TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toimintaohje – Vuotaneet tunnukset

Traficomin julkaisuja
22/2022

Sisällysluettelo

1 Johdanto

1.1 Ohjeen tarkoitus

Tämän Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen laatiman ohjeen tavoitteena on neuvoa organisaatioita tilanteessa, jossa epäillään tunnusten vuotaneen asiattomille henkilöille tai tahoille, ja joita on käytetty hyväksi kyberhyökkäyksessä. Ohje keskittyy tämän tietoturvallisuuden poikkeamatyypin erityispiirteiden käsittelyyn. Tilanteen ratkaisemiseksi kokonaisuudessaan organisaation on hyvä ylläpitää ja noudattaa laatimaansa hallintasuunnitelmaa tietoturvapoikkeamatilanteita varten (engl. Incident Response Plan).

Tämä ohje opastaa yleisellä tasolla tietoturvaloukkaustilanteessa toimimista ja siitä toipumista. On suositeltavaa, että organisaatio laatii itselleen erillisen oppaan, joka huomioi sen oman teknisen ja toiminnallisen ympäristön tarkemmalla tasolla. Projektin on rahoittanut Huoltovarmuuskeskus.

1.2 Mitä tarkoittavat vuotaneet tunnukset

Vuotaneet tunnukset ovat yksi yleisimmistä keinoista, jonka avulla hyökkääjä voi päästä sisään organisaatiosi tietojärjestelmiin. Vuotaneita tunnuksia käytetään useasti ensimmäisen jalansijan saavuttamiseksi hyökkäyksissä. Käyttäjätunnuksilla käydään kauppaa rikollisten käyttämillä kauppapaikoilla sekä niitä jaetaan suurina tietokantoina julkisesti.

Tunnukset joutuvat useimmiten vääriin käsiin kolmannen osapuolen tietovuodon, salasanojen uudelleenkäytön tai kalasteluviestien seurauksena. On ensisijaisen tärkeää, että organisaatiosi salasanakäytännöt ovat ajan tasalla ja henkilöstöä koulutetaan riskien minimoimiseksi.

1.2.1 Toimitusjohtajahuijaus

Toimitusjohtajahuijauksessa (eng. Business Email Compromise) yrityksen rahaliikenteestä huolehtivaa työntekijää huijataan maksamaan lasku tai muu tilisiirto yrityksen varoista rikollisten tilille. Verkkorikolliset ostavat pimeiltä kauppapaikoilta käyttäjätunnuksia, joita hyväksikäyttämällä he kirjautuvat työntekijän sähköpostiin ja seuraavat sähköpostiliikennettä etsien esimerkiksi mahdollisuuksia tehdä muutoksia olemassa olevien viestiketjujen sisältöön kuten tilinumeroihin. He voivat luoda myös kokonaan uusia laskuja, ja ohjata niiden maksut omille tileilleen.

2 Varautuminen

Varautuminen poikkeamiin on hyvä tapa vähentää poikkeaman vakavuutta ja mahdollistaa nopea toipuminen ja liiketoiminnan jatkuminen. Organisaatio voi arvioida omaa valmiuttaan käyttämällä hyväksi esimerkiksi Kyberturvallisuuskeskuksen Kybermittaria[1]. Etukäteen laadittu poikkeamanhallintasuunnitelma antaa hyvät lähtökohdat toimia, kun poikkeamatilanne tapahtuu. Organisaation tulee myös varmistaa, että toimet kuten käyttäjätunnusten lukitseminen, palvelinten ja päätelaitteiden eristäminen verkosta, sekä verkkoliikenteen rajoittaminen haitallisiin IP-osoitteisiin tai verkkotunnuksiin on teknisesti mahdollista ja henkilöstöltä löytyy tähän myös osaaminen.

Lokitietojen kerääminen, kokoaminen ja monitorointi on tärkeää poikkeaman havaitsemiseksi ajoissa. Lokitiedot mahdollistavat myös poikkeaman perusteellisen tutkimisen ja täten nopeuttavat mahdollista ympäristön siivousta sekä palauttamista. Kyberturvallisuuskeskus on laatinut lokitietojen keräämisestä ja käyttämisestä oppaan.[2] Riippuen organisaation käyttämistä järjestelmistä, kattavaan havainnointiin vaaditaan tyypillisesti lisäksi verkko- ja järjestelmätason ratkaisuja.

Yrityksen yleinen salasanapolitiikka, kirjautumislähteiden rajoittaminen sekä monivaiheinen tunnistus ovat erinomaisia keinoja estää vuotaneiden tunnusten hyväksikäyttöä.

2.1 Hallinnolliset toimet

- Ota käyttäjätunnusten tietovuotoon liittyvissä poikkeamissa käyttöön poikkeamanhallintasuunnitelma, josta käy ilmi selkeät toimintaohjeet henkilöstölle.
- Suunnittele organisaatiollesi salasanapolitiikka, jossa määritetään vähimmäisvaatimukset salasanoille.
- Kouluta henkilöstö tunnistamaan kalastelusähköpostit.
- Selvitä etukäteen, miten voit ilmoittaa tietoturvaloukkauksesta Kyberturvallisuuskeskukselle[3]. Ota seurantaan Kyberturvallisuuskeskuksen ajankohtaiset tiedotteet.[4]
- Käy läpi hyökkäysskenaariot yrityksen johdon kanssa ja sovi käytännön toimet sekä johtovastuut ja -valtuudet tieturvaloukkaustilanteissa.
- Harjoittele[5] ja kehitä poikkeamanhallintasuunnitelmaa säännöllisesti kehysharjoitusten (engl. Tabletop Exercise) avulla, jossa vastuuhenkilöt ja sidosryhmät harjoittelevat tietoturvapoikkeaman käsittelyprosessia kuvitteellisessa skenaariossa.
- Määrittele tarkasti tarvittavat käyttöoikeudet perustuen käyttäjien ja teknisten toiminnallisuuksien tarpeisiin.
- Harkitse tietoturvavalvomopalvelun perustamista tai vastaavan palvelun ostamista. Valvomotoiminnon tarkoituksena on nimensä mukaisesti valvoa yrityksesi verkkoliikennettä ja järjestelmien tietoturvatapahtumia.

[1] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari
[2] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja
[3] https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

[4] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaiset

[5] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta

2.2 Tekniset toimet

- Ota käyttöön monivaiheinen tunnistautuminen.
- Rajoita kirjautumislähteitä maista, joissa organisaatiosi ei harjoita liiketoimintaa.
- Ota käyttöön identiteetin ja pääsynhallinnan (engl. Identity and Access Management, IAM) kontrollit.
- Virtuaalista erillisverkkoa (engl. Virtual Private Network, VPN) käyttämällä voit estää ulkoverkon kirjautumisyritykset kriittisimpiin järjestelmiin.
- Pyri havaitsemaan hyökkäykset mahdollisimman varhain erilaisilla keskitetyillä monitorointiratkaisuilla, ja testaa niiden toiminnallisuutta säännöllisesti.
- Ota käyttöön jo olemassa olevien järjestelmien ominaisuuksia tai hanki tietoturvatuote, joka kykenee suodattamaan haitallista sisältöä sisältäviä sähköpostia, roskapostia ja ei-toivottua verkkoliikennettä.

2.3 Varautuminen ja harjoittelu käytännössä

Tärkeä osa varautumista on myös uhkaskenaarioiden harjoittelu. Harjoittelemalla tämän toimintaohjeen kaltaista skenaariota etukäteen, organisaatiosi voi varmistaa olevansa valmis kohtaamaan kuvatun kaltaisen tilanteen. Harjoittelemalla varmistut muun muassa siitä, että organisaatiosi henkilöstö ymmärtää, mitä tämän toimintaohjeen työnkulku-vuokaaviossa ja tarkistuslistassa olevat kohdat tarkoittavat, ja että heiltä on valmiudet toimia kuvattujen ohjeiden mukaisesti.

On suositeltavaa tutustua myös Kyberturvallisuuskeskuksen harjoitustoimintamateriaaleihin.[6]

Esimerkkiskenaariona voisi olla tilanne, jossa yrityksen työntekijän tunnukset ovat joutuneet verkkorikollisten käsiin. Tunnuksilla on kirjauduttu sähköpostiin, josta on lähetetty väärennettyjä laskuja. Tietoturvaloukkaus ilmenee, kun yhteistyökumppani huomaa saaduissa laskuissa olevan epäilyttäviä yksityiskohtia.

Miten organisaatiossanne toimittaisiin kuvatun kaltaisessa tilanteessa? Harjoitelkaa ainakin seuraavat vaiheet tästä toimintaohjeesta:

- Loukkauksesta ilmoittaminen ja tilanteen eskalaatio.
- Saastuneiden tunnusten lukitseminen ja aktiivisten istuntojen katkaisu.
- Kirjautumistapahtumien tunnistetietojen kerääminen ja lokianalyysi.
    - Pystytäänkö selvittämään miten käyttäjätunnukset ovat vuotaneet?
    - Keiden käyttäjätunnukset ovat vaarantuneet?
- Kerättyjen tunnistetietojen käyttäminen muiden käyttäjätunnusten tarkastamiseksi saastumisen varalta.
- Kalasteluviestin vastaanottajien selvitys.
- Loukkauksen loppuselvityksen prosessi.

[6] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta

Kaikkien harjoiteltavien vaiheiden ohessa tulee pitää mielessä, miten organisaatio johtaa tietoturvaloukkauksen hallintaa, miten sisäinen kommunikaatio toimii, ja ketkä ovat missäkin aiheessa vastuuhenkilöitä ja ketkä heidän varahenkilöitään.

3 Tietoturvaloukkauksen havaitseminen

Vuodetuista tunnuksista aiheutuva tietoturvaloukkaus voidaan havaita esimerkiksi seuraavilla tavoilla:

- Organisaatio saa ilmoituksen epäilyttävästä toiminnasta tai sähköpostista esim. sosiaalisen median, asiakkaan, yhteistyökumppanin tai viranomaisten välityksellä.
- Tietoturvatuotteen tai palveluntarjoajan tuottama hälytys.
- Uhkatietopalvelun tuottama ilmoitus vuotaneista tunnuksista.

Ilmoita tietoturvaloukkauksesta Kyberturvallisuuskeskukselle.[7] Neuvomme teitä luottamuksellisesti ja maksutta vahinkojen rajoittamisessa, tapahtuman analysoinnissa sekä palautumistoimenpiteissä. Samalla tuette kansallisen tietoturvan tilannekuvaa ja mahdollistatte muiden mahdollisten uhrien varoittamisen ja auttamisen.

Tutustu Kyberturvallisuuskeskuksen oppaaseen tietomurtojen havaitsemisesta.[8]

[7] https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

[8] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

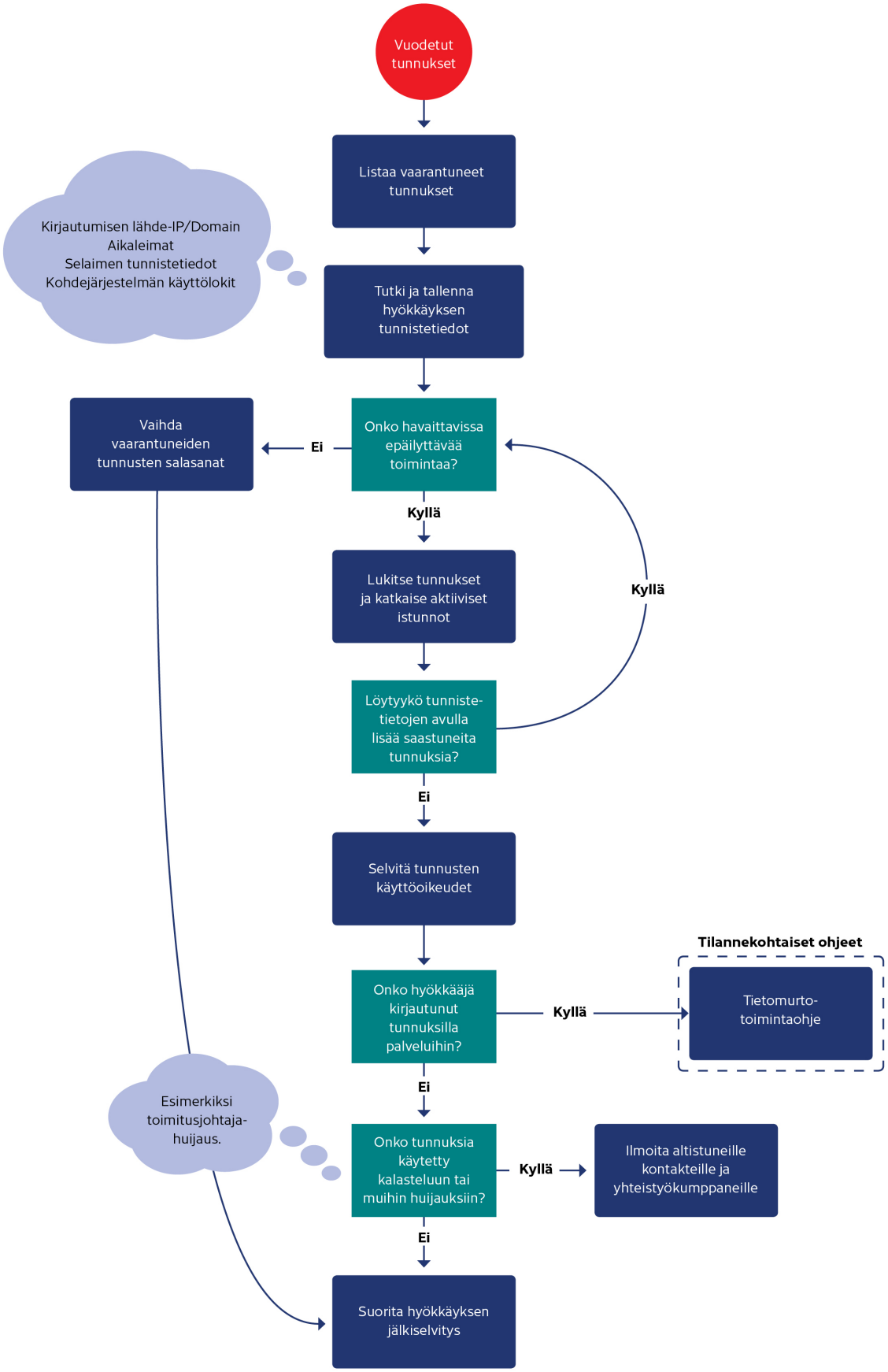
4 Toimintaohjeet

Käytä oheista toimenpiteiden tarkistuslistaa apuna, kun havaitset käyttäjätunnuksiin liittyvän tietoturvaloukkauksen. Tarkistuslista auttaa organisaatiota priorisoimaan ja vaiheistamaan toimintaa loukkauksen selvittämisessä.

4.1 Tietoturvaloukkauksen selvityksen työnkulku

Alla oleva vuokaavio kuvaa toimia, joita noudattamalla loukkausta voidaan selvittää oikeassa järjestyksessä. Vuokaavio tukee tarkistuslistan käyttöä. Tutkinnan aikana on myös ehdottoman tärkeää ylläpitää tarkkaa tapahtumalokia tehdyistä toimenpiteistä. Lokista tulisi käydä ilmi tehty toimenpide, aikaleima ja toimenpiteen suorittaja.

Myös mahdollinen todistusaineiston kerääminen on syytä dokumentoida huolellisesti. Ylös tulisi kirjata kuka keräsi, mitä aineistoa, mistä ja milloin se kerättiin. Huolellisesti laadittu tapahtumaloki helpottaa tutkintaa sekä yhteistyötä poliisin ja tietoturvatutkijoiden kanssa merkittävästi.


Vuodetut tunnukset
Listaa vaarantuneet tunnukset
Kirjautumisen lähde-IP/Domain
Aikaleimat
Selaimen tunnistetiedot
Kohdejärjestelmän käyttölokit
Tutki ja tallenna hyökkäyksen tunnistetiedot
Onko havaittavissa epäilyttävää toimintaa?
Ei
Vaihda vaarantuneiden tunnusten salasanat
Kyllä
Lukitse tunnukset ja katkaise aktiiviset istunnot
Kyllä
Löytyykö tunniste-tietojen avulla lisää saastuneita tunnuksia?
Ei
Selvitä tunnusten käyttöoikeudet
Tilannekohtaiset ohjeet
Onko hyökkääjä kirjautunut tunnuksilla palveluihin?
Kyllä
Tietomurto-toimintaohje
Ei
Esimerkiksi toimitusjohtaja-huijaus.
Onko tunnuksia käytetty kalasteluun tai muihin huijauksiin?
Kyllä
Ilmoita altistuneille kontakteille ja yhteistyökumppaneille
Ei
Suorita hyökkäyksen jälkiselvitys

4.2 Välittömät toimenpiteet

Vaiheen tavoitteet	Toimenpiteiden tarkkuus ja nopeus ovat molemmat tärkeitä. Välittömien toimenpiteiden tavoite on pysäyttää haittaohjelman leviäminen, estää hyökkääjien jalansija verkossa sekä alustaa palautumisprosessin aloittaminen.

Vaihe	Tarkoitus	Toimenpiteet
Lukitse käyttäjätunnus	Lukitsemalla käyttäjätunnuksen ja katkaisemalla aktiiviset istunnot estetään käyttäjätunnusten hyväksikäyttö.	Lukitse käyttäjätunnus siten, ettei sitä voi käyttää. Katkaise kaikki aktiiviset istunnot.
Selvitä käyttäjätunnusten valtuudet	Riippuen käyttäjätunnusten valtuuksista voidaan niitä hyväksikäyttää eri tavoilla. Etsi vastauksia kysymyksiin: • Mihin järjestelmiin tunnuksia käyttämällä voi kirjautua? • Onko tunnuksilla hallintaoikeuksia järjestelmiin tai toisiin käyttäjätunnuksiin?	Selvitä käyttäjätunnusten valtuudet.
Arvioi, tarvitsetko tietoturvaloukkauksen käsittelyyn ulkoista apua	Organisaatio voi tarvita apua toimenpiteiden organisoinnissa, loukkauksen hallinnassa ja teknisissä toimenpiteissä. Jos omasta organisaatiosta tai omalta IT-palveluntarjoajilta ei löydy riittävää osaamista, tulee harkita ulkopuolisen avun tarvetta.	Tekniset toimet poikkeaman käsittelyssä voivat vaatia ulkopuolista osaamista. Tällaisia toimia voivat olla muiden muassa tunnistetietojen kerääminen ja niiden perusteella uhan selvittäminen. Kyberturvallisuuskeskus voi auttaa organisaatioita erityisesti tapauksen ensivasteessa ja tarjoamalla lisätietoja vastaavista tapauksista Suomessa ja kansainvälisesti. Alaviitteessä listatuista resursseista löydät suomalaisia palveluntarjoajia.[9]
Raportoi tietoturvaloukkauksesta viranomaisille	Raportoi poikkeamasta viranomaistahoille. Organisaatiolla voi olla vastuu ilmoittaa tietoturvaloukkauksesta säädösten tai kybervakuutuksen ehtojen velvoittamana.	Tee tapauksesta rikosilmoitus poliisille.[10] Ilmoita tapauksesta myös Kyberturvallisuuskeskukselle[11] tilannekuvan ylläpitämiseksi ja avun saamiseksi. Mikäli henkilötietoja tai muita tietosuojalainsäädännön (GDPR) alaisia tietoja on saattanut päätyä hyökkääjän käsiin, tee ilmoitus Tietosuojavaltuutetun toimistolle[12]. EU:n verkko- ja tietoturvadirektiivin (ns. NIS-direktiivi) alaisten huoltovarmuuskriittisten toimijoiden ja palveluntarjoajien tulee ilmoittaa verkko- ja tietojär-

[9] https://dfir.fi/
https://www.fisc.fi/fi
https://www.hansel.fi/yhteishankinnat/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/

[10] https://poliisi.fi/tee-rikosilmoitus

[11] https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

[12] https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta

		jestelmässä olevista tietoturva-loukkauksista valvontaviran-omaisille[13].

[13] https://www.kyberturvallisuuskeskus.fi/fi/asioi-kanssamme/ilmoita-tietoturvapoikkeamasta-nis-ilmoitusvelvollisuus

4.3 Tietoturvaloukkauksen selvitys

Vaiheen tavoitteet	Loukkauksen selvityksen tavoitteena on selvittää hyökkäyksen laajuus ja vaikutus organisaatiossa. Huolellisella tutkinnalla varmistetaan, että hyökkääjällä ei ole enää pääsyä järjestelmiin ja kaikki vaarantuneet tunnukset on palautettu hallintaan.

Vaihe	Tarkoitus	Toimenpiteet
Tunnista haitallinen toiminta ja kerää tunnistetiedot	Tunnistetietoja käytetään kartoittamaan saastuneita laitteita ja tunnuksia. Huolellinen tunnistetietojen kerääminen ja niiden käyttö tapauksen tutkimisessa on elintärkeää ympäristön puhdistamisessa riittävälle tasolle, jotta palautumisen voi aloittaa turvallisesti.	Etsi saatavilla olevista lokitiedoista poikkeamia tunnistaaksesi, onko vuotaneita tunnuksia käytetty hyväksi. Poikkeavuudet voivat olla esimerkiksi: • Kirjautumisajankohta • Lähde-IP-osoite • Käyttöjärjestelmän tai selaimen versio Vahvista havainnot haastattelemalla tunnusten omistajaa varmistaaksesi, etteivät toimenpiteet ole hänen tekemiään. Tallenna poikkeamista havaitut tunnistetiedot, joita voit käyttää etsimään muita käyttäjätunnuksia, joiden tiedot ovat mahdollisesti vuotaneet.
Käytä tunnistetietoja selvittääksesi kaikki vuotaneet tunnukset	Kerättyjen tunnistetietojen avulla voidaan selvittää, kuinka laajalle hyökkääjä on päässyt tunkeutumaan organisaatiossa. Keräämällä tunnistetietoja ja etsimällä niitä kohdejärjestelmistä voidaan varmistua siitä, että kaikki saastuneet laitteet ja tunnukset löydetään ja siivotaan.	Vuotaneita tunnuksia voidaan etsiä keskitettyjen valvontaohjelmistojen avulla. Ohjelmistot tarjoavat usein mahdollisuuden hakea tapahtumia kaikilta päätelaitteilta halutuilla tunnisteilla. Jos organisaatiolla on käytössä myös keskitetty lokienhallinta, voidaan sen avulla etsiä tapahtumia tehokkaasti useista eri lähteistä samanaikaisesti. Mikäli kumpikaan edellä mainituista ratkaisusta ei ole käytettävissä, tulee tunnisteita hakea manuaalisesti kaikilta päätelaitteilta ja palvelimilta. On olemassa riski, että hyökkääjä on laitteelle päästyään kytkenyt lokien keräämisen pois päältä, jolloin hänen toimistaan ei ole jäänyt mitään jälkiä. Tämän vuoksi on tärkeää tarkastella kaikista eri lähteistä kerättyjä tunnistetietoja, ja niiden avulla pyrkiä muodostamaan kokonaiskuva hyökkääjän toimista.
Tallenna kaikki saatavilla olevat lokitiedostot sekä muut todisteet verkosta eristetylle kovalevylle myöhempää tutkimusta varten	Todisteiden keräämisellä ja säilömisellä pyritään takaamaan laadukas tapauksen jälkitutkinta, jotta tapauksen juurisyyt saadaan selvitettyä. Todisteita voidaan tarvita rikosilmoituksen yhteydessä ja oikeuskäsittelyä varten. Jos organisaatiolla on kybervakuutus, voi myös vakuutusyhtiö vaatia poikkeamasta tarkempia tietoja sekä todisteita tutkintaa varten.	Tallenna lokitiedostot, joista löytyy poikkeaman tutkinnan kannalta oleellista tietoa, verkosta eristetylle kovalevylle. Kerää talteen myös mahdolliset haitalliset sähköpostit ja muut viestit. Pyri säilyttämään todisteet, kuten kokonaiset levykuvat ja muistinäytteet, mahdollisimman eheinä. Ota niistä eheystiivisteet tämän varmistamiseksi.

		Pyri ottamaan haittaohjelmista näytteet ja säilö ne. Käsittelyssä tulee noudattaa erityistä varovaisuutta. Säilömisen turvallinen toteuttaminen vaatii usein ammattiosaamista. Lähetä näytteet Kyberturvallisuuskeskukselle.[14]
Haastattele käyttäjää	Vahvista havainnot haastattelemalla käyttäjää, joka omistaa vuotaneet tunnukset. Käyttäjältä voidaan mahdollisesti saada tietoa siitä, miten tunnukset on vuodettu. Käyttäjä on saattanut esimerkiksi ladata koneelleen tiedostoja, klikata sähköpostissa olevaa linkkiä tai avata etäyhteyden IT-tukihenkilönä esiintyvälle hyökkääjälle. Käyttäjää ei haastateltaessa pidä syyllistää tapahtuneesta, sillä tämän toimilla ei ole välttämättä ollut osuutta tietojen vuotamisessa, eikä käyttäjä välttämättä ole havainnut mitään poikkeavaa.	Haastattele käyttäjää, jonka käyttäjätunnuksilla on havaittu epätavallista toimintaa, ja pyri selvittämään tunnusten vuotamisen syitä.

[14] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/sahkopostin-valittaminen-ja-naytteiden-lahettaminen-kyberturvallisuuskeskukselle

4.4 Palautuminen

Vaiheen tavoitteet	Pyritään palauttamaan kaikki vuotaneet tunnukset takaisin hallintaan ja varmistamaan, että tunnukset ovat taas turvassa. Parannetaan toimintamalleja, jotta vastaavalta voidaan välttyä tulevaisuudessa.

Vaihe	Tarkoitus	Toimenpiteet
Vaihda käyttäjätunnuksen salasana	Varmistetaan, että kaikkien saastuneiden tunnusten kirjautumistiedot vaihdetaan, jotta hyökkääjällä ei olisi enää pääsyä tunnusten avulla organisaation järjestelmiin.	Vaihda salasana ja pyydä käyttäjää vaihtamaan salasana itse uudestaan ensimmäisellä kirjautumiskerralla. Toimita uudet salasanat käyttäjille joko suullisesti, tekstiviestillä tai soittamalla, mutta älä sähköpostilla tai organisaation suosimilla pikaviestimillä, sillä hyökkääjällä saattaa edelleen olla pääsy niihin. Harkitse kaksivaiheisen tunnistautumisen käyttöönottoa ylläpitotunnuksille sekä niille tunnuksille, joita oli käytetty hyväksi hyökkäyksessä. Valvo myös hyökkäyksessä käytettyjä tunnuksia tarkemmin tunnusten palauttamisen jälkeen siltä varalta, että hyökkääjä saa ne uudelleen käsiinsä. Mikäli jää epäselväksi, miten hyökkääjä oli saanut tietyt tunnukset käsiinsä, harkitse niiden tuhoamista ja täysin uusien tunnusten luomista. Näin varmistat, että hyökkääjä ei saa tunnuksia haltuunsa uudelleen tällä tuntemattomalla tavalla. Harkitse myös uuden työaseman antamista vuotaneiden tunnusten omistajille.
Tarkista sähköpostilaatikoiden uudelleenohjaussäännöt	Toimitusjohtajahuijauksissa asetetaan usein sähköpostitileihin uudelleenohjaussääntöjä, joiden avulla rikolliset voivat seurata organisaation sähköpostiliikennettä.	Tarkista vuotaneiden tunnusten sähköpostitilien uudelleenohjaussäännöt, ja poista havaitsemasi haitalliset säännöt.
Kovenna käyttäjien kirjautumisvaatimuksia	Vuotaneiden käyttäjätunnusten hyväksikäyttöä voidaan rajoittaa koventamalla kirjautumisvaatimuksia.	Aseta kirjautumisvaatimukset sopivalle tasolle ottamalla käyttöön seuraavia kovennuksia: • Monivaiheinen tunnistautuminen • Sertifikaattipohjainen kirjautuminen • Domain-liitetty tai muuten yrityksen hallitsema päätelaite • Lähde-IP-osoitteeseen perustuva rajoitus
Arvioi nykyiset salasanakäytännöt	Ylläpitämällä salasanakäytäntöjä asetetaan vähimmäisvaatimukset salasanan monimutkaisuudelle.	Arvioi ja päivitä salasanakäytäntöihin liittyvät ohjeistukset.

