OPAS KIRISTYSHAITTAOHJELMILTA SUOJAUTUMISEKSI

Kuinka kehittää suojautumista ja palautumista kyberhyökkäyksiä vastaan?

Mikael Inkinen

Julkaistu 1/2022

Tämä opas on pääosin käännetty Ranskan viranomaisten julkaisemasta ja englanniksi käännetystä oppaasta "Ransomware Attacks, All Concerned. How to Prevent Them and Respond to an Incident". *https://www.ssi.gouv.fr/uploads/2021/08/anssi-guide-ransomware_attacks_all_concerned-v1.0.pdf*

Opas ei kuitenkaan ole pelkkä käännös alkuperäisestä tekstistä, vaan siihen on tuotu elementtejä suomalaisesta ohjeistuksesta erityisesti julkishallinnon näkökulmasta. Kaikki mahdolliset virheet alkuperäisen tekstin tulkinnassa ovat kirjoittajan omia, mutta vastuu ohjeiden soveltamisesta omaan organisaatioon on lukijalla.

Muita suomenkielisiä oppaita aiheesta on esim. Viestintäviraston julkaisu 005/2016 "Selviytymisopas kiristyshaittaohjelmia vastaan – Kokemuksia kiristyshaittaohjelmista Suomessa ja neuvoja niistä selviytymiseen". *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teema-kooste_07_2016.pdf.* *Lisää oppaita ja ohjeita löydät linkkilistasta tämän oppaan lopussa.*

Sisältö

Pieni sanasto

Käsite	Selitys
Haittaohjelma Malware	Haittaohjelma on yleiskäsite tai kattotermi tietokoneohjelmille, jotka tarkoituksellisesti aiheuttavat ei-toivottuja tapahtumia tietokoneessa tai tietojärjestelmässä. Haittaohjelmia voi jaotella sen mukaan, miten ne leviävät, suoritetaan tai mitä ne tekevät.
Troijalainen Trojan horse	Alun perin ohjelma, joka näyttää hyödylliseltä, mutta sisältää piilotettuja haitallisia piirteitä. Nykyisin troijalainen on yleisesti käytetty synonyymi haittaohjelmalle.
Lunnastroijalainen Kiristyshaittaohjelma Ransomware Cryptolocker	Kiristyshaittaohjelma salakirjoittaa uhrin tiedostot, jonka jälkeen verkkorikolliset vaativat lunnaita tiedostojen salauksen purkamisesta. Usein kiristyshaittaohjelma naamioidaan viranomaisen viesteiksi, joissa vaaditaan sakkoja jostain käyttäjän väitetystä toiminnasta. Toinen yleinen tapa on ilmoittaa tietokoneen käyttäjälle, että hänestä on olemassa arkaluontoista (esim. sextortion) tai muuten tärkeää materiaalia, jonka vastineeksi vaaditaan lunnaita. Oikeasti sellaista aineistoa ei ole. Troijalainen on piilossa jossain ihan tavallisessa ohjelmassa (esim. videossa tai pienohjelmassa, kuten näytönsäästäjässä). Sen avulla verkkorikollinen pääsee käyttäjän tietokoneen sisälle ja voi käyttää sitä omiin tarkoituksiinsa: esimerkiksi levittämään haittaohjelmia tai roskapostia. Pahimmassa tapauksessa verkkorikollinen pääsee lukemaan tallennetut salasanat ja muita tärkeitä yksityisiä tietoja.
Vakoiluohjelma Spyware	Vakoiluohjelmat keräävät tietokoneesta käyttäjän tietoja, esimerkiksi henkilötietoja, joita voitaisiin hyödyntää mainostamisessa. Ne voivat myös seurata internetissä tapahtuvaa toimintaa. Yleensä näitä tietoja käytetään roskapostin levittämiseen.
Virus Tietokonevirus Computer virus	Tietokonevirus on tietokoneohjelma, joka leviää laitteesta toiseen ja pyrkii häiritsemään niiden toimintaa. Vähäisimmillään virukset voivat olla käyttäjälle kiusallisia, mutta ne voivat aiheuttaa myös ihan oikeaa tuhoa käyttöjärjestelmälle tai tietokoneelle. Tietokonevirukset leviävät usein liitteinä sähköposteissa ja pikaviesteissä. Jos et tunnista viestin lähettäjää tai saat odottamatta liitetiedostoja sähköpostiisi, älä avaa tiedostoa. Virus voi tulla myös erilaisten netistä ladattavien ohjelmien mukana. Siksi kannattaa harkita, millaisilta sivustoilta niitä lataa. Ensimmäiset haittaohjelmat syntyivät ennen kuin mikrotietokoneet olivat kytkettynä Internettiin. Ne levisivät passiivisesti kytkemällä itseensä tiedostoihin ja levykkeisiin, ja odottamalla että niitä siirretään toiseen tietokoneeseen. Analogia biologisiin viruksiin oli siis ilmiselvä. Haittaohjelmat leviävät nykyisin eri tavalla, mutta virus on silti yhä yleisesti käytetty synonyymi haittaohjelmalle. Nykyisin puhtaasti viruksiksi määriteltyjä ohjelmia ei juuri ole. Virus on kuitenkin säilynyt puhekielessä ja usein viruksiksi sanotaan kaikenlaisia haittaohjelmia.

Anti-virus	Perinteinen nimitys ohjelmalle, jonka tarkoituksena on tunnistaa haittaohjelma ja estää sen pääsy organisaation verkkoon tai käyttäjän tietokoneelle. Nykypäivän tilannetta paremmin kuvaava nimi olisi Anti-haittaohjelma, koska viruksia ei nykyisin enää käytännössä ole, vaan on troijalaisia, kiristysohjelmia, pelotteluohjelmia, matoja, vakoiluohjelmia, mainosohjelmia ja tiedostottomia haittaohjelmia. Näistä lisää voi lukea verkosta esim. googlettamalla ”haittaohjelma” tai ”malware”. Anti-virus nimi on jäänyt kieleen, koska se on ollut pitkään käytössä ja on sama sana sekä suomeksi, että englanniksi.
Loki Lokitus Log	Loki tarkoittaa aikajärjestyksessä kirjattua tallennetta tapahtumista ja niiden aiheuttajista. Tapahtumat ja muutokset tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöissä kirjataan lokiin, eli lokitetaan
Verkkorikollinen Cyber criminal	Rikollinen tai rikollisjoukko (voi myös olla valtiollinen toimija), jonka tarkoituksena on tehdä rikoksia tietoverkkoa hyväksikäyttäen. Rikollinen voi olla missä päin maailmaa tahansa, jonka vuoksi verkkorikollisten kiinnisaaminen on äärimmäisen vaikeaa ja vaatii viranomaisilta globaalia yhteistyötä. Motiivina on useimmiten raha tai tiedon/datan avulla sen hankkiminen. Motiivina voi myös olla kosto tai poliittinen teko.
Varmuuskopiointi Backup	Varmuuskopioinnilla tarkoitetaan yleensä tapahtumaa, jossa jokin tärkeä tieto kopioidaan ja varastoidaan. Jos alkuperäinen tieto häviää tai tuhoutuu, voidaan tieto palauttaa varmuuskopioista. Varmuuskopioita tulisi aina säilyttää fyysisesti erillään tilasta, jossa kopioitavat tiedot ovat vähentäen näin riski niiden tuhoutumisesta alkuperäisten tietojen kanssa esim. tulipalossa.
Tietoturvallisuus tai Tietoturva Information Security	Järjestelyt, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus. *Nykyisin tietoturvallisuus, kyberturvallisuus ja digitaalinen turvallisuus käsitetään puhekielessä samoiksi asioiksi ja niitä sekoitetaankin sujuvasti myös ammattilaisten puheissa. Todennäköisesti vaikeaselkoiseksi ymmärretty ”kyberturvallisuus” tulee sanana katoamaan ja koska digitaalisuus ja fyysinen maailma menevät entistä tiukemmin yhteen, tullaan jatkossa puhumaan vain ”turvallisuudesta” tai ”digitaalisesta turvallisuudesta”, jos halutaan erotella digitaalinen ja fyysinen turvallisuus.*
Kyberturvallisuus Cyber Security	Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Kybertoiminta- ympäristön synonyyminä voidaan käyttää termiä digitaalinen toimintaympäristö. **Perinteisempi määritelmä:** Kyberturvallisuus on turvallisuuden osa-alue, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin. Kyberturvallisuusajattelussa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelua. Yhteiskunnan elintärkeitä toimintoja ovat johtaminen, kansainvälinen toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus, väestön toimintakyky ja palvelut sekä henkinen

	kriisinkestävyys. Lue lisää Yhteiskunnan turvallisuusstrategiasta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf
Digitaalinen turvallisuus Digital Security	Usein kyberturvallisuuden synonyymi. Digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaa ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita. Terminä uusi ja vakiintumaton. Kansainvälistä yhteisymmärrystä termeistä ei ole.
Riskienhallinta Risk Management	Järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet.
Jäännösriski Residual Risk	Riskiin käsittelyn jälkeen jäävä riski, jota ei voida tai ei haluta poistaa. Jäännösriskeihin voi sisältyä tunnistamattomia riskejä.
Jatkuvuuden hallinta Continuity Management	Organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa.
Varautuminen Preparedness	Toiminta, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa.

Lisää sanastoja verkossa

Rikosuhripäivystys – Verkon sanasto haltuun
https://www.riku.fi/rikosuhripaivystys/riku-lehti/riku-lehti-2-2017/verkon-sanasto-haltuun/

Kyberturvallisuuden sanasto (2018)
https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Kokonaisturvallisuuden sanasto (2017)
https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

TEPA Termipankki – Erikoisalojen sanasto ja sanakirjojen kokoelma TSK
https://termipankki.fi/tepa/fi/

1 Pikaohje

Jotta lukija saisi nopean tilannekuvan aiheen sisällöstä olen sisällyttänyt tähän alkuun pikaohjeen, jossa keskeiset asiat on koottu yhteen taulukkoon. Tee tästä itsellesi vaikka huoneentaulu!
Lähteenä on pääasiassa ”No More Ransom” -projektin tiivistetty ohjeistus osoitteessa https://www.nomoreransom.org/fi/prevention-advice-for-businesses.html

KIRISTYSHAITTAOHJELMAHYÖKKÄYSTEN TORJUNNAN PIKAOHJE	
Hyökkäykseen varautuminen	**Jos hyökkäys on onnistunut**
1. Pidä organisaatiolaitteiden käyttöjärjestelmät ja sovellukset ajan tasalla. 2. Tunnista erityisen arvokkaat tietosi ja säilytä niitä hajautetusti. 3. Käytä turvattua etäkäyttöyhteys protokollaa (RDP) jos et muuten voi rajoittaa resurssien käyttöä verkon kautta. 4. Valvo tietoliikennettä datan kaappaamisen huomaamiseksi. 5. Testaa järjestelmiä säännöllisesti tunkeutumistestauksella verkon tietoturvaa vastaan ja tärkeiden tietojen palautusprosessia. 6. Vähennä haitallisen sisällön todennäköisyyttä päästä verkkoosi. 7. Käytä vahvoja salasanoja ja vaihda niitä säännöllisesti. 8. Käytä vahvaa monivaiheista todennusta aina kun se on mahdollista. 9. Hallitse etuoikeutettujen (admin) tilien käyttöä. 10. Suojaa etätyövälineet salaamalla kiintolevyt, ottamalla käyttöön käyttämättömyyden aikakatkaisu, vahva todennus ja tietosuojakalvot sekä siirrettävän median hallinta (USB-liitettävät muistit). 11. Lataa applikaatioita vain luotettavista lähteistä. 12. Ole varovainen käsitellessäsi organisaation tietoja julkisen Wi-Fi verkon kautta. 13. Tarjoa henkilökunnallesi kyberturvallisuuskoulutusta sekä pyri lisäämään tietoisuutta. 14. Tutustu kybervakuutukseen. 15. Kytke päälle paikalliset palomuurit. 16. Poista Windows PowerShell käytöstä.	1. Älä sammuta hyökkäyksen kohteena olevaa laitetta, mutta irrota se internetyhteydestä 2. Harkitse myös onko tarpeen sammuttaa koko Wi-Fi verkko, verkkokytkimet ja koko internet yhteys organisaation tiloista. Tämä saattaa olla edessä vakavissa tilanteissa haittaohjelman leviämisen estämiseksi. 3. Nollaa kaikki salasanat aloittaen pääkäyttäjien salasanoista. 4. Tee rikosilmoitus ja ilmoita tarpeen mukaan Kyberturvallisuuskeskukselle, Tietosuojavaltuutetun toimistoon (jos henkilötiedot vaarassa) ja sidosryhmille. 5. Säilytä kaikki todisteet hyökkäystä tutkivaa toimivaltaista viranomaista varten: Luo forensinen kopio haavoittuneista järjestelmistä tai ota tilannekuvakopio (snap-shot) järjestelmästä. Käytä apuna asiantuntijoita tai alan yrityksiä, jos olet epävarma, miten toimia. Säilytä kaikki verkkoliikennelokit. 6. Vieraile sivustolla www.nomoreransom.org tarkistaaksesi, onko yrityksesi joutunut sellaisen kiristyshaittaohjelman kohteeksi, johon on kehitetty ilmainen salauksenpurkutyökalu . **Jos näin ei ole, etene seuraavaan vaiheeseen.** 7. Tyhjennä hyökkäyksen kohteena olleet laitteet turvallisesti ja asenna käyttöjärjestelmä uudestaan. 8. Palauta tiedostot varmuuskopioista, mutta varmista ensin, ettei siinä ole haittaohjelmaa. 9. Yhdistä laitteet turvallisesti verkkoon, jotta voit ladata, asentaa ja päivittää käyttöjärjestelmän ja kaikki muut ohjelmistot. 10. Lataa, päivitä ja suorita haittaohjelmien torjuntaohjelmisto. 11. Muodosta uudelleen verkkoyhteys. 12. Seuraa verkkoliikennettä ja suorita haittaohjelman torjuntaskannauksia, jotta voit havaita mahdolliset jäljelle jääneet haitat.

2 Johdanto

Kaikki organisaatio, pienet ja suuret, julkiset ja yksityiset, Suomessa, Euroopassa ja maailmalla, ovat nyt ja entistä enemmän tulevaisuudessa riippuvaisia digitalisaatiosta. Kaikki mikä voidaan digitalisoida, tullaan digitalisoimaan. Digitalisaatio ulottuu kaikille elämän aloille, koska sen edut ovat kiistattomat ja selvästi havaittavissa. Meillä on valtavasti palveluita, joihin digitalisaatio on tuonut ylivoimaisia etuja ja saavutettavuutta. Digitalisaation lähtökohtana on kuitenkin, että organisaatiot voisivat luottaa digitaalisen ympäristön turvallisuuteen. Samalla kun digitaalisuus tuo uusia mahdollisuuksia, on digitaalinen maailma täynnä erilaisia riskejä. Erityisen vahingolliseksi on viime aikoina noussut uhka kiristyshaittaohjelmista ja riski joutua verkosta tulevan kiristyksen uhriksi. Kiristyshaittaohjelmaan perustuvalla kyberhyökkäyksellä on dramaattiset vaikutukset uhriin, mutta riskin vähentämiseen siedettävälle tasoille, on hyvät mahdollisuudet nostamalla tietoisuuttaa tästä riskistä ja ottamalla käyttöön hyviä käytänteitä.

Kiristyshaittaohjelmat ovat yksi suurimmista organisaation toimintaa uhkaavista tekijöistä. Rikolliset saavat rikoshyötynä vuosittain satoja miljoonia euroja kiristyshaittaohjelmien avulla. Kiristyshaittaohjelmilla on vakavat vaikutukset liiketoiminnan jatkuvuuteen tai jopa organisaation kykyyn selviytyä ja jatkaa olemassaoloaan. Hyökkäysten laajuus ja säännöllisyys sekä niiden hienojakoisuus ja kehittyneisyys ovat nousseet merkittävästi. Jokaisen valtion ja organisaation tulisi varautua näiden uhkien torjumiseen sekä kanallisella, että kansainvälisellä tasolla. Suomessa kyberturvallisuuskeskus on tehnyt jo vuosikymmenen hyvää työtä myös kiristyshaittaohjelmien torjunnassa, mutta se ei yksi riitä, vaan tarvitaan aktiivista toimintaa ja osaamisen kehittämistä myös jokaisessa digitaalisen yhteiskunnan organisaatiossa.

ISACA (Information Systems Audit and Control Association) on kansainvälinen hallinnollisen johtamisen asiantuntijajärjestö, joka toimii yli 180 maassa ja palvelee yli 145.000 jäsentään järjestämällä koulutusta, resurssienjakoa, tukea, verkostoitumista ja muita etuja. Nykyään sen jäsenet toimivat mitä erilaisimmilla ammattinimikkeillä vakuutusalalla, hallinnollisissa tehtävissä sekä riski- ja tietoturvatehtävissä ympäri maailmaa. Järjestö julkaisee näihin aloihin liittyviä uusia tutkimuksia ja resursseja säännöllisesti. ISACA:n vuoden 2020 raportin mukaan lausunto maailman muuttumisesta dramaattisesti vuonna 2020 ei ole liioiteltua, koronapandemia lieveilmiöineen on pitänyt siitä huolen. Teknologia on tullut avuksi koronan selättämisessä, sillä ihmisten linnoittautuessa koteihinsa tekemään työtä, teknologia mahdollistaa kommunikaation ja yhteistyön organisaatioiden työntekijöiden välillä fyysisen yhteyden puuttuessa. Tietoturva-alalla on tavattu sanoa, että liike-elämä toimii teknologian avulla – nykyisin maailma ei enää pysty pyörimään täysillä ilman teknologiaa, sillä se on globaali ratkaisu myös pandemiaan. Se on myös saanut tietoturva-alan ihmiset sopeutumaan nopeasti: he ovat nopeampia, joustavampia ja innovatiivisempia kuin ennen sekä uusien haasteiden että tuntemattoman edessä. Monet IT-organisaatiot kohtaavat taloudellista epävakautta ja pandemiasta johtuvaa pelkoa ja inhimillistä tragediaa hyödyntävät kyberrikolliset kehittävät uusia strategioita varastaakseen ja muuten häiritäkseen normaalia

toimintaa. Kyberturvallisuus on muuttunut entistä tärkeämmäksi, jotta yhteiskunta ja liikeelämä voivat toimia edelleen tehokkaasti [1]

ISACA listaa useita uhkakuvia perustuen alkuvuoden 2020 tapahtumiin:

- Tietoturvahyökkäykset ovat kasvussa, vaikka kasvukäyrä onkin loivempi kuin viime vuosikymmenellä.
- Tietoturvan toteuttaminen on edelleen hajallaan IT-osastojen harteilla. Vaikka monissa organisaatioissa on erillinen DevOps-toimintamalli, johon on keskitetty ohjelmistokehityksen, testauksen ja ylläpidon IT-palvelutoiminnot, kyberturvallisuudesta vastaavat toiminnot ovat edelleen kyselyn mukaan alimiehitettyjä ja ne ovat usein vain yksi työtehtävä IT-osastolla.
- Kyberrikokset ovat edelleen huonosti raportoituja. 62 % alan ammattilaisista uskoo organisaatioiden jättävän kyberrikokset ilmoittamatta, jopa silloin kun niillä olisi lain mukainen ilmoitusvelvollisuus.
- Tietoturvahenkilöiden vähyys yrityksissä vaikuttaa yrityksen operatiivisiin toimintoihin. Alan ammattilaisista 62 % ilmoittaa olevansa liian vähällä henkilökunnalla ja tietoturvaa ei silloin pystytä tuottamaan täydellä teholla.
- Kiristyshaittaohjelmat palasivat suosituimmaksi rahaa tuottavaksi strategiaksi kryptovaluutan louhimisen pidettyä johtoasemaa viime vuonna.

Erityisesti viimeinen kohta kertoo, miksi kiristyshaittaohjelmilta suojautumiseen kannattaa organisaatioissa, pienissä ja suurissa, käyttää resursseja.

3 Kiristyshaittaohjelmat ja oppaan tarkoitus

Lunnasohjelma tai lunnastroijalainen tai kiristyshaittaohjelma (ransomware) on verkon kautta leviävä haittaohjelma, jonka tarkoituksena on kiristää uhria maksamaan lunnaat. Kiristyshaittaohjelmaan perustuvan kyberhyökkäyksen tarkoitus on kerätä rahaa rikollisille. Tällä rahalla rahoitetaan terrorismia, ihmiskauppaa, huumekauppaa ja uusia kyberhyökkäyksiä. Rikollisten tulot ovat kasvaneet exponentiaalisesti viime vuosina ja puhutaankin miljardibisneksestä maailmanlaajuisesti. Käytän tässä oppaassa kuvaavaa kiristyshaittaohjelma nimikettä

Kiristyshaittaohjelmaan perustuvassa kyberhyökkäyksessä hyökkääjä estää uhrin tietokoneen käytön. Käytännössä suurin osa hyökkäyksistä tehdään niin, että kiristyshaittaohjelma salaa uhrin tietokoneen tai järjestelmän tiedot vahvalla salauksella, joka tekee tietokoneen käytön mahdottomaksi. Uhri siis menettää täysin pääsyn koneella oleviin tietoihin ja jos koneessa on kiinni ulkoinen kovalevy tai USB-muisti, voidaan myös sen tiedot salata. Tämän jälkeen hyökkääjä toimittaa selväkielisen viestin uhrille esim. tietokoneen ruudulle nousevan ikkunan kautta, jossa kerrotaan tietokoneen tietojen olevan salattu ja että tämä salaus voidaan purkaa, maksamalla lunnaat kiristäjälle. Yleensä maksua pyydetään

[1] Virta, T. (2020). ISO 27001 standardiin perustuva Tietoturvan johtamisen hallintamalli THL:lle.

virtuaalivaluuttana, kuten bitcoinina. Kiristäjä vielä neuvoo yksityiskohtaisesti, miten maksun saa suoritettua. Lunnaita ei kuitenkaan tule missään tapauksessa maksaa (tästä on eriäviä mielipiteitä, mutta pääsääntöisesti niitä ei kannata maksaa). Yksittäisen käyttäjän ja organisaation keinot välttää uhriksi joutuminen ja lunnaiden maksaminen, on tämän oppaan tarkoitus. Oppaassa annetaan ohjeita, miten hyökkäyksen kohteeksi joutumisen riskiä voidaan vähentää ja miten reagoida, jos on joutunut hyökkäyksen kohteeksi.

Tämän oppaan tarkoitus on antaa tietoa kiristyshaittaohjelmista ja niihin liittyvästä rikollisesta toiminnasta. On tärkeää ymmärtää, että kiristyshaittaohjelman uhriksi voi joutua kuka tai mikä tahansa, mutta tätä riskiä voidaan pienentää esim. tämän oppaan ohjeilla. Pahimmillaan uhriksi joutuminen voi vaarantaa koko organisaation (liike)toiminnan ja siksi tietoturvallisuus, kyberturvallisuus, digitaalinen turvallisuus sekä kyberhyökkäyksiin varautuminen on johdon asia. Tämä opas on tarkoitettu sekä operatiivisen toiminnan asiantuntijoille, että johdolle ja kaikille, jotka ovat kiinnostuneet tai pitäisi tehtäviensä puolesta olla kiinnostunut asiasta.

Organisaation ei tule tukeutua vain yhteen oppaaseen, vaan tulee käyttää eri lähteitä. Suomeksi saatavia lähteitä löytyy esim. Kyberturvallisuuskeskukselta, Tietosuojavaltuutetun toimistolta, poliisilta ja kaupallisilta yrityksiltä. Joitakin linkkejä on tekstissä ja oppaan lopussa on myös lyhyt linkkilista.

4 Trendit

Suurin osa kiristyshaittaohjelmaan perustuvista kyberhyökkäyksistä on opportunistisia ja niissä hyödynnetään kohteen matalaa digitaalisen turvallisuuden maturiteettitasoa. Kuitenkin vuodesta 2018 lähtien on ollut nousussa eri kyberrikollisryhmien tekemiä hyökkäyksiä, jotka kohdistavat hyökkäyksen yksittäisen henkilön kautta organisaatioon, joilla on huomattavaa varallisuutta tai kriittistä toimintaa. Tämä toiminta tuo kiristyshaittaohjelmiin perustuvat kyberhyökkäykset kategoriaan, josta käytetään nimitystä ”Big Game Hunting” (”suurriistan metsästystä”) viitaten hyökkäyksen kohteen kokoon. Vahvistaakseen hyökkäyksen ulottuvuutta, hyökkääjä joskus liittää hyökkäykseen yhden tai useamman muun haittaohjelman (kryptolouhija, troijalainen jne.) yhdessä kiristyshaittaohjelman kanssa. Se mahdollistaa tietokoneresurssien laittoman käytön haltuun otetussa järjestelmässä tai kaapata tietokoneella olevat tiedot omaan käyttöön. Näistä tiedoista analysoidaan esim. tietoja

Uutinen:
Nettikiristäjät iskevät yrityksiin – kannattaako lunnaita maksaa? (TIVI 11.10.2019)
https://www.tivi.fi/uutiset/nettikiristajat-iskevat-yrityksiin-kannattaako-lunnaita-maksaa/01d4b48a-cec2-4990-ba1e-ddafacaf527d

Uutinen:
”Lunnaiden maksaminen kiristäjille ei ole laitonta” – vakuutusyhtiöt puolustavat linjaansa (TIVI 27.1.2021)
https://www.tivi.fi/uutiset/lunnaiden-maksaminen-kiristajille-ei-ole-laitonta-vakuutusyhtiot-puolustavat-linjaansa/ff49c07f-7626-4027-a9dd-c7cc102fe9f3

organisaation likviditeetistä, jonka avulla voidaan määritellä, kuinka paljon organisaatiolla on varaa maksaa lunnaita. Rikolliset ovatkin viime aikoina palkanneet data-analyytikkoja tekemään tätä analyysia.

Toinen viimeaikainen trendi on, että kerättyjä arkaluonteisia tietoja uhataan julkaista, ellei lunnaita makseta. On selvää, että tällaisten hyökkäysten takana on rikollisryhmiä, joilla on sekä varallisuutta, että syvää teknistä osaamista. Osaajia voidaan hankkia esim. peiteyritysten kautta. Yritys saattaa julkisesti myydä penetraatiotestauskonsultaatiota, mutta todellisuudessa yritys toimii peitefirmana kyberrikollisille, jotka sekä kehittävät omaa hyökkäysosaamista, mutta myös keräävät organisaation luvalla (koska organisaatio on palkannut ne tekemään penetraatiotestausta) tietoa yrityksestä ja sen kumppaneista. Näiden rikollisryhmien taustalla voi myös olla valtioita, jotka ostavat palveluita rikollisryhmiltä, mutta voivat tarvittaessa kiistää olevansa missään tekemisissä niiden kanssa, jos rikollisryhmä jää kiinni jossain operaatiossa. Lunnaat, joita vaaditaan voivat olla satoja tuhansia euroja tai jopa miljoonia, riippuen kohteen maksukyvystä. Lisäksi nykyisin ovat lisääntyneet myös ns. toimitusketju hyökkäykset, jossa hyökkäyksen kohteena on jonkin alan avainyritys tai alihankintaa tekevä yritys, jonka kautta johonkin toimialaan kohdistuva epäsuorahyökkäys voi aiheuttaa epävakautta koko toimialalla. Tästä esimerkkinä oli SolarWinds -ohjelmistoyrityksen toimitusketjuun kohdistunut hyökkäys, joka oli laajuudessaan poikkeuksellinen. Muista esimerkkejä oli huhtikuussa 2021 tapahtunut Codecovin hakkerointi ja tuoreempi Kasey -tapaus. Tällaisten hyökkäysten vaikutukset ovat paljon pahemmat kuin datan menetys lunnaiden maksaminen. Uhriksi joutunut organisaatio voi joutua kokemaan monia seurauksia kuten tuotannon pysähtyminen, myynnin lasku, laista tulevat seuraukset (GDPR erityisesti henkilötietoihin liittyvän datan osalta), maineeseen liittyvä haitta, asiakkaiden luottamuksen menettäminen jne. Uhrin toimintakyky häiriintyy usein tai on muuten heikentynyt hyökkäyksen seurauksena. Yritysten tapauksessa jopa yrityksen selviytyminen voi olla vaakalaudalla. Esimerkiksi Suomessa terapiakeskus Vastaamo meni konkurssiin tietomurron johdosta. Tässä tapauksessa ei tosin ollut kyse kiristyshaittaohjelmasta, vaan törkeästä arkaluonteisten tietojen suojaamisen laiminlyönnistä ja sitä hyväksikäyttäneestä rikollisesta tai rikollisista. Vastaamon tapauksen rikostutkinta on kesken, eikä tekijää tai tekijöitä ole saatu kiinni.

Kiristyshaittaohjelma on vakava uhka sen pitkään kestävien seurausten johdosta niin yksilölle, kuin organisaatiollekin. Kiristyshaittaohjelmat tarjoavat rikollisille erittäin tuottoisan liiketoimintamallin. On tärkeää ymmärtää, että maksamalla lunnaat, uhriksi joutunut pitää yllä tätä liiketoimintaa, saamatta kuitenkaan varmuutta siitä, että saisi menettämänsä tiedot takaisin. Lunnaita ei siis koskaan pidä maksaa, vaan valmistautua etukäteen näiden hyökkäysten torjumiseen ja tarvittaessa niistä toipumiseen. Mainittakoon, että lunnaiden maksamisesta ollaan jonkin verran erimielisiä, mutta tämä opas lähtee siitä, että lunnaita ei pidä maksaa, koska se ruokkii uutta rikollisuutta.

5 Hyökkäysriskin vähentäminen

Tässä kappaleessa annetaan ohjeita, miten organisaatiossa voidaan vähentää riskiä joutua kyberhyökkäyksen kohteeksi pitämällä tietoteknisen ympäristön terveenä, estämällä kiristyshaittaohjelman vaikuttamasta organisaation toimintaan tai vähentämällä sen aiheuttamia menetyksiä.

5.1 Johdanto

Kiristyshaittaohjelman päätarkoitus on estää uhria käyttämästä tietojaan, tavallisesti salaamalla tiedot. Tätä uhkaa ajatellen perinteinen varmuuskopiointi on pääasiallinen keino vähentää tämän riskin toteutumista ja tietojen menettämistä kiristyshaittaohjelmaan perustuvassa hyökkäyksessä. Käytännön toimet kiristyshaittaohjelmiin perustuvien hyökkäysten torjunnassa ovat tuttuja yleensä tietoturvallisuuden parantamiseen liittyvinä keinoina: ohjelmistojen tietoturva-aukkojen tukkiminen päivittämällä ohjelmistot ja käyttöjärjestelmä, pitämällä anti-virus ohjelman virustietokannat päivitettynä (yleensä tämä on automatisoitu), ottamalla käyttöön suodatustoimenpiteitä työasemissa ja poistamalla pääkäyttäjän oikeudet työasemien käyttäjiltä.

Lisäksi syvyyteen perustuvan puolustusperiaatteen soveltaminen tietojärjestelmien eri osiin vähentää riskiä kriittisen tiedon ja tietojärjestelmän joutumisesta kiristyshaittaohjelman uhriksi. Tämä tarkoittaa, että verkko segmentoidaan eri osiin ja näiden osien välillä on rajoitetut pääsyoikeudet käyttäjillä ja järjestelmien välisellä liikenteellä. Tärkeimmät tiedot ja järjestelmät ovat syvällä organisaation verkossa ja rajoitetun verkkoliikenteen takana internetistä katsoen ja näin voidaan heikentää hyökkäyksen vaikutusta kriittiseen tietoon ja järjestelmiin.

Viimeisenä mainittakoon, että on tärkeää lisätä käyttäjien tietoisuutta riskeistä, selvittää onko mahdollista ottaa organisaatiolle kyberturvavakuutus, valmistautumalla ja harjoittelemalla kyberhyökkäyksiin vastaamista sekä siihen liittyvää kommunikaatioita ja viestintää kriisiviestinnän periaatteilla. Organisaatiolla pitää olla selvillä vastuut ja toimenpiteet kyberhyökkäyksen kohdatessa ja tärkeää on myös määritellä vastuullisten varahenkilöt, ettei toiminta katkea kesälomiin tai sairaspoissaoloon. Seuraavassa käydään näitä eri keinoja läpi.

5.2 Varmuuskopiointi

Perinteinen ja arkinen kaikkien tietojen varmuuskopiointi sisältäen tiedostoissa olevat tiedot ja infrastruktuurin ja kriittisten tietojärjestelmien palvelimet, on asia, joka on tehtävä jatkuvasti ja säännöllisesti. On syytä muistaa, että myös nämä tiedostot voivat kiristyshaittaohjelma hyökkäyksessä kohteena. Itseasiassa yhä useammat kyberrikolliset tähtäävät varmuuskopioihin kohdistuviin hyökkäyksiin, jonka tarkoituksena on vähentää uhrin kykyä toipua hyökkäyksestä ja näin ollen maksimoida mahdollisuus kiristykseen suostuminen ja lunnaiden maksaminen.

Varmuuskopioista on syytä olla yksi versio tai ainakin kriittiset tiedot fyysisesti irti operatiivisen toiminnan tietoverkosta, jotta voidaan estää niiden salakirjoittaminen kiristyshaittaohjelmaan perustuvan hyökkäyksen yhteydessä, muiden tiedostojen tavoin. Tämän ns. ”kylmäsäilytys ratkaisun”, kuten ulkoisen kovalevyn tai magneettinauhan, käyttö suojaa varmuuskopioita järjestelmän infektoitumiselta ja säilyttää kriittiset tiedot palauttamista varten kriisin jälkeen. On tärkeää huomata, että varmuuskopioton arkkitehtuuri[2], jolla suojaudutaan tietojen häviämistä vastaan laitteiden rikkoontumisen tapauksissa, ei suojaa järjestelmää kiristyshaittaohjelmaan perustuvassa kyberhyökkäyksessä, koska hyökkäyksessä salataan kaikkien palvelimien data, myös niiden, joissa nämä nämä snap-shotit ovat.

Muista varmuuskopiot

Tee tärkeimmistä tiedoista ja palveluista varmuuskopiot. Säilytä varmuuskopiot erillään suojattavista järjestelmistä ja tiedoista, ettei esimerkiksi kiristyshaittaohjelma tee myös varmuuskopioista käyttökelvottomia. Testaa varmuuskopioiden palauttamista säännöllisesti, esimerkiksi vuosittain. Näin varmistut, että varmuuskopioiden palauttaminen onnistuu ja tarvittavat järjestelmäasetukset on varmuuskopioitu.

- Kyberturvallisuuskeskus: Suojaudu tietomurroilta. -

5.3 Ohjelmistojen ja järjestelmien pitäminen ajantasaisena

Päivittämättömiä haavoittuvuuksia käyttöjärjestelmässä ja ohjelmistossa voidaan käyttää hyväksi tietojärjestelmien vaarantamiseksi tai haittaohjelman levittämiseksi. Päivitykset mukaan lukien suojauskorjaukset (security patches) täytyy säännöllisesti ajaa järjestelmiin ratkaisun toimittajan toimesta. On erityisen tärkeää asentaa ne heti kun mahdollista, noudattamalla ennalta sovittua, selkeää prosessia. Jos päivitysten ajaminen ei ole mahdollista esim. liiketoiminnallisista syistä (esim. liiketoimintasovelluksia ei voida keskeyttää järjestelmän uudelleen käynnistämisen ajaksi), täytyy kyseessä olevat järjestelmät eristää ennalta sovitulla tavalla siksi aikaa, kunnes ne voidaan päivittää.

Päivitysten osalta erityisesti tulee kiinnittää huomiota käyttäjän työasemalle asennettuihin ohjelmiin (verkkoselain, toimisto-ohjelmat, PDF lukijat, multimedia soittimet, jne.). Laitteistojen elinkaaren ennakointi ja hallinta on tärkeää, jotta ne voidaan pitää ajan tasalla. Tällä hetkellä esim. Windows 7 käyttöjärjestelmään ei saa enää päivityksiä kuin lisämaksusta, vaikka se edelleen on käytössä kymmenissä miljoonissa tietokoneissa.

[2] Varmuuskopioton arkkitehtuuri (backup-less architectures) tarkoittaa järjestelmää, jossa järjestelmästä otetaan valokuva (snap-shot), jota käytetään tarvittaessa palautukseen perinteisen varmuuskopioinnin sijasta.

Samalla tavalla organisaation internettiin näkyviä resursseja, joita ei ole päivitetty (sähköposti, verkkopalvelut, extranet, jne.) käytetään jatkuvasti hyväksi hyökkääjien toimesta. Sen vuoksi näihin palveluihin on erityisen tärkeää ajaa suojauspäivitykset heti kun mahdollista.

Pidä ohjelmistot ja järjestelmät päivitettynä

Tietomurtojen torjunnan kannalta on erittäin tärkeää pitää järjestelmien ja laitteiden päivitykset ajan tasalla. Suuri osa ohjelmistopäivityksistä sisältää haavoittuvuuksien korjauksia, joten ne on syytä asentaa pian niiden julkaisemisen jälkeen. Haavoittuvilla järjestelmillä on aina suurempi riski joutua tietomurron kohteeksi.
- Kyberturvallisuuskeskus: Suojaudu tietomurroilta. -

Lisäksi jokaisessa organisaatiossa tulee olla henkilöitä, joiden tehtävä on jatkuvasti seurata ohjelmistojen ja laitteiden haavoittuvuuksia eri lähteistä. Erityisesti Kyberturvakeskuksen haavoittuvuusilmoitukset auttavat tässä työssä, mutta sen lisäksi kannattaa ottaa seurantaan esim. käyttöjärjestelmän (kuten Microsoft tai Apple) toimittajan oma sivusto ja muita kansainvälisiä, haavoittuvuuksiin keskittyviä sivustoja (tietokantoja) kuten NIST, CVE, SNYK ja Exploit Database. Linkit näihin on kohdassa ”Linkkejä”.

5.4 Anti-virusohjelmien käyttö ja ylläpitäminen

Anti-virus ohjelmisto on vähimmäisvaatimus suojeltaessa työasemia, tiedostopalvelimia ja muita julkisessa verkossa olevia resursseja kiristyshaittaohjelmien hyökkäyksiltä. Nämä työkalut suojaavat vain tunnetuilta haittaohjelmilta, mutta ei nollapäivähaavoittuvuuksilta[3] ja muilta tuntemattomilta uhilta, mutta useissa tapauksissa anti-virus -ohjelmisto suojaa riittävästi näitä resursseja ja estää tiedostojen salakirjoittamisen. Jotta nämä työkalut olisivat tehokkaita, pitää huolehtia siitä, että ne ovat päivitettyjä ja ajan tasalla. On tärkeää, että anti-virusohjelmiston virustietokannat ovat ajan tasalla sekä että suojattavat tiedostot tarkistetaan säännöllisesti tunnetuilta haittaohjelmilta skannaamalla tietokone anti-virusohjelmalla sekä muistitikut ja muut ulkoiset muistivälineet aina, kun ne liitetään tietokoneeseen USB-portin kautta.

5.5 Tietoverkkojen segmentointi

Tietoverkkojen segmentoinnilla tarkoitetaan verkon jakamista osiin ja suojaamista niiden väliseltä liikenteeltä. Ilman suojausta yksittäinen saastunut tietokone levittää haittaohjelmaa verkon kautta kaikkiin samassa segmentissä oleviin koneisiin. Tietoverkko, joka ei ole segmentoitu pienempiin ja toisistaan loogisesti eroteltuihin osiin, mahdollistaa hyökkääjien laajamittaisen verkossa olevien tietokoneiden saastuttamisen ja haltuunoton. Pahimmillaan hyökkääjä saa pääsyn pääkäyttäjän oikeuksiin, toimintoihin ja laitteisiin.

Riskin rajaamiseksi yksi tai useampi verkon suodattava komponentti (yleensä palomuuri) pitää olla asennettuna verkkosegmenttien väliin, joilla on erilainen turvallisuustaso. Jako voi olla esim. sisäinen palvelinverkko, palvelinverkko internetiin näkyville palveluille,

[3] Nollapäivähaavoittuvuus (Zero Day Vulnerability) tarkoittaa tietoturva-aukkoa, jolle ei ole olemassa korjausta, mutta haavoittuvuudelle on olemassa hyväksikäyttömenetelmä.

työasemaverkko, pääkäyttäjä verkkoalue, jne. Hallintotason verkon segmentointi voidaan myös ottaa käyttöön varmistaakseen, että korkeimman johtotason käyttäjät ovat vaikeasti saavutettavissa hyökkäyksen kautta. Suomessa viranomaisten käyttämä hallinnon turvallisuusverkko (TUVE) on erityisen tarkasti suojattu ulkoisiltä hyökkäyksiltä. Verkosta vastaa Valtion tieto- ja viestintätekniikka keskus, Valtori. Lisätiedot osoitteesta https://valtori.fi/etusivu

Näiden lisäksi yhteyden käyttäjien työasemien välillä pitää olla lähtökohtaisesti estetty. Työaseman sovelluspohjainen palomuuri estää data liikkumisen työasemien välillä ja näin ollen vähentää riskiä kiristyshaittaohjelman leviämiselle työasemasta toiseen.

5.6 Käyttöoikeuksien ja sovellusten oikeuksien rajoittaminen

Ensimmäiseksi kannattaa tarkistaa, että työaseman käyttäjillä ei ole pääkäyttäjän oikeuksia työasemassaan. Ohjelmien asentaminen ja haitallisen koodin ajaminen työasemassa tulee näin ollen oletusarvoisesti mahdottomaksi.

Toinen hyvä keino tässä kohdassa on ottaa käyttöön vain ylläpitoon dedikoidut työasemat. Näissä työasemissa on vain ylläpitoon tarkoitetut sovellukset eikä niissä saa olla mitään ylimääräistä asennettuna. Työasemissa ei myöskään saa olla internetyhteyttä (aivan, luit oikein). Hyökkääjä pyrkii aina löytämään korkean tason käyttöoikeuksia, jos se saa verkon pääkäyttäjän oikeudet, on peli menetetty eikä millään voida estää hyökkääjän etenemistä verkon resursseissa sillä hetkellä. Edellä mainituissa ”Big Game Hunting” tapauksissa erityisesti pyritään saamaan verkon pääkäyttäjän oikeudet ja niiden avulla levittää kiristyshaittaohjelmaa kaikkialle verkkoon, jotta tiedostojen salaaminen olisi mahdollisimman täydellistä. Kyseessä voi siis olla koko organisaation olemassaoloa uhkaava toiminto, jos hyökkääjällä on pääkäyttäjän oikeudet verkossa. Pääkäyttäjän oikeuksilla varustettuja käyttäjiä pitäisikin olla hyvin rajoitettu minimi määrä ja erityistä huomiota tulisi kiinnittää niiden käyttöön. Pääkäyttäjänkin tulisi normaalisti operoida vain peruskäyttäjän oikeuksilla ja vain tarvittaessa käyttää pääkäyttäjän oikeuksia varsinkin, jos työasemaa käytetään muuhun kuin ylläpitoon. Näillä rajoituksilla voidaan estää kiristyshaittaohjelmaa toimimasta tai rajoitetaan sen kykyä salakirjoittaa tiedostoja.

Kiristyshaittaohjelman avulla tehtyä kyberhyökkäyksen riskiä voidaan tietoverkossamme pienentää kovettamalla[4] (hardening) työasemia, palvelimia, usein käytettyjä sovelluksia erityisesti sellaisia, joita käytetään internetistä, kuten sähköposti. Windows ympäristössä voidaan lisäksi ottaa käyttöön joitakin lisäturvaa tuovia komponentteja, kuten Windows Defender ATP ja Windows Applocker). Näistä voi lukea lisää Microsoftin sivustoilta.

5.7 Internetyhteyden rajoittaminen

Kiristyshaittaohjelmat usein käyttävät internet yhteyttä kommunikoidakseen infrastruktuurin kanssa, jota isännöi verkossa kyberrikolliset. Jos organisaation työntekijä tai muu

[4] Kovettaminen eli hardening tarkoittaa ei-välttämättömien ominaisuuksien poistamista käytöstä, kuten avoimien verkkoporttien sulkeminen tai macrojen poistaminen käytöstä.

käyttäjä menee kyberrikollisten isännöimälle verkkosivulle, hän saattaa tietämättään ladata ja aiheuttaa haittaohjelman automaattisen asennuksen työasemalleen. Haittaohjelma saa näin pääsyn organisaation verkkoon.

Turvallisen internet yhteyden käyttöönotto, joka estää haitallisten ohjelmien saamisen verkkoselaimen kautta, nojaa siihen, että otetaan turvallisuustoimintoja esim. proxy -palvelin verkkosivustojen lataamiseen (web liikenne) ja oma DNS palvelin verkkosivujen nimipalveluksi. Näillä vähennetään kiristyshaittaohjelmiin liittyviä riskejä. Lisäksi näillä voidaan suodattaa yhteydenotto organisaation työntekijöiltä verkkosivuille, joilla on tunnetusti maine tai ovat muuten kategorisoitu haittaohjelmien levittäjinä. Samoin voidaan tunnistaa epänormaalia toimintaa, kuten isojen tiedostojen lähettämistä tietojärjestelmästä palvelimelle käytössä olevien operaattoreiden palveluiden ulkopuolelle.

5.8 Lokiin perustuvan valvonnan käyttöönotto

Tietojärjestelmien tietoturvatapahtumien tarkkailemiseksi ja käytön jälkiselvittelyyn esim. tietomurtotapauksissa, tarvitaan lokienhallintajärjestelmää erilaisissa tiedonhallintajärjestelmissä. Näihin kuuluvat järjestelmän infrastruktuurin palvelimet, pääkäyttäjien ja muiden käyttäjien työasemat, liiketoimintajärjestelmien palvelimet sekä tietoverkko- ja turvallisuuslaitteistot, jotka sijaitsevat sekä tietojärjestelmien reunoilla, että keskiössä. Näitä ovat esim. Active Directory (AD) ja Domain Controller (DC) palvelimet, nimipalvelimet (Domain Name Servers, DNS) sekä erilaiset välityspalvelimet (proxies).

Tietokoneet, puhelimet, reitittimet ja operaattorit keräävät säännöllisesti lokitietoja käyttämistämme laitteista. Lokien avulla asiat varmistetaan, virheet korjataan ja tietomurrot havaitaan. Huolehdi siitä, että järjestelmiesi lokien keräys on kunnossa.

On huomattava, että julkisen hallinnon toimijalla on Lain julkisen hallinnon tiedonhallinnasta (tiedonhallintalain) 17 § nojalla velvollisuus tallentaa lokitapahtumat luovutus- ja käyttölokin osalta. Lisätietoa aiheesta oheisessa tietolaatikossa.

Lokiohjeita

Laki julkisen hallinnon tiedonhallinnasta
https://www.finlex.fi/fi/laki/alkup/2019/20190906

Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamiseksi (2020)
https://julkaisut.valtioneuvosto.fi/handle/10024/162433

Kyberturvallisuuskeskuksen lokiohje (2020)
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

VAHTI lokiohje (2009)
https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-32009-lokiohje

Lokien hallinta osana tiedonhallintalain vaatimuksia (opinnäytetyö (2020)
https://www.theseus.fi/bitstream/handle/10024/423456/ONT_MinnaRyyppo_lopullinen.pdf?sequence=2&isAllowed=y

Lokitiedot kertovat, mitä, miksi ja milloin jotakin tapahtui. Tiedoilla selvitetään virhetilanteita, tai varmistetaan että virheitä ei ole syntynyt ja käsitelty tieto on oikeaa. Ilman

asianmukaista lokitietoa virheiden syitä on mahdoton selvittää ja niiden korjaaminen hyvin vaikeaa. Usein järjestelmiltä vaaditaan tiedon kiistämättömyyttä ja autenttisuutta, minkä todistaminen vaatii monipuolista lokitusta. Lokitietoja säilytetään riittävän pitkään, jotta niihin voidaan tarpeen vaatiessa palata pitkänkin ajan kuluttua. Tietoturvapoikkeamien havainnoimiseksi lokeja voidaan analysoida joko reaaliaikaisesti tai jälkeenpäin.

5.9 Työtekijöiden tietoisuuden lisääminen ja tietoturvakulttuuri

Kiristyshaittaohjelmahyökkäykset alkavat usein, kun sähköpostin liitteenä tullut epämääräinen liite avataan tai ollaan vierailemassa jossain ilkeämielisellä verkkosivulla. Käyttäjien kouluttaminen havaitsemaan erilaiset hyökkäysyritykset ja kehittämään omia digitaalisen turvallisuuden taitoja, ovat näin ollen ensiarvoisen tärkeitä taistelussa näitä verkkorikollisia vastaan, vaikkakin pelkästään käyttäjien toiminnalla ei täydellisesti estetä kiristyshaittaohjelmien aiheuttamaa uhkaa. Käyttäjät ovat silti avainasemassa, koska mikään tekninen turvallisuusratkaisu ei kokonaan poista käyttäjien kautta tulevien hyökkäysten uhkaa organisaation järjestelmiin. Kouluttamalla käyttäjiä heille kehittyy kyky tunnistaa erilaiset hyökkäysyritykset ja kynnys raportoida niistä eteenpäin madaltuu. Käyttäjät ovat tietoturvasta vastaavien ihmisten silmät ja korvat koko organisaatiossa siellä missä teknisiä valvontajärjestelmiä ei ole. Kiristyshaittaohjelmat tulevat usein organisaation verkkoon esim. USB-tikkujen kautta, joten kouluttamalla käyttäjiä vähennetään myös tätä fyysisestä maailmasta tulevaa uhkaa. Hyökkäystapana voi olla, että kohdeorganisaation parkkipaikalle pudotetaan haittaohjelman sisältäviä USB-tikkuja tai niitä jaetaan messuilla jollakin tekosyyllä (esim. hieno valo tietokoneeseen, joka saa virtansa USB-tikun kautta). Näitä ei käyttäjät ehkä osaa ajatella uhkina, ellei niistä ole puhuttu koulutuksissa tai tietoiskuissa. Samoin sähköpostin kautta tulevat haitalliset liitteet tai epämääräiset pyynnöt vieraille verkkosivuilla eivät välttämättä nouse esille, ellei niiden havaitsemiseen kouluteta. Tietoturvatietoinen ihminen on organisaation vahvin lenkki verkkorikollisia vastaan.

Tietoisuuden kehittämiseen on erilaisia keinoja riippuen organisaation koosta, työntekijöiden määrästä, organisaation toiminnasta ja merkityksestä, vaikka osana yhteiskunnan kokonaisturvallisuutta, työntekijöiden koulutustasosta ja esim. organisaation tietoturvakulttuurista. Voidaan järjestää tietoiskuja, verkkokoulutuksia, jakaa hyviä käytänteitä, posterikampanjoita, videokoulutusta, puhua asioista viikkopalavereissa, ottaa jokin tunnettu puhuja pitämään parin tunnin koulutuksen, tehdä materiaalia intranettiin, järjestää erilaisia tietoturva-aiheisia tietokilpailuja, palkita osaamisesta, tehdä sisäisiä videopätkiä (meidän oma Tictoc), ottaa jokaiseen viikkopalaveriin tietoturvaminuutin, jne.

Pehmeiden keinojen lisäksi kannattaa aika ajoin tuoda esiin esim. pääkäyttäjien velvollisuudet kaikille ICT-tehtävissä työskenteleville. Heidän velvollisuutenaan on kehittää omaa tietoturvaosaamistaan ja jakaa osaamistaan myös muiden kanssa, jos havaitsee, että heidän osaamistaan kaivataan. On tärkeää havaita, että organisaation tietojärjestelmien pääkäyttäjät ovat usein primäärikohde verkkorikollisille. Kun verkkorikollinen saa pääkäyttäjän oikeudet organisaation verkkoon, on peli usein menetetty. Tästä johtuen pääkäyttäjien tulee ymmärtää asemansa organisaation ”kruununjalokivien vartijana”. Se tarkoittaa eri asioita eri organisaatioissa, mutta asian tiedostaminen ja sen esille nostaminen ja huolehtiminen sen merkityksestä ja ymmärtämisestä kuuluu organisaation johdolle. Tässä yhteydessä puhutaankin usein kyberhygieniasta eli siitä, että järjestelmät pysyvät puhtaina ja turvallisina. Pääkäyttäjä on siinä avainasemassa.

Tietoturvakulttuurissa on parannettavaa

”Meitä hämmästyttää se, että monien yritysten tietoturvakulttuurista saama pistemäärä jää edelleen melko alhaiseksi. Yli yhdeksässä yrityksessä kymmenestä turvallisuuskulttuurin taso on kohtalainen. Rikolliset iskevät yritysten IT-toimintoihin joka päivä aiheuttaen niille suoranaisia kustannuksia ja pakottaen ne käyttämään merkittävästi resursseja digitaalisten arvojen turvaamiseen. Siksi hämmästyttää, että monissa yrityksissä rikollisuudelta suojautumiseen ei panosteta enempää”, kertoo KnowBe4-konserniin kuuluvan CLTRe:n toimitusjohtaja Kai Roer.
Tämä yritys toimii KnowBe4-tietoturvakonsernin maailmanlaajuisena tietoturvakulttuurin tutkimuskeskuksena.

Lue lisää tietoturvakulttuuritutkimuksesta https://www.sttinfo.fi/tiedote/tietoturvakulttuurissa-on-eniten-parannettavaa-koulutus--ja-kuljetusaloilla?publisherId=69818153&releaseId=69886526

Tietoturvakulttuuria kehitetään Suomessa myös kansallisella tasolla. Esimerkiksi Digi- ja väestötietovirasto (DVV) tuottaa kuukausittaisia verkko-ohjelmia henkilöstölle, asiantuntijoille ja johdolle, joiden tarkoituksena on kehittää henkilöstön ja organisaation digiturvaosaamisen tasoa Tarjolla on muita maksuttomia digiturvaan liittyviä verkkokoulutuksia ja digiturvapeli – https://digiturvallinenelama.fi. Katso DVV:n tapahtumakalenteri osoitteessa https://dvv.fi/digiturva .

5.10 Selvitetään mahdollisuudet saada kybervakuutus

Kybervakuutus voi nykypäivänä mahdollistaa sen, että organisaatio voi jakaa vastuuta mahdollisen kyberhyökkäyksen kohdatessaan. Vastuun jakaminen tarkoittaa varautumista taloudellisiin menetyksiin aineellisissa ja aineettomissa vahingoissa tai lainopillisten neuvojen saamista oman kyberympäristön suojaamisessa teknisin ja hallinnollisin keinoin.

Suomessa kybervakuutuksia tarjoaa ainakin Osuuspankki (OP), LähiTapiola, vakuutusyhtiö If, Turva, AON, Howden, AIG Finland, IB Partners, DUAL Finland, Söderberg Partners jne.

Kybervakuutus korvaa esim. seuraavia asioita (Howden sivuston mukaan)

- Vahinkotukipalvelu (24/7 puhelinpalvelu) auttaa saamaan teknisen avun paikan päälle viipymättä ja palauttamaan toimintakykysi mahdollisimman nopeasti.
- IT-turva- ja rikostekniset kustannukset, kriisitiedotuskustannukset, hallinnolliset ja oikeudenkäyntikustannukset sekä henkilötietomurron käsittelykustannukset, muut ylimääräiset kustannukset.
- Järjestelmien korjaamisesta ja vahinkojen minimoinnista aiheutuvat kustannukset
- Keskeytysvahinko ja liikevaihdon menetys
- Vastuuvahingot ja selvittelykustannukset
- Lain mukaan vakuutettavissa olevat seuraamusmaksut
- Tietomurtokiritystilanteesta aiheutuvat selvittelykustannukset ja lunnaat

Lähitapiola on listannut joitakin esimerkkitapauksia, jossa kybervakuutuksesta on hyötyä:

- **Yrityksen tietojärjestelmiin on tarttunut kiristyshaittaohjelma**. Tällöin korvaamme IT asiantuntijan tekemän työn, kun tietojärjestelmiä palautetaan toimintakuntoon eli poistetaan haittaohjelma ja palautetaan tiedostot. Tilanteesta aiheutunut keskeytysvahinko korvataan myös.
- **Hakkeri on kaapannut toimitusjohtajan sähköpostin ja lähettää toimitusjohtajan nimissä laskutukseen perusteettoman maksun.** Kun maksu on jo maksettu, käy ilmi, että maksu menikin hakkerin tilille. Tällöin korvataan tietojärjestelmissä tarvittavat selvitystyöt, selvitetään miten sähköposti on kaapattu, estetään sähköpostitilin käyttäminen ja kerrotaan mitä on tehtävä, jotta tilannetta ei pääse tapahtumaan uudelleen. Korvaamme myös väärälle tilille maksetun summan.
- **Yrityksen tietoja on vuotanut sähköisesti tietosuojaloukkauksen takia tai inhimillisestä erehdyksestä.** Vakuutuksesta korvataan asiakkaalle viestintäkustannukset, joita tilanteessa on tehtävä lain vaatimuksesta. Korvaamme myös viestintätoimistokustannukset, mikäli sellaista on käytetty maineriskin pienentämiseksi sekä toiselle aiheutuneen puhtaan taloudellisen vahingon, joka on johtunut tästä tapauksesta.

Lisää esimerkkejä voi lukea verkosta. Kybervakuutuksia on siis tarjolla runsaasti, joten ennen kuin ottaa vakuutuksen sen ehdot pitää lukea tarkasti. Esim. inhimillinen erehdys voi estää korvauksen saannin, mutta lähtökohtaisesti vakuutukset ovat melko kattavia ja ovat yksi tärkeä osanen organisaation varautumisessa kyberiskuja vastaan. On kuitenkin hyvä muistaa, että vastuuta ei voi ulkoistaa. Yrityksen ja organisaation johto tai viranhaltija on kuitenkin aina vastuussa turvallisuudesta kokonaisuutena.

5.11 Varautumissuunnitelman käyttöönotto

Kiristyshaittaohjelman erityistekijä on, että hyökkäyksen kohteena olevan organisaation toiminta voidaan saattaa epävarmaan tilaan. Monet normaalit toiminnot lakkaavat tai voivat lakata toimimasta, kuten puhelimet, pikaviestiohjelmat, liiketoimintasovellukset, turvallisuusjärjestelmät, kulunvalvonta, kassajärjestelmät, jne. Kiristyshaittaohjelmalla saattaa olla mittavat vaikutukset koko organisaation toiminnan lamauttamisessa. Pahimmillaan joudutaan palaamaan paperi ja kynän käyttöön ja syvästi digitalisoituneessa yhteiskunnassa, kuten Suomi, se ei ole edes mahdollista kaikissa toiminnoissa. Olemme ottaneet niin laajasti

digitaalisia järjestelmiä käyttöön, että olemme niistä riippuvaisia ja tavallaan niiden vankina ilman mahdollisuutta palata vanhaan maailmaan.

Organisaatiolle on tärkeää, että sillä on olemassa suunnitelma, jonka avulla se voi jatkaa (liike)toimintaa jonkin aikaa ilman tietoverkkojen toimivuutta siihen saakka, kunnes on palattu takaisin normaalitilaan. Tämä suunnitelma ei saa olla siellä tiedostokansiossa tietojärjestelmissä tai Teamsissa, vaan sen tulee olla paperisena sellaisessa paikassa, josta se tarvittaessa on saatavilla. Kiristyshaittaohjelman lisäksi voi organisaatioon kohdistua toinen, kiristyshaittaohjelmahyökkäystä tukeva kyberhyökkäys, jolla on saatu sähköt pois käytöstä. Silloinkin suunnitelmien tulee olla saatavilla. Ne eivät siis esimerkiksi saa olla tilassa, joka on sähkölukon takana.

Suunnitelma on päivitettävä säännöllisesti esim. organisaation tai kumppanuuksien yhteystietojen muuttuessa. Suunnitelman käyttöönottoa ja käyttöä on myös harjoiteltava. Se tarkoittaa, että jollakin on vastuu siitä, että harjoittelu on osana organisaation vuosikelloa ja se huomioidaan esim. budjetoinnissa.

Varautumissuunnitelma on organisaation lisävakuutus, jota ei kannata teettää konsultilla ja varautumissuunnitelman harjoittelu on organisaation testi siitä, miten se selviytyy digitaalisissa ääriolosuhteissa. Vain suunnittelemalla ja harjoittelemalla voi löytää ne kriittiset kohdat, joihin organisaation toiminta voi kaatua kriisin alla. Siihen kannattaa siis käyttää aikaa ja voimavaroja.

5.12 Viestintästrategia kyberkriisissä

Viimeisenä hyökkäysriskin vähentämisen kohtana on kyberturvallisuuden viestintästrategia. Oikea-aikaisen ja oikean tasoisen viestinnän merkitystä ei voi liiaksi korostaa. Viestintä on osa kyberkriisin hallintaa, koska hyvällä viestintästrategialla voidaan rajoittaa kyberhyökkäyksen vaikutuksia ja rajata tai poistaa organisaation maineeseen kohdistuvia haittoja. Samalla tässä annetaan yleisiä neuvoja kriisiviestinnästä, joita voi soveltaa mihin tahansa organisaation kohtaamaan kriisiin. Kiristyshaittaohjelmalla tehty hyökkäys eroaa kuitenkin muista kriiseistä viestinnän näkökulmasta, koska silloin saattaa kaikki normaalit viestintäkanavat olla poissa käytöstä ja joudutaan turvautumaan ei-digitaalisiin keinoihin.

Kiristyshaittaohjelma hyökkäyksen torjumiseksi ja vaikutusten rajaamiseksi tulee organisaatiossa olla etukäteen suunniteltu ja vastuutettu viestintästrategia. Sen tulee olla ulottua kaikkiin organisaation sidosryhmiin niin kansallisesti kuin kansainvälisestikin riippuen organisaation toiminnan laajuudesta. Kriisin sattuessa on tärkeä rajata sen vaikutus organisaation julkikuvaan ja maineeseen liittyen sekä sisäisesti, että ulkoisesti.

Käyttökelpoisen viestintästrategian kehittäminen tulee perustua yhteistyöhön liiketoiminnan tai virkavastuullisten julkishallinnossa sekä organisaation digitaalisen turvallisuuden toimijoiden kanssa. Yhdessä heidän tulee suunnitella toimenpiteet ja asianmukaiset viestit, jotka esitetään organisaation johdolle toimitettavaksi sidosryhmille ja tarvittaessa julkisuuteen. Jos mahdollista viestinnässä tulee käyttää viestinnän asiantuntijoita tai konsultteja.

Kriisiviestintää tulee harjoitella ja sitä voi oppia vain kahdella tavalla: läpikäymällä kriisin ja oppimalla sen kautta tai harjoittelemalla. Jälkimmäinen on useasti se mukavampi tapa oppia. Kriisin käynnistymiselle on tyypillistä sekaannus. On vaikeaa tietää kenen pitäisi toimia ja onko ylipäänsä pakko tehdä jotain. Kokonaiskuva hahmottuu hitaasti, eikä ilman sitä toiminta ole kovinkaan järkevää ulkopuolelta katsottuna. Kokonaiskuvan luomisessa auttaa, kun tilannetta on joukolla harjoitelu. Istumalla pöydän ääreen voi kuvitella mitä voi tapahtua, miten asia sitten etenisi ja mitä niissä tilanteissa pitäisi tehdä. Kirjoituspöytäharjoitus on halpa ja helppo tapa harjoitella ja usein se jo riittää tuomaan esiin epäkohtia ja parantamisen tarpeita niin viestinnän laajuudessa kuin laadussakin.

Seuraavassa on professori Elisa Juholinin kirjasta ”Communicare! Viestinnän tekijän käsikirja” kriisiviestintäsuunnitelmaan sisällytettäviä elementtejä. Nämä jakaantuvat kolmeen kokonaisuuteen: Varautuminen, Toimiminen sekä Tuki ja kehittäminen.

Varautuminen	1. Kriisityypit, joita organisaatio saattaa kohdata 2. Viestinnän periaatteet 3. Kohde- ja sidosryhmät tärkeysjärjestyksessä (voi vaihdella eri kriiseissä) 4. Julkisuudet, mediat ja foorumit 5. Vastuut eriteltyinä eri henkilöille ja ryhmille 6. Yhteistyökumppanit erilaisissa kriiseissä
Toimiminen	7. Prosessi vaihe vaiheelta 8. Keinot ja toimintaohjeet
Tuki ja kehittäminen	9. Aineistot (missä saatavilla, kuka vastaa päivittämisestä) 10. Valmennus, koulutus ja harjoittelu

Kiristyshaittaohjelman kohdatessa organisaation on suuri mahdollisuus sille, että kaikki perinteiset viestintäkanavat ovat käyttökelvottomia. Kun tietokoneet eikä tietoverkot toimi, on nykyinen digitaalinen ympäristö polvillaan. Kyberhyökkäys saatetaan toteuttaa yhdessä kiristyshaittaohjelmaan perustuvan hyökkäyksen kanssa siten, että myös sähköverkko ei toimi tai on epästabiili, joka aiheuttaa itsessään laajaa epävarmuutta ja paniikkia niissäkin, joiden tarkoitus on toteuttaa kriisiviestintää. Jos hyökkäys koskee laajemmin yhteiskuntaa, myös läheisten pärjääminen voi olla mielessä ja häiritä omaa kriisinhallinnan tehtävää. Kyberhyökkäyksessä vaikutusalue voi olla suuri ja siksi vain harjoittelemalla voidaan saada rutiinia toimintaan kriisitilanteessa ja samalla löydetään heikkoja kohtia niin kriisinhallinnan, jatkuvuuden hallinnan kuin viestinnänkin suunnitelmista. Harjoittelulla myös madalletaan tarvetta tukeutua kirjalliseen materiaaliin kriisin keskellä. Jos kirjallista materiaalia esim. prosessin kulku, viestinnän vastuuhenkilöiden yhteystiedot, viestittävien yhteystiedot jne. tarvitaan, niin on hyvä muistaa, että sen ainoat kopiot ei saa olla tietojärjestelmissä. Suunnitelmista ja

Kriisiviestijän työkalupakki

Lue lisää kriisiviestinnästä tästä Suomen tietotoimiston, STT:n (2021) ohjeesta ”Kriisiviestijän työkalupakki – Näillä pysyt askelen edellä.
https://www.viestintapalvelut.fi/blogi/kriisiviestinta-tyokalupakki-nailla-pysyt-askeleen-edella

yhteystiedoista pitää olla paperiversiot, jossa helposti saatavilla (ei esim. sähkölukon takana) ja niiden käytettävissä oikea-aikaisesti, joilla on toiminnallinen vastuu.

Harjoitusten osalta voi osallistua esim. kansalliseen TAISTO- harjoitukseen aina jokaisen vuoden marraskuussa (https://dvv.fi/taisto) ja harjoitella omatoimisesti TAISTOmaatin avulla. Lisätietoja löydät DVV:n osoitteesta https://www.eoppiva.fi/koulutukset/taisto-maatti-digitaalinen-harjoitus-organisaation-toiminnan-ja-jatkuvuuden-mahdollistamiseksi/

6 Miten reagoida hyökkäykseen?

Tässä kappaleessa annetaan ohjeita siitä, miten tulee vastata kiristyshaittaohjelmaan perustuvaan hyökkäykseen. Teknisillä keinoilla on mahdollista vastata hyökkäykseen nopeasti ja rajoittaa tai estää sen aiheuttamia menetyksiä. Uhriksi joutuneelle kriisiviestintä ja rikosilmoituksen tekeminen on tärkeää, jotta voidaan jatkossa paremmin estää samankaltaiset rikokset, saada rikolliset vastuuseen sekä antaa tietoa sidosryhmille, jotta he voivat valmistautua mahdolliseen haittaohjelman leviämiseen.

6.1 Toimenpiteiden käyttöönotto

Ensimmäisenä (1) vastauksena hyökkäykseen tulee käydä läpi lokitiedot ja muut verkon käyttöä tarkkailevat järjestelmät, jotta saadaan selville mitä toimintoja ja tapahtumia tähän hyökkäykseen liittyy. On siis tärkeää, että organisaatiolla on käytössä lokitus ja järjestelmät, joilla lokia voidaan lukea (SIEM-CSOC[5]). Lokit tulee myös olla varmistettu, ettei niihin voida tehdä muutoksia hyökkääjän toimesta. Erillinen lokipalvelin on tähän hyvä keino. Lokituksen ja muun verkon kautta tulevan tiedon kerääminen SIEM järjestelmään sekä itsellä tai kumppanilla oleva CSOC-tietoturvan hallintakeskus mahdollistaa keskitetyn lokien hallinnan sekä verkossa tapahtuvan epänormaalin toiminnan havainnoinnin tekoälyn avulla ja siihen reagoinnin jopa proaktiivisesti.

Toinen vaihe (2) on varmistaa, että organisaation varmuuskopiot on suojattu kiristyshaittaohjelman vaikutukselta. Varmuuskopiot sisältävät mediat tulee tässä vaiheessa irrottaa verkosta. Jos varmuuskopiot salataan hyökkääjän toimesta, ei organisaatiolla ole mitään keinoa saada tietojaan takaisin. Varmuuskopiot ovat arvokasta tietoa, joka pitää suojata myös fyysisellä etäisyydellä organisaation järjestelmien toimintaympäristöstä. Sillä varmistetaan, että mahdollisen kiristyshaittaohjelmaan perustuvan kyberhyökkäyksen lisäksi tehtävällä tukihyökkäyksellä ei onnistuta vahingoittamaan tai tuhoamaan konesalin fyysisiä järjestelmiä. Suurempi uhka varmuuskopioille on kuitenkin, että ne tuhoutuvat esim. tulipalossa tai muussa onnettomuudessa, kun ne sijaitsevat samassa tilassa varmuuskopioitavien järjestelmien kanssa. Toinen varmuuskopioita uhkaava riski on, että niistä palauttamista ei koskaan

[5] SIEM, Security Incident and Event Management, tarkkailee organisaation tietojärjestelmiä ja -verkkoja sekä hälyttää havaitessaan normaalista poikkeavaa toimintaa. Tietoturvauhkien havaitseminen mahdollisimman aikaisessa vaiheessa mahdollistaa nopean reagoinnin ja minimoi vahingot.
CSOC (Cyber Security Operation Center) tarkoittaa tietoturvan tai kyberturvallisuuden hallintakeskusta, jossa eri lähteistä tullutta tietoa analysoidaan ja sen avulla havaitaan esim. epänormaalia käytöstä verkossa.

harjoitella ja tositilanteessa palauttaminen varmuuskopioista ei onnistukaan, koska ne ovat syystä tai toisesta korruptoituneet tai muuten vahingoittuneet.

Kolmannessa vaiheessa (3) varmistetaan, että saastunut kone ei jatka kiristyshaittaohjelman levittämistä muualle verkkoon. Tämä tehdään poistamalla tietokone internetyhteydestä, mutta tietokoneen virtoja ei saa sammuttaa. Tällä myös katkaistaan hyökkääjän komentokanava ja estetään sitä kontrolloimasta kiristyshaittaohjelmaa. Toimenpiteellä myös estetään organisaation dataan kohdistuvat manipuloinnit. Näillä toimenpiteillä on merkittävät vaikutukset hyökkääjän aktiivisuuteen.

Kun haittaohjelma on tunnistettu, on mahdollista etsiä lokeista tähän liittyviä ominaisuuksia, kuten verkko-osoite, johon haittaohjelma ottaa yhteyttä, tiedostonimiä, tiivistefunktioita, sähköposteissa olevia aiheeseen liittyviä tietoja jne. eli kaikkea mahdollista haittaohjelmaan liittyvää tietoa, jotta hyökkääjä voidaan tunnistaa ja jotta kerätään kaikki hyökkäykseen liittyvä data talteen mahdollista oikeudenkäyntiä varten. Näillä tiedoilla voidaan myös estää uusia hyökkäyksiä laittamalla palomuuriin ja muihin verkon tietoturvalaitteisiin suodatuksia, joilla estetään esim. yhteydenotto hyökkääjän määrittelemään verkko-osoitteeseen (CC, Command and Control) lisätyökalujen lataamista varten.

Tilannetta pitää johtaa ja estää lisävahingot

Edellä mainitut vaiheet1-3 ovat kaikki kiireellisiä ja ne tulee mahdollisuuksien mukaan suorittaa samaan aikaan. Kriisinhallintayksikön tehtävä on jakaa ja vastuuttaa tehtävät niin, että nopeasti leviävän haittaohjelman vahingot jäävät mahdollisimman pieneksi (ei leviä) ja että tilanteesta jää luotettava digitaalinen jälki esim. rikostutkintaa varten (lokit) sekä varmistaa, että organisaation haittaohjelman salaamat tiedot voidaan palauttaa varmuuskopioista. On tärkeää, että on ennalta mietitty, kuka tekee mitäkin ja että tilannetta johtaa muut kuin operatiivista toimintaa tekevät, jotta heille jää rauha tehdä asioita, eikä esim. joudu vastailemaan puheluihin. (Kts. kappale 5.2).

Jos kaikki hyökkäyksen kohteena olevan koneen tiedostot on hyökkääjän toimesta salattu, tietokoneen sammuttaminen (voi) heikentää mahdollisuuksia kerätä hyökkäykseen liittyviä tietoja ja samalla on vähemmän mahdollisuuksia löytää elementtejä, jolla laitteen muistista löytyy keinoja tiedoston salauksen purkuun. Kannattaa sen sijaan laittaa kone unitilaan (hibernation) jos se on mahdollista. Tämä lopettaa haittaohjelman aktiivisen toiminnan ja koneen muisti voidaan kopioida myöhempää tarkastelua varten.

Estääkseen haittaohjelman leviämisen muihin verkossa oleviin tietokoneisiin ja näiden tiedostojen salaamisen, on suositeltavaa, että kaikki tietokoneet, joita ei ole käynnistetty jätetään käynnistämättä ja tietokoneet, jotka toimivat normaalisti sammutetaan, jos mahdollista tai ainakin kielletään liittämästä niihin mitään siirrettävää tallennusvälinettä (USB-muisti, ulkoinen kovalevy, tms.)

Vaikka tietokoneen tiedostot on kiristyshaittaohjelman toimesta salattu, on mahdollista, että salauksen purkuun löydetään myöhemmin keinoja ja ne julkaistaan. Sen vuoksi on tärkeää säilyttää salattu data. Europolin, McAfeen ja Hollannin poliisin kyberrikostorjunta -

yksiköllä on projekti nimeltä *No More Ransom,* jonka tarkoituksena on tunnistaa salauksenpurkumenetelmiä, jotka soveltuisivat laajaan kirjoon erilaisia kiristyshaittaohjelmia. Lue lisää projektista täältä https://www.nomoreransom.org/fi/index.html

6.2 Johtamisen koordinointi kyberkriisissä

Kiristyshaittaohjelman uhrille vaikutuksen menevät paljon pidemmälle, kuin menetetyn datan tai lunnaiden maksun arvoon. Organisaatiolle seuraukset voivat olla moninaiset, mistä syystä on suositeltavaa perustaa kriisinhallinta yksikkö organisaation korkeimmalla tasolla. Kriisinhallinnassa tulee olla mukana henkilöitä, jotka ovat erillään operatiivisesta toiminnasta, jotta operatiivisessa toiminnassa olevat henkilöt voivat keskittyä ongelman ratkaisuun.

Kyberturvallisuuskeskuksen havainnointi ja avunanto -palvelu auttaa tietoturvaloukkausten selvittelyssä: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto

Tietosuojavaltuutetun toimisto auttaa henkilötietojen tietoturvaloukkauksissa https://tietosuoja.fi/tietoturvaloukkaukset

Kriisinhallintayksikkö on vastuussa strategisen tason toiminnasta aloittamalla esim. sisäisen ja ulkoisen viestinnän tarpeisiin strategisen toiminnan ja olemalla yhteydessä viranomaisiin, kuten Kyberturvallisuuskeskukseen ja poliisiin sekä tietosuojavaltuutetun toimistoon erityisesti, jos kiristys koskee henkilötietoja sisältävää dataa ja se on saattanut vuotaa ulospäin.

6.3 Teknisen avun käyttö

Erityisesti pienillä ja keskisuurilla yrityksillä ei välttämättä ole omia resursseja ja osaamista kiristyshaittaohjelmien tai muiden haittaohjelmien tai kyberturvallisuutta muuten uhkaavien tilanteiden selvittelyyn ja siitä toipumiseen. Tällaisissa tilanteissa tulee olla yhteydessä näitä palveluita tarjoaviin yrityksiin tai viranomaisiin. Edellä mainittu Kyberturvallisuskeskus auttaa tässäkin, mutta myös kaupallisilla yrityksillä kuten Nixulla on tarvittavaa osaamista. On hyvä etukäteen selvittää myös, miten kybervakuutus kattaa tällaisissa tilanteissa ja olla heti yhteydessä vakuutusyhtiöön, kun tapaus on sattunut.

Kyberturvallisuuskeskuksen havainnointi ja avunanto -palvelu auttaa tietoturvaloukkausten selvittelyssä: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto

Nixu Oy:n kyberhyökkäysten torjuntapalvelu https://www.nixu.com/fi/palvelut/kyberhyokkaysten-torjunta

Tietoa kybervakuutuksista saat vakuutusyhtiöiden sivulta tai laittamalla hakukoneeseen ”kybervakuutus”.

6.4 Oikean tason viestintä

Kun kiristyshaittaohjelman avulla isketään organisaatioon, on hyvä olla valmiina viestintästrategia tai viestintäsuunnitelma. Pelkkä suunnitelma ei kuitenkaan riitä, vaan sitä on

täytynyt myös harjoitella yhdessä sekä teknisen tiimin, että liiketoiminnan tai muut toiminnan sekä organisaation johdon kanssa.

Sen mukaan missä hyökkäys on tapahtunut, tulisi olla määriteltynä toimenpiteet viestinnälle. Viestiminen teknisistä asioista asiantuntijoille tai kyberturvallisuuteen erikoistuneelle lehdistölle tai sosiaaliseen mediaan eroaa toisistaan huomattavasti. Viestintästrategiassa tulee huomioida erilaiset kohderyhmät ja miettiä etukäteen kuka, miten, kenelle, missä muodossa jne. viestintää tehdään.

Organisaation jäsenille on tärkeää nopeasti jakaa tietoa tilanteesta. Tällä estetään huhujen leviäminen ja rauhoitetaan ihmisiä.

Kriisiviestinnästä voi lukea lisää esim. YLE:n kriisiviestintäoppaasta tai MIF:n kriisiviestintäsuunnitelman ohjeista linkkiluettelosta.

6.5 Älä maksa lunnaita

Kiristyshaittaohjelman pyytämiä lunnaita ei kannata koskaan maksaa. Ei ole mitään takeita, että salatut tiedostot saadaan takaisin lunnaita maksamalla, mutta se kannustaa kyberrikollisia jatkamaan toimintaansa ja sitten ylläpitää rikollista toimintaa. Lunnaita maksamalla ei myöskään ole takeita, etteikö organisaatio joutuisi uudelleen kiristyshyökkäyksen kohteeksi kyberrikollisten toimesta. Lunnaiden maksaminen on rikollisille myös tieto siitä, että haittaohjelma toimii.

Lisäksi kokemuksen kautta on todettu olevan riski, että rikollisten lunnaita vastaan antamalla salausavaimella, tiedostot todella aukeaisivat. Monesti kiristyshaittaohjelma muuttaa tiedostoja salauksen aikana niin, että ainakin osa niistä korruptoituu salauksen aikana, eikä ole enää palautettavissa alkuperäiseksi.

Mainittakoon, että on muitakin mielipiteitä ja joissakin tapauksissa lunnaat ovat tarkoituksenmukaista maksaa, mutta pääsääntöisesti lunnaita ei pidä maksaa. (Kts esim. ”Uutiset” sivulla 9).

6.6 Ilmoituksen tekeminen

On suositeltavaa tehdä aina rikosilmoitus, mikäli joutuu kyberhyökkäyksen kohteeksi kiristyshaittaohjelman toimesta. Ensiksikin tekemällä rikosilmoituksen poliisin on mahdollista tutkia tapausta ja etsiä mahdollista avainta, jolla tiedostojen salaus voidaan purkaa (Tutustu myös No More Ransom -projektin salauksenpurkutyökaluihin https://www.nomoreransom.org/fi/decryption-tools.html).

Rikosilmoitus poliisille
https://poliisi.fi/tee-rikosilmoitus

Ilmoitus kyberturvallisuuskeskukselle
https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

Ilmoitus tietosuojavaltuutetun toimistolle
https://tietosuoja.fi/tietoturvaloukkaukset

Toiseksi tekemällä rikosilmoituksen, voidaan tekijää syyttää, mikäli hänet saadaan kiinni ja nykyisin tekijät jäävät kiinni yhä useammin. Yleensä heillä on

maailmanlaajuisesti suuri määrä uhreja ja vain ne, jotka ovat tehneet rikosilmoituksen voivat saada oikeutta ja mahdollisen korvauksen.

Kolmanneksi tekemällä rikosilmoituksen poliisit saavat käsityksen siitä, miten yleistä tällaiset hyökkäykset ovat ja voivat perustella lisäresursseja ja erikoisosaamisen tarvetta tällä alueella. Rikoksia, joista ei tehdä rikosilmoitusta, ei tilastoida minnekään ja silloin niiden selvittelyynkään ei panosteta. Neljänneksi on tärkeää myös suurelle yleisölle saada tietoa kiristyshaittaohjelmien avulla tapahtuvasta rikollisuudesta ja sitä kautta niitä osataan tunnistaa ja varoa sekä valmistautua niiden torjuntaan esim. tämän oppaan avulla.

Rikosilmoituksen lisäksi ilmoitus voi olla syytä tehdä myös kyberturvallisuuskeskukselle ja tietosuojavaltuutetun toimistolle. Tutustu infolaatikossa olevien linkkien kautta, milloin ilmoitus eri instansseille tulee tehdä. Muista myös, että tietosuojaloukkauksissa pitää ilmoittaa myös loukkausten kohteeksi joutuneille rekisteröityneille henkilöille, joiden henkilötiedot ovat vaarantuneet.

6.7 Järjestelmien palauttaminen puhtaista tiedostoista

Kiristyshaittaohjelman saastuttama laite on syytä uudelleen asentaa puhtaalta medialta eli alkuperäiseltä tai luotettavalta taholta ladatulta asennusmedialta. Datat tulee luonnollisesti palauttaa varmuuskopioista, jotka ovat luotu ennen kuin järjestelmä on vaarantunut, jotta voidaan olla varmoja, että palautettava data ei ole saastunut kiristyshaittaohjelmalla. On vaikea arvioida miten tehokasta tai turvallista datan palauttaminen olisi muilla tavoin. Seuraavia turvallisuuteen liittyviä ohjeita kannattaa noudattaa palautusmedian ja kaikkien terveiden koneiden osalta

- Haavoittuvuus, jota hyökkääjä oli käyttänyt, tulee välittömästi korjata, jotta lisätartunnat voidaan välttää. Tämä sisältää myös ohjelmistojen päivitykset ja palomuurisääntöjen muuttamisen.
- Jos kiristyshaittaohjelma on tunnistettu, täytyy varmistaa ettei haittaohjelma ole tehnyt sellaisia muutoksia, jolla se voisi uudelleen aktivoitua, kun saastunut kone uudelleenasennuksen jälkeen käynnistetään. Tämä tarkoittaa esim. rekisterien arvojen muutoksia tai haitallisia tiedostoja.
- Salasanat tulee vaihtaa kaikkialla, minne hyökkäys on vaikuttanut.
- Suorita toimenpiteitä, joita tässä oppaassa on annettu kiristyshaittaohjelmien välttämiseksi.

7 Kyberturvallisuusjohtaminen ja ennakointi

Kyberjohtamisen keskeinen tekijä on ennakointi. Kyberrikolliset näyttävät löytävän aina astetta parempia hyökkäysmenetelmiä, kuin mitä puolustus. On luonnollista, että näin on. Rikollisen tarvitsee löytää vain yksi heikko kohta, kun puolustuksen pitää huolehtia siitä, että kaikki ohjelmistot, käyttöjärjestelmät, tietojärjestelmät, päätelaitteet, verkon komponentit, käyttäjähallinta, järjestelmien seuranta, verkon valvonta, yksittäinen IoT laite ja varmistaa

vielä ihmiset ovat ”päivitettyjä” ja ajantasalla nykyisistä ja uusista uhista. Rikolliselle riittää, että yksi näistä pettää ja aika usein se on ihminen, mutta tietotekninen ympäristömme on niin monimutkainen, että tarvitaan monta erilaista apuvälinettä, jotta sitä voidaan hallinnoida. Yksi näistä on tekoäly, joka osaa analysoida mitä verkossa tapahtuu ja huomata sekä nostaa esiin havaitut epänormaaliudet. Tekoäly tai koneoppiminen ei ole seppä syntyessään, vaan sitä pitää hitaasti ja kärsivällisesti opettaa tunnistamaan se mikä on normaalia ja mikä on epänormaalia. Tekoälystä on suuresti apua analysoimaan tilannetta eri lähteistä tulevien tietojen perusteella ja tekemään siitä sopivia kuvioita ihmiselle näytettäväksi (CSOC). Loppukädessä ihminen aina päättää toimenpiteet, mutta paljon voidaan myös automatisoida erilaisia vastauksia tekoälyn tuottaman informaation perusteella.

Ennakointiin kuuluu varautuminen ja ihmisten kouluttaminen. Kyberturvallisuus on kaikkien organisaation osapuolten vastuulla, mutta johto tekee päätöksen, siitä paljonko turvallisuuteen resurssoidaan rahaa ja työvoimaa ja mitkä ovat organisaation arvot, joita tulee erityisesti suojella. Näiden arvojen suojaamiseksi organisaatiossa tehdään toimenpiteitä, joilla ennakoidaan näihin arvoihin kohdistuvia uhkia ja niiltä suojautumista. Riskienhallinta on siis keskeisessä osassa myös kyberhyökkäyksiin varautumisessa. Turvallisuus on lähtökohtaisesti itseisarvoton eli sen arvo tulee siitä mitä turvallisuuden avulla suojataan ja miten voidaan havaita erilaisia uhkia ja miten estää näiden havaintojen perusteella nousevia uhkia toteutumasta.

Kyberturvallisuus tarvitsee asiantuntevaa johtamista. Organisaation johtaminen on itsessään vaativa tehtävä, joten ei ole todennäköistä, että organisaation johto on myös kyberturvallisuuden asiantuntija. Siihen tarvitaan erikseen henkilö, joka johtaa ja koordinoin kyberturvallisuuden asioita ja tuo niitä ymmärrettävässä muodossa organisaation johdon päätettäväksi.

Kyberturvallisuuden johtamista voi opiskella sekä ammattikorkeakouluissa, että yliopistoissa, kuten Aalto-yliopisto tai Jyväskylän yliopisto. Valtiovarainministeriö on julkaissut vuonna 2018 kyberturvallisuusasiantuntijoiden kirjoittaman teoksen ”Kyberturvallisuuden strateginen johtaminen Suomessa”, jossa asiaa tarkastellaan yhteiskunnan kokonaisturvallisuuden näkökulmasta. Linkki teokseen on https://julkaisut.valtioneuvosto.fi/handle/10024/160717

8 Loppusanat

Olen tähän oppaaseen kerännyt tietoa siitä, miten kiristyshaittaohjelmilta voidaan suojautua ja miten vähennetään todennäköisyyttä joutua kiristyshaittaohjelmalla toteutetun hyökkäyksen kohteeksi. Kuten olen todennut, tämä suomenkielinen opas perustuu pääosin kansilehdellä mainitun oppaan suomennokseen, mutta olen pyrkinyt tuomaan myös muita tietoa ja vinkkejä.

Toivottavasti tästä oppaasta on apua ainakin niin, että se saa lukijan kiinnostumaan asiasta ja etsimään lisää tietoa, sillä kiristyshaittaohjelmat ovat todellinen uhka digitalisoituneelle

maailmalle ja pahimmillaan seuraukset ovat sekä henkilökohtaisella tasolla, että organisaatiotasolla valtavat ei pelkästään taloudellisesti, vaan menetettyinä tietoina, yksityisyyksinä, mielenrauhoina ja luottamuksina. Kiristäjät ovat häikäilemättömiä rikollisia, jotka lypsävät kohdeorganisaatiosta kaiken mahdollisen ja jatkavat sitten seuraavan uhrin kimppuun. Onneksi monet valtiot, joissa nämä rikolliset toimivat, ovat itse ryhtyneet heitä jahtaamaan ja joitakin rikollisryhmiä on saatu kiinnikin. Tietoisuuden lisääminen sekä uhreista, että rikollisista ja heidän menetelmistään palvelee kaikkia niitä, jotka elävät digitaalisessa maailmassa eli käytännössä meitä kaikkia.

Oppaan kirjoittaja Mikael Inkinen on suorittanut turvallisuusjohtamisen BBA ja MBA tutkinnot sekä tietoliikennetekniikan insinöörin ja sähkövoimatekniikan teknikon tutkinnot. Hän on myös tietotekniikan ylioppilas Aalto-yliopistossa sekä valmistumassa keväällä 2022 ammatillisesta opettajakorkeakoulusta Haaga-Heliasta. Hän työskentelee tietoturvapäällikkönä julkishallinnossa. Lisätiedot LinkedInissä https://www.linkedin.com/in/mikael-inkinen-a5ba351b0/

Jos haluat kysyä oppaan aiheesta tai yleensä kyberturvallisuudesta tai haluat koulutusta tai puhujaksi tilaisuuteen tietoturvallisuudesta, kyberturvallisuudesta tai turvallisuusjohtamisesta, ota yhteyttä osoitteeseen mikaelink@icloud.com tai LinkedInin kautta.
Jos haluat vapaaehtoisesti tukea kirjoitustyötäni niin voit sen tehdä haluamallasi summalla tilille FI56 5790 2620 1899 84, viestiksi laita ”kyberturvallisuus”. – Mikael -

9 Linkkejä

Linkit eivät ole missään erityisessä järjestyksessä.

Kyberturvallisuus ja yrityksen hallituksen vastuu (Kyberturvallisuuskeskus 2020)
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas

Kyberturvallisuuden kehittämisopas (Valtioneuvosto 2021)
https://julkaisut.valtioneuvosto.fi/handle/10024/163219

Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (Valtiovarainministeriö 2020)
https://julkaisut.valtioneuvosto.fi/handle/10024/162433

Suomen kyberturvallisuusstrategia 2019 ja toimeenpano-ohjelma 2017-2020 (Valtiovarainministeriö)
https://vm.fi/kyberturvallisuusstrategia

Turvallisuuskomitea
https://turvallisuuskomitea.fi/

Laki julkisen hallinnon tiedonhallinnasta (2017)
https://www.finlex.fi/fi/laki/alkup/2019/20190906

Kyberrikos on poliisiasia (Poliisiammattikorkeakoulu 2021)
https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisiasia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212?t=1616740405258

Poliisin tietoa kyberrikoksista
https://poliisi.fi/kyberrikokset

Tietosuojavaltuutetun toimiston tietoturvaloukkaussivusto
https://tietosuoja.fi/tietoturvaloukkaukset

Digi- ja väestötietoviraston TAISTO harjoittelu
https://dvv.fi/taisto

Digi- ja väestötietoviraston TAISTOmaatti -harjoitusautomaatti
https://www.eoppiva.fi/koulutukset/taistomaatti-digitaalinen-harjoitus-organisaation-toiminnan-ja-jatkuvuuden-mahdollistamiseksi/

Lokien keräys ja käyttö (Kyberturvallisuuskeskus 2016)
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Lokitusohje.pdf

Selviytymisopas kiristyshaittaohjelmia vastaan (Kyberturvallisuuskeskus 2016)
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf

No More Ransom -projekti suomenkieliset sivut
https://www.nomoreransom.org/fi/index.html

No More Ransom -projekti kysymyksiä ja vastauksia
https://www.nomoreransom.org/fi/ransomware-qa.html

Salauksen purkutyökaluja
https://www.nomoreransom.org/fi/decryption-tools.html

Kyberturvallisuuskeskuksen tietoturvan ohjeet ja oppaat.
https://www.kyberturvallisuuskeskus.fi/fi/ohjeet

Kyberturvallisuuskeskuksen kybermittari, jolla voi arvioida organisaation kyberturvallisuuden tilaa.
https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari

Jyväskylän yliopiston Johdatus kyberturvallisuuteen avoin verkkokurssi.
https://peda.net/jyu/it/do/kkv

Yle Digitreenit: Kirotut haittaohjelmat – kuinka tunnistaa, onko kone saastunut. Ohjeita kotikäyttöön.
https://yle.fi/aihe/artikkeli/2019/06/02/digitreenit-kirotut-haittaohjelmat-kuinka-tunnistaa-onko-kone-saastunut

STT Viestintäpalvelut – Kriisiviestijän työkalupakki – Näillä pysyt askeleen edellä.
https://www.viestintapalvelut.fi/blogi/kriisiviestinta-tyokalupakki-nailla-pysyt-askeleen-edella

Kriisiviestintäsuunnitelman teko-ohje
https://mif.fi/kriisiviestintasuunnitelma-miten-se-tehdaan/

How ransomware happens and how to stop it?
https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

Stop Ransomware. Ransomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

Tietoa haavoittuvuuksista

- Kyberturvallisuuskeskus haavoittuvuusilmoitukset https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet?limit=20&offset=0&query=&sort=updated
- NIST National Vulnerability Database https://nvd.nist.gov/
- CVE Details https://www.cvedetails.com/
- SNYK Vulnerability database https://security.snyk.io/

- Exploit database https://www.exploit-db.com/
- Microsoft vulnerabilities https://msrc.microsoft.com/update-guide/vulnerability
- CVE Details Apple https://msrc.microsoft.com/update-guide/vulnerability
- Tietoa Applen suojauspäivityksistä https://support.apple.com/fi-fi/HT201222