TRAFICOM
Kyberturvallisuuskeskus

Kyberhygieniaopas

Kuinka pitää huolta kyberturvallisuudesta?

Sisältö

1 Johdanto

Poliittiset vaikuttajat ovat monia tahoja kiinnostava kohde – myös verkkorikollisia.

Poliittisiin vaikuttajiin kohdistetuilla kyberrikoksilla on mahdollista saada laajaa näkyvyyttä. Esimerkkejä tällaisista tietotekniikan avulla tehdyistä rikoksista voivat olla esimerkiksi vandalismi, palvelunestohyökkäykset, tietojenkalastelu, identiteettivarkaus jne. Poliitikkoihin voidaan kohdentaa myös erilaista mielipide- ja informaatiovaikuttamista sekä suoranaista vakoilua. Lisäksi on hyvä muistaa, että poliittisessa toiminnassa mukana olevat henkilöt ja organisaatiot – myös puolueet henkilöstöineen – ovat myös muiden kansalaisten ja organisaatioiden tavoin tavanomaisen kyberrikollisuuden kohteina.

Jokaisen politiikassa ja yhteiskunnallisessa päätöksenteossa mukana olevan henkilön ja organisaation on hyvä tiedostaa tietoturvan merkitys verkkorikollisuudelta suojautumiseksi. *Kyberhygienialla* tarkoitetaan hyviä tietoturvallisuuteen liittyviä käytäntöjä, joilla voi suojautua kyberuhkia vastaan. Tämä pätee sekä yksittäisten henkilöiden että organisaation tietojen suojaamiseen. Tietoturvasta huolehteminen on myös yksi keskeinen tekijä luottamuksen rakentamisessa. Tietoturvan laiminlyönti tarjoaa vihamielisille tahoille helpon pääsyn sekä sinun tietoihisi että niihin tietoihin, joihin sinulla on pääsy tai joita muut ovat sinulle jakaneet.

Tässä oppaassa käsitellään vain keskeisimmät hyviksi todetut kyberhygieniakäytännöt. Se on laadittu puolueille käytettäväksi vaalien alla – ja muutenkin.

Oppaassa käsitellään yksityishenkilön varautumista koskevia asioita kappaleessa kaksi ja organisaation näkökulmaa kappaleessa kolme. Kappale neljä koskee sekä yksityishenkilöitä että organisaatioita. Kappaleiden 2–4 alusta löydät lyhyen koosteen keskeisistä asioista, jotka sinun on ainakin hyvä huomioida, minkä jälkeen teemat avataan tarkemmin. Viimeisessä kappaleessa neuvotaan vielä miten toimia, mikäli kohtaat tietoturvaloukkauksen.

2 Yksityishenkilölle

Tietosi ovat kultaa, suojaa niitä siis yhtä hyvin kuin passiasi tai luottokorttiasi.

Tietokoneiden, -järjestelmien ja sosiaalisen median tilejä on lähes kaikilla. Usein käytön helppous ajaa turvallisuuden edelle, mikä on ymmärrettävää. Tietojen menettämisestä voi kuitenkin aiheutua paljon merkittävääkin haittaa, tai ainakin kiusallisia tilanteita ja kuluja. Yksinkertaisilla menetelmillä voit parantaa turvallista internetin ja internetiin kytköksissä olevien palveluiden käyttöä. Samalla suojaat itsesi ja tietosi.

Huolehdi ainakin näistä:

1. **Salasanat**, riittävän pitkä ja monimutkainen. Käytä yhtä salasanaa vain yhdessä palvelussa. Jos salasanojen muistaminen eri palveluihin tuntuu haastavalta, voit ottaa käyttöösi jonkin salasanojen hallintaohjelman. Voit kysyä lisätietoa salasanan hallintaohjelmista ja niiden käytöstä omasta organisaatiostasi.

2. **Mieti mitä klikkaat.** Sähköpostin liitetiedostot voivat sisältää haittaohjelmia tai haitallisia linkkejä. Haitallisia linkkejä voi olla myös sosiaalisessa mediassa tai tavallisilla internet-sivustoilla, ja niitä on levitetty myös tekstiviesteillä. Lisäksi erilaisia ponnahdusikkunoita voidaan käyttää siihen, että sinut huijataan lataamaan tietokoneellesi tai mobiililaitteeseesi haittaohjelma. Jos et ole varma viestin lähettäjästä tai sen sisällöstä, varmista asia soittamalla lähettäjälle. Jos epäilet linkin aitoutta, älä klikkaa.

