TIETOTURVA MICROSOFT WINDOWS -VERKOISSA

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietotekniikan koulutusohjelma

Forssan yksikkö, 20.12.2012

Jukka Moisander

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

FORSSAN YKSIKKÖ
Tietotekniikan koulutusohjelma
Tietokonetekniikan suuntautumisvaihtoehto

Tekijä Jukka Moisander **Vuosi** 2012

Työn nimi Tietoturva Microsoft Windows -verkoissa

TIIVISTELMÄ

Tietoturva on asia, johon kiinnitetään paljon huomiota nykypäivänä, mutta käytännössä monet Microsoft-käyttöjärjestelmiin perustuvat verkot ovat silti erittäin alttiita tietoturvaongelmille. Tietotekniikka-alalla tietoturvalla ja sen kehittämisellä on siis erittäin tärkeä rooli, sillä tietoturvauhat lisääntyvät koko ajan.

Tämän työn tarkoitus oli saada lukija ymmärtämään, millaisia uhkia nykyaikaisessa Microsoft-käyttöjärjestelmiin perustuvassa verkossa on ja miten näitä uhkia voidaan mahdollisimman tehokkaasti yrittää torjua ja estää. Työssä annettiin yleisiä neuvoja ja esimerkkejä, joiden avulla tietoturvauhkia voi pyrkiä minimoimaan ja joiden avulla myös Microsoft Windows -käyttöjärjestelmiä käyttävistä verkoista voidaan tehdä mahdollisimman turvallisia.

Työn sisältö perustuu osaltaan työelämässä opittuihin asioihin sekä eri tietoturva-yhteisöjen kautta kerättyihin tietoihin. Työn kirjoittajalla on työkokemusta useiden vuosien ajalta tietotekniikka-alan yrityksissä. Erityisesti kirjoittaja on erikoistunut tietoturvaohjelmiin ja niiden käyttämiseen.

Avainsanat Tietoturva, verkkojen tietoturva, haittaohjelmat, palomuurit ja salaus

Sivut 26 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

Forssa
Degree Programme in Information Technology
Computer Engineering

Author Jukka Moisander **Year** 2012

Subject of Bachelor's thesis Security in Microsoft Windows Networks

ABSTRACT

Data security gathers a lot of space in media nowadays, but still many Microsoft-based Networks suffer from problems with data security. New threats are developed nowadays faster than before. That is why data and computer security play a very important role in security industry.

The aim of this work was that the readers could learn to understand what kind of threats there are nowadays in Microsoft Windows Networks and how those threats could be blocked. Some general advice and hints how to minimize the possible security risks were given, as well as how to make Microsoft Windows Networks safer.

This work is based on experience that the author has gained in the professional life and from different data security communities. The author of this thesis has years of experience of working in IT-companies. In addition, he has focused on data security programs during his career.

Keywords Data security, network security, malware, firewalls and data encryption

Pages 26 p.

admin/verkon pääkäyttäjä/järjestelmänvalvoja – Nämä käsitteet tarkoittavat verkon pääoikeuksien haltijaa, joka ylläpitää järjestelmiä ja jakaa verkko-oikeuksia muille käyttäjille.

adware – Adware on mainostusohjelma.

antirootkit – Antirootkit-ohjelmisto on ajuritasolla ja järjestelmän ytimeen asentuvia haittaohjelmia tunnistavaohjelmisto.

antivirus – Antivirus-ohjelmisto on haittaohjelmien tunnistamista toteuttava virustorjuntaohjelmisto.

blacklisting – Blacklisting tarkoittaa kiellettyjen toimintojen listaamista.

bot – Botti tai bot-ohjelma yleensä suorittaa järjestelmässä jotakin sille annettua tehtävää, esimerkiksi verkkohyökkäyksiä.

DDoS attack/palvelunestohyökkäys – DDoS (Distributed Denial-of-Servise attack) eli palvelunestohyökkäys on hyökkäys, jolla koetetaan lamaannuttaa laitteisto, jotta se ei pystyisi vastaamaan verkkopyyntöihin.

DLP – DLP (Data Leak Prevention/Data Loss Prevention/Data Leak Protection) tarkoittaa tekniikkaa, jolla estetään tiedon leviäminen järjestelmän ulkopuolelle.

DNS – DNS (Domain Name System/ Domain Name Service) on nimipalvelinjärjestelmä, joka luo verkkoon liitetyille kohteille domain nimet ja muuntaa näitä nimiä IP-osoitteiksi.

Exchange – Exchange on Microsoftin sähköpostipalvelin.

Fileserver – Fileserver tarkoittaa tiedosto palvelinta.

haittaohjelma – Haittaohjelma on ohjelma, jolla on haitallinen tarkoitus. Näitä ohjelmia yleensä kutsutaan myös viruksiksi tai muilla vastaavilla nimikkeillä.

heurestiikka – Haittaohjelmien torjunnassa heurestiikka tarkoittaa tapaa etsiä tuntemattomia haitallisia ohjelmia.

HIPS – HIPS eli ”Host-based Intrusion Prevention System” on ohjelmisto, jolla ehkäistään ei-toivottuja muutoksia käyttöjärjestelmässä.

HTTPS – HTTPS (Hypertext Transfer Protocol Secure) tarkoittaa salattua verkkoyhteyttä.

IDS – IDS (Intrusion Detection System) tarkoittaa tunkeutumisen tunnistamisjärjestelmää, jolla tunnistetaan järjestelmään tunkeutuvia kohteita.

image/levykuva – Imagen eli levykuvan luominen tarkoittaa kokonaisen kiintolevyn, kiintolevyn osion tai median tallentamista tiedostoksi.

IPS – IPS (Intrusion Prevention System) tarkoittaa tunkeutumisen estojärjestelmää, joka estää järjestelmään tunkeutumisen.

keylogger – Keylogger-ohjelmisto on ohjelmisto, jonka avulla tallennetaan näppäinpainalluksia.

malware – Malware on englanninkielinen termi sanalle haittaohjelma.

palomuuri – Palomuuri on verkkoliikennettä tarkkaileva laite tai ohjelma, joka sallii tai estää verkkoyhteyksiä.

PGP – PGP (Pretty Good Privacy) on salakirjoitus ohjelmisto, jonka avulla salauksia voi purkaa ja luoda.

pilvipalvelu – Pilvipalvelu on palvelu, jota käytetään verkon yli.

portti – Portti on verkkoon liittyvä kohde, mistä tieto lähtee tai minne tieto toimitetaan, jotta se kulkisi oikealle ohjelmalle.

proaktiivinen suojaus – Proaktiivinen suojaus tarkoittaa ennalta ehkäisevää suojausta.

protokolla – Protokolla on säännöstö tai standardi, joka mahdollistaa ja määrittelee yhteydet, joiden avulla laitteet tai ohjelmat kommunikoivat keskenään.

ransomware – Ransomware tarkoittaa panttivankiohjelmaa, joka ottaa tietoja panttivangiksi.

rogue – Rogue-ohjelmisto on jokin ohjelmisto, joka on naamioitunut tekemään jotakin muuta, mitä se oikeasti tekee.

rootkit – Rootkit-ohjelmisto on järjestelmän sisällä tai ytimessä, esimerkiksi ajuritasolla, toimiva haitallinen ohjelmisto.

sandbox – Ohjelmissa sandbox eli hiekkalaatikko tarkoittaa koodin suorittamista virtuaalijärjestelmässä eristyksissä varsinaisesta käyttöjärjestelmästä. Tietoturvassa sama käsite tarkoittaa selvittämistä, pyrkiikö ohjelmisto haitalliseen toimintaan.

screenlogger – Screenlogger-ohjelmisto tallentaa kuvakaappauksia kuvaruudusta.

spyware – Sypware tarkoittaa vakoiluohjelmaa.

SSH – SSH (Secure Shell) tarkoittaa salattua verkkoyhteyttä.

troijalainen – Troijalainen on takaporttiohjelma, jonka avulla koetetaan käyttää järjestelmää, jossa troijalainen sijaitsee.

virus – Virus on haittaohjelma, jonka avulla esimerkiksi yritetään aiheuttaa haittaa järjestelmälle, jossa virus on.

VPN – VPN (Virtual Private Network) on julkisen verkon yli käytettävä lähiverkkoyhteys.

whitelisting – Whitelisting tarkoittaa luvallisten toimintojen listaamista.

zeroday/0-päivä – Tarkoittaa hetkeä, jona käytetään tuntematonta haavoittuvuutta tai uutta haittaohjelmistoa, johon ei vielä ole olemassa mitään puolustuskeinoa, järjestelmää vastaan.

SISÄLLYS

1 JOHDANTO

Tietoturva on asia, joka on esillä jatkuvasti tämän päivän tietoverkoissa. Tämä näkyy etenkin Microsoft Windows -käyttöjärjestelmissä, sillä niiden kanssa tietoturvaan liittyviä ongelmia tulee vastaan jatkuvasti. Lähes kaikki verkot on nykyään yhdistetty Internetiin, jonka tarjoamia palveluja käytetään jatkuvasti ympäri maailmaa. Tämän takia kaikki Internetiin kytketyt verkot ovat alttiita myös Internetistä tuleville uhkatekijöille.

Median meille tarjoamissa otsikoissa nähdään todella usein, että yleisesti käytössä olevista ohjelmista löytyy monia haavoittuvuuksia. Näitä haavoittuvuuksia haittaohjelmien kirjoittajat yrittävät käyttää hyväkseen ennen kuin ohjelmistovalmistajat saavat tarvittavat päivitykset valmiiksi ja toimitettua tuotteiden loppukäyttäjille.

Haittaohjelmien suunnittelu ja valmistaminen on nykyään muuttunut yhä ammattimaisemmaksi rikollisissa piireissä liikkuvien suurten rahasummien takia. Haittaohjelmistojen avulla pyrkivät rikolliset esimerkiksi hyötymään rahallisesti haittaohjelman käyttäjästä tai keräämään arvokasta tietoa käyttäjän koneelta.

Nykypäivän haittaohjelmistojen avulla yritetään siis tehdä muun muassa seuraavia asioita:

- kerätä rahaa mainoksia näyttämällä
- kerätä yhteystietoja tai muuta tietoa, kuten salasanoja, käyttäjältä
- seurata esimerkiksi käyttäjän kulutus- tai Internetin-käyttötottumuksia
- huijata rahaa käyttäjältä
- ottaa käyttäjän tietoja panttivangiksi
- ohjata käyttäjää Internetissä haittaohjelman ohjelmoijan haluamille sivuille
- rakentaa botnet-verkkoja
- etähallita käyttäjän konetta tai verkkoa.

Tietoturvan kannalta verkkoliikenteen suojaaminen ja tiedon turvallinen käsittely on nykyaikana erittäin tärkeää. Tämä pätee myös nopealle reagoimiselle verkon ohjelmistohaavoittuvuuksiin.

2 PERUSTIETOJA TIETOTURVASTA JA VERKOISTA

Tässä luvussa käsitellään perustietoja tietoturvasta ja verkoista. Tietoturvasta kerrotaan, mitä se käytännössä tarkoittaa, ja verkoista kerrotaan, mitä Microsoft Windows -verkoilla tarkoitetaan.

2.1 Tietoturva yleisesti

Tietoturvalla tarkoitetaan sitä, että tieto on turvallisesti saatavilla sallituille käyttäjille luotettavana ja muuttumattomana. Käytännössä tämä tietotekniikassa tarkoittaa, että tieto on käytettävissä, turvallisesti tallennettu ja käyttö estetty ulkopuolisilta käyttäjiltä.

Teknisesti tämä tarkoittaa Microsoft Windows -ympäristössä, että työasemat ja palvelimet, joilla tietoa säilytetään tai käsitellään, on luottamuksellisesti sekä asiallisesti tallennettu ja varmennettu ja että ne on suojattu haittaohjelmilta ja luvattomalta käytöltä.

Yleisesti käytetty käsite tietoturva voidaan jakaa kolmeen tietoturvaa kuvaavaan osaan, joita ovat käytettävyys, luottamuksellisuus ja eheys. Termit ovat tietoturvan peruskäsitteitä. (Tietoturvalliseen yhteiskuntaan 2012.) Käytännössä nämä käsitteet tarkoittavat seuraavia asioita:

- Käytettävyys – Tieto on saatavilla esteettä, kun sitä tarvitaan. Tämä tarkoittaa, että tiedostoihin on pääsy ja niitä voidaan käyttää, kunhan käyttäjällä on oikeus käyttää kyseistä tietoa.

- Luottamuksellisuus – Tieto on saatavilla vain niille, joilla siihen on oikeudet. Ulkopuolisten pääsy tietoon on estetty.

- Eheys – Tieto pysyy muuttumattomana ja luotettavana. Myös vikatilanteissa tieto on asiallisesti varmistettu.

2.2 Microsoft Windows -verkot

Microsoft Windows -verkoilla tarkoitetaan verkkoja, joissa on yhdistetty samaan verkkoon Microsoft Windows -käyttöjärjestelmillä varustettuja laitteita. Tämän tyylisiä verkkoja ovat suurin osa suomen pienten ja keskisuurten yritysten käyttämistä verkoista.

Kun puhutaan Microsoft Windows -verkosta, tarkoitetaan tilannetta, jossa työasemissa käyttöjärjestelmänä käytetään Microsoft Windows -käyttöjärjestelmää. Lisäksi palvelinlaitteissa käytetään Microsoftin palvelinsovelluksia, joita ovat esimerkiksi Small Business Server, Windows Server, Exchange, Microsoft SQL Server tai Sharepoint Server.

3 TIETOTURVAUHAT

Tämän päivän tietoverkkoja ja käyttöjärjestelmiä uhkaavat monet erilaiset uhat. Uhkien määrä kasvaa jatkuvasti, koska tietoturvarikokset ovat usein tuottoisia ja vähän riskiä sisältäviä rikoksia.

Tietoturvarikoksista on olemassa tutkimustietoa, joka osoittaa, miten paljon taloudellista vahinkoa verkkorikollisuus aiheuttaa. Symantecin tekemän tutkimuksen mukaan 431 miljoonaa aikuista ihmistä joutui vuonna 2010 verkkorikoksen uhriksi. Rikosten kustannukset olivat kokonaisuudessaan 388 miljardia Yhdysvaltain dollaria. Symantecin mukaan verkkorikollisuudessa liikkuu enemmän rahaa kuin huumerikollisuudessa. (Skantz & Kestilä 2011.)

3.1 Luottamuksellisen tiedon leviäminen

Luottamuksellista tietoa voi vuotaa verkon ulkopuolelle useilla eri tavoilla. Riskiin kannatta varautua huolella, jos järjestelmässä käsitellään tietoa, jonka päätyminen vääriin käsiin voi aiheuttaa suuria kustannuksia tai ongelmia verkon käyttäjille tai verkon omistavalle organisaatiolle.

Suurimpia riskejä, jotka voivat altistaa tiedon menettämiselle, ovat huono tietoturvapolitiikka, käyttäjien oikeuksien hallinta, haittaohjelmien torjunnassa olevat puutteet tai verkkokäyttäjien aiheuttama uhka. Jos esimerkiksi verkon käyttäjä tallentaa luottamuksellista tietoa ulkoiselle medialle ja jatkaa tiedon käsittelyä turvattomassa verkossa, voi tämä aiheuttaa luottamuksellisen tiedon päätymisen vääriin käsiin.

3.2 Haittaohjelmat

Haitalliset ohjelmat, kuten virukset, madot, Troijan-hevoset ja muut malware-haittaohjelmistot, ovat eniten otsikoissa viihtyviä tietoturvauhkia Microsoft-käyttöjärjestelmille. Haittaohjelmat ovat periaatteessa tavallisia ohjelmia, mutta niiden tarkoitus on toimia haitallisesti loppukäyttäjää kohtaan.

Haittaohjelmistot voidaan jakaa useaan eri ryhmään, joista käydään seuraavaksi muutamia läpi.

- Mainostusohjelmat
  → Pyrkivät esittämään mainoksia käyttäjälle.
- Huijausohjelmistot (rogue, fakealert)
  → Pyrkivät huijaamaan käyttäjältä rahaa tai luottokorttitietoja.
- Madot (worm)
  → Yrittävät levitä automaattisesti eteenpäin.
- Troijalaiset ja takaporttiohjelmat (Trojan, backdoor)
  → Yrittävät saada laitteen, jossa ohjelmat sijaitsevat, etäkäyttäjän haltuun.
- Vakoiluohjelmat (spyware)
  → Pyrkivät keräämään tietoja järjestelmästä ja lähettämään niitä eteenpäin.

Haittaohjelmien pääasiallinen tarkoitus on kerätä rahaa niiden kehittäjille, mutta osa haittaohjelmista on myös kohdennettu jotain yritystä tai tiettyä laitetta kohtaan. Näissä tapauksissa voidaan puhua kohdennetuista haittaohjelmahyökkäyksistä. (Tietoturvakatsaus 3/2007 2007.)

Nykypäivän haittaohjelmia on myös allekirjoitettu tunnettujen ohjelmistovalmistajien digitaalisilla sertifikaateilla. Tällaisissa tapauksissa tietoturvaohjelmistot saattavat sallia haittaohjelmien toiminnan. Esimerkkinä tällaisesta tapauksesta voidaan pitää Adoben varmenteilla allekirjoitettuja haittaohjelmia. (Adoben ohjelmistovarmenteella allekirjoitettu haittaohjelmia 2012.)

3.2.1 Haittaohjelmien aiheuttamat uhat

Haittaohjelmat ovat ohjelmistoja, joiden tarkoitus on olla jollekin osapuolelle hyödyllinen toisen osapuolen kustannuksella. Haittaohjelmia kutsutaan usein myös viruksiksi. Kuitenkin nämä ohjelmat ovat aivan normaalisti ohjelmoituja ohjelmia eli ne ovat perimmäiseltä rakenteeltaan samankaltaisia kuin ei-haitalliset ohjelmat.

Aluksi haittaohjelmat tehtiin kiusantekoa ja ohjelmointitaitojen näyttämistä varten, mutta nykyään ne ovat ammattimaisesti koodattuja monimutkaisia ohjelmistokokonaisuuksia, joilla on jokin tietty tarkoitus. Yleensä tämä tarkoitus on joko vakoilu tai rahan ansaitseminen.

Esimerkkinä rahan ansaitsemiseen tarkoitetusta haittaohjelmasta on Suomessa levinnyt ohjelma, joka yritti poliisin nimissä saada uhrin maksamaan rahaa rikollisille. Haittaohjelma lukitsi käyttäjän Windows-järjestelmän käyttökelvottomaksi ja näytti käyttäjälle viestin, jossa kehotettiin poliisin nimissä maksamaan rahaa tietokoneen lukituksen avaamiseksi. Tämän maksun piti tapahtua käyttämällä Paysafe-palvelua, jonka kautta siirrettyä rahaliikennettä ei voi seurata. Vaikka käyttäjä maksoi vaaditun summan, ei lukitus poistunutkaan koneelta. (Haittaohjelma vaatii rahaa Suomen poliisin nimissä – älä maksa 2012.)

Ammattimaisesti kirjoitetuista ohjelmistoista on hyvänä esimerkkinä Yhdysvaltojen ja Israelin hallitusten tuella tehty Stuxnet-haittaohjelma. Tässä tapauksessa kyseessä oli kohdistettu hyökkäys Iranin ydinvoiman kehityslaitoksia vastaan. (Anderson 2012.) Stuxnet käytti leviämiseen varastettuja sertifikaatteja ja pystyi näin asentumaan helposti järjestelmiin. Stuxnet pystyi leviämään myös muistitikkujen kautta erittäin tehokkaasti. F-Securen mukaan USA aloitti verkkohyökkäysprojektin Irania vastaan jo vuonna 2008. (New Info on Stuxnet 2011.)

On huhuttu, että Saksan valtiolla olisi oma haittaohjelmansa kansalaisten vakoiluun. Intelnews-sivuston mukaan Saksan valtio olisi myös myöntänyt vakoilleensa kansalaisia. (Fitsanakis 2012.) Samoin on liikkunut huhua, että saksalaisviranomaiset olisivat olleet yhteyksissä tietoturvayrityksiin, jotteivät tietoturvaohjelmat estäisi heidän vakoiluohjelmaansa. (Jääskeläinen 2011.)

Haittaohjelmat pyrkivät leviämään käyttämällä hyväkseen ohjelmistohaavoittuvuuksia, ihmisten hyväluuloisuutta, kopioimalla itsensä automaattisesti tai ne pyrkivät asentumaan järjestelmään esimerkiksi massamuistilta. Yleinen tapa saada käyttäjä avaamaan haitallinen tiedosto on naamioida se joksikin muuksi tiedostoksi. Tässä käytetään yleensä hyväksi ihmisten hyväuskoisuutta ja uteliaisuutta. Tiedosto tai linkki tiedostoon voidaan esimerkiksi jakaa sähköpostilla tai sosiaalisella medialla uhrille.

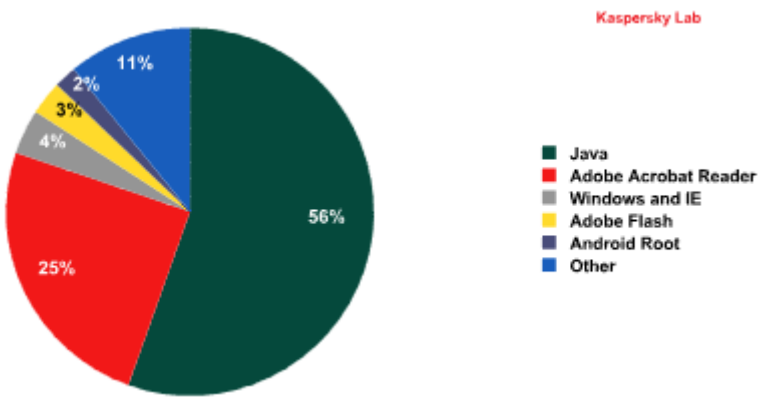
3.3 Ohjelmistojen haavoittuvuudet

Ohjelmistojen haavoittuvuudet ovat tietoturvan kannalta erittäin haastava ongelma. Mitä enemmän eri ohjelmia on käytössä, sitä tärkeämpää on pitää ohjelmistot ajan tasalla. Ohjelmistohaavoittuvuuksilla tarkoitetaan ohjelmointivirheitä, jotka voivat pahimmassa tapauksessa antaa haavoittuvuuden tuntijalle valtuudet suorittaa mielivaltaisesti haluamaansa koodia järjestelmässä, jossa käytetään haavoittunutta ohjelmaa.

Esimerkiksi Microsoft Windows -käyttöjärjestelmistä ja Microsoft-oheisohjelmista löytyy säännöllisesti haavoittuvuuksia, joiden avulla järjestelmässä voidaan suorittaa haitallista toimintaa. Microsoft päivittää käyttöjärjestelmiään tämän takia säännöllisesti. Esimerkiksi marraskuussa 2012 Microsoft julkaisi kuusi päivitystä, joilla korjattiin 19 haavoittuvuutta. (Baumgartner 2012.)

Esimerkki haavoittuvuuksien hyväksikäytöstä on tiettyjen PDF-tiedoston lukuohjelmistojen hyväksikäyttäminen niin, että avattavan PDF-tiedoston sisään on lisätty koodia, jonka lukuohjelma haavoittuvuuden takia suorittaa tiedostoa avattaessa.

Kaspeskyn syksyllä 2012 julkaisemasta osavuosikatsauksesta voidaan tarkastella yleisimpiä haavoittuvuuksia. Eniten ohjelmistohaavoittuvuuksista ovat kärsineet vuoden 2012 kolmannella neljänneksellä Java ja Adoben Acrobat Reader. (Namestnikov 2012.) Tulokset löytyvät kuviosta 1, jossa on esitetty tulokset ympyrädiagrammissa.



KUVIO 1 *Kasperskyn syksyn 2012 osavuosikatsauksen tulokset (Namestnikov 2012.)*

3.4 Laiterikot

Myös laiterikot ovat uhka tietoturvalle. Näissä tapauksissa etenkin huonosti järjestetty varmuuskopiointi saattaa altistaa tiedon katoamiselle.

Rikkinäisen laitteen poisheittäminen saattaa altistaa tiedon päätymiselle vääriin käsiin. Riskialtista on esimerkiksi rikkoutuneen kovalevyn heittäminen roskiin ilman ylikirjoittamista. Rikkoutuneelta levyltä saatetaan pystyä helpollakin tavalla lukemaan tietoja. Erityisesti luottamuksellista tietoa sisältänyt laite tai muisti on hyvä tuhota luotettavalla tavalla, jotta vältetään tiedon joutuminen vääriin käsiin.

Mikäli rikkoutuneen massamuistin sisältämää dataa ei pystytä enää ylikirjoittamaan, on syytä hävittää muisti murskaamalla se palasiksi tietoturvavuodon ehkäisemiseksi.

3.5 Laitteisto- ja komponenttipohjaiset uhat

Laitteistopohjaisiin tietoturvauhkiin ei yleensä kiinnitetä paljon huomioita. Yksi esimerkki hardware-uhasta on langattomien laitteiden käyttö. Niiden kohdalla uhkana on, että langattomien laitteiden lähettämiä signaaleja on mahdollista vastaanottaa myös ei-toivotuissa kohteissa.

Yksinkertaisena esimerkkinä langattomiin laitteisiin liittyvistä uhista voidaan mainita langattoman näppäimistön aiheuttama tietoturvariski. Ulkopuolisen tahon on mahdollista tallentaa tällaisen näppäimistön laitteiston vastaanottimeen lähettämää signaalia. Tallennettua signaalia voidaan käyttää käyttäjän tietojen varastamiseen.

Myös langallisen näppäimistön ja PC-laitteen väliin on tehty laitteita, jotka tallentavat näppäimistöpainallukset. Niillä voidaan pyrkiä samoihin asioihin kuin langattomien näppäimistöjen painallusten tallentamisella eli saamaan epärehellisellä tavalla käyttäjän tietoja haltuun.

Laitteistojen, komponenttien ja oheislaitteiden muisteihin saattaa päästä haitallisia ohjelmakoodeja, joita voidaan suorittaa ilman, että tietoturvaohjelmat pystyvät havaitsemaan suoritettavaa koodia. Esimerkiksi näytönohjaimen BIOS-piirille piilotettu haitallinen ohjelmakoodi on mahdollista ajaa PC-laitteiston muistiin ilman, että käyttäjä tai tietoturvaohjelmistot sitä havaitsevat.

3.6 Verkkolaitteiden kaappaukset

Palomuureja, modeemeja, kytkimiä ja reitittimiä on mahdollista etäkonfiguroida. Tämä luo riskin, että tunkeutuja voi muokata käyttäjän laitteiston asetuksia haluamallaan tavalla. Esimerkkinä voidaan mainita DSL-

päätelaitteen kaappaukset, joissa tunkeutuja vaihtaa esimerkiksi nimipalvelinasetukset, joiden avulla hän voi ohjata Internetin käyttäjät haluamilleen sivustoille.

Myös verkkoliikenteen seuranta ja tallennus voi onnistua kaapatulta verkkolaitteelta. Tämä aiheuttaa riskin, että ulkopuolinen taho pääsee käsiksi verkossa liikkuvaan dataan.

Reititin ja palomuuri saattavat myös aiheuttaa tietoturvariskin. Tunkeutuja voi muokata laitteen asetuksia haluamallaan tavalla, esimerkiksi avaamalla itselleen pääsyn sisäverkkoon (LAN, Local Area Network) Internetin yli.

3.7 Käyttöoikeuksien hallinta

Käyttäjäoikeuksien avulla säädellään, kenellä on oikeus päästä käyttämään palvelimella mitäkin tiedostoja. Tämä aiheuttaa tietoturvariskin, jos käyttäjälle annetaan vääriä oikeuksia. Tästä voidaan esimerkkinä mainita pääsy muiden verkon käyttäjien kansioihin, jolloin luottamuksellisen tiedon tallentaminen asemalle on turvatonta.

3.8 Verkkohyökkäykset

Verkkohyökkäyksillä yritetään yleensä etsiä haavoittuvuuksia, avoimia portteja tai ruuhkauttaa hyökkäyksen kohteena oleva verkko tai järjestelmä toimintakyvyttömäksi. Tietoviikko uutisoi syksyllä 2012, että viikoittain tehdään 102 onnistunutta verkkohyökkäystä. (102 onnistunutta nettihyökkäystä viikossa 2012.)

Yksi esimerkki verkkohyökkäyksestä on palvelunestohyökkäys, jossa lähetetään kohteelle niin paljon dataa, ettei kohde pysty enää käsittelemään muita verkkopyyntöjä. Tämänkaltaista hyökkäystä käytetään usein verkkopalvelimia kohtaan tarkoituksena lamauttaa palvelimien sujuva toiminta.

Toinen esimerkki verkkohyökkäyksestä on Man-in-the-middle attack, jossa hyökkääjä pyrkii pääsemään verkkoliikenteen väliin ja väärentämään verkkoliikennettä. Tällainen tilanne voisi olla esimerkiksi verkkopankin käyttö, jossa käyttäjän ja verkkopankin välillä hyökkääjä väärentää verkkoliikennettä omiin tarkoituksiinsa sopivaksi ja samalla pyrkii olemaan näkymätön molempiin suuntiin.

Botnet-verkkojen avulla hyökkääjä voi tukkia esimerkiksi sähköpostipalvelimen roskapostilla tai lähettää jollekin WWW-palvelimelle niin paljon sivunlatauspyyntöjä, että palvelin ei pysty vastaamaan kaikkiin pyyntöihin.

Uutena verkkohyökkäystrendinä ovat olleet niin kutsutut evaasiohyökkäykset, joissa IDS-järjestelmiä (Intrusion Detection System) ja IPS- (In-

trusion Prevention System) järjestelmiä hämätään pakkaamalla tai pilkkomalla haluttu data niin monta kertaa, etteivät järjestelmät pysty sitä havaitsemaan. Kuitenkin näissä tapauksissa esimerkiksi työaseman käyttöjärjestelmä on pystynyt suorittamaan paketteihin tai osiin jaetun koodin.

Yksinkertaisimmillaan evaasiohyökkäys on TCP/IP-pakettien lähettämistä osissa viiveellä. Tällöin tunkeutumisenestojärjestelmä ei huomaa haitallista verkkoliikennettä ja datapaketit saadaan välitettyä kohdejärjestelmälle. (Lehto 2010.)

Myös langattomien verkkojen liikennettä voidaan kaapata, jos liikenne ei ole salattua tai salaus on purettu. Etenkin käyttäjätunnuksia ja salasanoja kaapataan usein salaamattomista langattomista verkoista, jos verkkopalveluihin kirjaudutaan ilman kunnollista salausta.

3.9 Kohdennettu hyökkäys

Kohdennetulla hyökkäyksellä tarkoitetaan sitä, että haluttuun kohteeseen tehdään uniikki haittaohjelma tai verkkohyökkäys. Esimerkkinä voidaan mainita yritysvakoilua varten tehty haittaohjelma, jota levitetään vain kohdeyritykselle. (Seeling 2011, 12–13.)

Toisena esimerkkinä on haittaohjelma, jolla yritetään saada etäkäyttöön jokin tietty järjestelmä halutusta verkosta. Haittaohjelma aktivoituu vasta silloin, kun se huomaa olevansa tietynlaisessa ympäristössä. Tästä esimerkkinä toimii Yhdysvaltain tekemä Stuxnet-haittaohjelma, joka hyökkäsi Lähi-idässä oleville tietokoneille yrittäen ilmeisesti saada haltuunsa ydinvoimalaitoksia ohjaavia yksikköjä. Erityistä tässä hyökkäyksessä oli, että siinä käytettiin väärennettyjä sertifikaatteja. Tapauksesta mainittiin tarkemmin jo aiemmin opinnäytetyössä. (ks. sivu 4)

3.10 Mobiililaitteet

Mobiililaitteet voivat olla monitahoinen riski verkossa olevalle tiedolle. Mobiililaitteita ovat esimerkiksi kannettavat tietokoneet, taulutietokoneet, kämmentietokoneet, matkapuhelimet ja muut kannettavat älylaitteet.

Kannettavat tietokoneet, jotka kytketään verkkoon, saattavat aiheuttaa tietoturvaongelmia, mikäli ohjelmistot eivät ole ajan tasalla tai laitteessa on asennettuna haittaohjelmia. Verkonvalvojan on lisäksi vaikea olla ajan tasalla laitteista, jotka satunnaisesti ovat kytkettynä verkkoon. Lisäksi monet älylaitteet voivat olla yhteydessä yrityksen sisäverkkoon ja samalla käyttää 3G- tai 4G-verkkoyhteyksiä Internetiin. Tämä luo riskin, että verkkoliikennettä pääsee lähiverkon palomuurin ohi. Pahimmillaan etäkäyttöön kaapattu mobiililaite voi avata hyökkääjälle pääsyn suojattuun lähiverkkoon.

Toinen suuri riski mobiililaitteissa ja niiden käytössä on laitteen mahdollinen katoaminen ja tätä kautta tiedon päätyminen vääriin käsiin. Kannettavia laitteita katoaa paljon ja usein laitteet on asennettu käyttämään etänä kodin tai työpaikan verkkoresursseja. Tämä luo riskin, että kadonneella tai varastetulla mobiililaitteella voidaan käyttää näitä verkkoresursseja haitallisesti.

3.11 Massamuistit

Erilaisten massamuistien kytkeminen verkossa oleviin laitteisiin aiheuttaa riskin, että haitalliset ohjelmat tarttuvat massamuistilta järjestelmään. Myös massamuistin katoaminen aiheuttaa riskin, että tieto päätyy vääriin käsiin. Massamuistit, kuten pienet USB-muistitikut, on helppo kadottaa.

3.12 Sisäiset uhkatekijät

Verkon käyttäjät aiheuttavat suurimman tietoturvariskin. Huolimaton työskentely, tietämättömyys ja inhimilliset virheet ovat usein tietoturvaongelmien taustalla. On tärkeää määritellä, kuka tietoa saa käyttää ja miten sitä käytetään. Käyttäjien oikealla ohjeistuksella voidaan ehkäistä tehokkaasti tietoturvaongelmia. Käyttäjille tulisi myös määritellä oikeudet siitä, miten ja mihin heillä on pääsy laitteistossa.

3.13 Verkon käyttäjät

Verkon käyttäjän tietotaitoja on syytä ylläpitää. Etenkin tiedostojen käsittelyn ja käyttöjärjestelmän ja käytettävien ohjelmien käytön tulisi olla hyvällä mallilla.

Verkon käyttäjän asenne tietoturvaa kohtaan voi olla ratkaiseva tekijä tietoturvaongelmien ennaltaehkäisyssä. Välinpitämättömyys voi johtaa siihen, että tärkeää tietoa voi kadota tai joutua vääriin käsiin tai että haitallista toimintaa pääsee tapahtumaan verkossa.

Verkon pääkäyttäjä eli ”admin” on yleensä verkon suurin tietoturvariski. Pääkäyttäjällä on yleensä pääsy verkon kaikkeen tietoon ja verkonkäyttäjien tileihin, eli tätä kautta mahdollisuus aiheuttaa suurinta mahdollista tieturvaan liittyvää tuhoa. Jotta pääkäyttäjän aiheuttamat ongelmat voitaisiin välttää, verkon pääkäyttäjä tulisi valita huolella ja hänen toimiaan tulisi valvoa.

3.14 Ulkoiset uhat

Yksi verkon ulkopuolisista uhkatekijöistä on muun muassa sosiaalinen hakkerointi, jolla verkon käyttäjiltä yritetään saada haltuun käyttäjätun-

nuksia tai salasanoja, joita myöhemmin hyödyntämällä verkkoa voidaan luvatta käyttää.

Muita ulkoisia uhkia tiedon kannalta ovat esimerkiksi tulipalot ja luonnon katastrofit, jotka voivat aiheuttaa fyysisiä uhkia tiedoille. Myös kaikki laitteisiin käsiksi pääsevät ihmiset voidaan lukea ulkoisiksi uhiksi.

3.15 Puutteet verkon tietoturvapolitiikassa

Tietoturvapolitiikalla tarkoitetaan sovittuja käytäntöjä ja sääntöjä liittyen siihen, miten verkossa työskennellään ja mitä asioita otetaan huomioon, ettei tietoturva vaarannu. Näitä tietoturvan vaarantavia käytäntöjä, joista tietoturvapolitiikan avulla pyritään eroon, ovat esimerkiksi laitteiden kytkeminen luvatta verkkoon, helppojen salasanojen käyttö, salasanan alhainen vaihtotiheys ja luotettavan tiedon puutteellinen salaus.

3.16 Etäkäyttö

Etäkäytön aiheuttamat tietoturvaongelmat liittyvät usein käyttäjän tunnistamiseen, etäkäyttäjän oman järjestelmän luotettavuuteen ja luvattomaan etäkäyttöön.

Jos verkon resursseja on sallittu etäkäyttää, on myös mahdollista, että verkon resursseja saattaa käyttää taho, jolla ei olisi oikeuksia verkon käyttöön.

3.17 Verkkorikollisuus

Verkkorikollisuus on tänä päivänä erittäin tuottoisaa, ja rikollisilla on paljon resursseja käytettävänään tietoverkkorikoksiin. Verkkorikolliset aiheuttavat paljon haittaa niin yksityisille kuin julkisille yrityksillekin. Useimmiten tietoturvayhtiöt tulevat hieman perässä verkkorikollisuuteen nähden, sillä yleensä pitää ensiksi olla jokin uhka tai haavoittuvuus, jota käytetään hyväksi ennen kuin siihen saadaan tehtyä korjaus.

Verkkorikolliset ovat siis siellä, missä raha liikkuu. Verkkokauppahuijauksia, verkkopankkien väärinkäytöksiä, palvelunestohyökkäyksiä, kiristämistä ja tietojen panttivangiksi ottamista tapahtuu jatkuvasti. Osa verkkorikollisten hyökkäyksistä on jopa kohdistettu vain tiettyjä organisaatioita kohtaan.

4 SUOJAUTUMINEN TIETOTURVAUHKIA VASTAAN

Tässä luvussa käsitellään suojautumista yleisimpiä tietoturvauhkia vastaan. Täydellistä tietoturvaa ei pysty takaamaan mitenkään, mutta uhkatekijöitä voidaan minimoida. Aluksi pitää kartoittaa, millainen tarve verkolla on tietoturvan osalta sekä miten arvokasta ja luottamuksellista tietoa verkossa on. Tämän jälkeen valmistellaan järkeväntasoinen tietoturvasuunnitelma.

4.1 Tietoturvasuunnitelma

Tietoturvasuunnitelma on oleellinen osa tietoturvan hyvää toimivuutta. Suunnitelmassa määritellään, mitä pitää suojata, miten suojata ja miksi. Samoin siinä määritellään, kenellä on pääsy mihinkin tietoon ja miten tiedot tulisi varmistaa. Suunnitelma on yleensä ”elävä” ja sitä muokataan ajan kanssa vastaan tulevien tarpeiden mukaisesti.

Yksinkertaisimmillaan tietoturvasuunnitelma voidaan tehdä laskemalla, miten paljon vahinkoa ja kuinka suuret kustannukset tiedon katoamien tai päätyminen vääriin käsiin voi aiheuttaa. Tämän jälkeen mitoitetaan tietoturva ja sen kustannukset mahdolliseen uhkakuvaan.

4.2 Suojautuminen haittaohjelmia vastaan

Haittaohjelmia vastaan suojautuminen toteutetaan perinteisesti virustorjuntaohjelmistoilla. Nykypäivänä tämä ei pelkästään kuitenkaan riitä kehittyneitä haittaohjelmia ja niiden nopeaa julkaisutahtia vastaan.

Nouseva trendi tällä hetkellä haittaohjelmatorjunnassa ovat whitelisting- ja blacklisting-teknologiat. Whitelisting tarkoittaa sitä, että vain tietyt tiedostot ja toiminnot sallitaan, ja kaikki muu on estetty. Blacklisting tarkoittaa kieltolistaa, jossa listataan, mitkä tiedostot ja toiminnot ovat kiellettyjä.

Esimerkkinä whitelisting-teknologiasta ovat HIPS-sovellukset, jotka yleensä toimivat niin, että kaikki paitsi järjestelmässä sallitut toimenpiteet estetään tai kysytään käyttäjältä lupaa toimenpiteen suorittamiselle.

Blacklisting-teknologiasta esimerkkinä voidaan pitää perinteistä antivirusohjelmistoa, jossa tietokannalla tunnistetaan haitallisia tiedostoja ja toimenpiteitä. Tunnistamisen jälkeen haitalliset toiminnot sitten estetään ja muut toimenpiteet sallitaan.

4.2.1 Antivirus-ohjelmistot työasemissa

Antivirus-ohjelmistoissa on suuria eroja, eikä minkään valmistajan ohjelmisto tuo täydellistä turvaa. Perinteisesti haittaohjelmia tunnistetaan ”fingerprint” -tietokantojen avulla. Käytännössä tämä tarkoittaa sitä, että hai-

tallisesta tiedostosta määritellään tunniste, jonka perusteella antivirus-ohjelmisto tunnistaa haitallisen sovelluksen.

Viime vuosina antivirus-ohjelmistoja on pyritty parantamaan proaktiivisella suojauksella, jolla pyritään tunnistamaan haittaohjelmia ilman ”finger-print” -tunnistetta.

Antivirus-ohjelmistoissa saattaa olla suuriakin eroja tietokannoissa ja päivittämisnopeudessa. Ohjelmaa valitessa kannattaa ottaa huomioon seuraavat asiat:

- Resurssien käyttö. Työaseman käyttöä hidastavat ohjelmat vaikeuttavat työn tekemistä ja kannustavat käyttäjää tietoturvaohjelman sammuttamiseen.

- Tietokantojen päivitysnopeus. Kertoo, miten nopeasti ohjelmisto reagoi uusiin uhkiin. Valmistajien välillä saattaa olla suuria eroja. Siinä missä toinen tunnistaa liikkeelle lähteneen haittaohjelman muutaman tunnin viiveellä, voi toiselta valmistajalta kestää viikkoja saada haittaohjelma tunnistetuksi.

- Väärä hälytys, eli niin kutsuttu ”false positive”, jolloin ohjelma tunnistaa laillisia ohjelmia haitalliseksi. Tämä voi aiheuttaa pahimmassa tapauksessa jopa käyttöjärjestelmän kaatumisia.

4.2.2 Antivirus-ohjelmistojen testituloksia

Testitulosten seuraaminen on hyvä tapa pysyä selvillä tietoturvaohjelmistojen eroista.

Suuri osa testeistä perustuu passiivisten haittaohjelmatiedostojen tunnistamiseen. Testejä on tehty tämän lisäksi myös ohjelmistojen käytettävyydestä ja nopeudesta. Lisäksi uusia uhkia vastaan on olemassa niin kutsuttuja ”real world” -testejä, joissa haittaohjelmia pyritään suorittamaan järjestelmässä.

AV-Comparatives.org-sivusto on hyvä esimerkki laadukkaasta tietoturvaohjelmistojen testaussivustosta. Tämä kyseinen sivusto tekee kattavia testejä haittaohjelmien tunnistuksessa ja antivirus-ohjelmien proaktiivisessa suojauksessa. (Independent Tests of Anti-Virus Software 2012.)

MRG Effitas Ltd. sivuilla esitetään hyvin, miten nopeasti eri tietoturvaohjelmat reagoivat uusiin uhkiin. Etenkin vuoden 2012 aikana tehtyjä ”flash testejä” on tällä sivustolla runsaasti. (Efficacy Assessment & Assurance 2012.)

AV-Test.org-sivustolla on runsaasti testejä, joissa testataan tietoturvaohjelmia ja niiden tehoa ja käytettävyyttä. (The Independent IT-Security Institute 2012.)

Vuoden 2012 aikana tekemissäni havainnoissa eri testisivujen suhteen olen huomannut, että haittaohjelmien torjunnassa ovat pärjänneet hyvin BitDefender-pohjaiset tuotteet. Näitä tuotteita ovat muun muassa BitDefender, G-data, F-secure, BullGuard ja eScan. Myös Avira, Kaspersky ja Symantec ovat onnistuneet hyvin haittaohjelmatorjunnassa vuoden 2012 aikana.

Seuraavassa esimerkissä esittelen AV-Comparatives.org -sivuston top5-tulokset haittaohjelmien tunnistuskykytestissä syyskuulta 2012. Testissä testattiin ohjelmien kykyä tunnistaa hiljattain kerätyistä 240859 haittaohjelmasta mahdollisimman suuri osa. Seuraavassa on lista eri tietoturvaohjelmien tuloksista:

1. G-Data tunnisti 99,9 % haittaohjelmista
2. Avira tunnisti 99,8 %
3. Panda, Trend Micro tunnistivat 99,6 %
4. F-secure tunnisti 99,3 %
5. Kaspersky, BitDefender, BullGuard, Fortinet ja eScan tunnistivat 99,2 %

(File Detection Test of Malicious Software 2012.)

4.2.3 HIPS työasemissa

HIPS on lyhenne sanoista ”Host-based Intrusion Prevention System”. Käytännössä tämä tarkoittaa ohjelmistoa, joka estää järjestelmän muutokset ilman hyväksyntää. (Chee 2008.)

HIPS-ohjelmistojen avulla voidaan haittaohjelmilta suojauduttaessa päästä lähelle sataprosenttista suojaustasoa. Käytännössä nämä ohjelmat valvovat järjestelmän muutoksia ja pyytävät luvan jokaiseen muutokseen, jota järjestelmään yritetään tehdä. Jatkuvia muutospyyntöjä on joissakin ohjelmistoissa helpotettu whitelisting-teknologialla, jossa tunnettujen ohjelmistojen annetaan tehdä muutoksia, mutta tuntemattomilta pyydetään aina lupa.

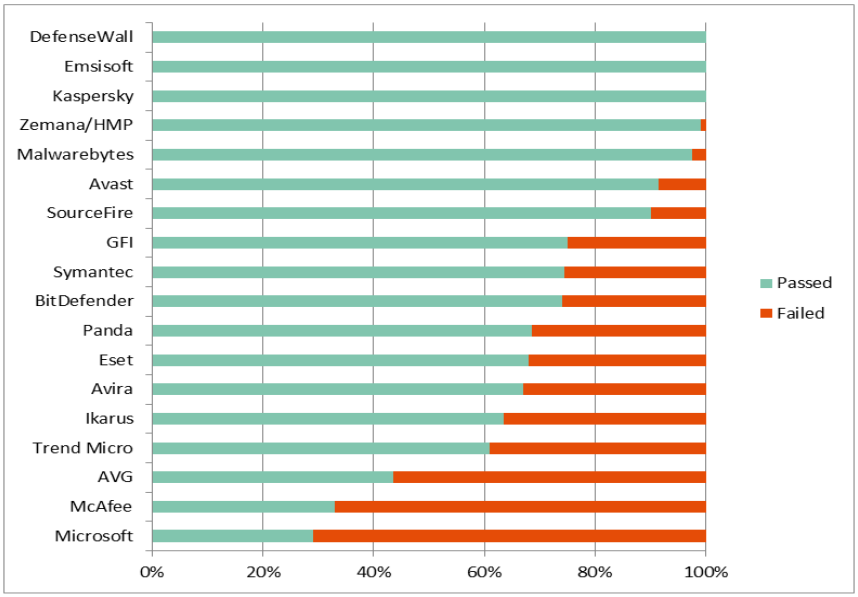
HIPS-ohjelmista on syytä mainita ainakin DefenceWall ja Zemana-Antilogger. Nämä ohjelmistot ovat pärjänneet erittäin hyvin järjestelmän suojana erilaisia haittaohjelmistoja vastaan.

HIPS-ohjelmistoja on testattu esimerkiksi Matousec-sivustolla. Testiin on osallistunut palomuuri, HIPS ja muita tietoturvaohjelmistoja. Uusimmassa testissä on testattu ohjelmistojen kykyä selvitä proaktiivisesti tietoturvauhista.

Esimerkkeinä näistä testeistä ovat erilaiset leak-testit, joilla testataan ohjelmistojen kykyä estää tiettyjä haitallisia toimintoja, kuten tiedon lähettämistä, kuvakaappausten ottoa ja näppäinten painalluksia.

Testit ja niiden tulokset löytyvät Matousecin sivuilta, joilla pääsee myös katsomaan vanhojen testien tuloksia. (Proactive Security Challenge 2012.) Myös 64-bittisten järjestelmien tulokset löytyvät samalta sivustolta. (Proactive Security Challenge 64 2012.)

Myös MRG Effitasin ”Flash Test Results” -sivustolla on nähtävissä testituloksia testeistä, joissa tietoturvaohjelmia on testattu yleisesti kutsutuilla nollapäivähyökkäyksillä. (Flash Test Results 2012.) Testeissä on esitetty ohjelmistojen kyky estää uhka uhan löytöhetkellä, kuusi tuntia löytöhetkestä ja kaksitoista tuntia löytöhetkestä. Saavutetuista testituloksista on tehty taulukko, jossa osoitetaan, miten ohjelmistot ovat suoriutuneet vuoden 2012 testeissä. Tämä taulukko on nähtävissä kuviossa 2.



KUVIO 2 *MRG Effitasin nollapäivähyökkäystestien tulokset vuodelta 2012 (Flash Test Results 2012.)*

Testissä parhaan tuloksen on saavuttanut Defencewall HIPS -ohjelmisto, joka pystyi suoriutumaan tietoturvauhista lähes sataprosenttisesti jo uhan löytöhetkellä. Lisää päivittyviä testejä voi käydä lukemassa MRG Effitasin sivustolta. (Efficacy Assessment & Assurance 2012.)

4.2.4 Haittaohjelmien torjunta palvelimilla

Haittaohjelmien torjuntaa voidaan tehdä myös palvelintasolla. Säilytetyn tiedon ja sähköpostiviestien turvaamiseksi palvelimilla on syytä käyttää antivirus-ohjelmistoja. Yleensä tämä tarkoittaa palvelimelle asennettua antivirus-ohjelmistoa, joka käy läpi sähköpostiliikennettä ja tiedostoliikennettä palvelimilla.

Palvelinohjelmistoja on olemassa erilaisille palvelimille, kuten Exchange-sähköpostiin, SharePoint-palvelimiin ja tiedostopalvelimiin.

4.2.5 Haittaohjelmien torjunta verkon rajalla

Verkon rajalla voidaan haittaohjelmia torjua monitoimilaittein, joiden ominaisuutena on haittaohjelmien suodatus. Tämänkaltainen laite yleensä asennetaan yhdyskäytävän eli ”gatewayn” ja lähiverkon väliin, missä verkkoliikenteen tutkiminen tapahtuu.

Huonoja puolia monitoimilaitteiden käytössä ovat pakatut haittaohjelmat ja osissa toimitetut haittaohjelmat, joiden tunnistaminen verkkoliikenteen seasta on hyvin vaikeaa. Vaikka haittaohjelmia suodatetaan verkon rajalla, se ei ole yksin riittävä suoja haitallisia ohjelmia vastaan. Tämän takia myös työasemille tarvitaan suoja tämänkaltaisia ohjelmia vastaan.

4.2.6 Nimipalvelimet

Suojattujen DNS- (Domain Name Service/Domain Name System) eli nimipalvelimien käyttäminen ehkäisee Internetin kautta levitettäviä haitallisia uhkia. Suojatulla DNS-palvelimella tunnetut haitalliset sivustot on estetty, eikä loppukäyttäjä saa yhteyttä palvelimeen, johon domain viittaa.

Esimerkkinä nimipalvelimista voidaan käyttää Symantecin Norton ConnectSafe palvelua, jossa nimipalvelimeksi vaihdetaan Symantecin palvelin. Symantecin tarjoamassa palvelussa on haitalliset sivustot pyritty suodattamaan pois, mikä estää haitallisille sivuille vahingossa joutumisen. Tämä kyseinen palvelu löytyy Nortonin ConnectSafe-sivustolta ja se on ilmainen yksityiskäyttöön. (Norton ConnectSafe 2012.)

Myös rikolliset käyttävät omia nimipalvelimiaan ja koettavat haittaohjelmien avulla vaihtaa käyttäjien nimipalvelinasetuksia. Tästä syystä nimipalvelimen asetukset on hyvä tarkistaa säännöllisesti. Haitallisella nimipalvelimella käyttäjä voi käyttää Internetiä lähes normaalisti huomaamatta, että palvelin on vääränlainen. Kuitenkin tietyt palvelut, kuten verkkopankit, saattavat johtaa väärennetyille sivuille, joiden avulla koetetaan kaapata verkkopankkitunnuksia tai varastaa käyttäjän tililtä rahaa.

4.3 Ajan tasalla pysyminen

Käyttöjärjestelmä ja käytettävät ohjelmistot on syytä pitää uusimissa versioissaan uusimilla päivityksillään. Tämä on tärkeää silloin, kun halutaan minimoida haavoittuvuuksien hyväksikäyttäminen, josta voi seurata tietoturvaongelmia.

Työkaluja ohjelmistohaavoittuvuuksien hallintaan ja ehkäisyyn on olemassa, ja monet nykypäivän tietoturvaohjelmistot varoittavat, jos kriittisiä päivityksiä puuttuu käyttöjärjestelmästä tai usein käytetyistä ohjelmista. Myös erillisiä tarkistusohjelmia on olemassa, kuten Secunian Personal Software Inspector (PSI). Tällä kyseisellä ohjelmistolla voi tarkistaa työ-

asemakohtaisesti, mitä tunnettuja ohjelmia pitäisi päivittää turvallisempaan versioon. (Free computer Security 2012.)

Suuremmille palvelinpohjaisille verkoille voi järjestelmän pääkäyttäjä tehdä haavoittuvuustarkistuksen kerralla esimerkiksi GFI LANguard -ohjelmistolla. Tämä ohjelma on maksullinen. (Comprehensive network security for businesses 2012.)

4.3.1 Käyttöjärjestelmän ajan tasalla pitäminen

Windows-käyttöjärjestelmissä on syytä pitää automaattiset päivitykset päällä, jotta käyttöjärjestelmä päivittyisi aina automaattisesti uusimpaan versioon. Joka kuukauden toinen tiistai Microsoft laittaa kuukauden päivitykset jakoon automaattisten päivitysten kautta.

Välillä päivityksiä saattaa tulla myös muina aikoina. Tätä tapahtuu etenkin, kun jokin erittäin kriittinen haavoittuvuus, josta on jo olemassa hyväksikäytön merkkejä, on julkistettu.

4.3.2 Ohjelmistojen ajan tasalla pitäminen

Ohjelmistot, joiden käytettävä versio ei ole päivitetty uusimpaan mahdolliseen versioon, saattavat sisältää tietoturvaongelmia. Ohjelmistojen ajantasaisuutta voidaan tarkistaa erilaisilla haavoittuvuusskannereilla, joista esimerkkinä on Secunian Personal Software Inspector -ohjelmisto (PSI). Tämä ohjelmisto tarkistaa, onko käytettävistä kolmannen osapuolen ohjelmista saatavilla uudempia versioita. Tämän jälkeen PSI ilmoittaa, jos käytössä on tunnettuja haavoittuvuuksia sisältäviä ohjelmia, minkä jälkeen se tarjoaa tarpeelliset turvallisuuspäivitykset. (Free computer security 2012.)

Hyvän tietoturvan säilyttämisen kannalta erittäin tärkeää on pitää ajan tasalla Sun Microsystemsin kehittämä ja nykyään Oracle Corporationin ylläpitämä Java sekä Adoben Flash Player ja PDF Reader -ohjelmistot. Näiden kaikkien kautta tapahtuu hyökkäyksiä jatkuvasti.

4.4 Suojautuminen verkon sisäisiä uhkia vastaan

Kattavalla verkon käyttäjien koulutuksella pystytään ehkäisemään osa inhimillisten virheiden aiheuttamista tietoturvaan vaikuttavista uhkatekijöistä.

Verkon käyttäjät voivat vaikuttaa tietoturvan tasoon myös omalla käytöksellään. Jotkut käyttäjät jopa tarkoituksella yrittävät päästä käsiksi tiedostoihin, joihin kyseisillä käyttäjillä ei ole luvallista pääsyä. Verkon käyttäjien aiheuttamaa uhkaa vastaan voi suojautua hyvillä käyttäjäasetuksilla,

joissa on rajattu, mitä käyttäjä saa tehdä ja mihin resursseihin hänellä on pääsy.

Verkon käyttäjien aiheuttamat tietoturvariskit voidaan minimoida hyvällä tietoturvapolitiikalla. Käytännössä tämä tarkoittaa sitä, että tehdään sääntöjä, joilla voidaan parantaa tietoturvaa.

Verkonkäyttäjien ohjeita luodessa on kiinnitettävä huomiota

- salasanojen laatuun. On suositeltavaa käyttää hyviä ja pitkiä salasanoja ja vaihtaa ne säännöllisesti.

- laitteelta poistumiseen. Jos poistuu laitteelta, pitää kirjautua ulos käyttäjätililtä.

- varmuuskopiointiin. Käyttäjiä kehotetaan varmistamaan, että heidän tietonsa on varmuuskopioitu turvallisesti.

- luottamuksellisten tietojen käsittelyyn. Luottamukselliset tiedot on salattava huolellisesti ja niitä on käsiteltävä varoen.

- Internetin käyttöön. Internetiä tulisi käyttää varovasti, jos työasemalla käsitellään arkaluontoisia tietoja.

- avun pyytämiseen ajoissa. Jos ei tiedä, mitä on tekemässä, on syytä kysyä apua.

- julkisiin ja suojaamattomiin verkkoihin.

Verkon pääkäyttäjä eli ”admin” aiheuttaa tietoturvariskin siinä, että hänellä on yleensä pääsy lähes kaikkiin verkon resursseihin. Halutessaan tai vahingossa pääkäyttäjä voi aiheuttaa suuriakin tietototurvan kannalta ongelmallisia tilanteita, joita ovat muun muassa palvelimien asetusten huono konfigurointi ja muut tietoturvavuotoja mahdollistavat virhetilanteet verkkopalveluissa.

Suojautumista verkon pääkäyttäjän aiheuttamia ongelmia vastaan voidaan lisätä valvonnalla ja dokumentoinnilla, joiden hoitaminen on jaettu useammalle käyttäjälle. Tämä minimoi pääkäyttäjän aiheuttamien ongelmien riskejä ja seurauksia, sillä esimerkiksi pilalle menneet ja haitalliset muutokset ohjelmassa voidaan joko ennaltaehkäistä tai ehkä korjata jälkeenpäin.

Pääkäyttäjän aiheuttamilta tietovuodoilta voidaan suojautua esimerkiksi käyttämällä tiedonsalausta siten, että vain tiedon haltijalla on hallussaan salasanat ja salausavain salattua tietoa varten.

4.5 Ulkoiset uhat

Suojautumiskeinoja ulkoisia uhkia vastaan ovat hyvä varmuuskopiointi ja salasanapolitiikka.

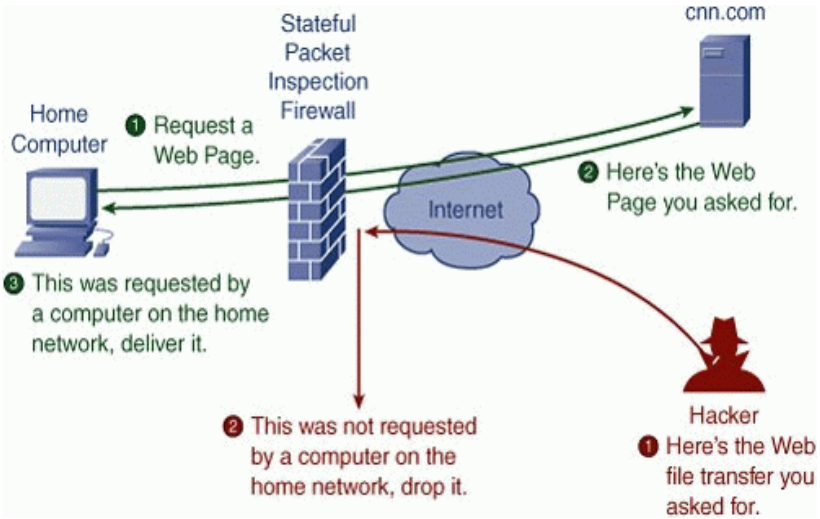
Sosiaalista hakkerointia, missä käyttäjältä udellaan tietoja, joiden avulla luottamuksellisen tiedon hyväksikäyttö tai tietomurrot olisivat mahdollisia, on vaikea estää. Ihmiset kertovat helposti esimerkiksi IT-tukena esiintyvälle henkilölle tietoja, joita ei kannattaisi ja pitäisi kertoa.

Tähän ongelmaan auttavat hyvä tietoturvapolitiikka ja -koulutus, sekä lisäksi esimerkiksi lista asioista, joita ei saa kertoa puhelimitse, sähköpostitse tai muullakaan tavalla kenellekään vieraalle ihmiselle.

4.5.1 Suojautuminen verkkohyökkäyksiltä

Verkkohyökkäyksiltä suojaudutaan yleensä palomuurilaitteella tai palomuuriohjelmistolla. Palomuurin tarkoituksena on estää ei-haluttu verkkoliikenne ja yhteys. Samoin hyökkääjän lähettämät paketit ja luvattomat verkkoyhteydet pyritään estämään palomuurien avulla.

Alla olevassa kuviossa 3 esitetään SPI:n (Stateful Packet Inspection) eli pakettiensuodatusta palomuurissa. Kyseisessä esimerkissä palomuuri hylkää datapaketin, joka ei tule pyydetystä osoitteesta. (Firewalls (2) - How Firewalls Work 2006.)



KUVIO 3 *Esimerkki pakettisuodatuksen toteuttavan palomuurin toiminnasta (Firewalls (2) - How Firewalls Work 2006.)*

Muita verkkohyökkäykseltä suojaavia laitteita ovat IDS (Intrusion Detection System) ja IPS (Intrusion Prevention System), joilla pyritään tunnistamaan ja ehkäisemään haitallista verkkoliikennettä.

Tunkeutumisenestojärjestelmät ja palomuurit pyrkivät tunnistamaan haitallisen verkkoliikenteen ja estämään haitallisten pakettien saapumisen perille. Haitallista liikennettä voivat olla esimerkiksi porttiskannaus, palve-

lunestohyökkäys, väärennetystä osoitteesta tulevat datapaketit ja muut ei-toivotut verkkoliikennemuodot.

Verkon etäkäyttö tulisi tehdä suojatun VPN-yhteyden yli ja samalla tulisi huolehtia etäkäyttölaitteen tietoturvasta. VPN-yhteydellä voidaan käyttää lähiverkon resursseja turvattoman verkon kautta rakentamalla salattu ”tunneli” verkkojen välille.

5 LUOTTAMUKSELLINEN TIETO JA SEN SÄILYTYS

Luottamuksellinen tieto tulisi säilyttää niin, että halutut käyttäjät voivat käyttää tietoa pienellä vaivalla, mutta muiden käyttäjien osalta tieto olisi saavuttamattomissa.

5.1 Käyttöoikeudet

Käyttöoikeuksilla voidaan hallita Microsoft Windows -ympäristössä, mihin hakemistoihin käyttäjällä on pääsy. Käyttöoikeuksien määrittelyssä tapahtuva virhe voi antaa käyttäjälle pääsy tiedostoihin, joihin käyttäjällä ei tulisi olla pääsyä. Huonolla käyttöoikeuksien hallinnalla henkilö, jolla ei olisi verkon käyttöön oikeuksia, pystyisi lukemaan verkossa olevia dokumentteja virheellisen käyttöoikeusasetusten sallimana. Tästä voi seurata muun muassa sitä, että luottamuksellisia tietoja voi joutua vääriin käsiin.

5.2 Salaus

Luottamuksellinen tieto on syytä säilyttää salattuna, mikä käytännössä tarkoittaa tiedon muuttamista muotoon, jota ei saa luettua ilman oikeita välineitä. Tietotekniikan maailmassa nuo välineet tarkoittavat salausavainta ja salasanaa. Hyvä esimerkki salauksesta on AES ”Advanced Encryption Standard” -tekniikka.

Salausta ja salakirjoitusta käytetään monissa yhteyksissä. Tällainen yhteys voisi olla esimerkiksi verkkoliikenne, jota pyritään salaamaan. Useissa tapauksissa verkkoliikennettä salataan palvelimen ja päätteen välissä, kuten esimerkiksi HTTPS-liikenteessä. Myös tiedostoja ja sähköpostiliikennettä salataan usein.

Salausta käytetään esimerkiksi siksi, etteivät verkkoliikennettä välissä lukevat tahot pystyisi selvittämään, mitä dataa verkkoliikenne pitää sisällään. Tapausesimerkkinä voisi olla esimerkiksi verkon etäkäyttö tapaus, jossa joku ulkopuolinen taho käyttää etänä jotakin verkkoa.

5.2.1 Tiedostojen salaus

Säilytettäviä tiedostoja voidaan salata ja niihin voidaan estää pääsy luvattomilta käyttäjiltä melko tehokkaasti. Salauksessa on kuitenkin muistettava, että ennen pitkää mikä tahansa salaus voidaan murtaa. Vaikka sillä hetkellä ratkaisu tuntuisikin hyvältä, täysin varmaa keinoa tiedostojen salaamiseksi ei ole. Tiedosta voidaan kuitenkin tehdä erittäin hankalasti purettavaa.

Hyvä ohjelmisto tiedostojen salaamiseen on esimerkiksi DESlock+. (Protecting your data and your budget. 2012.) Kyseisellä ohjelmistolla voidaan salata yksittäisiä tiedostoja, hakemistoja, ulkoisia medioita tai kokonaisia kiintolevyjä käyttöjärjestelmineen. Ohjelmistossa voidaan valita käytettävä salausalgoritmi useasta eri vaihtoehdosta.

5.2.2 Sähköpostiviestien salaus

Erilaisia sähköpostin ja tekstin salaukseen käytettäviä ohjelmistoja ovat esimerkiksi PGP-ohjelmistot (PGP = Pretty Good Privacy). Näitä ohjelmia käytetään yleensä niin, että jaetaan julkinen avain, jonka avulla viesti salataan niin, että vain vastaanottaja voi sen avata.

5.2.3 Verkkoyhteyksien salaus

Verkkoyhteyksiä salataan, jottei verkossa kulkeva tieto pääsisi ulkopuolisten käsiin. Salattuja yhteyksiä ovat esimerkiksi SSH-, SSL/TLS- ja VPN-yhteydet.

SSH-yhteydellä voidaan suojata esimerkiksi FTP- ja HTTP-liikennettä usealla eri salausalgoritmilla.

SSL/TLS-salauksen avulla voidaan käyttää verkkosivuja HTTPS-protokollan avulla. Myös sähköpostin SMTP-, POP- ja IMAP-yhteyksiä voidaan salata SSL/TLS:n avulla. Tämänkaltainen salaus perustuu varmenteisiin eli sertifikaatteihin.

VPN eli ”Virtual Private Network” on tapa, jolla voidaan julkisen verkon yli käyttää toista verkkoa näennäisesti lähiverkkona. Salaus protokollina käytetään esimerkiksi IPsec-, ECP- ja MPPE-protokollia (Internet Protocol Security, Encryption Protocol ja Microsoft Point-to-Point Encryption).

5.3 Data Leak Prevetion

DLP eli ”Data Leak Prevention”, ”Data Leak Protection” tai ”Data Loss Prevention” tarkoittaa tekniikkaa, jolla estetään tiedon vuotaminen järjestelmän ulkopuolelle. DLP-ohjelmisto pyrkii estämään valitun tiedon lähettämistä eteenpäin tai sen kopioimista massamuisteille.

DLP-ohjelmistoja löytyy nykyään useilta valmistajilta. Esimerkiksi SafenSoftin SysWatch Workstation -ohjelmistolla voidaan rajoittaa käyttäjän käyttämiä ohjelmia, tallennusvälineitä ja tiedostoihin pääsyä. (SysWatch Workstation 2012.)

5.4 Luottamuksellisen tiedon tuhoamien

Luottamuksellisen tiedon poistaminen järjestelmästä on syytä tehdä aina ylikirjoittamalla tieto. Ylikirjoittaminen on tarpeellista tehdä, jotta tietoa ei voitaisi helposti palauttaa massamuisteilta. Ylikirjoittamiseen on olemassa erilaisia algoritmeja, joilla tieto ylikirjoitetaan niin monta kertaa kuin halutaan. Yksi yleinen tapa on Peter Gutmannin algoritmi.

5.5 Varmuuskopiointi

Varmuuskopiointi on syytä suunnitella huolella. Huonosti suunniteltuna varmuuskopiointi voi käydä kalliiksi suuren tilantarpeen takia.

Yleisiä varmuuskopiointityyppejä ovat käytettävien datatiedostojen tallentaminen ulkoiselle medialle, serverille tai online-palveluun. Koko järjestelmän varmuuskopioiminen ulkoiselle medialle tarkoittaa käytännössä image-tallennusta, jossa levynkuva tallennetaan medialle.

Varmuuskopioiden tallennusväli ja tallennusmetodit on syytä miettiä huolella kuntoon. Kysymyksiä, joita miettimisvaiheessa voidaan esittää, ovat muun muassa seuraavat:

- Tarvitaanko useita versioita samoista tiedostoista?
- Tehdäänkö varmuuskopio aina täydellisenä vai tallennetaanko vain muuttuneet tiedostot?
- Tarvitseeko käyttöjärjestelmää ja käytettäviä ohjelmia varmuuskopioida?

6 YHTEENVETO JA POHDINTAA

Työn tarkoituksena oli herättää lukijoissa ajatuksia liittyen siihen, millaisia tietoturvauhkia nykypäivän Microsoft Windows -järjestelmiin kohdistuu. Lisäksi työssä annettiin vinkkejä ja neuvoja opastamaan, miten näihin tietoturvauhkiin voidaan varautua mahdollisimman hyvin. Nykypäivänä lähes jokaisella ihmisellä on mahdollisuus käyttää Internetiä. Tämän seu-

rauksena on, että haitallisten ohjelmien kehittäjille tarjoutuu mahdollisuus levittää ohjelmiaan nopeasti ympäri maailman.

Verkossa liikkuva raha ja tieto ovat tehneet verkkorikollisuudesta tuottavimman rikosmuodon. Haittaohjelmat monimutkaistuvat jatkuvasti ja niitä kehitetään lisää erittäin suurella vauhdilla, joten perinteiset virustorjuntaratkaisut vain harvoin enää riittävät torjumaan uusia kehittyneitä haittaohjelmia. Sekä yksityisten ihmisten että yritysten on lisättävä resursseja tietoturvan hallintaan ja kehittämiseen, jotta käytettävät työasemat voitaisiin suojata tehokkaasti. Lisäksi on tarpeellista varmistaa, että tiedot salataan ja talletetaan turvallisesti. Nämä kaikki piirteet on otettava huomioon tietoturvasuunnitelmia laadittaessa, jotta vältyttäisiin luomasta liian riskialttiita verkkoja ja järjestelmiä.

Windows-verkoista voidaan saada melko turvallisia tietoturvan kannalta. Aluksi on syytä tehdä hyvä tietoturvasuunnitelma, jossa käydään läpi, mitä tietoja pitää turvata, mitä tietojen katoaminen tai muuttuminen kustantaa ja miten paljon tietoturva saa kustantaa. Seuraavaksi esitellään teoreettinen malli, jolla tietoturva saadaan Windows-verkoissa vähintäänkin kohtuulliselle tasolle, mikäli verkon käyttäjät eivät aiheuta toimillaan suurta riskiä tietoturvalle.

Teoriassa Microsoft Windows -verkko perustietoturvalla voi esimerkiksi pienessä yrityksessä muodostua Microsoft Small Business Server -palvelimesta ja viidestä Windows 7 Professional -työasemasta.

Laitteet on yhdistetty toisiinsa kytkimillä, jotka on yhdistetty päätelaitteisiin RJ-45 -verkkokaapeleilla. Internetin ja lähiverkon väliin on laitettu palomuurilaite, jossa on myös IDS/IPS-ominaisuudet ja verkkoliikenteen virustarkistus. Lisäksi laitteen tulisi tukea VPN-yhteyksiä. Tällainen laite voisi olla esimerkiksi Fortinetin FortiGate-40C-palomuurilaite IPS- ja VPN-ominaisuuksilla. Lisäksi verkon IP-alue kannattaa rakentaa niin, ettei ylimääräisiä IP-osoitteita ole jaettavana verkon käyttöön.

Small Business Server on suojattu haittaohjelmia vastaan. Mikäli käytössä on Exchange-sähköposti, voidaan myös roskapostin suodattaminen tehdä palvelintasolla. Ohjelmistoja, joilla nämä toimet voidaan toteuttaa, ovat esimerkiksi BitDefender for Fileservers ja BitDefender for Exchange.

Työasemat on suojattu haittaohjelmilta ja tiedon katoamiselta. Suoja haitallisia ohjelmia vastaan työasemassa voidaan hoitaa esimerkiksi Kaspersky Small Office Security- ja Zemana Antilogger -ohjelmistoilla.

Varmuuskopiointi voidaan järjestää siten, että työasemat päivittävät reaaliajassa työdokumentit palvelimelle tai käyttävät dokumentteja suoraan palvelimelta. Lisäksi säännöllisesti voidaan ottaa levykuva-muotoinen varmuuskopiointi työasemista ja palvelimesta. Levykuva varmuuskopio-ohjelmista hyvä esimerkkiohjelma on Acronis Backup & Recovery -ohjelmisto. (Acronis Backup & Recovery® 11.5 2012.) Reaaliaikainen tiedostojen varmuuskopiointi voidaan toteuttaa esimerkiksi Genie Timeline Professional -ohjelmistolla. (Genie Timeline Professional 2012 2012.)

Jos verkon ylläpitäjä on ajan tasalla tehtävistään, pitäisi näillä suojausmenetelmillä saavuttaa erittäin hyvätasoinen tietoturva niin haittaohjelmia vastaan kuin tiedon katoamisen ehkäisemiseksi.

LÄHTEET

102 onnistunutta nettihyökkäystä viikossa. 2012. Tietoviikko. Viitattu 13.11.2012. http://www.tietoviikko.fi/kaikki_uutiset/102+onnistunutta+nettihyokkaysta+viikossa/a845960

Acronis Backup & Recovery® 11.5. 2012. Acronis International GmbH. Viitattu 3.12.2012. http://www.acronis.com/backup-recovery/smallbusiness.html

Adoben ohjelmistovarmenteella allekirjoitettu haittaohjelmia. 2012. Cert-fi. Viitattu 6.11.2012. http://www.cert.fi/tietoturvanyt/2012/09/ttn201209282139.html

Anderson N. 2012. Confirmed: US and Israel created Stuxnet, lost control of it. Ars Technica. Viitattu 10.11.2012. http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

Baumgartner K. 2012. Microsoft Updates November 2012 - IE, Kernel+Shell, and .NET Critical Patches. Kaspersky Lab ZAO. Viitattu 3.12.2012. http://www.securelist.com/en/blog/208193932/Microsoft_Updates_November_2012_IE_Kernel_Shell_and_NET_Critical_Patches

Chee, J. 2008. Host Intrusion Prevention Systems and Beyond. SANS Institute InfoSec Reading Room. Viitattu 31.10.2012. http://www.sans.org/reading_room/whitepapers/intrusion/host-intrusion-prevention-systems_32824

Comprehensive network security for businesses. 2012. GFI Software. Viitattu 1.11.2012. http://www.gfi.com/network-security-vulnerability-scanner

Efficacy Assessment & Assurance. 2012. MRG Effitas Ltd. Viitattu 2.11.2012. http://www.blog.mrg-effitas.com/

File Detection Test of Malicious Software. 2012. AV-Comparatives e.V. Viitattu 8.11.2012. http://www.av-comparatives.org/images/docs/avc_fdt_201209_en.pdf

Firewalls: Firewalls (2) - How Firewalls Work. 2006. Best Security Tips. Viitattu 3.12.2012. http://www.bestsecuritytips.com/xfsection+article.articleid+2.htm

Fitsanakis J. 2011. German government admits using Trojan to spy on private computers. Intelnews.org. Viitattu 10.11.2012. http://intelnews.org/2011/10/11/01-842/

Flash Test Results. 2012. MRG Effitas Ltd. Viitattu 4.11.2012. http://www.mrg-effitas.com/current-tests/flash-test-results/

Free computer security. 2012. Secunia. Viitattu 25.10.2012. http://secunia.com/vulnerability_scanning/personal/

Genie Timeline Professional 2012. 2012. Genie9 Corporation. Viitattu 3.12.2012 http://www.genie9.com/business/Genie_Timeline_Pro/overview.aspx

Haittaohjelma vaatii rahaa Suomen poliisin nimissä – älä maksa. 2012. Cert-fi. Viitattu 6.11.2012. http://www.cert.fi/tietoturvanyt/2012/03/ttn201203082020.html

Independent Tests of Anti-Virus Software. 2012. AV-Comparatives e.V. Viitattu 2.11.2012. http://www.av-comparatives.org/

Jääskeläinen O. 2011. Valtion tekemäksi epäilty ”Star Wars -vakoiluohjelma” tallentaa käyttäjän näppäinpainallukset ja nettipuhelut. MicroPC. Viitattu 10.11.2012. http://www.mikropc.net/kaikki_uutiset/valtion+tekemaksi+epailty+quotstar+wars+vakoiluohjelmaquot+tallentaa+kayttajan+nappainpainallukset+ja+nettipuhelut/a700457

Lehto T. 2010. Stonesoft: Hyökkääjät pääsevät evaasioilla turvalaitteiden ohi. Tietokone. Viitattu 6.11.2012. http://www.tietokone.fi/uutiset/stonesoft_hyokkaajat_paasevat_evaasioilla_turvalaitteiden_ohi

Namestnikov Y. 2012. IT Threat Evolution: Q3 2012. Kaspersky Lab ZAO. Viitattu 11.11.2012. http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012

New Info on Stuxnet. 2011. F-Secure.com. Viitattu 10.11.2012. http://www.f-secure.com/weblog/archives/00002083.html

Norton ConnectSafe. 2012. Norton. Viitattu 31.10.2012. https://dns.norton.com/dnsweb/homePage.do

Proactive Security Challenge 64. 2012. Matousec.com. Viitattu 8.11.2012. http://www.matousec.com/projects/proactive-security-challenge-64/

Proactive Security Challenge. 2012. Matousec.com. Viitattu 8.11.2012. http://www.matousec.com/projects/proactive-security-challenge/results.php

Protecting your data and your budget. 2012. DESlock Ltd. Viitattu 3.12.2012. http://www.deslock.com/

Seeling M. 2011. Sinulle on sähköpostia. Signaali. 2011 (3), 12–13. Viitattu 25.10.2012. http://www.epaper.fi/reader/?issue=22816;994069d08c17f4cff4d5df3d0ac88216;13

Skantz E. & Kestilä M. 2011. Tietoturvatutkimus: yli miljoona ihmistä maailmassa joutuu verkkorikollisuuden uhriksi päivittäin. Symantec Corporation. Viitattu 6.11.2012. http://www.symantec.com/fi/fi/about/news/release/article.jsp?prid=20110907_01

SysWatch Workstation. 2012. SafenSoft. Viitattu 4.11.2012. http://www.safensoft.com/security.phtml?c=719

The Independent IT-Security Institute. 2012. AV-TEST GmbH. Viitattu 2.11.2012. http://www.av-test.org/index.php?L=1

Tietoturvakatsaus 3/2007. 2007. Viestintävirasto. Cert-fi. Viitattu 25.10.2012. http://www.cert.fi/katsaukset/2007/tietoturvakatsaus_3-2007.html

Tietoturvalliseen yhteiskuntaan. 2012. Viestintävirasto. Viitattu 6.11.2012. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html