Kohdistettujen haittaohjelma-hyökkäyksien uhka on otettava vakavasti

Viestintävirasto
Kyberturvallisuuskeskus

Sisällysluettelo

Organisaatioihin kohdistuvat haittaohjelmahyökkäykset

1 Raportin tavoite

Kohdistetut haittaohjelmahyökkäykset ovat yleistyneet viime vuosina, mikä näkyy muuan muassa tietoturvayhtiöiden lisääntyneinä haittaohjelmaraportteina [Liite 2]. Tämän raportin tarkoituksena on kohdistettuihin haittaohjelmahyökkäyksiin liittyen:

- lisätä organisaatioiden tietoisuutta
- auttaa tunnistamaan organisaatiokohtaiset riskit
- antaa tukea organisaatiolle päätöksenteossa uhilta suojautuessa

Kyberturvallisuuskeskuksen koostaman raportin tavoitteena on parantaa Suomen kyberturvallisuutta sekä yksittäisissä organisaatioissa että kansallisesti. Tämän toteutumiseksi organisaatioissa tarvitaan ymmärrystä kohdistettujen haittaohjelmien toiminnasta ja lisääntyvää toimialojen välistä yhteistyötä sekä tiedonjakoa.

Raportti on laadittu viranomaisyhteistyössä Viestintäviraston Kyberturvallisuuskeskuksen, Suojelupoliisin ja Puolustusvoimien kanssa. Lisäksi asiantuntijalausunnot raporttiin ovat antaneet tietoturvayhtiöt F-Secure, Nixu ja nSense. Kyberturvallisuuskeskus kiittää toimijoita yhteistyöstä.

2 Johdanto

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.

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.

Kybervakoilussa tavoitteena ei yleensä ole tehdä näkyviä muutoksia kohdejärjestelmissä. Hyökkääjä pyrkii pitkäaikaiseen ja huomaamattomaan läsnäoloon voidakseen seurata organisaation toimintaa ja tarvittaessa rikkoakseen kohteensa tietojen eheyttä. Tilanne on lähes sama kuin, jos ulkopuolisella olisi avaimet ja täydelliset kulkuoikeudet vieraan organisaation tiloihin läpi vuorokauden. Harva organisaatio hyväksyisi tällaista tilannetta, mistä kertovat fyysistä turvallisuutta ylläpitävät valvontakamerat, ovien lukitusjärjestelmät ja vartiointiliikkeet. Fyysisen turvallisuuden lisäksi myös organisaatioiden verkot on suojattava nykymaailman vaatimusten mukaisesti.

Kyberhyökkäykset kriittistä infrastruktuuria vastaan voivat aiheuttaa välittömiä vakavia seurauksia. Pääsy esimerkiksi vesilaitosten järjestelmiin, sähköntuotannon ohjaukseen, maksupäätteisiin tai terveydenhuollon järjestelmiin voi vaarantaa ihmishenkiä, omaisuutta ja sekoittaa yhteiskunnan toimintoja. Hyökkäysten tarkoitusperät voivat olla monet: ilkivalta, terrorismi tai kybersodankäynti. Toisaalta syiden ennalta pohtiminen on toisarvoista, sillä ensisijaista on suojata järjestelmät. Näin estetään uhkakuvien toteutuminen.

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.

Yksittäisetkin kyberhyökkäykset organisaatioihin voivat heikentää Suomen mainetta uskottavana kyberosaajana. Laajamittaisina hyökkäykset voivat aiheuttaa merkittävän uhkan Suomen turvallisuudelle. Vain kattava havainnointi, toiminta- ja reagointikyky ja niiden kehittäminen kaikentasoisiin kyberuhkiin voi vahvistaa organisaatioiden tietoturvallisuutta. Tämä vaatii jatkuvia ja aktiivisia toimenpiteitä tietoturvallisuuden edistämiseksi sekä runsasta yhteistyötä niin julkisten kuin yksityisten toimijoiden kesken.

Vinkki: Raportin lukeminen nyt voi säästää aikaa ja rahaa myöhemmin

On organisaatioita, joiden hallussa on ainoastaan julkista tietoa ja järjestelmiin on tarkoituksenmukaista ylläpitää osin avointa pääsyä. Näissäkin tapauksissa on huomioitava organisaation sidosryhmien tietojen suojaustarve. Suurin osa organisaatioiden tietojärjestelmistä kuitenkin vaatii suojausta, myös kohdistetuilta haittaohjelmahyökkäyksiltä.

OSA I

Kuinka hyökkäys alkaa ja kuinka se saavuttaa kohteensa?

1 Kohdistetulle haittaohjelmahyökkäykselle altistavat ja onnistuneen hyökkäyksen mahdollistavat tekijät

Lähes kaikilla organisaatioilla tai, yleistetysti ilmaistuna, *toimijoilla* on hallussaan tietoa, taitoa, yhteyksiä ja järjestelmiä, joista ulkopuolinen voi hyötyä. Jokaisen toimijan on itse tunnistettava omat kohteensa, joista ulkopuolinen voisi laittomalla käytöllä hyötyä. Lisäksi organisaation on hyvä tiedostaa, että hyökkäyksen voi mahdollistaa myös puutteellinen kyky havaita hyökkäykset ja käynnistää toimenpiteet, joilla havaittuun hyökkäykseen reagoidaan. Keskeisiä hyökkäykselle altistavia ja hyökkäyksen torjumisen hankaloittavia syitä ovat (kuva 1):

- kiinnostava informaatio (1)
- merkittävät yhteistyökumppanit (2)
- verkon ja järjestelmien teknisesti tarjoamat mahdollisuudet (3)
- puutteet hyökkäysten havainnointi- ja reagointikyvyssä (4)

Mitä useampi edellä mainituista hyökkäykselle altistavista (1 - 2) tai hyökkäyksen mahdollistavista (3 - 4) tekijöistä toteutuu, sitä todennäköisempää on, että organisaatio päätyy kohdistetun hyökkäyksen uhriksi. Merkittävä tieto ja puutteet tekevät kohteesta mielenkiintoisen ja motivoivat hyökkääjiä. Kokonaisuudessa hyökkäyksen vaatiman panostuksen ja siitä saatavan hyödyn suhde viimein määrittää, mitkä organisaatiot lopulta päätyvät kohdistetun haittaohjelmahyökkäyksen kohteeksi. Uhriksi voi silti päätyä, vaikka kaikkiin osa-alueisiin olisi kiinnitetty huomiota. Tällöin organisaation turvallisuusvaatimustason on oltava yleistä perustasoa korkeampi.

Kuva 1: Organisaatioon kohdistuvan haittaohjelmahyökkäyksen uhkaan vaikuttavia tekijöitä

1.1 Kiinnostuksen kohteena tiedot, taidot ja resurssit

Organisaation on tärkeää tunnistaa, mitkä sen hallussa olevista tiedoista tai verkon kautta käytettävistä järjestelmistä voivat olla ulkopuoliselle hyödyksi. Kyse voi olla teknisestä innovaatiosta, organisaation toiminnan kannalta kriittisistä tiedoista, neuvotteluihin valmistautumisesta tai jopa tietoisuus siitä, mitä tietoa organisaatiolla ei ole käytössä. Ulkopuolinen voi hyötyä myös kohteen kommunikoinnin seuraamisesta: ketkä keskustelevat, kuinka paljon ja mistä asioista, vaikka kommunikoinnin sisältö olisikin julkista. Näin voidaan selvittää esimerkiksi henkilöt, jotka pitävät toisiinsa usein yhteyttä ja siten näyttäisivät luottavan toisiinsa.

1.2 Yhteistyöverkostot ja kauttakulkureitit ovat myös arvokasta tietoa

Kaikki kiinnostava tieto ei välttämättä ole hyökkäyksen kohteen omaa. Myös organisaation hallussa olevat sidosryhmien asiakastiedot, -sopimukset ja etäyhteydet yhteiskäyttöisiin järjestelmiin tai asiakasjärjestelmien ylläpito houkuttelevat hyökkääjää. Esimerkiksi turvallisuuspoliittisen *vakoilun* kohteeksi voivat joutua yritykset, jotka suunnittelevat ja toteuttavat puolustusvoimien järjestelmiä. Tällöin kohdistetun hait-

taohjelmahyökkäyksen varsinaisena tavoitteena voi olla esimerkiksi Suomen puolustuskyvyn arvioiminen.

1.3 Teknisiä ratkaisuja on suunniteltava ja seurattava

Hyökkäyksen toteutuksen helppouteen vaikuttaa organisaation käytössä olevat ohjelmat, verkon rakenne ja sen valvonta. Hyökkääjät hyödyntävät jo olemassa olevia työkaluja, jotka on suunniteltu yleisessä käytössä olevien ohjelmistojen hyväksikäyttöä varten. Tapa on kustannustehokas ja kannattava. On muistettava, että yleisesti käytössä olevien ohjelmien vanhentuneet ja päivittämättömät versiot ovat haavoittuvia ja lisäävät siten onnistuneiden hyökkäysten riskiä.