3. **Varo huijauksia.** Jos jokin kuulostaa liian hyvältä ollakseen totta, se on todennäköisesti huijaus. Yksikään vastuullinen taho ei kysy esimerkiksi salasanojasi tai pankkitunnuksiasi puhelimitse tai sähköpostilla. Terve varovaisuus on siis hyvästä.

4. **Tee tunnustesi ja tiliesi varastamisesta vaikeampaa.** Ota kaksi- tai monivaiheinen tunnistautuminen käyttöön sähköpostissasi ja sosiaalisen median tileissäsi. Ne antavat merkittävää lisäsuojaa luvattomalta tunkeutumiselta. Selvitä myös, miten saat palautettua tilit itsellesi, jos ne onnistutaan varastamaan varotoimenpiteistä huolimatta. Kysy asiasta lisää organisaatiosi IT-henkilöiltä.

5. **Ilmoita havainnoistasi.** Kerro välittömästi organisaatiosi IT-henkilöstölle, jos koneesi tai mobiililaitteesi käyttäytyy omituisesti. Ilmoita myös välittömästi, mikäli olet epähuomiossa klikannut epäilyttävää linkkiä tai antanut käyttäjätunnuksesi ja salasanasi palveluun, jonka luotettavuutta alat epäillä. Suojaat samalla muita järjestelmän käyttäjiä organisaatiossasi. Mitä nopeammin ilmoitat, sitä paremmin mahdollisia vahinkoja saadaan rajoitettua.

Muista, että voit aina olla avun ja lisätiedon saamiseksi yhteydessä Kyberturvallisuuskeskukseen sähköpostitse cert@traficom.fi . Kyberturvallisuuskeskus käsittelee kaikkia tietojasi ehdottoman luottamuksellisesti. Muista myös tehdä rikosilmoitus!

2.1 Salasanat

Salasana toimii avaimena henkilökohtaisiin tileihisi. Hyvä salasana on helposti muistettava, vaikeasti ulkopuolisten arvattava ja riittävän pitkä. Hyviä esimerkkejä salasanoista voit käydä katsomassa Kyberturvallisuuskeskuksen Pidempi parempi -kampanjasivuilta[1]. Huomioithan, että kampanjasivuilla nostetaan esiin hyviä esimerkkejä, mutta salasanakoneen avulla tuotetut salasanat eivät itsessään ole suositeltavia salasanoja, mutta auttavat hyvin alkuun.

Muistathan myös, että jokaiseen palveluun tulee käyttää eri salasanaa. Palveluita on nykyään niin monia, että kaikkien käyttäjätunnus-salasanaparien muistaminen on todella vaikeaa. Siksi suosittelemme käyttämään salasanojen hallintaohjelmaa, joista esimerkkejä on listattu esimerkiksi tähän artikkeliin[2]. Tällöin joudut muistamaan vain yhden hyvän salasanan salasananhallintaohjelmaan, jonka takana ovat kaikkien käyttämiesi palveluiden salasanat käyttäjätunnuksineen. Voit kysyä organisaatiosi riskienhallinnalta, mikä niistä sopii parhaiten organisaatiosi käyttöön.

2.2 Henkilökohtaiset tilit

Sähköposti, Facebook, Twitter, Instagram, LinkedIn, vast.

Julkisten ja työhön liittyvien tilien lisäksi monilla on myös henkilökohtaisia tilejä. Niiden tietoturvallisuudesta kannattaa huolehtia yhtä lailla, erityisesti jos julkinen ja yksityinen profiili on yhdistetty. Yksityisen tilin kohdalla on hyvä miettiä, onko kaikkien ihmisten tarpeellista nähdä myös tämän tilin toiminta, vai olisiko näkyvyyttä ja pääsyoikeuksia hyvä rajata.

Twitter[3]- ja Facebook[4]-tilien suojaamisesta on kirjoitettu aika ajoin. Suositukset kannattaa huomioida ja pohtia, onko helppokäyttöisyys tärkeämpää kuin se, että tietosi ovat turvassa.

Julkisia sosiaalisen median tilejä voidaan myös hyödyntää lähteenä tiedonkeruussa. On tervettä pohtia, millaisia asioita kannattaa laittaa helposti saataville. Esimerkiksi tilapäivitys siitä, että et ole kotona, voi kasvattaa riskiä kotiisi murtautumisesta. Erityisen helpoksi sen tekee myös kotiosoitteen ilmoittaminen profiilitiedoissa.

Avoimista lähteistä tehtävää tiedonkeruuta hyödynnetään monenlaisiin tarkoituksiin. Paikkatietojen avulla tiedetään poissaolojesi lisäksi myös se, missä liikut. Vaikka et olisi ilmoittanut tarkkaa paikkatietoa, mutta olet laittanut julkaisuun kuvan, taustalla olevista maamerkeistä voi päätellä paljon.

Kun on tiedossa, minkälaisista asioista olet kiinnostunut, voi sinulle lähettää kohdennettuja sähköposteja. Näiden avulla sinut todennäköisesti saadaan joko avaamaan liitteenä oleva haitallista sisältöä sisältävä

[1] https://pidempiparempi.fi/
[2] https://kuluttaja.fi/testit/salasanaohjelmat/
[3] https://nakedsecurity.sophos.com/2018/12/29/how-to-secure-your-twitter-account/
[4] https://nakedsecurity.sophos.com/2018/12/28/how-to-protect-your-facebook-account-a-walkthrough/

dokumentti tai klikkaamaan viestissä olevaa linkkiä. Tämä altistaa sinut ja tietokoneesi haittaohjelmille ja tietojenkalastelulle.

Muista, että henkilökohtaisen tilin tietojen päätyminen vääriin käsiin voi vaikuttaa myös läheisiisi ja muihin kontakteihisi. Väärissä käsissä tiliäsi voidaan hyödyntää myös muiden ihmisten huijaamiseen.

2.3 Julkiset profiilit

Moni tarvitsee työssään julkisen sosiaalisen median sivun tai profiilin. Tili kannattaa kuitenkin suojata yhtä hyvin kuin henkilökohtaiset tilit. Ota käyttöösi kaksivaiheinen tunnistautuminen sähköpostiisi ja sosiaalisen median tileihisi.

Kaksivaiheinen tunnistautuminen tarkoittaa sitä, että käyttäjätunnuksen ja salasanan lisäksi palvelu kysyy kertakäyttöistä koodia tai muuta avainta päästäksesi käsiksi omiin tileihisi. Kertakäyttöinen koodi voi tulla joko palveluun yhdistettyyn sovellukseen, tekstiviestillä tai sähköpostitse. Mikäli saat koodin puhelimeesi vaikka et itse ole kirjautumassa palveluun, joku toinen todennäköisesti yrittää päästä luvattomasti käsiksi tiliisi. Tällöin kannattaa vaihtaa salasana palveluun (älä klikkaa mahdollisesti sähköpostissa olevaa linkkiä, vaan mene palvelun verkkosivustolle verkkoselaimen kautta tai vaihda salasana sovelluksessa). Ilmoita asiasta myös organisaatiosi riskienhallintaan. On hyvä tiedostaa myös, ettei kaksi- tai monivaiheinen tunnistautuminen takaa täydellistä suojaa, mutta se estää yleensä satunnaiset yritykset.

2.4 Pilvipalvelut

Microsoft Office 365, DropBox, One Drive, Google cloud, Amazon – mieti mitä laitat pilveen.

Pilvipalvelut helpottavat arkea, kun kaikki tarvittava tieto on saatavilla melkein mistä tahansa ja tietoon on pääsy useilla laitteilla. Moni pilvipalvelun tarjoaja kiinnittää erityistä huomiota palveluidensa tietoturvallisuuteen, mutta iso datamassa keskitetyssä paikassa kiinnostaa myös rikollisia. Siksi arkaluonteisen materiaalin tallentamista pilvipalveluihin kannattaa harkita, ja siitä kannattaa yhdessä esimerkiksi organisaation riskienhallinnan kanssa tehdä riskiarvio.

Erilaiset pilvipalvelut ovat myös riippuvaisia käyttäjän taidoista asettaa käyttörajoituksia tiedolle. Ne kannattaa katsoa tarkkaan läpi, etteivät ulkopuoliset pääse epähuomiossa käsiksi palveluun tallennettuun sisältöön.[5]

5 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvavinkkeja_henkilokohtaisten_pilvitallennuslaitteiden_turvallisempaan_kayttoon.pdf

2.5 Social engineering

"Social engineering" tarkoittaa sitä, että ihmistä huijataan tai harhautetaan auttamaan rikollista esimerkiksi luovuttamalla tietoja. . Rikolliset käyttävät tätä hyväkseen, sillä ihmiset ovat usein melko hyväuskoisia. On paljon helpompaa ja halvempaa tehdä sähköpostitse välitettävä lasku, jonka avaamiseksi pyydetään käyttäjätunnus-salasanaparia ja lähettää se kohdeorganisaatioon, kuin yrittää murtautua järjestelmään arvaamalla salasanoja. Tietojärjestelmissä sellaisten tietojen väärentäminen, johon olemme tottuneet luottamaan tai joita emme aina muista kyseenalaistaa, on helppoa. Esimerkiksi huijaussivusto saattaa näyttää oikean sivuston kanssa täysin identtiseltä, mutta osoiterivi yleensä paljastaa sen olevan huijaus. Samoin tuttu lähettäjän sähköpostiosoite saattaa olla väärennetty. Näiden keinojen avulla ihmisille uskotellaan sivuston tai sähköpostin olevan luotettava, jolloin on todennäköisempää, että käyttäjä luovuttaa käyttäjätunnuksensa ja salasanansa.

Mikäli saat epätyypillisen viestin tutulta lähettäjältä, voit soittaa hänelle ja kysyä asiasta ennen viestin tai liitetiedoston avaamista. Viime aikoina on nähty myös hyvällä suomenkielellä tehtyjä sähköpostiviestejä, joissa ohjataan avaamaan esimerkiksi tutun lähettäjän SharePoint-linkin takaa löytyvä liite. Linkkiä klikatessa vastaanottaja ohjataan antamaan käyttäjätunnus-salasanaparinsa dokumentin avaamiseksi. Tämä on kuitenkin huijaus. Älä anna käyttäjätunnuksiasi, vaan ilmoita viestistä sekä lähettävälle taholle että oman organisaatiosi tietoturvasta vastaaville ihmisille.

Muita esimerkkejä huijauksista, joissa hyödynnetään luontaista auttamishaluamme tai luottamustamme, ovat esimerkiksi salasanan tai muiden kriittisten tietojen luovuttaminen rikollisille puhelimitse, kutsumattomien vieraiden päästäminen suljettuihin tiloihin pyydettäessä tai tietojen paljastaminen rikollisille sellaisista asioista, että tietoja voidaan hyödyntää muiden rikollisten tarkoitusperien toteuttamisessa.

3 Organisaatioille

Organisaatioiden suurimpia riskejä ovat mainehaitta ja luottamuksen menetys. Vaalien alla on useissa maissa esimerkiksi murtauduttu tietojärjestelmiin ja varastettu sieltä tietoja, joita on pyritty esimerkiksi levittämään sopivalla hetkellä medialle maineen menettämisen tai skandaalin aiheuttamisen toivossa. Joissain tapauksissa järjestelmään murtautumisen syynä on myös ollut tiedon muokkaaminen ja väärennetyn tiedon levittäminen.

Huolehdi ainakin näistä:

1. **Edellytä kaikilta organisaatiosi käyttäjiltä** riittävän pitkiä ja monimutkaisia salasanoja. Ohjeista käyttäjiä hyvistä salasanakäytännöistä.

2. **Kouluta ja opasta organisaatiosi käyttäjiä toimimaan turvallisesti.** Hyödynnettäviä ohjeita ja oppaita mm. internetin ja sähköpostin turvalliseen käyttöön löydät esimerkiksi Kyberturvallisuuskeskuksen verkkosivuilta.

3. **Edellytä** kaikilta organisaatiosi käyttäjiltä kaksi- tai monivaiheista tunnistautumista.

4. **Muista huolehtia päivityksistä.** Päivitykset suojaavat järjestelmiäsi, kun niistä on löytynyt haavoittuvuuksia. Haavoittuvuuksia hyödyntämällä hyökkääjä voi tunkeutua organisaatiosi järjestelmiin.

5. **Ennakoi sopimalla.** Organisaation on hyvä huolehtia siitä, että palveluntarjoajan kanssa on sovittu myös häiriötilanteiden hallinnasta ja niistä palautumisesta.

6. **Varmuuskopioi.** Muista ottaa säännöllisesti varmuuskopioita tiedostoista. Mikäli tietokoneesi hajoaa, kiristys- tai muu haittaohjelma lukitsee tiedostosi tai ne korruptoituvat, voit aina palauttaa varmuuskopioidut versiot.

Muista, että voit aina olla avun ja lisätiedon saamiseksi yhteydessä **Kyberturvallisuuskeskukseen sähköpostitse cert@traficom.fi . Kyberturvallisuuskeskus käsittelee saamiaan tietoja ehdottoman luottamuksellisesti. Muista myös tehdä rikosilmoitus!**

3.1 Organisaation käytössä olevat tietojärjestelmät

Verkkosivuilta ja julkaisualustoista löydetään usein haavoittuvuuksia, minkä vuoksi ne ovat yleisiä tietomurron kohteita. Kyberturvallisuuskeskus suosittelee esimerkiksi automaattisten päivitysten ottamista käyttöön

julkaisualustoilla. Kyberturvallisuuskeskus on myös julkaissut ohjeen sisällönhallintajärjestelmien kyberuhkien torjunnasta[6].

Erilaiset rekisterit ja verkkosivustot ovat hakkereille mielenkiintoisia kohteita. Moni loppukäyttäjä ei juuri pysty vaikuttamaan palveluiden suojaukseen, minkä takia ylläpitosopimuksiin kannattaa kiinnittää huomiota.

Huolehdi siitä, että häiriönhallintaprosessi on mietitty ja perehdytetty – kuka on vastuussa, kenellä on oikeus pyytää palveluntarjoajalta lisäpalveluita palveluiden palauttamiseksi ym. Onhan myös palveluehdoissa määritelty, kuinka pian palvelun pitää häiriötilanteen jälkeen palautua toimintakuntoiseksi? Vaikka tiedot eivät olisi vaarassa, voi pelkkä palvelun tai julkisen verkkosivun saavuttamattomuus aiheuttaa mainehaittaa.

3.2 Organisaation käytössä olevat yhteiset tilit

Kaksi- tai monivaiheinen tunnistautuminen kannattaa ottaa käyttöön myös organisaatioiden tileillä tai muilla sellaisilla tileillä, jonne tilapäivityksiä tekee useampi kuin yksi ihminen. Tällöin kaksivaiheisen tunnistautumisen varmennuskoodi kannattaa tilata sellaiseen paikkaan, mistä siihen pääsevät käsiksi kaikki sitä tarvitsevat ihmiset. Kannattaa myös huomioida, että useampaa kuin yhtä puhelinnumeroa tai sähköpostiosoitetta ei yleensä pysty rekisteröimään palveluun.

Yhteiskäyttöisten tilien salasanoista on huolehdittava yhtä tarkasti kuin henkilökohtaisista käyttäjätunnuksista. Vaikka on helppoa napata salasana teipillä pöytään kiinnitetystä paperilapusta, sen voi lukea kuka tahansa muukin. Tässä on hyvä huomioida myös tilaturvallisuus, eli kenellä on pääsy tiloihin, huoneeseen, tietokoneelle tai näkeekö työpisteelle ikkunasta.

3.3 Riskienhallinta

Riskienhallinnan tai turvallisuustoimintojen tehtäväkenttä on laaja. Yksi merkittävistä tehtävistä on organisaation henkilöstön kouluttaminen ja tietoisuuden lisääminen turvallisuusasioista. Kokonaisvaltaiseen riskienhallintaan kuuluvat olennaisesti fyysinen ja matkustusturvallisuus, maineriskien hallinta, ympäristö- ja tilaturvallisuus sekä tietoturvallisuus. Tietoturvallisuus poikkileikkaa useat edellä mainitut asiat, minkä vuoksi myös tietoturvallisuuskoulutukseen on hyvä panostaa.

Olennaisin osa riskienhallintaa on käyttäjien koulutus hyvistä käytännöistä, käytettävistä ohjelmistoista sekä hyvistä tiedonhallintatavoista. Onko kaikkien organisaation jäsenten tarpeen päästä kaikkeen organisaatiossa käsiteltävään tietoon? Entä miten eri ohjelmistoja ja salasanoja käytetään? Lukitaanko tietokoneet ja kännykät silloin, kun niiden ääressä ei olla?

Riskienhallinnan voi myös olla tarpeen linjata, millaisia sovelluksia käytetään ja minkälaisen tiedon viestimiseen. Jotkut henkilökohtaisten

6 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Sisallonhallintajarjestelmien_kyberuhkia.pdf

asioiden hoitamiseen soveltuvat ohjelmistot saattavat kierrättää liikenteen jonkun muun maan kautta, jossa esimerkiksi EU:n tietosuoja-asetuksia ei noudateta, jolloin arkaluontoinen materiaali saattaisi joutua vääriin käsiin.

Myös organisaatiosta saatavien laitteiden käyttöpolitiikka suhteessa henkilökohtaisiin laitteisiin kannattaa määritellä. Organisaation valvonnassa olevat laitteet voivat olla turvallisempia, ja niissä voi olla asennusrajoituksia. Myös erilaisten kannettavien laitteiden, kuten kameroiden, USB-tikkujen ja kännyköiden liittämistä organisaation laitteisiin kannattaa miettiä, sillä niistä saattaa siirtyä myös haittaohjelmia.

Kyberturvallisuuteen sisältyy myös fyysinen turvallisuus eli se, ettei ulkopuolisilla ihmisillä ole pääsyä tietokoneisiin, mobiililaitteisiin tai toimitiloihin, sillä myös sitä kautta pystyy loukkaamaan tietoturvallisuutta. Fyysinen turvallisuus kannattaa huomioida erityisesti paikoissa, joissa on organisaation ulkopuolisia henkilöitä paikalla. Edes lukittavat tilat, kuten hotellihuoneet, eivät aina suojaa tunkeutumiselta.

3.4 Matkustusturvallisuus

Matkustusturvallisuus liittyy olennaisesti myös kannettaviin tietokoneisiin ja mobiililaitteisiin. Erilaisten USB-tikkujen ja muiden muistilaitteiden kautta voidaan ujuttaa haittaohjelmia laitteisiin, tai kopioida valvomatta jätetystä laitteista tiedostoja. Vastaavia tapauksia on maailmalla sattunut myös lukituissa hotellihuoneissa.

Hotellien ja julkisten paikkojen langattomat internetyhteydet (WLAN-verkot) voivat aiheuttaa tietoturvariskejä. Avoimia langattomia verkkoja on helppo salakuunnella[7], ja erilaiset väliintulohyökkäykset[8] paljastavat käyttäjän internetselailun hyökkääjälle.

3.5 Tietojärjestelmien ja nettisivujen ylläpito

Ylläpito voi olla joko oman organisaation vastuulla, tai se voi olla ulkoistettu. Kummassakin tapauksessa on tärkeää varmistua siitä, että organisaatiossa tiedetään millaisia ohjelmistoja on käytössä, onko niihin julkaistu tunnettuja haavoittuvuuksia ja saako niihin päivityksiä. Automaattiset päivitykset kannattaa huolehtia ajettavaksi kaikkiin organisaation laitteisiin.

Häiriöiden hoitaminen ja niistä palautuminen on hyvä varmistaa. Häiriöiden selvittämisessä myös lokitus[9] on keskeisessä asemassa. Palveluntarjoajan ja ylläpitäjien kanssa on hyvä määritellä sopimustasolla siitä, miten häiriötilanteet ilmoitetaan organisaation vastuutahoille, miten ja kuka niitä hoitaa, ja mikä on palvelun palautumisen vastuuaika. Lokien osalta

---

7 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

8 https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/10/ttn201710161625.html

9 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf

kannattaa myös varmistaa keillä niihin on pääsy, miten niiden tutkiminen ja analyysi hoidetaan, ja millä vasteajalla.

Kyberturvallisuuskeskuksen päivystäjä auttaa mielellään häiriötilanteissa. Apua saa esimerkiksi lähettämällä tilannekuvauksen osoitteeseen cert@traficom.fi. On hyvä pohtia, onko organisaatiolla teknistä osaamista vai hoitaako ylläpidon joku ulkoistettu taho. Myös nämä asiat kannattaa kertoa Kyberturvallisuuskeskukselle, jotta häiriötilannetta päästään selvittämään mahdollisimman nopeasti.

Kyberturvallisuuskeskus kohtelee jokaista asiakasyhteydenottoa ehdottoman luottamuksellisesti eikä kerro tapauksista ulkopuolisille. Suosittelemme myös tekemään rikosilmoituksen. Mikäli organisaatiolle sopii, Kyberturvallisuuskeskus voi auttaa poliisia tapauksen selvittämisessä. Organisaation on hyvä tuoda myös tämä ilmi sähköpostissa.

4 Kohdistetut hyökkäykset eli kybervakoilu

Nykyorganisaatioissa lähes kaikki tietojen käsittely ja välitys on sähköistä. Tietoverkkojen hyödyntäminen tekee työskentelystä joustavaa ja tehokasta paikkariippumattomuuden sekä suurten tietomäärien käsittelyn avulla. Samat edut hyödyttävät myös verkkorikollisia, mikä altistaa organisaatiot uudenlaisille kyberuhille. Näistä vakavimmat ovat kybervakoilu ja kyberhyökkäykset kriittistä infrastruktuuria vastaan. Kyberhyökkäyksiä järjestelmällisesti seuraavissa länsimaissa havaitaan vuosittain kymmeniä kybervakoilutapauksia, joissa teknisenä apukeinona on käytetty kohdistettua haittaohjelmaa. Uhka kohdistuu myös suomalaisiin organisaatioihin.

Poliittiset vaikuttajat ovat monia tahoja kiinnostava kohde, joihin voidaan kohdentaa ja joita voidaan hyödyntää mielipide-, informaatio- ja hybridivaikuttamiseen. Siksi jokaisen poliittisessa kentässä toimijan on hyvä tiedostaa miten hyvästä tietoturvasta huolehtiminen ja muut hyvät tietoturvakäytännöt voivat vähentää riskiä joutua kohdennetun hyökkäyksen, ja sitä myöten kybervakoilun, kohteeksi.

Yleisimpiä kohdistettujen hyökkäysten menetelmiä ovat haitalliset sähköpostiviestit ja varastettujen käyttöoikeuksien väärinkäyttö. Käyttöoikeudet on yleensä saatu varastettua tietojenkalasteluviestien avulla.

Huomioi ainakin nämä

Käyttäjä:

1) Mikäli sähköpostissa saamasi liitetiedosto pyytää aktivoimaan lisätoimintoja tai asentamaan ohjelmia, ÄLÄ TEE SITÄ.

2) Mikäli sähköpostissa ollut linkki vie sivustolle, joka pyytää syöttämään käyttäjätunnuksen salasanoineen, ÄLÄ TEE SITÄ.

3) Epäilyttävissä tapauksissa pyydä apua tietohallinnolta ja kehota heitä olemaan yhteydessä Kyberturvallisuuskeskukseen.

Tietojärjestelmävastaava tai ylläpitäjä:

1) Muista, että käyttäjän ohjeet koskevat myös sinua.

2) Tietojärjestelmistä ja niiden käytöstä tulee kerätä kattavat lokitiedot. Lisäohjeistusta lokitietojen keräämisestä ja säilyttämisestä on saatavilla.

Taustaa kohdistetuista hyökkäyksistä

Kohdistetussa haittaohjelmahyökkäyksessä on kyse tarkasti suunnitellusta toiminnasta ja kohteen mukaan räätälöidystä haittaohjelmasta. Tunkeutujan tavoitteena on päästä käsiksi nimenomaisesti tietyn organisaation tietoihin tai järjestelmiin. Hyökkäys ei varsinaisesti kohdistu

tavallisiin internetin käyttäjiin, mutta vaikutukset voivat ulottua myös heihin.

Kohdistettujen haittaohjelmahyökkäysten kohteita ovat organisaatiot, joilla on hallussaan hyökkääjää kiinnostavaa tietoa liittyen poliittiseen päätöksentekoon, talouteen tai teknologiaan. Näihin kuuluvat julkishallinnon organisaatiot, yliopistot ja yritykset koosta riippumatta. Kiinnostuksen kohteena voivat lisäksi olla tekniset resurssit tai yhteydenpidon seuranta. Kohteeksi voi joutua myös välillisesti, jos hyökkääjä haluaa tavoittaa varsinaisen kohteensa tai tavoitteensa toisen organisaation kautta.

Haitallinen sähköpostiviesti sisältää tyypillisesti joko haitallisen liitetiedoston tai linkin haitalliselle sivustolle. Haitallinen liitetiedosto yrittää suorittaa hyökkääjän haitallista ohjelmakoodia uhrina olevan käyttäjän koneessa. Nykyään yhä useammin liitetiedosto yrittää huijata käyttäjää aktivoimaan lisätoimintoja nappia painamalla tai asentamaan muka tarpeellisen lisäosan. Näiden avulla hyökkääjä kykenee asentamaan uhrin koneelle lisää haittaohjelmia, joilla saa koneen lopullisesti haltuunsa.

Haitallisella sivustolla yritetään yleensä huijata käyttäjää syöttämään käyttöoikeutensa, eli käyttäjätunnus-salasanaparinsa, hyökkääjän hallinnoimalle sivustolle. Varastetuilla käyttöoikeuksilla kirjaudutaan myöhemmin organisaation etäkäyttöpalveluihin ja yritetään sitä kautta tunkeutua syvemmälle tietojärjestelmiin.

Tunkeutumisen ensivaiheen eli käyttäjän työaseman saastumisen estäminen on hyvin haastavaa, mutta tunkeutumisen etenemisen pysäyttäminen on täysin tehtävissä. Etenemisen pysäyttämisen edellytyksenä on tunkeutumisen havaitseminen. Havaitsemisen peruspilarina on kattava lokitietojen keruu ja seuranta.

5 Mitä teen, jos jotain tapahtuu?

Mikäli kyseessä on organisaation järjestelmissä tapahtunut tietomurto tai palvelunestotila, ota yhteyttä järjestelmien ylläpitoon. Ota myös yhteyttä Kyberturvallisuuskeskukseen. Suosittelemme tekemään rikosilmoituksen.

Mikäli kyseessä on omaan sähköposti- tai sosiaalisen median tiliin kohdistunut loukkaus, ota yhteyttä poliisiin. Kyseessä on silloin rikosasia.

Akuutin tilanteen ollessa päällä organisaatiossanne voitte ottaa yhteyttä Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen päivystäjään osoitteessa https://www.kyberturvallisuuskeskus.fi/fi/ilmoita tai lähettämällä sähköpostia osoitteeseen cert@traficom.fi. Sähköpostissa on hyvä kertoa mahdollisimman tarkkaan:

- tapauksen luonne
- teknisiä yksityiskohtia
- häiriön alkamisaika ja mahdollinen päättymisaika, sekä
- keneen päivystäjämme voi olla yhteydessä. Esimerkiksi järjestelmien ylläpitäjän tai palveluntarjoajan kanssa setvittävän asian selvittämiseen tarvitaan kummankin yhteystiedot.

5.1 Kyberturvallisuuskeskuksen julkaisemia ohjeita

Palvelunestohyökkäys
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta.pdf

Palvelunestohyökkäysten tekniikkaa puolustajille
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_liite_1_Palvelunestohyokkaysten_tekniikkaa_puolustajille.pdf

Palvelunestohyökkäyksen kohteeksi joutuneelle
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_liite_2_Toimintaohjeet_palvelunestohyokkayksen_kohteeksi_joutuneelle.pdf

Matkapuhelimen turvalliseen käyttöön
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvavinkkeja_matkapuhelimen_turvalliseen_kayttoon.pdf

Internet-sivujen sisällönhallinnan turvaamiseksi
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Sisallonhallintajarjestelmien_kyberuhkia.pdf

Kohdennettujen hyökkäysten uhka on todellinen
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf

Kaikki Kyberturvallisuuskeskuksen ohjeet
https://www.kyberturvallisuuskeskus.fi/fi/ohjeet

Yhteystiedot
PL 313
Erik Palménin aukio 1
00561 Helsinki
puh: 0295 390 100
fax: 0295 390 270
www.viestintävirasto.fi