5 Tietoturvaloukkauksen jälkiselvitys

Kriisin päätyttyä ja liiketoimintojen normalisoiduttua on tärkeää käynnistää hyökkäyksen jälkiselvitys ja oppia tapahtuneesta tulevaisuutta varten. Samalla kriisinhallintasuunnitelmat on syytä päivittää tehtyjen havaintojen mukaan. On mahdollista, että organisaatio joutuu uudelleen vastaavan hyökkäyksen uhriksi, mikäli tapahtuneen juurisyyt eivät selviä eikä tapauksesta oteta opiksi.

Jälkiselvityksessä (engl. Post Incident Review) tarkastellaan toimintaa kriisitilanteessa: mitkä toimet tehtiin hyvin, missä oli parantamisen varaa ja kuinka voidaan parantaa turvallisuustasoa ja -suunnitelmia. Jälkiselvityksestä on syytä laatia raportti, joka tarkastelee tapahtumien kulun lisäksi ainakin seuraavia kysymyksiä:

- Tapahtuman juurisyyt
    - Mitkä tekniset tai toiminnalliset heikkoudet johtivat tilanteeseen?
- Oman suojauksen tehokkuus
    - Olivatko hyökkäyksien havaitsemista varten käytetyt kontrollit riittäviä?
    - Aiheuttivatko hyökkääjän toimet hälytyksiä?
    - Miten hälytyksiin reagoitiin? Välittyikö tieto hälytyksistä oikeille vastuuhenkilöille?
- Toiminta kriisitilanteessa
    - Noudatettiinko kriisisuunnitelmaa? Miten käyttökelpoinen se oli?
    - Jaettiinko kriisiryhmän vastuut oikeille henkilöille?
    - Miten hyökkäyksen rajaamisessa ja hyökkääjän karkottamisessa onnistuttiin?
    - Kuinka kriisiryhmän viestintä onnistui? Miten sidosryhmät huomioitiin?
- Palautuminen
    - Miten kriittisten tietojen ja palveluiden palautuminen onnistui?
- Jälkiselvitys
    - Onko tapahtumien kulku ja selvitystyö dokumentoitu?
    - Oliko tapauksen tekninen tutkinta riittävää? Onko esim. viranomaisten käyttöön voitu toimittaa riittävät aineistot hyökkäyksestä?
    - Arvioi palvelutoimittajien toimintaa. Oliko vasteaika ja sovitut palvelut riittäviä tapauksen selvittämistyötä varten?

Organisaation tulee päivittää omaa poikkeamanhallintasuunnitelmaansa ja tarkempia erilaisten poikkeamien torjuntaan suunniteltuja pelikirjoja tapahtuneen jälkeen. On myös suositeltavaa harjoitella eri skenaarioita säännöllisin väliajoin, jotta niiden hyöty kriisitilanteissa voidaan varmistaa.

Kyberturvallisuuskeskus toivoo, että yritykset ja organisaatiot jakaisivat sillekin tärkeimmät poikkeamasta saamansa opit. Tapausraporttien avulla Kyberturvallisuuskeskus voi auttaa muita organisaatioita Suomessa ja kansainvälisesti vastaavien tapauksen selvittämisessä. Palautumisesta saadut opit auttavat kehittämään kaikkien organisaatioiden varautumist

HUOLTOVARMUUSKESKUS

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-814-0

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus