tietosuojapolitiikka ja ohjeistukset
- Uusien palveluiden hyväksyntäprosessi sisältäen tarvittavat (riskienhallinta)arvioinnit tietosuojan eri osa-alueiden ja myös tietoturvan osalta
- Huolehdi rekisteröityjen oikeuksien toteuttamisesta
- Tietosuojan huomioiminen kaikissa palvelusopimuksissa
- Henkilöstön ja palvelutoimittajien ohjeistaminen henkilötietojen käsittelijöinä
- Prosessi henkilötietojen tietoturvaloukkausten käsittelemiseksi

5. Tietoturvallisuus

- Tietoturvapolitiikka sekä tätä tukevat muut ohjeistukset
- Tietoaineistojen turvallisen käsittelyn ohjeistus – esimerkiksi 4T-malli eli Tunnista | Tilat | Tiedot | Työkalut
- Tekninen tietoturva
  - Laitehallinta / cmdb / asset-management
  - Tietoturvapäivitysten hallintaprosessi
  - Päätelaitteiden (tietokoneet, älylaitteet) tietoturvallisuuden varmistaminen
- Oman IT-ympäristön dokumentointi ja muu ymmärrys
- Haavoittuvuusskannaukset oman ulkopuolelta
  - Hyödyntäkää KTK:n Hyöky-palvelua!
- Havainnointikyvykkyys mielellään siinä vaiheessa, kun organisaatioon YRITETÄÄN murtautua, mutta myös kyky toimia tietomurron tai muun kyberhyökkäyksen tapahduttua
- Tietoturvan huomioiminen palvelusopimuksissa
- Käytössänne olevien pilvipalveluiden tietoturvaominaisuuksien tehokas hyödyntäminen

Ja vielä #AI-Kimmon kontribuutio:

Tässä ovat 12 keskeistä kyber- ja digiturvaan liittyvää asiaa, joiden toiminta kannattaa ehdottomasti varmistaa Tyrskylän kunnassa:

1. **Verkkoinfrastruktuurin suojaus:**
    1. Varmista palomuurien, reitittimien ja kytkimien ajantasaisuus ja suojaus.
    2. Käytä tunkeutumisenestojärjestelmiä (IDS/IPS) havaitsemaan ja estämään epäilyttävää toimintaa.
2. **Tietojärjestelmien päivitykset:**
    1. Suorita säännölliset ohjelmisto- ja järjestelmäpäivitykset.
    2. Korjaa tunnetut haavoittuvuudet nopeasti.
3. **Tietosuojakäytännöt ja GDPR:n noudattaminen:**
    1. Suojaa henkilötiedot ja noudata tietosuojalainsäädäntöä.
    2. Kouluta henkilöstöä tietosuojakäytännöistä.
4. **Henkilöstön koulutus ja tietoisuus:**
    1. Järjestä säännöllisiä koulutuksia tietoturvauhkien tunnistamiseksi.
    2. Kannusta turvallisiin työskentelytapoihin, kuten vahvojen salasanojen käyttöön.
5. **Varautuminen kyberhyökkäyksiin ja kriisinhallinta:**
    1. Laadi ja päivitä tietoturvapoikkeamien hallintasuunnitelma.
    2. Harjoittele toimintaa mahdollisissa tietoturvahyökkäystilanteissa.
6. **Varmuuskopiointi ja palautusjärjestelmät:**
    1. Ota säännöllisesti varmuuskopiot kriittisistä tiedoista.
    2. Testaa palautusprosessit varmistaaksesi niiden toimivuuden.

7. **Pääsynhallinta ja autentikointi:**
    1. Käytä monivaiheista tunnistautumista (MFA) tärkeissä järjestelmissä.
    2. Rajoita pääsyoikeudet tehtävien ja tarpeiden mukaan.
8. **Mobiililaitteiden ja etätyön turvallisuus:**
    1. Ota käyttöön mobiililaitteiden hallintaratkaisut (MDM).
    2. Varmista, että etäyhteydet ovat suojattuja (esim. VPN).
9. **Pilvipalveluiden turvallisuus:**
    1. Arvioi pilvipalveluntarjoajien tietoturvakäytännöt.
    2. Salaa pilvipalveluissa säilytettävät tiedot.
10. **Kolmannen osapuolen riskienhallinta:**
    1. Tarkista toimittajien ja kumppaneiden tietoturvakäytännöt.
    2. Sisällytä sopimuksiin tietoturvavaatimukset.
11. **Verkon ja järjestelmien valvonta:**
    1. Käytä valvontatyökaluja poikkeavuuksien havaitsemiseksi.
    2. Toteuta lokien keräys ja analysointi ongelmien jäljittämiseksi.
12. **Säännölliset tietoturva-auditoinnit ja testaukset:**
    1. Suorita sisäisiä ja ulkoisia auditointeja tietoturvan arvioimiseksi.
    2. Tee tunkeutumistestauksia haavoittuvuuksien havaitsemiseksi.
13. **Sisäisen ja ulkoisen viestinnän toteuttaminen**
    1. Muistakaa nostaa esille, millaisia mahdollisuuksia digitalisaatio tuo mukanaan!
    2. Kertokaa ajankohtaisista uhkista ja riskeistä säännöllisesti
    3. Olettehan harjoitelleet säännöllisesti häiriö ja kriisiviestintää?
    4. Oletteko sopineet viestintävastuista sidosryhmien ja palveluverkostonne kanssa?

Entä kun jotain tapahtuu?

Miten otat yhteyttä poliisiin ja mitä tietoja on hyvä olla selvillä?

DIGI- JA VÄESTÖTIETOVIRASTO

KESKUSRIKOSPOLIISI – https://poliisi.fi

Yhteydenotto poliisiin

- Hätätilanne/kiireellinen tilanne: 112
- Kiireetön rikosilmoitus:
  - Ensisijaisesti: Sähköinen rikosilmoitus: https://asiointi.poliisi.fi/fi/yritys/rikos
  - Palvelu on poissa käytöstä klo 22.45 - 06.00.
  - Sähköisen rikosilmoituksen asiointipalveluun kirjautuminen edellyttää vahvaa tunnistautumista
- Puhelimitse poliisiaseman palvelupäivystykseen (vain jos muita ilmoituskanavia ei ole käytössä)
- Paikan päällä poliisiaseman palvelupäivystykseen

Yleisneuvonta ja apu kiireettömissä asioissa (esim apua rikosilmoituksen tekoon):
Poliisin valtakunnallinen neuvontapuhelin 0295 419 800 (arkisin klo 8-16.15).
Lisätietoa: https://poliisi.fi/neuvontapalvelu

Rikoksiin liittyvät vihjeet (myös anonyymi ilmoitus onnistuu):

- Poliisin Nettivinkki: https://poliisi.fi/nettivinkki
- Vihjeyhteystiedot poliisilaitoksittain: https://poliisi.fi/vihjeyhteystiedot

Alkutoimiohjeet asianomistajaorganisaatiolle tietoverkkorikostapauksessa

- Tietojärjestelmiin tai muuhun tietotekniseen ympäristöön kohdistuneiden rikosten selvittämisessä hyödynnetään samankaltaisia tietoja kuin teknisen häiriötilanteen diagnostiikassakin. Esimerkiksi palvelunestohyökkäyksessä rikostutkinnan tukena toimivat hyvin **lokit, joissa perusasiat ovat hyvällä tasolla**. Palvelunestohyökkäyksen lisäksi tietoverkkorikoksia ovat esimerkiksi yritykseen kohdistuneet tietomurrot ja haittaohjelmat. Mikäli epäilee rikosta, on asiasta hyvä ilmoittaa poliisille epäselvissäkin tapauksissa. Poliisi arvioi ilmoituksen jälkeen, täyttääkö teko jonkin rikoksen tunnusmerkistön.
- Pitkäkestoisen ja laajan rikosasian esitutkinnan turvaamisen kannalta tärkeimmät asiat voidaan jakaa kahteen kategoriaan:
  - 1. Rikoksen kohteena olevaa organisaatiota eli rikosasian varsinaista asianomistajaa koskeviin tietoihin. Näihin kuuluvat tiedot sekä organisaatiosta että sitä edustavista henkilöistä.
  - 2. Rikoksen kohteena olevaa tietojärjestelmää koskeviin tietoihin.

- Poliisi suosittelee, että **organisaatiossa otettaisiin rikosilmoituksen tekeminen ja todistusaineiston taltiointi osaksi tietoturvaprosesseja.** Mikäli mahdollista, rikosta epäiltäessä esitutkinnan turvaamiseksi asianomistajaa pyydetään **olemaan tekemättä korjaavia toimenpiteitä** ennen kuin tutkinnan kannalta tarvittavat taltioinnit (kappaleet 3.1-3.5) on tehty. Tässä dokumentissa on kerrottu, mitä alkutoimia ja taltiointeja organisaation olisi hyvä suorittaa tietoverkkorikostapauksessa.

1. Tekotapa ja vaikutukset

- Tapahtumakuvaus epäillystä rikoksesta, hyökkäyksen vaikutuksista ja sen kestosta sekä ilmoitus rangaistusvaatimuksesta.
- Alustava arvio aiheutuneista vahingoista. Tarkka tieto vahinkojen määrästä ja vahingonkorvausvaatimuksesta tarkentuu tutkinnan edetessä, mutta alustava arvio auttaa esitutkinnan alkuvaiheessa. Vahingonkorvauksen määrää arvioitaessa kannattaa huomioida myös kaikki tilanteeseen käytetyt henkilötyötunnit.

2. Tiedot organisaatiosta

- Organisaation eli oikeushenkilön tiedot
- Virallinen nimi
- Y-tunnus
- Organisaation kotipaikka sekä toimipisteen nimi ja sijainti
- Organisaation laillinen edustaja

2.1 Organisaation edustajan ja varahenkilön tarkat yhteystiedot:

- Sukunimi, etunimi, henkilötunnus
- Tehtävänimike
- Puhelinnumero ja sähköpostiosoite
- Edustusoikeuden peruste (esim. asemavaltuutus)
- Varsinaisen edustajan lisäksi organisaation olisi hyvä valita myös tekninen yhteyshenkilö, joka osaa vastata järjestelmiin liittyviin kysymyksiin
- Teknisen yhteyshenkilön yhteystiedot

2.2 Tiedot mahdollisista alihankkijoista ja asiakkaista sekä niiden yhteyshenkilöt

- Vastaavat tiedot kuin kohdissa 2. ja 2.1
- Alihankkijalla tarkoitetaan mm. rikoksen kohteena olevan palvelun taustalla olevaa konesalipalveluntarjoajaa.
- Asiakkaalla tarkoitetaan palvelun omistajaa.
- Rikoksen kokonaiskuvan hahmottamiseksi, asianomistajien selvittämiseksi ja esitutkinnan suorittamiseksi on tärkeää ilmoittaa myös kaikista niin sanotuista ”sijaiskärsijöistä”, jotka eivät ole olleet esim. varsinaisen hyökkäyksen kohteena, mutta joiden toiminta on verkon-rakenteesta johtuen kärsinyt.

2.3 Lupa jakaa tietoja muiden tapahtuman selvittelyyn osallistuvien tahojen kanssa

Poliisi ja muut tapauksen selvittelyyn liittyvät tahot (esim. Kyberturvallisuuskeskus tai SOC) tarvitsevat organisaation luvan, jotta voivat jakaa tietoja ja havaintoja ristiin. Mikäli organisaatio antaa luvan tietojen vaihtoon, asian voi ilmoittaa jo rikosilmoituksen tekovaiheessa.

3.1 Tiedot tietojärjestelmästä ja sen roolin kuvaus

- Rikoksen kohteena olevasta tietojärjestelmästä ja sen käyttötarkoituksesta tulisi laatia lyhyt ja ajantasainen kuvaus pelkän palvelunimen lisäksi. Palvelun käyttötarkoitus voi olla olennainen tieto rikosasian selvittämisen kannalta.
- Lyhyt kuvaus hyökkäyksen/poikkeaman vaikutuksista organisaatioon, jotta poliisi osaa arvioida teon vakavuutta.
- Kuvaus hyökkäyksen kohteena olevan tietojärjestelmän teknisistä yhteyksistä ja rajapinnoista (verkko- ja palvelindokumentaatio) sillä tarkkuudella, että hyökkäyksen todellinen kohde ja hyökkäyksessä mahdollisesti lamaantunut laitteisto voidaan tunnistaa. Tarvittaessa myös tieto, mistä kohdista on olemassa lokia ja mitä on varmuuskopioitu minnekin.
- Mikäli käytössä on virtuaalikoneita, RAM-dumpin ottaminen, snapshotin ottaminen ja jäädyttäminen rikoksen kohteena olleesta koneesta. Tätä kannattaa harjoitella jo etukäteen.
- Rautakoneiden osalta suunnitelma siitä, kuka tekee ensitoimet. Tämän henkilön ei tarvitse olla poliisi, jos omasta SOC-toiminnosta tai vastaavasta löytyy osaaminen ottaa muistidumppi yms.

Karkeimmillaan dokumentaatiosta tulisi käydä ilmi yhteys ulkoverkon reitittimeltä hyökkäyksen kohteeseen ja niiden käyttämät IP-osoitteet sekä muut tekniset tiedot. Muita teknisiä tietoja voivat olla esimerkiksi reitittimen tyyppi ja palvelimen käyttämät ohjelmistot kuten WEB-palvelimen tuotteet.

3.2 Tapahtumalokit

- Organisaation tulisi omistaa omat lokinsa ja retentioaikojen olla tarpeeksi pitkiä (mieluiten vuosia). Jos palvelimen edustalle on asennettu kuormantasaajia tai palomuurilaitteistoa, joka kirjoittaa tapahtumalokia, kannattaa lokin sisältö tarkastaa hyvissä ajoin, jotta voidaan varmistua, että lokitetaan oikeita asioita. Esimerkiksi osa yleisesti käytössä olevista kuormantasaus- ja palomuurilaitteistoista kirjoittaa lokia verkkoyhteyksistä siten, että se maskeeraa sisään tulevat verkkoyhteydet omalla sisäverkon IP-osoitteella.

- Lokin sisällöstä on hyvä varmistaa myös se, että se sisältää tarkat aikaleimat, lähde- ja kohdeosoitteet ja muut perusasiat. Lisäksi lokien formaatti kannattaa dokumentoida ja lokien käytettävyys varmistaa siltä osin, että ne ovat saatavissa laitteistosta luettavassa (teksti)muodossa ulos ja niiden käsittely onnistuu tavallisilla työkaluilla. Lokit tulisi toimittaa poliisille aina sellaisenaan, mutta kaikki stilisoitu tai analysoitu lokitietokin otetaan mielellään vastaan alkuperäisen lisäksi. Kaikki alkuperäisestä muuttunut data tulee kuitenkin merkitä selvästi muokatuksi ja sen tulisi toimia vain alkuperäisen datan tukena. Lokia tarvitaan usein myös selvästi hyökkäystä tai poikkeamaa edeltävältä ajalta sekä sen jälkeen, jotta saadaan näyte ns. normaalista tilasta.
- Jos tietyllä ajanjaksolla havaitaan tavallista enemmän poikkeavaa verkkoliikennettä, kuten matalan volyymin palvelunestohyökkäyksiä tai porttiskannauksia, kannattaa tapahtumalokit ottaa talteen.
- Mikäli organisaatio on tehnyt hyökkäyksestä alustavaa analyysiä ja tunnistanut tietoturvapoikkeamaan/verkkohyökkäykseen liittyviä tunnisteita, kuten hyökkäyksessä käytetyn IP-osoitteen, tulisi tiedot niistä toimittaa poliisille niin pian kuin mahdollista. Tämä mahdollistaa poliisin tutkintatoimien nopean käynnistämisen.

3.3 Verkkolokit tietoliikenneoperaattorilta tai palomuurilaitteistosta

- Verkkoliikenteestä kirjoitetaan ymmärrettävästi hyvin eri tasoista lokia liikennemääristä riippuen, mutta varsinkin palvelunestohyökkäyksissä niistä tulisi olla perustiedot saatavilla.
- Hyökkäyksen tarkat aikaleimat aikavyöhyketietoineen
- Hyökkäyksen lähde- (myös väärennetyt) ja kohdeosoitteet
- Tietoliikenteen tyyppi: protokolla- / porttitiedot
- Hyökkäyksen volyymi: ppt- / bps-tiedot (numeeriset ja graafiset jos mahdollista)

- **3.4 Sähköpostit**
- Mikäli tutkittavaan tapaukseen liittyy sähköpostiviesti, esim. kalasteluviesti tai haitallinen liitetiedosto, tulee se ehdottomasti säilyttää tutkintaa varten. Se kannattaa tallettaa kokonaisena viestitiedostona liitteineen ja header-tietoineen poliisille toimittamista varten. Viestin välittäminen suoraan sähköpostiohjelmasta poliisin sähköpostiosoitteeseen ”välitä”-toiminnon avulla ei ole oikea toimintatapa, sillä se muuttaa alkuperäisen viestin header-tiedot ja haitallinen liitetiedosto aiheuttaa myös riskin.

- **3.5 Muut mahdolliset tiedot**
- Lisäksi pyydämme toimittamaan meille kaiken muun kiinnostavan materiaalin, mikä teidän mielestänne liittyy epäiltyyn rikokseen. Tässä tapauksessa olemme esimerkiksi kiinnostuneita mahdollisista lunnasvaatimuksista yms.

Perusasiat ja ennakoiva varautuminen

1. Kriittisten tietojen ja järjestelmien tunnistaminen:

Selvittäkää, mitkä tiedot ja järjestelmät ovat elintärkeitä (esim. HR-järjestelmät, päiväkotien tietojärjestelmät, verkkosivut).

Dokumentointi: Laaditaan tarkka dokumentaatio tiedoista, niiden sijainnista ja käsittelytavoista.

Koulutus ja harjoittelu: Järjestäkää henkilöstölle säännöllistä koulutusta ja harjoituksia, jotta he osaavat toimia kriisitilanteessa.

Riskianalyysi: Analysoikaa palvelut ja järjestelmät riskien näkökulmasta ja arvioikaa, miten kriittiset palvelut pysyvät toiminnassa eri häiriötilanteissa.

Tietoturvakulttuuri: Luokaa kulttuuri, jossa tietoturva nähdään kaikkien vastuuna.

2. Tekninen varautuminen

Monivaiheinen tunnistautuminen (MFA): Varmistakaa sen käyttö erityisesti kriittisissä järjestelmissä.

Vara- ja hajautusjärjestelmät: Hyödyntäkää pilvipohjaisia ja hajautettuja järjestelmiä kestävyyden parantamiseksi.

Valvonta ja lokitiedot: Seuratkaa järjestelmien käyttöä ja poikkeamia, ja varmistakaa, ettei lokitiedot ylikirjoitu kriisitilanteissa.

Automaatiotyökalut: Käyttäkää automaattisia mekanismeja, kuten tunnusten resetointia ja istuntojen sulkemista, hyökkäyksen estämiseksi.

Verkkojen segmentointi: Rajoittakaa pääsyä järjestelmien välillä.

3. Toiminta häiriötilanteessa

Tilannekuvan muodostaminen: Kerätkää nopeasti tietoa tilanteesta ja jakakaa se osallisille.

Toimintojen eristäminen: Katkaiskaa verkkoyhteydet tarvittaessa ja minimoikaa vahingot säilyttäen todistusaineistoa.

Viestintä: Viestikää selkeästi ja avoimesti, milloin lisätietoja on saatavilla. Suunnitelmallinen kriisiviestintä estää huhujen leviämisen ja ylläpitää luottamusta.

Johtaminen ja vastuut: Jakakaa roolit ja vastuut selkeästi. Varmistakaa sijaiset ja kriisiviestinnän vastuuhenkilö.

Priorisointi: Keskittäkää resurssit kriittisimpiin toimenpiteisiin.

4. Tekninen tutkinta ja analyysi

Resurssien kohdentaminen: Varmistakaa, että tutkijoilla on riittävät työkalut ja aineisto.

Playbookit ja prosessit: Hyödyntäkää valmiita toimintamalleja, jotka nopeuttavat analyysiä.

Yhteistyö ulkoisten tahojen kanssa: Käyttäkää asiantuntijoita tarvittaessa.

5. Palautuminen ja oppien hyödyntäminen

Tilannekuvan varmistaminen: Selvittäkää tarkasti, mitä tapahtui ja miten tilanne saatiin hallintaan.

Lessons learned: Järjestäkää tilaisuuksia, joissa analysoidaan opit ja kehityskohteet.

Jatkuvuussuunnittelu: Päivittäkää varautumissuunnitelmat ja parantakaa järjestelmien kestävyyttä.

Lokien ja tietojen hallinta: Varmistakaa, että lokitiedot säilyvät ja niiden analysointi onnistuu.

6. Viestintä ja maineenhallinta

Avoimuus ja ajoitus: Viestintä tulee hoitaa nopeasti, mutta huolellisesti. Kohderyhmän (esim. kuntalaiset, henkilöstö) osaamistaso tulee huomioida.

Viranomaisten informointi: Raportoikaa tilanteesta poliisille, Kyberturvallisuuskeskukselle ja muille viranomaisille tarvittaessa.

Luottamuksen ylläpitäminen: Selkeä ja vastuullinen viestintä ylläpitää organisaation uskottavuutta.

7. Konkreettiset vinkit pienille organisaatioille

Yhteiset toimintamallit: Hyödyntäkää valtakunnallisia ohjeistuksia ja toimintamalleja.

Ulkoisen avun hyödyntäminen: Käyttäkää asiantuntijapalveluita, jos oma osaaminen ei riitä.

Tekoälyn mahdollisuudet: Tekoäly voi auttaa erityisesti lokien analysoinnissa ja häiriöiden havainnoinnissa, mutta se ei korvaa kriittistä ajattelua.

Lopuksi: Tärkein oppi

Ennakointi, jatkuva kehitys ja oppien hyödyntäminen ovat avaimia häiriötilanteista selviämiseen. Tyrskylän kaltaisessa kunnassa, jossa resurssit ovat rajalliset, tehokas varautuminen ja suunnitelmallisuus ovat keskeisiä kykyjä toiminnan turvaamiseksi. "Älähän häthäile!" on hyvä ohjenuora kriisitilanteessa – rauhallisuus ja suunnitelmallisuus ovat ratkaisevia.

Tyrskylän kunnan varautumisesta kyberhyökkäyksiin, tietomurtoihin ja häiriöihin

1. Perusasiat ja ennakoiva varautuminen

- **Kriittisten tietojen ja järjestelmien tunnistaminen:** Kunnan tulee kartoittaa, mitkä tiedot ja järjestelmät ovat elintärkeitä toimintojen kannalta. Näihin kuuluvat esimerkiksi HR-järjestelmät, päiväkotien tietojärjestelmät ja kunnan verkkosivut.
- **Dokumentointi:** Kaikkien tietojen, prosessien ja järjestelmien tulee olla dokumentoituja. Tämä sisältää tiedot siitä, mitä tietoa käsitellään, missä sitä säilytetään ja miksi.
- **Koulutus ja tietoisuuden lisääminen:** Henkilöstön jatkuva koulutus ja kyky tunnistaa kyberhyökkäykset, tietomurrot ja muut häiriöt. Harjoituksia tulee järjestää säännöllisesti, jotta henkilöstö osaa toimia kriisitilanteessa.
- **Riskianalyysi ja suunnittelu:** Jokainen kunnan järjestelmä tulee analysoida riskien varalta ja arvioida, miten kriittiset palvelut voidaan pitää toiminnassa esimerkiksi sähkökatkon tai hyökkäyksen aikana.

2. Tekninen varautuminen ja toimenpiteet

- **Monivaiheinen tunnistautuminen (MFA):** Tämä on tärkeää kaikille kriittisille järjestelmille.
- **Vara- ja hajautusjärjestelmät:** Pilvipohjaiset ja hajautetut järjestelmät voivat parantaa kestävyyttä hyökkäyksiä vastaan.
- **Valvontajärjestelmät ja lokitiedot:** Järjestelmien käytön ja poikkeamien seuraaminen on tärkeää. On varmistettava, ettei lokitiedot ylikirjoitu poikkeustilanteessa.
- **Automaattiset reaktiot:** Automaattiset mekanismit, kuten tunnusten resetointi ja istuntojen sulkeminen, voivat estää hyökkäyksen leviämisen.

- **3. Harjoittelu ja prosessien kehittäminen**
- **Poikkeamaryhmät ja vastuut:** Jokaisella henkilöllä tulee olla selkeä rooli kriisitilanteessa. Vastuuhenkilöiden tulee olla tavoitettavissa ja tietoisia omista tehtävistään.
- **Säännölliset harjoitukset:** Harjoitusten avulla voidaan tunnistaa heikkoudet prosesseissa ja testata esimerkiksi varajärjestelmien toimivuutta.
- **Yhteistyö ulkoisten tahojen kanssa:** Palveluntarjoajien, viranomaisten ja mahdollisten kumppaneiden kanssa sovitut toimintatavat ovat elintärkeitä kriisitilanteissa.
- **4. Viestintä ja maineenhallinta**
- **Avoin ja oikea-aikainen tiedottaminen:** Viestinnän tulee olla selkeää ja suunnitelmallista. Viestintästrategiassa tulee huomioida niin sisäiset kuin ulkoiset sidosryhmät.
- **Kriisiviestinnän rooli:** Kriisiviestintä auttaa hallitsemaan tilannetta, estää huhujen leviämisen ja ylläpitää luottamusta kuntalaisiin sekä yhteistyökumppaneihin.
- **Sidosryhmien informointi:** Viranomaiset (esim. poliisi ja Kyberturvallisuuskeskus) ja kuntalaiset tulee pitää ajan tasalla.

- **5. Palautuminen kriisitilanteesta**
- **Tilannekuvan muodostaminen:** Ensimmäinen askel kriisin jälkeen on selkeän tilannekuvan luominen: mitä tapahtui, miten, ja mitä vaikutuksia sillä oli.
- **Jatkuvuussuunnittelu ja kehitys:** Palautumisen yhteydessä tulee varmistaa, että vastaavaa hyökkäystä ei voi tapahtua uudelleen. Samalla järjestelmien kestävyyttä ja prosesseja kehitetään.
- **Dokumentointi ja analyysi:** Kaikki kriisin aikana tehdyt toimenpiteet ja havainnot tulee dokumentoida myöhempää analyysia varten.
- **6. Konkreettiset vinkit pienille organisaatioille**
- **Yhteiset toimintamallit:** Selkeät valtakunnalliset mallit ja ohjeet, joita jokainen organisaatio voi käyttää.
- **Ulkoisen avun hyödyntäminen:** Jos omat resurssit eivät riitä, on tärkeää turvautua ulkopuoliseen apuun, esimerkiksi konsultteihin tai palveluntarjoajiin.
- **Tietoturvakulttuurin luominen:** Organisaation kulttuuri, jossa tietoturva nähdään kaikkien vastuuna, vähentää merkittävästi riskejä.
- **Lopuksi:** Tyrskylän kaltaisessa kunnassa, jossa yhdistyvät pienet resurssit ja moninaiset haasteet, on tärkeää panostaa varautumiseen ja jatkuvaan kehittämiseen. Näillä toimenpiteillä voidaan merkittävästi parantaa kunnan valmiuksia kohdata kyberuhkia ja palautua niistä tehokkaasti.

Palautuminen normaaliin kyberhyökkäyksen jälkeen

1. **Ennakointi ja valmistautuminen:**
   - Kartoitus: Tunnistakaa organisaationne kriittiset tiedot, järjestelmät ja infrastruktuuri.
   - Dokumentointi: Kirjatkaa tarkasti, mitä tietoja on olemassa, missä niitä säilytetään ja miksi.
   - Harjoittelu: Järjestäkää säännöllisesti teknisiä ja toiminnallisia harjoituksia, joissa testataan kyvykkyyksiä ja toimintamalleja.
   - Varmistukset: Tarkistakaa, että varmuuskopioiden tallennus ja palautus toimivat, ja testatkaa niitä säännöllisesti.
2. **Ensitoimet häiriötilanteessa:**
   - Tilannekuvan muodostaminen: Kerätkää nopeasti tietoa siitä, mitä on tapahtunut, jotta voitte tehdä tarkkoja päätöksiä.
   - Lokitietojen säilyttäminen: Älkää ylikirjoittako lokitietoja ja varmistakaa, että tallennettu data on käyttökelpoista tutkimusta varten.
   - Toimintojen eristäminen: Katkaiskaa verkkoyhteydet ja minimoikaa vahingot samalla, kun säilytätte mahdollisimman paljon todistusaineistoa.
3. **Tekninen tutkinta ja analyysi:**
   - Resurssien kohdentaminen: Varmistakaa, että teknisillä tutkijoilla on riittävästi aineistoa ja työkaluja analyysin suorittamiseen.
   - Playbookit ja prosessit: Hyödyntäkää valmiita toimintamalleja ja työkaluja nopeuttaaksenne analyysiä ja ehkäistäksenne inhimillisiä virheitä.
   - Yhteistyö ulkoisten tahojen kanssa: Tarvittaessa kutsukaa ulkopuolinen asiantuntija avuksi.

1. **Viestintä ja tiedottaminen:**
    - Selkeys: Viestikää tilanteesta ajoissa ja selkeästi, mutta älkää spekuloiko. Tiedottakaa seuraavan päivityksen ajankohta.
    - Kohderyhmän huomioiminen: Muokatkaa viestintänne sidosryhmien (esim. henkilöstö, kuntalaiset) osaamistasolle sopivaksi.
    - Maineenhallinta: Varmistakaa, että organisaationne luottamus pysyy korkealla avoimen ja vastuullisen viestinnän kautta.
2. **Palautuminen ja oppien hyödyntäminen:**
    - Dokumentointi: Kirjatkaa kaikki tehdyt toimenpiteet ja havainnot kriisitilanteen aikana.
    - Lessons learned: Järjestäkää tilaisuuksia, joissa analysoidaan, mitä tapahtui ja mitä voitaisiin tehdä paremmin tulevaisuudessa.
    - Kehitys: Päivittäkää varautumissuunnitelmat ja prosessit havaintojen perusteella.
3. **Strateginen oppiminen ja pitkäjänteinen kehitys:**
    - Teknologian päivittäminen: Hyödyntäkää uusia teknologioita, kuten tekoälyä, erityisesti lokien analysoinnissa ja valvonnassa.
    - Riskienhallinta: Ottakaa oppia muista organisaatioista ja kehittäkää organisaationne valmiuksia ennakoivasti.
    - Jatkuvuussuunnittelu: Laajentakaa suunnitelmia kattamaan monipuolisesti erilaisia häiriö- ja uhkatilanteita.

- **Tärkein oppi:** Panostamalla ennakointiin ja järjestelmälliseen varautumiseen sekä oppimalla jokaisesta tilanteesta voidaan merkittävästi parantaa organisaation kykyä toimia häiriö- ja kriisitilanteissa.

Yhteenveto: Tietosuoja ja kriisinhallinta Ennakointi ja varautuminen

1. **Tietojen ja järjestelmien hallinta:**
   - Dokumentoi mitä tietoja on, missä ja miksi.
   - Tee asset management: selvitä käytössä olevat järjestelmät, niiden kriittisyys ja toimivuus hätätilanteissa.
   - Harjoittele varamenettelyt ja pidä yllä toimivat varajärjestelmät.
2. **Sopimukset ja resurssit:**
   - Huolehdi henkilötietojen käsittelysopimuksista ja määritä selkeät SLA-aikataulut.
   - Varaudu riittävin resurssein ylläpitoon ja kriisinhallintaan.
3. **Testaus ja harjoittelu:**
   - Testaa tietoturvaa, kuten haavoittuvuuksien skannausta ja varmuuskopioiden toimivuutta.
   - Harjoitukset paljastavat prosessien pullonkaulat ja parantavat toimintaa.
4. **Tietoturvaratkaisut:**
   - Suosi pilvinatiiveja ratkaisuja, mutta arvioi niiden kustannukset ja tietoturvamekanismit.
   - Segmentoi verkot ja järjestelmät.

Toiminta kriisitilanteessa

1. **Tilannekuvan hallinta:**
   - Kerää tilannekuva nopeasti ja jaa se kaikille osallisille.
   - Pidä lokit ja järjestelmät päällä, mutta katkaise verkkoyhteydet. Älä sotke forensiikkaa.
2. **Viestintä:**
   - Luo selkeät tiedotuskanavat sisäisesti ja ulkoisesti, esim. sosiaalinen media tai riippumattomat kanavat.
   - Ole avoin kuntalaisille ja kerro milloin lisätietoja on saatavilla.
   - Viesti ymmärrettävästi, huomioi ikä ja taitotasot.
3. **Johtaminen ja vastuut:**
   - Jaa roolit ja vastuut selkeästi. Varmista sijaisuudet.
   - Pidä johdon tiedossa, mitä tehdä ja missä järjestyksessä.
   - Nimeä kriisiviestinnän vastuuhenkilö ja anna tietohallintojohtajan tiedottaa sidosryhmiä.
4. **Priorisointi:**
   - Keskity kriittisimpiin toimenpiteisiin ja kerää täydellisempi tilannekuva ennen lopullisia päätöksiä.
   - Varmista, että kaikki eivät toimi samojen tehtävien parissa.

Jälkitoimet

1. **Dokumentointi ja oppiminen:**
   - Tallenna, mitä tehtiin ja milloin. Analysoi, mitä opittiin ja mitä parannettavaa löytyy.
   - Järjestä lessons learned -tilaisuuksia.
2. **Budjetointi ja resurssit:**
   - Käytä dokumentaatiota budjetin suunnitteluun ja resurssien kohdentamiseen.
3. **Lokien ja tietojen hallinta:**
   - Varmista lokitiedon säilyvyys ja testaa niiden toimivuus.
   - Selvitä pilvipalvelujen lokien hallintaan liittyvät rajoitteet.

- *Huomioitavaa:*
- Älä paniikoi – rauhallinen analyysi on avain.
- Tekoäly voi olla hyödyllinen (tukiäly) työkalu, mutta se ei korvaa kriittistä ajattelua.
- Varmista organisaatiokulttuuri, joka tukee ongelmatilanteiden ratkaisua.
- Käsittele kriisitilanteita suunnitelmallisesti ja pidä organisaationne toimintakykyisenä myös paineen alla.
- **Muista: "Älähän häthäile!"**

DIGI- JA VÄESTÖTIETOVIRASTO

dvv.fi