Ensimmäiset päivät ohjelmapäivityksen julkaisun jälkeen ovat todennäköisintä aikaa, jolloin *haavoittuvuuksia* hyödynnetään. Hyökkääjän kannalta kannattavia kohteita ovat myös verkot, jotka on rakennettu niin, että yhdestä verkon haavoittuvasta yhteyspisteestä on mahdollista päästä sisään ja sen jälkeen levittäytyä hyökkääjän kannalta tarpeellisiin verkon eri laitteisiin ja järjestelmiin. Tällaisia ovat esimerkiksi etäpäivitettävät päätelaitteet ja keskitetyt tunnistautumisjärjestelmät. Jos puolestaan sisäverkko on rakennettu yksilölliseksi, hyökkääjä joutuu näkemään enemmän vaivaa rakenteen ja pääsyreittien selvittämiseksi.

1.4 Havaitsemis- ja reagointikyvyn valmiudet

Tärkeimpänä on kiinnitettävä huomiota havaitsemis- ja reagointikyvyn valmiuksiin, sillä kaikki järjestelmät sisältävät tietoturva-aukkoja ja tehokkaatkaan tekniset menetelmät eivät suojaa henkilöstön inhimillisiltä erehdyksiltä. Sen vuoksi jatkuva seuranta, toteutuneiden hyökkäysten aikainen havaitseminen ja reagointivalmiudet ovat ensiarvoisen tärkeitä suojautuessa kohdistettujen hyökkäysten aiheuttamilta vaikutuksilta.

Jo pienilläkin toimenpiteillä voidaan merkittävästi parantaa hyökkäysten ennaltaehkäisykeinoja, havainnointia ja niihin reagointia. Oleellista on luoda valmiudet havainnoida hyökkäyksiä usealla tasolla - kaikkien vaiheiden kontrollien kiertäminen on hyökkääjälle hankalaa ja lisää epäilyttävän toiminnan tunnistamisen todennäköisyyttä.

Vinkki: Kustannukset pysyvät kohtuullisina oikeilla toimenpiteillä

Perustietoturvan ajantasainen ylläpito ja henkilöstön koulutus lisää merkittävästi suojausta myös kohdistetulta hyökkäyksiltä. Suojauksen lisätarpeet on tunnistettava organisaatiokohtaisesti ja arvioitava onnistuneesta hyökkäyksestä aiheutuvien kustannusten sekä sen estämiseksi vaadittavien investointien perusteella.

2 Kohdistetun haittaohjelmahyökkäyksen toteutus

Kohdistetuilta haittaohjelmahyökkäyksiltä suojautumista edesauttaa ymmärrys hyökkäyksen toteutusvaiheista ja niissä hyödynnettävistä menetelmistä. Hyökkääjä arvioi hyökkäyksen toteutuksen ja sen vaatiman panostamisen kustannustehokkuuden, hyökkäyksen paljastumiseen liittyvien riskien ja tarvittavan *haittaohjelman* hienostuneisuuden mukaan. Hyökkäysten toteutukseen vaatiman työmäärän, teknisten menetelmien ja tietotaidon perusteella voidaan olettaa, että tekijät ovat järjestäytyneitä ryhmittymiä, jotka toteuttavat hyökkäykset organisoidusti. Hyökkäysten torjuminen vaatii vähintään vastaavaa panosta. Kuvassa 2 on kuvattu hyökkäyksen päävaiheet.

Kuva 2 Toteutuksen vaiheet

2.1 Valmistelussa kerätään tietoa organisaatiosta

Kohdistettu hyökkäys valmistellaan huolella. Kohdeorganisaatiosta voidaan kerätä merkittävä määrä hyödyllisiä tietoja pelkästään julkisia lähteitä käyttämällä. Kiinnostavia tietoja ovat sekä sosiaaliset että tekniset tiedot. Esimerkkejä on kuvattu taulukossa 1.

Taulukko 1: Esimerkkejä valmisteluvaiheessa kerättävistä tiedoista

Sosiaaliset	Tekniset
• Henkilöstön nimet • Henkilön tehtävät ja asema • Ajankohtaiset tapahtumat • Yhteistyökumppanit	• Verkon rakenne • Käytössä olevat järjestelmät • Käytössä olevat ohjelmistot ja ohjelmistoversiot • Etäyhteydet

Valmistelussa kerättyjä tietoja hyödynnetään hyökkäyksen seuraavissa vaiheissa. Teknisiä tietoja hyödyntämällä kyetään ohittamaan verkon havainnointijärjestelmät valitsemalla kohdeverkossa käytettävien järjestelmien ja ohjelmistojen sisältämät tietoturva-aukot eli *haavoittuvuudet* ja konfiguraatiovirheet. *Haittaohjelma* voidaan myös sovittaa toimimaan erilaisten kohdeverkossa olevien laitteiden käyttöjärjestelmien mukaisesti. Tässä vaiheessa hyökkääjä mahdollisesti testaa kohdeverkon havainnointikykyäkin. Toisaalta sosiaalisten tietojen perusteella hyökkääjä voi luoda kohdettaan kiinnostavaa sisältöä, jota voidaan tarjota esimerkiksi sähköpostin tai murrettujen www-sivujen kautta. Kun sisältö räätälöidään koskemaan kohteen ajankohtaisia substanssiasioita, ei viesti tai sivusto välttämättä herätä kohteen epäilyksiä.

2.2 Tunkeutuja tavoittaa kohteensa esittäessään luotettavaa

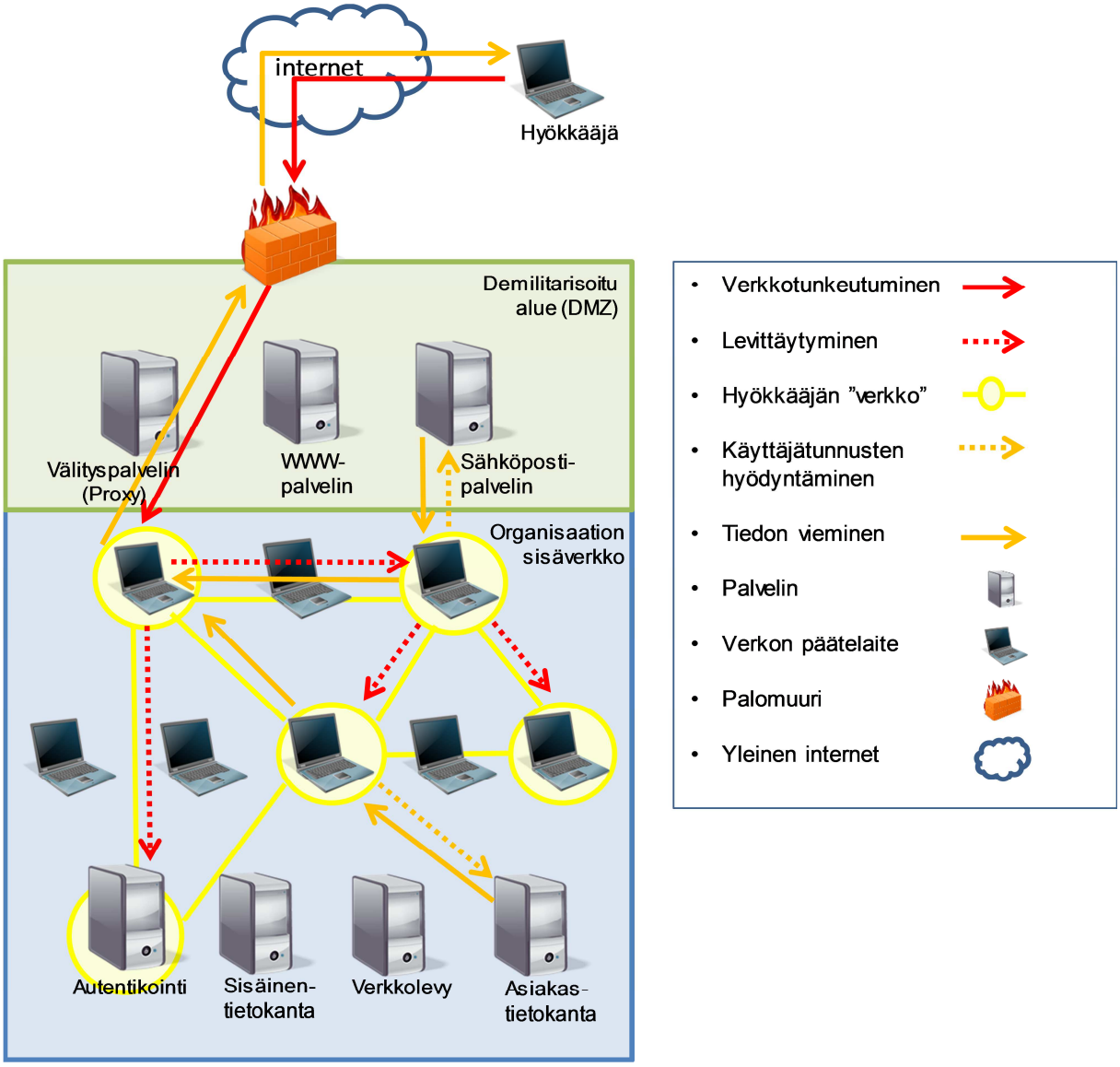
Tunkeutumiseen käytetään menetelmiä, joita kohdeorganisaatio käyttää päivittäisessä työssään. Hyökkääjä lähettää kohteellensa sähköposteja, houkuttelee sen luomilleen verkkosivuille mielenkiintoa herättävällä sisällöllä tai ujuttaa sille *haittaohjelman* sisältävän muistitikun. Lisäksi hyökkääjä selvittää, mitä ohjelmistoja *kohde* käyttää ja etsii niistä *haavoittuvuuksia*, joiden avulla pääsisi tunkeutumaan kohdeverkkoon. Tehokkaimpia ovat tuoreet ohjelmistoyhtiöiden julkisesti ilmoittamat *haavoittuvuudet*, joita kohdeorganisaatioissa ei ole vielä ehditty päivittämään ajantasaisiksi. Paljon puhutaan vielä tuntemattomien, niin kutsuttujen 0-päivä-*haavoittuvuuksien* hyödyntämisestä kohdistetuissa hyökkäyksissä. Koska 0-päivä-haavoittuvuuksien etsiminen tai hankkiminen on kuitenkin melko työlästä tai kallista, on niiden hyödyntäminen tunnetuissa kohdistetuissa hyökkäyksissä kokemusten mukaan ollut varsin vähäistä. Oletettavasti 0-päivä-haavoittuvuuksia hyödynnetään vain hyökkääjän kannalta merkittävimpiin kohteisiin. Merkittävässä osassa hyökkäyksiä käytetään tuoreita julkisia *haavoittuvuuksia*. Näitä hyökkäyksiä kyettäisiin estämään tehokkailla päivitysprosesseilla. Kohdistettujen haittaohjelmahyökkäysten levityskeinoja on tarkemmin kuvattu seuraavassa taulukossa 2.

Taulukko 2: Esimerkkejä hyökkääjän tunkeutumismenetelmistä

Menetelmä	Kuvaus
Ulkoiset verkkosivut (*Watering hole*)	Nykyään hyvin tyypillisesti kohdistettujen haittaohjelmien levityksessä käytetään kohteen ulkopuolisia verkkosivuja, jotka liittyvät kohteen työtehtäviin, päivittäiseen asiointiin tai voivat olla välttämättömiä tehtävien hoitamisen kannalta. Näitä voivat olla esimerkiksi yhteistyökumppaneiden, tapahtumien, lounasravintoloiden tai muiden alan organisaatioiden sivuja. Hyökkääjä on murtautunut ja lisännyt sivulle haitallista sisältöä, joka ohjaa kohdetta lataamaan haittaohjelman koneelleen. Joissakin tapauksissa on käytetty sivustojen mainoksia. Sivusto on voitu räätälöidä levittämään haitallista sisältöä vain tietyn organisaation vierailijoille. On todennäköistä, että hyökkäyksessä käytetyn sivuston ylläpitäjä ei ole tietoinen väärinkäytöksistä. Menetelmää kutsutaan kansainvälisesti Watering hole -hyökkäykseksi.
Alihankintaketjut (*Water carrier*)	Kasvamassa määrin haittaohjelman levityksessä hyödynnetään alihankintaketjuja. Kohteen alihankintaketjussa olevan yrityksen verkkosivuille murtaudutaan ja sivuilta ladattava ohjelmisto tai tiedosto saastutetaan haittaohjelmalla. Ohjelmiston tai tiedoston päivitetyn version latauksen yhteydessä latautuu myös haittaohjelma.
Sähköpostin liitetiedostot	Käytetään tavanomaisten massahaittaohjelmien levityksen tapaan. Erona on sisällön laadukas räätälöinti kohteen mielenkiinnon mukaan. Näin on todennäköisempää, että sisältö avataan ja ladataan kohdeverkon koneessa. Esimerkkeinä kohteen kalenterimerkinnät ja tulevat tapahtumat sekä työhön liittyvät kontaktitiedot. Kun tieto sähköpostiliitetiedostojen riskeistä on levinnyt, tunkeutumismenetelmänä ne ovat hieman hiipuneet.
Siirtomedia (esim. USB-muistitkut, CD-levyt, siirrettävät kovalevyt)	Haittaohjelman sisältäviä siirtomedioita voidaan jakaa tapahtumissa - seminaareissa tai konferensseissa - joihin kohde osallistuu. Esimerkiksi kokousmateriaalien ja -tiedostojen mukana voidaan jakaa haittaohjelmaa luotettavan oloisen toimijan kautta. On myös tapauksia, joissa muistitikku on pudotettu kohteen toimipisteen läheisyyteen.

2.3 Toiminta on pysyvää ja huomaamatonta

Jotta hyökkääjä saisi pysyvän aseman kohteensa verkossa, sisään saatu kohdistettu *haittaohjelma* pyritään levittämään kohdeverkon sisällä riittävään määrään päätelaitteita jalansijan säilyttämiseksi myös joidenkin koneiden vaihtuessa tai poistuessa verkosta. Lisäksi hyökkääjä voi asentaa kohteensa verkkoon pysyvän jalansijan eli niin sanotun takaoven. Tämä tapahtuu esimerkiksi lisäämällä itselle pääsytunnukset järjestelmään tai asentamalla haitallista koodia, jonka avulla hyökkääjän on mahdollista ottaa yhteyttä ja ohjata verkon päätelaitteita. Näin verkossa voidaan asioida jatkossakin ja tarpeen mukaan kuitenkaan lisäämättä kiinnijäämisen riskiä turhalla verkkoliikennöinnillä. Verkkoon levittäytymistä ja jalansijan hakemista on kuvattu kuvassa 3.



Kuva 3: Esimerkki kohdistetun haittaohjelman toiminnasta organisaation verkossa

Hyökkääjä asioi kohteensa verkossa muun muassa tiedostolatauksin, kuvakaappauksin, käyttäjätunnuksia muokkaamalla, "lukemalla" näppäimistöä tai muuttamalla järjestelmän prosesseja omien tarkoitusperien mukaisesti. Verkkovierailuissa voi olla pitkiäkin taukoja, jolloin hyökkääjän läsnäoloa on mahdotonta havaita. Myös *haittaohjelman* tekninen toiminta pyrkii olemaan vähäeleistä: liikennemäärät ovat vähäisiä ja liikennöintiajat normaaleja. Jos hyökkäyksen uhrin koneiden toiminta ei hidastu eikä tunnistamattomia taustaprosesseja havaita, epäilykset eivät myöskään herää.

Jälkien siivoaminen on oleellinen osa hyökkäystä, jotta kohdeverkkoon olisi mahdollista palata myös tulevaisuudessa. Näkyvät merkit vierailuista pyritään poistamaan, jotta historiatiedostoista eli lokeista ei paljastuisi viitteitä tai toimintatapoja meneillään olevasta tai menneestä laittomasta verkkovierailusta. Jälkikäteen havaitun kohdistetun hyökkäyksen tutkiminen on työlästä ja kokonaisuudesta ei välttämättä koskaan

selviä kaikki yksityiskohdat. Havainnoinnin ja jälkiselvitysten kannalta hyvä huomio on, että suuri osa haitallisista ohjelmistoista toimii ainakin osin kohdekoneen muistinvaraisesti.

Vinkki: Ole tietoinen ilmiöstä, siten ehkäiset pahimmat vauriot

Tieto ja käsitys organisaatiosta saatavilla olevista tiedoista ja järjestelmien ylläpidon kokonaisuudesta lisää kykyä tunnistaa riskit, joiden vuoksi organisaation verkkoon tunkeutuminen on mahdollista. Tiedon avulla voi keskittyä oleellisiin ennaltaehkäiseviin toimiin.

OSA II

Mitä tapahtuu nyt ja tulevaisuudessa?

1 Tilanne ja sen kehittyminen Suomessa ja maailmalla

Tietoisuus kohdistetuista haittaohjelmahyökkäysten riskeistä on viimeisen vuoden aikana lisääntynyt merkittävästi, koska sekä kotimaisia että kansainvälisiä tapauksia on käsitelty julkisuudessa. Lisäksi kansainväliset tietoturvayhtiöt ovat julkaisseet teknisiä raportteja haittaohjelmien toiminnasta [Liite 2].

Järjestelmällisesti *kyberhyökkäyksiä* seuraavissa länsimaissa kohdistettuja hyökkäystapauksia todennetaan kymmeniä vuosittain. Tapauksia on havaittu esimerkiksi Norjassa [1] ja Ruotsissa [2]. Ilmiön todellisuudesta kertovat myös havaitut ja torjutut hyökkäysyritykset, jotka eivät kuitenkaan näy tilastoissa. Oletettavasti on lukuisia tapauksia, joita ei ole edes havaittu. Suomesta ei ole saatavilla tilastollisesti vertailukelpoista tietoa.

Suomen nykytilannetta voidaan arvioida maamme yleisen kiinnostavuuden ja hyökkäystapausten tämänhetkisen havainnointikyvyn näkökulmista. Tulevaa kehitystä voidaan taas ennakoida tarkastelemalla ilmiön tähänastista kehitystä ja arvioimalla nykyisten käytössä olevien työvälineiden hyväksikäyttömahdollisuuksia. Useista hyökkääjän käyttämistä menetelmistä on varoitettu hyvissä ajoin, mutta yleensä tapauksiin reagoidaan vasta, kun havaitaan että hyökkääjä on onnistunut tunkeutumaan kohteensa verkkoon.

1.1 Nykytilanne: Havaittujen tapausten vertailu kiinnostavuuteen

Suomi on toistuvasti kärkijoukoissa kansainvälisissä maailmantaloutta seuraavan WEF:n (The World Economic Forum) kilpailukykymittauksissa [3]. Vertailuissa Suomen vahvuuksina pidetään hyvään koulutukseen perustuvaa teknologista kehitystä, innovaatioita ja yhteiskunnan instituutioiden toimivuutta. Lisäksi Suomessa on useita maailman teollisuuden alan kärkiyrityksiä. Pohdittaessa suomalaisten ja muiden maiden organisaatioiden kiinnostavuutta kohdistettujen hyökkäysten kohteena ovat Suomeen liitettävät vahvuudet myös tyypillisiä *laittoman tiedonhankinnan kohteita*.

Kun Kyberturvallisuuskeskus kysyi keväällä 2014 *tietoturvaloukkausten* tutkimiseen erikoistuneilta yrityksiltä kohdistetuista haittaohjelmahyökkäyksistä, vastanneet yritykset kertoivat käsittelevänsä yksittäisiä tai muutamia selkeästi kohdistetuksi haittaohjelmahyökkäykseksi todettua tapausta vuosittain. Vastausten perusteella Suomessa todennetaan vuositasolla muutamia, mutta alle kymmenen hyökkäystapausta. Luvut vastaavat myös Kyberturvallisuuskeskuksen käsitystä tiedossa olevien tapausten kokonaismäärästä. On myös hyvä huomioida, että osa kohteiksi päätyvistä organisaatioista käsittelee haittaohjelmatapaukset ilman, että ilmoittaa siitä viranomaiselle. Luonnollisesti tällaiset tapaukset jäävät tilastoimatta.

Suomeen kohdistuvia haittaohjelmahyökkäyksiä todetaan suhteellisen vähän. Syytä ei kuitenkaan selitä väite Suomen yleisten viestintäverkkojen puhtaudesta [4], sillä ne eivät suojaa kohdistetuilta hyökkäyksiltä. Lisäksi on huomioitava, että suomalaisten verkkojen puhtaus perustuu aktiivisiin toimiin ja yhteistyöhön. Suomalaisten päätelaitteissa havaitaan haittaohjelmia kuten muuallakin maailmassa, mutta yritysten ja viranomaisten vastatoimenpiteet ovat verrattain tehokkaita. Toiminnassa on hyödynnetty sekä teleyritysten omia että Kyberturvallisuuskeskuksen Autoreporter-järjestelmän teleyrityksille toimittamia tietoja.

Myöskään suomen kieli tai suomalaisten organisaatioiden tietoturvan korkea taso ei selitä tapausten vähäisyyttä. Kotimaisten tietoturvayritysten kokemusten mukaan organisaatioiden oma kyky havaita kohdistettuja hyökkäyksiä on heikko. Havainto vastaa myös Kyberturvallisuuskeskuksen kokemuksia ja käsitystä maailmanlaajuisesta tilanteesta. Esimerkiksi Kyberturvallisuuskeskuksen vakavien tietoturvaloukkausten havainnointi- ja varoitusjärjestelmän (HAVARO) avulla tehdään usein hyvin tavanomaisiakin haittaohjelmahavaintoja, etenkin uusien järjestelmää käyttävien asiakkaiden verkoissa. Tällöin edellytykset kehittyneimpien ja kohdennettujen haittaohjelmien havaitsemiseksi eivät ole riittäviä. Huomattavaa on, että HAVARO-asiakkaina on organisaatioita, joiden tietoturvan ylläpito on huomioitu suomalaisittain kohtuullisen hyvin. Panostuksesta kertoo myös suomalaisten organisaatioiden halukkuus ottaa HAVARO käyttöön. Oletettavaa onkin, että merkittävää osaa kohdistetuista haittaohjelmatapauksista ei ole kyetty havaitsemaan.

1.2 Kohdistettujen haittaohjelmahyökkäysten määrä lisääntyy yhä

Ilmiönä kohdennetut *haittaohjelmat* ovat olleet suomalaisten tietoturvaviranomaisten tiedossa jo vuodesta 2004. Vuosittain tapauksia on tullut tietoon maailmanlaajuisesti enenevissä määrin, mistä kertoo mm. kansainvälisten tietoturvayhtiöiden julkaisemien raporttien kokonaismäärä ja julkaisutiheyden kasvu [Liite 2].

Yleisen näkemyksen mukaan kohdistetut haittaohjelmahyökkäykset tulevat jatkossa yhä lisääntymään, koska useilla toimijoilla on sekä kyky että resurssit toteuttaa edistyneitä kohdistettuja haittaohjelmahyökkäyksiä. Perinteisiin vakoilumenetelmiin verrattuna kohdistettu haittaohjelmahyökkäys on kustannustehokas. Kiinnijäämisen riskikin on verrattain pieni, ja seuraukset paljastumisista ovat toistaiseksi jääneet vähäisiksi. Tällaisen tiedonhankkimiskeinon kiinnostavuutta lisää se, että tiedonkäsittely siirtyy yhä enemmän verkkoon, alihankintaketjut lisääntyvät ja tekniset menetelmät kehittyvät jatkuvasti. Ilmiön kansainvälistyessä myös Suomeen kohdistuvien hyökkäysten määrä tullee lisääntymään.

1.3 Kohteiden joukko laajenee

Tyypillisiä kohdistettujen haittaohjelmahyökkäysten ensimmäisiä kohteita olivat erittäin isot organisaatiot, muut keskeiset toimijat tai saavutettavissa oleva strategisesti tärkeä tieto. Tällä hetkellä tiedossa olevien ja toteutuneiden kohdistettujen haittaohjelmahyökkäysten kohteena ovat olleet muun muassa energia-alan yritykset, EU:n päätöksentekoon ja siihen liittyvien jäsenmaiden näkemyksiin liittyvä tieto, valtion talouteen liittyvät toimijat, puolustusteollisuus ja huipputeknologia. Lisäksi kohdistettuja hyökkäyksiä on todennettu mediassa ja organisaatioissa, joiden kautta kulkee isoja rahamääriä, mutta joiden käytössä ei ole nykyisellään pankkimaailman kontrolleja.

Tietoisuus hyökkäyksen riskeistä on lisääntynyt. Sen vuoksi suurten organisaatioiden sijaan kohteeksi ovat joutuneet myös pienemmät yhteisöt sekä varsinaisen kohteen alihankintaketjuun kuuluvat toimijat, joissa riskiä ei ole vielä tiedostettu vastaavalla tasolla. Ilmiö vaikuttaa kehittyvän edelleen tämänsuuntaisesti. Onkin todennäköistä, että jatkossa myös Suomessa hyökkäykset kohdistuvat erityisesti merkittävien organisaatioiden alihankintaketjuihin ja esimerkiksi keskikokoisiin yrityksiin.

Kun kohdistetuissa haittaohjelmahyökkäyksissä käytetyt teknologiset menetelmät tulevat markkinoille, myös rahaa tavoittelevat verkkorikolliset saavat ne käyttöönsä. Tällöin myös tavallisista yrityksistä tulee potentiaalisia haittaohjelmahyökkäysten uhreja.

1.4 Tekniset menetelmät monipuolistuvat

Tietojen mukaan tällä hetkellä kohdistetut hyökkäykset ovat pääosin keskittyneet perinteisiin työasemiin ja palvelimiin. Tietoa kuitenkin käsitellään lukuisilla päätelaitteilla. Merkittävä osa viestinnästä ja tietojen käsittelystä tapahtuu mobiililaittein. Lisäksi on mahdollista, että ajankohtaista tietoa pyritään saamaan esityksiin käytettävien televisioiden ja videotykkien kautta. Myös toimistoverkkoon liitetyt laitteet, joilla käsitellään suojattavia tietoja kuten tulostimet ja kopiokoneet, voivat olla tiedonhankintavälineinä kiinnostavia.

1.5 Uhkan vaikutukset Suomessa

Kokonaisuutena kybervakoilu on merkittävä uhka Suomelle. Sen avulla kerätään tietoja, joiden siirtyminen vieraan valtion käyttöön voi aiheuttaa huomattavaa vahinkoa Suomen maanpuolustukselle, turvallisuudelle, taloudelle ja ulkomaansuhteille. Tapaukset voivat vaarantaa Suomen suvereniteetin. Yrityksiin ja yliopistoihin kohdistuessaan *vakoilu* heikentää Suomen edellytyksiä pärjätä kovenevassa kansainvälisessä kilpailussa. Yksittäisetkin kybervakoilutapaukset heikentävät Suomen mainetta uskottavana kyberosaajana.

Vain kattava havainnointi, toiminta- ja reagointikyky kaikentasoisiin *kyberuhkiin* voi vahvistaa Suomen kehitystä *kyberturvallisuuden* kansainväliseksi kärkimaaksi. Tämä vaatii jatkuvia ja aktiivisia toimenpiteitä tietoturvallisuuden edistämiseksi sekä runsasta yhteistyötä niin julkisten kuin yksityisten toimijoiden kesken. Yhteistyön keinoin on saavutettu myös asema maana, jolla on maailman puhtaimmat viestintäverkot. Hyökkääjien vahvistaessa toimintaansa sekä taloudellisesti että teknisesti kohteiden puolustuskyvyn on oltava vähintään vastaavalla tasolla. Kyberturvallisuuden edelläkävijäasema saavutetaan vain, jos kaikki organisaatiot tunnustavat uhkan olemassaolon ja sitoutuvat sen torjumiseen sekä sisäisesti että yhteistoiminnallisesti.

Vinkki: "Maineen menetys" on käännettävissä arvostukseksi

Tietoturvaloukkaustapausten katsotaan tyypillisesti heikentävän organisaatioiden mainetta. Erityisesti jos organisaatio pitkittää julkituloaan sitä kohdanneesta tietoturvaloukkauksesta, maine kärsii erityisen paljon. Onneksi on havaittavissa myös päinvastainen ilmiö: organisaation maine voi parantua, jos se tuo julkisesti esille, että sillä on kyky havainnoida ja korjata järjestelmiensä heikkouksia sekä käyttää epäonnistumisiaan hyödyksi ennaltaehkäistessään tulevia tietoturvaloukkausyrityksiä. Organisaatio voi kääntää kokemuksensa ja oppinsa yleiseksi hyödyksi ja arvostukseksi jakamalla ne muiden kanssa.

2 10 opittua asiaa!

1. Havainnointi vaatii aktiivisista toimintaa ja osaavaa henkilöstöä.

Osaava henkilöstö tuntee verkkonsa perustoiminnot ja tyypillisen liikennevirran, jolloin voidaan nopeasti havaita poikkeavuudet normaalitilanteesta. Pelkkä lokien ylläpito ja tietoturvakontrollien tuottamien varoitusten seuranta ei riitä, vaan ne vaativat tulkintaa. Suomalaisten tietoturvayhtiöiden kokemusten mukaan organisaatioissa, joissa on havaittu kohdistettuja haittaohjelmahyökkäyksiä, havainnointi on ollut puutteellista.

2. Tiedon jakaminen parantaa kaikkien havainnointikykyä.

Hyökkääjät kehittävät jatkuvasti uusia hyökkäysmenetelmiä. Organisaation havaitessa kohdistetuksi hyökkäykseksi epäiltyjä tai todennettua tunnusmerkkejä, havainnoista on suositeltavaa kertoa keskitetylle toimijalle kuten Kyberturvallisuuskeskukselle. Näin esimerkiksi tunnusmerkkejä voidaan jakaa anonymisoidusti kansallisten tietoturvaviranomaisten sekä tietoturvayhtiöiden välityksellä. Kun yhteistyöverkosto jakaa tietoa toisilleen, myös sen jäsenten hyökkäysten havainnointikyky paranee.

3. Toimi harkiten ja aloita selvitys vastakohdistettuihin hyökkäyksiin perehtyneiden asiantuntijoiden avulla.

Kohdistettujen haittaohjelmahyökkäysten selvityksessä harkitsemattomat ja näkyvät estotoimet kertovat tunkeutujalle, että hyökkäys on paljastunut. Tunkeutuja voikin näennäisesti poistua verkosta, siivota jälkensä ja tuhota *tietoturvaloukkauksesta* kertovia todisteita, jolloin tapauksen selvittäminen hankaloituu. On kuitenkin mahdollista, että hyökkääjä jättää jälkeensä takaovia, joiden kautta se voi taas päästä takaisin kohteensa verkkoon. Jos siis epäilys kohdistetusta haittaohjelmahyökkäyksestä herää, tapauksen selvittäminen tulee aloittaa maltilla ja avuksi on haettava osaavia ammattilaisia.

4. Lokien tallennus ja pitkäaikainen säilytys on tärkeää.

Kohdistetut haittaohjelmahyökkäykset havaitaan tyypillisesti vasta ulkopuolisen hyökkääjän pitkäaikaisen läsnäolon jälkeen. Tapahtumaa on jälkikäteen mahdollista selvittää lokien perusteella. *Tietoturvaloukkausten* paljastuttua usein todetaan puutteita juuri verkkoliikenteen ja järjestelmäkirjautumisten seurannan systemaattisessa tallentamisessa ja säilytyksessä. Jos lokien hallintaa ei ole toteutettu kattavasti, tällöin on mahdotonta todentaa ulkopuolisen toimintaa verkossa. Lokien keräyksessä on siis varmistettava oleellisten tietojen tallennus ja kaikkien aikaleimojen täsmällisyys.

5. Kuka tahansa voi olla kohde.

Vain harva organisaatio kokee olevansa altis kohdistetun haittaohjelmahyökkäyksen uhalle. Välinpitämättömyys aiheuttaa riskin myös organisaation sidosryhmille, sillä heikosti suojattu, seurattu ja ylläpidetty verkko on helppo kauttakulkureitti tai tiedonhankintapaikka, jossa tietoa voidaan kerätä myös kohteen sidosryhmistä.

Samat käytännöt, jotka suojaavat verkkoa tavanomaisilta tietoturvauhilta, suojaavat verkkoa myös kohdistettuilta hyökkäyksiltä. Tietoturva voi olla organisaatiolle kilpailuetu, mutta heikosti toteutettuna se on riski organisaation hyvälle maineelle.

6. Suojaa kriittiset tiedot.

Kaikkea tietoa ei tarvitse suojata ja julkinen tieto tuleekin olla helposti saatavilla. Kriittisen tiedon käsitteleminen taas vaatii erillisiä järjestelmiä, samalla se hankaloittaa tiedon käsittelyä.

Osaaminen ei siis ole kaiken tiedon suojaamista, vaan suojaamistarpeen tunnistamista ja sen edellyttämiä suojauskäytäntöjä. On tarpeen miettiä, mitkä ovat riskit, jos omat tiedot päätyvät ulkopuoliselle.

7. Vastuu tietojen turvaamisesta ei siirry palveluja ulkoistettaessa.

ICT-palvelut ovat useissa organisaatioissa ulkoistettu erityisalan osaamisen parantamiseksi. Tällöin haasteena on ylläpitää tietoa siitä, kuka vastaa mistäkin osasta teknisiä toimintoja ja kenellä on pääsy organisaation verkkoon ulkoistussopimusten perusteella.

Ulkoistettaessa on varmistettava, että ulkoistamisen jälkeenkin organisaatiolla itsellään on yhä pääsy kaikkeen omistamaansa tietoon mukaan lukien palvelinten lokitiedot. Organisaation on myös tiedettävä, mihin kaikkialle sen verkossa pääsee ulkoistettujen toimintojen kautta. Organisaation omaa kokonaisvastuuta tietojensa käsittelyn tietoturvasta ei voi ylläpitosopimuksin siirtää. Lisäksi on sovittava reagoinnista ja vastuista tietoturvaloukkaustapausten selvityksessä.

8. Automaatio tukee tietoturvaloukkausten havaitsemista

Havainnointijärjestelmät ovat hyviä tukityökaluja *tietoturvaloukkausten* havainnoimiseksi. Tietoliikennemäärät ovat suuret ja lokiaineistoa runsaasti, joten automatisoiduilla mekanismeilla voidaan estää merkittävä osa tavanomaisista tietoturvaloukkausyrityksistä. Lisäksi automaattiset havainnointijärjestelmät nopeuttavat selvitystyötä, kun epäillään tai selvitetään kohdistetun hyökkäyksen laajuutta. Kohdistettujen haittaohjelmahyökkäysten havainnointiin ne eivät kuitenkaan yksin riitä.

9. Erillisjärjestelmätkin voivat olla saavutettavissa

Kriittiset tiedot säilytetään tyypillisesti erillisjärjestelmissä, jotka eivät ole suoraan yhteydessä julkisiin verkkoihin. Käytännön syistä tulee vastaan tilanteita, joissa erillisjärjestelmän ja internetiin kytketyn järjestelmän välillä on tarve siirtää tietoa. Tämä saatetaan toteuttaa esimerkiksi siirtomedialla tai liittämällä koneet hetkellisesti samaan järjestelmään.

On muistettava, että jos erillisjärjestelmää suojaavat ilmavälit kyetään ylittämään itse, siinä voi onnistua tarvittaessa myös ulkopuolinen taho.

10. Ei ole olemassa täysin luotettavaa järjestelmää.

On organisaatioita, joissa järjestelmäsuunnittelussa tietoturva on otettu huomioon alusta alkaen ja kokonaisuus on rakennettu huolella. Tämä tarjoaa hyvät lähtökohdat *tietoturvaloukkausten* ennaltaehkäisylle, mutta organisaatio ei kuitenkaan saa tuudittautua epärealistiseen turvallisuuden tunteeseen. Hyvin suunniteltua ja toteutettua järjestelmää tulee myös jatkuvasti seurata.

OSA III

Kuinka uhalta suojaudutaan?

1 Kuinka suojautua hyökkäykseltä?

Kohdistetuilta haittaohjelmilta suojautuminen vaatii monentasoisia toimenpiteitä. Näitä ovat

1. ***Ennaltaehkäisevillä toimilla*** voidaan hankaloittaa hyökkäyksen osumista organisaatioon ja parantaa organisaation tunkeutumisyritysten varhaista havaitsemista.

2. Pätevä ***havainnointikyky*** tekee mahdolliseksi havaita sisäänpääsy-yritykset ja *haittaohjelman* toiminta mahdollisimman varhain.

3. Koska useilla toimijoilla on kyky ja resurssit toteuttaa kohdistettuja haittaohjelmahyökkäyksiä, ***reagointivalmius*** on oleellinen osa sekä riskin tunnistamista että keino minimoida vahingot.

4. Tarvittaessa tämän jälkeen on aloitettava vaadittavat toimet organisaation verkon ***palauttamiseksi ja toipumiseksi***.

Lopulta toipumisen jälkeen palataan jälleen ennaltaehkäisevään toimintaan, jossa on syytä hyödyntää kokemuksia tiedossa olevista hyökkäystapauksista. Suojaavat vaiheet on esitetty kuvassa 4.

Kuva 4: Hyökkäykseltä suojautuminen on huomioitava monessa vaiheessa

1.1 Ennaltaehkäisevät toimenpiteet

Ennaltaehkäisevillä toimilla (taulukko 3) tavoitellaan tilannetta, jossa organisaatio on hyökkääjän näkökulmasta epämielekäs *kohde*. Tällöin hyökkäys on hankala toteuttaa, koska organisaatio kykenee havaitsemaan ja tarvittaessa reagoimaan hyökkäykseen juuri oikealla tavalla. Ennaltaehkäisyssä on tärkeää, että henkilökunta on koulutettu

riittävästi. Toimenpiteisiin kuuluvat myös poikkeamanhallinnan menettelytapojen määrittäminen ja käytössä olevien teknisten menetelmien käyttöönotto ja ylläpitäminen, jotta mahdolliset tunkeutumisyritykset kyetään havaitsemaan. Myös ajantasainen tiedonvaihto tuoreista uhista on osa ennaltaehkäisevää toimintaa. Sekä yritysten että valtiohallinnon toimintojen arvioinnin tukena voidaan hyödyntää kansallista turvallisuusauditointikriteeristöä (KATAKRI) [5].

Organisaatiot voivat hyödyntää myös toiminnan jatkuvuuden hallintaa koskevia suosituksia (SOPIVA) varautuessaan *tietoturvaloukkauksiin*. SOPIVA-suositusten tavoitteena on kannustaa ja helpottaa elinkeinoelämän yrityksiä sekä julkishallinnon organisaatioita parantamaan ja varmistamaan toimintansa jatkuvuutta. Suosituksia noudattamalla voidaan:

- kehittää kykyä ehkäistä mahdollisia toiminnan häiriöitä
- pienentää häiriön vaikutuksia toimintaan
- nopeuttaa häiriön vaikutuksista palautumista.

Taulukko 3: Ennaltaehkäisyssä merkittävässä osassa ovat henkilöstö, poikkeamanhallintaohjeet ja organisaation/toimijan tekninen ympäristö

Ennaltaehkäisy	Toimenpide esimerkkejä
Henkilöstö	• Valveutunut henkilöstö: matala kynnys raportoida poikkeustilanteista (esimerkiksi kannustimena palkkio poikkeaman ilmoittamisesta) • Tietojenkäsittelyperiaatteet tiedossa: tunnistaa hyökkääjän kannalta kiinnostavat tiedot ja osaa käsitellä niitä riittävän suojatusti (tuotekehitys, tarjouskilpailu, päätöksentekoon liittyvät tiedot, henkilörekisterit) • Tiedonvaihto tuoreista uhista
Poikkeamanhallinta	• Suunnitelma käynnistettäville toimenpiteille o Sisäinen prosessi ja selvitysryhmä o Käytännöt ulkoistuskumppanien kanssa o Tietoturvaloukkausten selvitysresurssit (omat/ulkoisten yhteistyökumppanien) • Yhteystiedot, minne tapahtumasta ilmoitetaan: o Organisaation sisäinen ilmoittamismalli o Kyberturvallisuuskeskus o Poliisi o Tilannekohtaisesti tarvittavat asiantuntijat • Suunnitelmien harjoittelu
Tekninen ympäristö	• Sovellusten valinta • Ajantasaiset ohjelmistoversiot • Uusien tai epäilyttävien ohjelmien luotettavaksi todentaminen (Sandboxing) • Luotettavien yhteyksien/kontaktien tunnistaminen (Whitelisting) • Järjestelmien koventaminen • Käyttöoikeuksien hallinta, muutosten seuranta ja pitäminen ajantasaisina henkilöstömuutoksissa • Luokittelu: Verkkojen ja tietokokonaisuuksien eriyttäminen • Tiedonvaihto teknisistä menetelmistä • Havainnointikyky • Oman ympäristön ansoittaminen ulkopuolisen läsnäolon tunnistamiseksi (esim. Honeynet)

1.2 Havainnointitoimenpiteet

Havainnoinnin tarkoituksena on tunnistaa tunkeutumisyritykset sekä kohdeorganisaation verkossa mahdollisesti jo toiminnassa olevat *haittaohjelmat*. Kohdistetuissa hyökkäyksissä käytetään usein niin kehittyneitä menetelmiä, että käyttäjän, tietohallinnon tai jopa tietoturvayhtiöiden on mahdotonta havaita niiden toimintaa. Niinpä kohdistettua haittaohjelmahyökkäystä ei voida estää vain tietojärjestelmiä kehittämällä, sillä olipa järjestelmä miten turvallinen tahansa, motivoitunut hyökkääjä löytää halutessaan keinon tunkeutua siihen. Tästä syystä kohdistettujen hyökkäysten torjunnan tulee perustua sekä hyvään havainnointi- että seurantakykyyn.

Havainnoiminen on tehokkainta, kun tietoturvaa kontrolloidaan ja seurataan usealla eri tasolla. Näin kun ulkopuolisen on hankala ohittaa useita mekanismeja jälkiä jättämättä, myös kiinni jääminen on todennäköisempää. Kohdistettuja haittaohjelmahyökkäyksiä voidaan havainnoida ja seurata muun muassa seuraavilla tasoilla:

1. järjestelmän sisäisellä valvonnalla
2. kohdejärjestelmän/verkon rajalla
3. verkon/järjestelmän ulkopuolella

Järjestelmän sisäinen taso tarkoittaa kohdeverkon järjestelmien sisällä tapahtuvien muutosten hallintaa, seurantaa ja liikennöintiä. *Kohteen rajalla* tarkoitetaan yksittäisen organisaation verkkoon ja järjestelmiin kohdistuvan uhkan havainnointia eli kohteen ja yleisen verkon välisiä yhteyksiä. Nämä toimet tulisi kuulua rutiininomaisiin havainnointijärjestelmän ylläpitäjän työtehtäviin; yhteistyö viranomaisten kanssa on myös suotavaa. Tähän tarkoitukseen vastaa esimerkiksi Kyberturvallisuuskeskuksen HAVARO, joka on rakennettu pääasiassa kriittisen infrastruktuurin ja valtionhallinnon toimijoille. Edellä mainitut tasot täydentävät toisiaan.

Vahinkojen minimoimiseksi *kyberuhkien* synty on kyettävä havaitsemaan ajoissa ja *kyberturvallisuuteen* liittyviä ilmiöitä seuraamaan reaaliajassa. Tämä on mahdotonta, jos riittävää tilannekuvaa kyberuhista ei osata muodostaa. Tietojen ajantasaisuuden ylläpitämiseksi Kyberturvallisuuskeskus toimittaa sidosryhmilleen toimialakohtaisesti ajantasaista tietoa ja ylläpitää HAVAROn tunnistetietoja. Tiedoista osa perustuu eikaupallisesti saatavilla olevaan kansainväliseen tiedonvaihtoon ja osa esimerkiksi energia-, finanssi- tai tietoturva-alan sisäiseen tiedonvaihtoon.

Taulukkoon 4 on koottu havainnoinnissa huomioitavat eri tasot.

Taulukko 4: Havainnointikontrolleissa huomioitavat tasot

Havainnointi	Toimenpide esimerkkejä
Seuranta	• Säännöllinen seuranta hälytyksille, ongelmatilanteille ja lokeille • Väärien hälytysten toteaminen ja loppuun käsittely hallitusti • Satunnaisotannat ja -tarkastukset • Tietotaito omien järjestelmien toiminnasta, jotta poikkeavuudet voidaan havaita nopeasti. • Huomattava, jos lokien kerääminen pysähtyy
Lokitus	• Järjestelmän rajapinta • Järjestelmän sisäiset lokit tunkeutujan mahdollisen liikkumisen seuraamiseksi sisäverkon puolella • Lokitus keskistetty ja erikseen suojattu, jotta tunkeutuja ei pääse muokkaamaan lokimerkintöjä • Lokien tallennusaika mahdollisimman pitkä: vähintään 2 mielellään 10 vuotta
Tekniset menetelmät	• Tietoliikennevirtojen ja/tai niitä kuvaavien tietojen tallennus ja analysointi (Netflow) • Haittaohjelmatunnistus verkko- ja sähköpostiliikenteestä • Uutta käynnistyvää koodia valvovat järjestelmät • Verkkolaitteiden konfiguraatiomuutosten seuranta • Välityspalvelin (Proxy) • Tunkeilijan havaitsemisjärjestelmä, IDS (Intrusion Detection System) o Tunnusmerkistöjen ylläpito • Passive DNS • Yhteydet vastarekisteröityihin verkkotunnuksiin • Kyberturvallisuuskeskuksen HAVARO

Tietoturvatoimenpiteet jaetaan usein hallinnollisiin ja teknisiin toimiin. *Hallinnollisia toimia* ovat esimerkiksi toiminnan ohjeistaminen ja tietoturvan tason aktiivinen seuraaminen. *Teknisiä toimenpiteitä* ovat muun muassa tietojärjestelmien käyttäjälokien kerääminen ja niiden seuraaminen. Toimenpiteet eivät pääsääntöisesti edellytä nimenomaista laissa säädettyä oikeutusta. Lainsäädännössä harvemmin rajoitetaan toimenpiteitä, joihin organisaatiot voivat tietoturvaperusteisesti ryhtyä. Rajoituksia on esimerkiksi välitettävään viestintään kohdistuville tietoturvatoimenpiteille [6].

Lähtökohta on, että yritykset vastaavat itse järjestelmiensä ja palveluidensa tietoturvallisesta toteuttamisesta ja arvioinnista. Voimassa oleva sääntely antaa suomalaisille organisaatioille hyvät mahdollisuudet huolehtia toimintansa turvallisuudesta.

Välitettävän viestinnän (esimerkiksi puheluiden, sähköpostien tai tekstiviestien) tietoturvatoimenpiteitä suunniteltaessa ja toteutettaessa perussääntö on, että käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa. Sillä ei myöskään saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä [7]. Näiden tietoturvatoimenpiteiden tarvetta ja laajuutta arvioitaessa on otettava huomioon muun muassa yritysten käytettävissä olevat tekniset mahdollisuudet ja niiden aiheuttamat kustannukset sekä uhkan vakavuus [8]. Lisäksi on huomioi-

tava käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan näkökulmasta [9].

Tietoturvatoimenpiteiden tarkoituksena on ehkäistä tietoturvauhkia ja selvittää tietoturvapoikkeamia. Tietoturvatoimenpiteistä saatuja teknisiä tietoja ei saa käyttää esimerkiksi työntekijän tekniseen valvontaan, jossa käytetyt työvälineet ja toimenpiteet ovat usein samoja, erona vain toiminnan tarkoitus ja päämäärä. Työntekijöiden tekniseen valvontaan sovelletaan omaa sääntelyään, ja sitä koskee oma erityinen YT-menettelynsä [10].

1.3 Reagoivat toimenpiteet

Kohdistettu hyökkäys havaitaan usein esimerkiksi yllättäen sisäisesti tai ulkopuolisen vinkistä. On tärkeää, että havainnon jälkeiset toimet ovat harkittuja ja suunnitelmallisia. Näin ei tehdä suotta paniikkiratkaisuja, joilla tuhotaan hyökkäykseen liittyviä tärkeitä todisteita. Tyypillinen harkitsematon ensitoimenpide on, että ajetaan omiin järjestelmiin täydellinen virusskannaus ja asennetaan tietokoneet uudelleen. Tästä seuraa, että kohdistetun haittaohjelman toimintaa ei voida havaita tai tarkkailla, eikä hätiköidyillä toimenpiteillä sitä välttämättä saada edes poistettua. Jos kohdistetun haittaohjelman toimintatavoista ei ole tietoa, toimet sen havaitsemiseksi ja torjumiseksi ovat lähes mahdottomia. Näin hyökkääjän on mahdollista tunkeutua kohteensa järjestelmiin uudelleen. On siis tärkeää, että organisaatiolla on valmis toimintamalli tietoturvaloukkaustapausten käsittelyyn, jossa kerrotaan myös kohdistettujen hyökkäysten erikoispiirteistä. Taulukossa 5 on lueteltu reagoiviin toimenpiteisiin kuuluvia vaiheita.

Taulukko 5: Reagoivien toimenpiteiden vaiheet

Reagointi	Toimenpide esimerkkejä
Kirjaa	• Lokit • Liikenneseuranta • Päätelaitteiden toiminta • Käyttäjän poikkeavat havainnot

Tiedota	• Sisäisesti
	• Kyberturvallisuuskeskus
	  o APT-ohje
	  o Tiedon jakaminen
	  o Tekninen tuki
	• Poliisi: Rikosilmoitus tietoturvaloukkauksesta

Toimi	• Hae tarvittaessa ammattitaitoista apua • Selvitä laajuus: mihin kaikkiin järjestelmiin hyökkääjällä on pääsy • Rajaa vahingot: estä ja hankaloita hyökkääjän läsnäoloa

1.4 Palautustoimenpiteet

Kun järjestelmään on onnistuttu hyökkäämään, siihen on vaikea enää luottaa. On mahdotonta täysin tietää, kuinka syvälle hyökkääjä on järjestelmissä tunkeutunut ja onko hän jättänyt takaovia järjestelmään. Saastuneita koneita ei voi vain sulkea ver-

kosta eikä liikennettä suodattaa vain tunnettuihin haitallisiin osoitteisiin. Hyökkäyksen todentamiseksi ja hyökkääjän toimien tunnistamiseksi esimerkiksi lokidata, käyttäjätunnukset ja järjestelmiin tehdyt muutokset on käytävä läpi systemaattisesti pitkällä aikavälillä. On muun muassa selvitettävä, onko järjestelmään ilmestynyt uusia käyttäjiä, onko käyttöoikeuksia muutettu tai uusia sovelluksia asennettu.

Varmin tapa hyökkääjän poissulkemiseksi kohdistetun hyökkäyksen poistamiseksi on rakentaa uusi verkko. Siirrettäessä vanhoista järjestelmistä tietoa uusiin järjestelmiin, on mahdollista, että tunkeutujan lisäämät takaovet, pääsyoikeudet tai haitallinen koodi siirtyvät vanhojen tietojen mukana myös uuteen ympäristöön. Siirtotoimenpiteet on suunniteltava ja toteutettava huolellisesti. Tämän jälkeen on huolehdittava asianmukaisesta jatkoseurannasta.

Verkon toimintaa palautettaessa on otettava huomioon seuraavat kokonaisuudet:

- Välittömät muutostarpeet: verkon siivoaminen ja seuranta
- Verkon luotettavuuden arvio: uusiminen ja rakennemuutokset
- Toimenpiteiden kustannusarvio

Kyberturvallisuuskeskukselta on mahdollista saada lisäohje palauttamiseen liittyvistä toimenpiteistä. Ohje luovutetaan pyynnöstä niille, joilla on vahva epäily organisaationsa kohdistetusta haittaohjelmahyökkäyksestä tai oman arvionsa mukaan suuri riski päätyä kohdistetun hyökkäyksen uhriksi.

Liite 1: Kohdistettuihin haittaohjelmiin liittyvää sanastoa

Sana	Selitys
Autentikointi	Käyttäjän tai palvelun varmennettu tunnistaminen. Usein keskitetty käyttäjätunnustautuminen toteutettu verkon yhteisen tietokannan avulla.
Demilitarisoitu alue (DMZ)	Väliverkko, joka yhdistää organisaation sisäisen verkon ja julkisen internetin toisistaan.
Haavoittuvuus, Haava	Ohjelmiston sisältämä ohjelmointivirhe. Avoimen haavan kautta tietokoneelle voi ladata haittaohjelman. Ohjelmistojen uusissa versioissa tunnetut haavat on pyritty korjaamaan.
Haittaohjelma	Tietokoneohjelma, joka suorittaa ei toivottuja toimenpiteitä tietokoneessa. Näitä voivat olla sähköpostiviestien lähetys, tiedostojen lukeminen, tiedostojen lähettäminen, näppäimistön käytön lukija. Perushaittaohjelmat eivät valitse uhreja vaan levittäytyvät mahdollisimman laajasti. Haittaohjelmia on useita eri alalajeja haittaohjelman tarkoituksen mukaan. Haittaohjelmat voivat olla muuntautumiskykyisiä.
Kohdistettu haittaohjelma	Haittaohjelma, joka on tarkoitettu tiettyyn ennalta määritettyyn kohteeseen. Ohjelma valitsee uhrinsa ennalta räätälöityjen tietojen perusteella. Kohdistetun haittaohjelman laatiminen vaatii ennakkotietoa uhrista.
Kohdistettu hyökkäys (APT-hyökkäys)	Tietoturvaloukkaus, joka on kohdistettu tiettyyn toimijaan tai toimijajoukkoon huomioiden kohteen erityispiirteet. Toteutuksessa hyödynnetään tyypillisesti tunnettuja ohjelmisto haavoja, jonka kautta saadaan asennettua kohdennettu haittaohjelma. (APT=Advanced Persistent Threat)
Kohde	Organisaatio (yritys, yhteisö, hallinnonelin, teollisuuden ala), johon hyökkäys kohdistettu.
Kohdentaminen	Mikä tahansa tekijä, joka osoittaa kohteen. Tyypillisesti: • IP-osoite • Kohdeorganisaation sähköpostiosoitteet • Tiedostojen nimet • Nimet, sähköpostit ja kirjautumisessa
Kyberhyökkäys	Tietoverkkoa, siihen kytkettyjä järjestelmiä, laitteita ja niissä käytettäviä ohjelmia/sovelluksia vastaan tehtävä hyväksikäyttö tai toimintaa haittaava teko.
Kyberturvallisuus	Tietoverkkojen sekä niihin kytkettyjen järjestelmien, laitteiden ja niissä käytettävien ohjelmien/sovellusten välisen viestinnän ja toiminnan turvaaminen.
Kyberuhka	Tietoverkkojen, siihen kytkettyjen järjestelmien, laitteiden tai niissä käytettävien ohjelmien/sovellusten toimintaa tai hyväksikäyttöön liittyvä uhka.
Kybervakoilu	Tietoverkkojen välityksellä toteutettu luvaton tiedustelutoiminta.
Kyberympäristö	Muodostuu toisiinsa kytkeytyneistä tietoverkoista ja niihin liitetyistä tietojärjestelmistä, laitteista sekä niissä käytettävistä ohjelmista ja sovelluksista.
Laiton tiedonhankinta	Rikosnimike jota käytetään kohdistetun haittaohjelmahyökkäyksen avulla hankitulle tiedolle.

Nollapäivähaavoittuvuus (Zero day)	Haava, joka ei ole yleisesti tiedossa eikä siihen ole olemassa korjausta. Paljastuu, kun löydetään sitä hyödyntävä haittaohjelma
Tiedustelu	Tiedonhankintamenetelmä, jossa kerätään tietoa tiettyyn tarkoitukseen. Kerätty tieto tulkitaan ja jaetaan päätöksenteon tueksi.
Tietoturvaloukkaus	Teko tai tapahtuma, jonka seurauksena järjestelmissä olevat tiedot, viestintäpalveluiden käyttö tai järjestelmän tietoturvaa ylläpitävät osat ovat vaarantuneet.
Tietomurto	Käyttää ilman oikeutta toisen käyttäjätunnusta tai tunkeutuu tietojärjestelmään.
Vakoilu	Luvatonta tiedustelutoimintaa, eli tiedonhankinta menetelmä, jonka avulla tietoa pyritään saamaan kohteen tietämättä ja vastentahtoisesti.
Välityspalvelin (Proxy)	Välittää ja varastoi verkossa siirrettävää liikennettä esimerkiksi käyttäjän päätelaitteen ja sisältöä tarjoavan palvelimen välillä.
Watering hole	Esim. luotettava verkkosivu (uutissivusto, yhteistyöorganisaation verkkosivu), jonne kohdehenkilöt houkutellaan. Sivustolle sijoitettu haitallista sisältöä.
Watering carrier	Alihankintaketjun kautta levitetty haittaohjelma saastuttamalla esimerkiksi ohjelmistopäivitys tai ohjedokumentti.

Liite 2: Tunnetut merkittävät kohdistetut haittaohjelmat – raportit maailmalla

Vuosi	Tapaus	Julkaisija
2005		
	Titan Rain	
2006		
	-	
2007		
	-	
2008		
	Agent.BTZ	
2009		
	GhostNet	Information Warfare Monitor
2010		
	Operation Aurora	Google
	Stuxnet	Symantec
	Shadows in the Cloud	Information Warfare Monitor
2011		
	Dugu	Kaspersky Lab
2012		
	Flame	CrySyS
	Gauss	Kaspersky Lab
2013		
	Red October	Kaspersky Lab
	APT1	Mandiant
	Miniduke	Kaspersky lab & CrySyS
	NetTraveller	Kaspersky Lab
2014		
	Careto, Mask	Kaspersky Lab
	Uroburos	G Data
	Snake	Bae Systems
	Energetic Bear	Crowdstrike
	Dragonfly	Symantec
	CosmicDuke	F-Secure

Lähteet

[1] PST, Trusler og Sårbarheter 2013,
http://www.pst.no/media/59018/Trusler_og_sarbarheter_2013.pdf

[2] FRA, Årsrapport,
http://www.fra.se/snabblankar/nyheterochpress/publicerat.115.html

[3] WEF, Global Competitiveness Report 2013-2014,
http://www.weforum.org/reports/global-competitiveness-report-2013-2014

[4] Viestintäviraston Kyberturvallisuus katsaus 1/2014, Onko Suomessa maailman puhtaimmat verkot?, s. 21-25

[5] Puolustusministeriö, Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio 2.0, 2011.
http://www.defmin.fi/hallinnonala/puolustushallinnon_turvallisuustoiminta/kansallinen_turvallisuusauditointikriteeristo_(katakri)

[6] Eri toimijoille on olemassa omaan tietoturvaan liittyvää sääntelyä. Esimerkkeinä voidaan mainita:

- Teleyritysten, lisäarvopalvelujentarjoajien sekä yhteisötilaajien on noudatettava sähköisen viestinnän tietosuojalakia (516/2004) 19§ ja 20§

- Pankkialaa velvoittaa pankkisalaisuus, joka esimerkiksi pankin asiakkaan kannalta on osa yksityisyyden suojaa. Katso laki luottolaitostoiminnasta (121/2007) ja luottotietolaki (527/2007) 7§

- Valtionhallintoa velvoittaa valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)

- Henkilötietojen käsittelyä koskee henkilötietolain (523/1999) 32§:n tietoturvavelvoitteet

[7] Katso esimerkiksi sähköisen viestinnän tietosuojalaki (516/2004) 8§ ja 20§, henkilötietolaki (523/1999) 5§ sekä luottotietolaki (527/2007) 7 §

[8] Katso esimerkiksi esimerkiksi sähköisen viestinnän tietosuojalaki (516/2004) 19§ ja luottotietolaki (527/2007) 7 §

[9] Katso esimerkiksi henkilötietolaki (523/1999) 32§ sekä luottotietolaki (527/2007) 7 §

[10] Katso esimerkiksi laki yksityisyyden suojasta työelämässä (759/2004) 21 §, laki yhteistoiminnasta valtion virastoissa ja laitoksissa (1233/2013) 13 §

Yhteystiedot
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi