

Tomi Syväsalmi

Pk-yrityksen kyberturvallisuus ja penetraatiotestaus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinööriytyö

6.4.2016

Tekijä Otsikko	Tomi Syväsalmi Pk-yrityksen kyberturvallisuus ja penetraatiotestaus
Sivumäärä Aika	57 sivua + 4 liitettä 6.4.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot ja tietoliikenne
Ohjaaja	Lehtori Kimmo Saurén
<p>Insinööriyön tavoitteena oli kehittää kahdelle keskisuurelle yritykselle parannusehdotuksia kyberturvallisuuteen liittyen ja suorittaa yritysten käytössä oleviin järjestelmiin Internetin välityksellä tehtävä penetraatiotestaus.</p> <p>Yritysten tietoturvaluudesta tehtiin tilannekatsaus parannusehdotusten löytämiseksi. Penetraatiotestaus suoritettiin erilaisilla porttiskannauksilla, jotka kertovat avoimien porttien lisäksi tietoa myös skannauksen kohteen käytössä olevista järjestelmistä. Kyberturvallisuuden ja sen uhkien sekä puolustuskeinoihin liittyvää ajankohtaista tietoa tutkittiin eri lähteistä. Yleishyödylliset tiedot koottiin insinööriyössä monipuoliseksi ja selkeäksi kokonaisuudeksi, joka hyödyttää myös muita yrityksiä ja jota kuka tahansa kyberturvallisuudesta kiinnostunut voi lukea. Työn tuloksena yrityksille koottiin tietoturvaraportit, joissa esiteltiin parannusehdotukset ja penetraatiotestauksen tulokset. Tietoturvaraportteja ei yritysten kanssa tehtyjen salassapitosopimusten vuoksi voida liittää julkiseen insinööriyöhön.</p> <p>Kyberturvallisuus on nyt ja myös tulevaisuudessa yritysten liiketoiminnan elinehto, sillä kyberrikollisuudessa liikkuu erittäin paljon rahaa. Kyberturvallisuuteen liittyvien uhkien jatkuva kehittyminen luo yrityksille haastetta liiketoiminnan turvaamisen ja ylläpidon suhteen. Näiden asioiden vuoksi insinööriyö on ajankohtainen ja antaa hyödyllistä tietoa yrityksille.</p>	
Avainsanat	kyberturvallisuus, tietoturva, penetraatiotestaus, murtotestaus

Author Title	Tomi Syväsalmi Cybersecurity and penetration testing for small to medium-sized enterprises
Number of Pages Date	57 pages + 4 appendices 6 April 2016
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Computer Networks and Telecommunications
Instructor	Kimmo Saurén, Senior Lecturer
<p>The goal of this final year project was to create suggestions for improvement regarding cyber security for two medium sized companies and to perform penetration testing on their systems over the Internet.</p> <p>In order to offer suggestions, the current state of information security of the companies was reviewed. Penetration testing was performed by various kinds of port scanning which discover not only open ports but also information about the systems used by the target. Various sources were used to find up-to-date information about cyber security and its threats and defense techniques. This thesis contains beneficial information also for other companies besides the client companies and can be read by anyone interested in cyber security. As a result of the work, reports which contain suggestions for improvement and penetration testing results were produced for the client companies. Due to the non-disclosure agreements made with the companies the information security reports cannot be attached to this thesis.</p> <p>Cyber security is essential to businesses today as well as in the future because a large amount of capital is involved in cyber-crime. Continuously evolving cyber threats pose challenges to companies in securing and maintaining their business. These facts make this thesis contemporary and helpful to companies.</p>	
Keywords	Cyber security, Information security, penetration testing

Sisällys

Lyhenteet

1	Johdanto	1
2	Pienen ja keskisuuren yrityksen kyberturvallisuus	1
2.1	Fyysinen turvallisuus	3
2.2	Hallinnollinen tietoturva ja henkilöturvallisuus	4
2.3	Tekninen tietoturva	6
3	Yritykseen kohdistuvat uhat	7
3.1	Fyysiset uhat	9
3.2	Hallinnolliset ja henkilöturvallisuuteen liittyvät uhat	10
3.3	Tekniset ja käytännön uhat	11
4	Fyysinen suojaus	19
4.1	Fyysiset alueet	19
4.2	Kulunvalvonta	20
4.3	Videovalvonta	20
4.4	Murtosuojaus	20
4.5	Palo- ja vesisuojaus	21
4.6	Muut fyysiset suojaustoimenpiteet	22
5	Hallinnollinen suojaava toiminta	23
5.1	Liiketoiminnan jatkuvuuden turvaaminen	24
5.2	Riskianalyysi ja tietoturvallisuuden testaaminen	26
5.3	Henkilöturvallisuuden suojaus	27
6	Tekniset ja käytännön suojaustoimenpiteet	28
6.1	Tietoverkkojen suojaus	28
6.2	Palvelinten suojaus	32
6.3	Työasemien ja kannettavien laitteiden suojaus	33
6.4	Ohjelmistojen suojaus	33
6.5	Datan suojaus ja varmuuskopiointi	35
6.6	Muut tekniset ja käytännön suojaustoimenpiteet	37
7	Järjestelmien valvonta ja poikkeamiin reagointi	37

7.1	Järjestelmien valvonta	39
7.2	Tietoturvapoikkeamiin vastaaminen ja reagointisuunnitelma	40
8	Penetraatiotestaus	43
8.1	Sopimusten laatiminen ja esityö	45
8.2	Testauksessa käytetyt työkalut	45
8.3	Testaus ja sen vaiheet	46
9	Yhteenveto	47
	Lähteet	49
	Liitteet	
	Liite 1. Reagointisuunnitelma	
	Liite 2. Nmapin yleiset optiot	
	Liite 3 Yritys X:n tietoturvaraportti ja testaustulokset (salainen)	
	Liite 4 Yritys Y:n tietoturvaraportti ja testaustulokset (salainen)	

Lyhenteet

CERT	<i>Computer emergency response team.</i> Ryhmä, joka käsittelee tietoteknis- ten laitteiden tietoturvapoikkeamia ja vastaa niihin liittyvistä toimenpiteis- tä.
DDoS	<i>Distributed denial-of-service.</i> Hajautettu palvelunestohyökkäys, jossa koh- teeseen hyökätään käyttämällä useita hyökkäyslähteitä.
DMZ	<i>Demilitarized zone.</i> Fyysinen tai looginen aliverkko, jolla osa järjestelmis- tä voidaan yhdistää turvattomampaan verkkoon, esimerkiksi Internetiin.
DPI	<i>Deep packet inspection.</i> Pakettisuodatusmenetelmä, jossa verkkopake- teista tutkitaan myös niiden sisältämä data.
EMP	<i>Electromagnetic pulse.</i> Sähkömagneettinen pulssi eli lyhytkestoinen ja korkeatehoinen sähkömagneettinen aalto, joka vaurioittaa elektronisia laitteita.
IR	<i>Incident response.</i> Tietoturvaan liittyviin poikkeamiin vastaaminen ja rea- gointi.
SQL	<i>Structured query language.</i> Kyselykieli, jolla voidaan tehdä hakuja, muu- toksia ja lisäyksiä relaatiotietokantaan.
UPS	<i>Uninterruptible power supply.</i> Laite, joka takaa tasaisen ja keskeytymät- tömän virransyötön sähkökatkosten ja epätasaisen syöttöjännitteen aika- na.
USB	<i>Universal serial bus.</i> Tietoteknis- ten laitteiden liitäntä, jonka avulla laittei- siin voidaan kytkeä muita oheislaitteita.
VLAN	<i>Virtual local area network.</i> Virtuaalilähiverkko, jonka avulla fyysinen tieto- verkko voidaan jakaa loogisiin osiin.
VPN	<i>Virtual private network.</i> Virtuaalinen erillisverkko, jonka avulla voidaan yhdistää kaksi tai useampia verkkoja salatun tunnelin läpi.

1 Johdanto

Insinööriyössä tutkitaan kyberturvallisuutta ja yritetään testaamalla löytää puutteita yritysten tietoturvassa Internetin kautta tulevia uhkia vastaan. Tavoitteena on monipuolisesti selvittää yritysten kyberturvallisuutta, siihen liittyviä yleisiä ja ajankohtaisia uhkia ja suojautumista uhkia vastaan. Työn on tilannut kaksi keskisuurta muoviteollisuuden yritystä, jotka haluavat työn avulla tarkastaa turvallisuustasoaan ja löytää parannuskeinoja, joilla yritykset voivat kasvattaa valmiuttaan kyberturvallisuuden uhkia vastaan. Aihe on valittu, koska kyberturvallisuuteen liittyvät uhat ovat merkittäviä ja ajankohtaisia. Yritykset käyttävät yhä enemmän Internetiin liitettyä tietotekniikkaa, esimerkiksi liittämällä tuotantojärjestelmiään Internetiin. Kyberturvallisuudesta huolehtiminen on yritykselle välttämätöntä, sillä sen laiminlyönti voi aiheuttaa merkittäviä taloudellisia tappioita. Esineiden Internet lisää myös kyberturvallisuuden merkitystä, kun Internetiin liitettävien laitteiden määrä kasvaa.

Työssä tehdään myös tietoturvapoikkeamien varalle yleinen reagointisuunnitelma, jonka avulla yritykset voivat pienentää hyökkäyksistä tai onnettomuuksista aiheutuvaa haittaa ja nopeuttaa vahingoista palautumista.

Insinööriyössä esiin tuotavat suojaustoimenpiteet ovat ehdotuksia, ja yritykset ovat itse vastuussa oman riskianalyyysinsä tekemisestä ja suojauskäytännöistään.

2 Pienen ja keskisuuren yrityksen kyberturvallisuus

Kyberturvallisuus koostuu sekä fyysisen että ihmisten luoman keinotekoisien bittien maailman turvallisuudesta. Kybermaailma on ihmisen luoma digitaalinen maailma, ja kyberturvallisuudella tarkoitetaan sen turvallisuutta. Kyberturvallisuuteen kohdistuu sähköisten uhkien lisäksi myös fyysisiä uhkia. Yhteiskunnan fyysiset toiminnot riippuvat jo varsin paljon tietojärjestelmien toiminnasta, ja häiriöt tietojärjestelmissä vaikuttavat näin myös fyysiseen toimintaan. [1, s. 31, 29; 2, s. 56–57.]

Kyberturvallisuudella ei ole tarkoitus pyrkiä suojautumaan kaikkia mahdollisia uhkia vastaan, vaan arvioida merkittävimmät uhat ja löytää taloudelliset ja tehokkaat keinot niiden ratkaisemiseksi. Olennaista on kartoittaa ja analysoida merkittävimmät yrityk-

seen kohdistuvat uhat ja laskea jokaiselle löydetylle uhalle riskikerroin, joka muodostuu uhan toteutumisesta aiheutuvien haittojen suuruudesta ja toteutumisen todennäköisyydestä. Tämän jälkeen uhkia vastaan suojaudutaan keskittymällä ensin merkittävimpiin ughiin. Ratkaisua mietittäessä tulee löytää sellainen ratkaisu, joka on tehokas ja taloudellinen ja suojaa riittävästi uhkaa vastaan. Sellaisia kyberturvallisuuteen liittyviä suojaustoimenpiteitä, jotka eivät tue yrityksen liiketoimintaa, tulee harkita tarkasti, sillä niiden tuoma lisäarvo turvallisuuteen ei välttämättä ole niistä aiheutuvien kustannusten arvoinen. Tasapaino tulee löytää myös toiminnallisuuden ja turvallisuuden välille niin, että turvallisuuteen liittyvät käytännöt eivät rajoita tuottavuutta. [1, s. 28; 3, s. 44; 4, s. 115–116; 5, s. 79–83, 17–18; 6, s. 74, 68–69.]

Kyberturvallisuudella pyritään turvaamaan tärkeiden järjestelmien ja tiedon kolme peruskäsitettä, jotka ovat luottamuksellisuus, eheys ja saatavuus. Erilaiset yrityksen suojattavat kohteet tai asiat vaativat eritasoisia näitä osa-alueita koskevia suojausmenetelmiä. Jokainen suojaustoimenpide tarjoaa vähintään yhteen näistä käsitteistä kohdistuvaa suojaa. Myös kaikki kyberturvallisuuteen liittyvät uhat arvioidaan sen perusteella, miten ne vaikuttavat yhteen tai useampaan näistä käsitteistä. [6, s. 22.]

Luottamuksellisuudella varmistutaan, että tieto pysyy luottamuksellisena kaikissa sen käsittelyn vaiheissa. Tiedon luottamuksellisuuden tulee siis säilyä tiedon ollessa tallennettuna verkkoon kytketyissä järjestelmissä ja laitteissa sekä tietoa lähetettäessä että vastaanotettaessa. [6, s. 24.]

Tiedon eheydellä tarkoitetaan, että tieto säilyy luotettavana ja alkuperäisessä muodossaan ja sen luvaton muokkaaminen estetään. Järjestelmien laitteiston, ohjelmiston ja tietoliikenteen tulee käsitellä ja lähettää tietoa oikein niin, ettei tieto muuta muotoaan. Järjestelmien ja verkon tulee siis olla ulkoisilta häiriöiltä ja uhilta suojattuja. [6, s. 23.]

Saatavuudella voidaan varmistaa, että oikeutetut tahot pääsevät luotettavasti ja riittävän nopeasti tietoon ja resursseihin käsiksi. Järjestelmien tulee siis toimia odotettavalla tavalla ja riittävän tehokkaasti. Niiden tulee voida palautua häiriöistä nopeasti ja turvalisesti, ettei tuotanto häiriydy. Järjestelmien tulee olla suojattuja kaikkia sellaisia sisäisiä ja ulkoisia uhkia vastaan, jotka voivat aiheuttaa saatavuudelle tai tuottavuudelle haittaa. [6, s. 23.]

Tietoturvallisuudesta huolehtiminen on keskeinen asia yrityksen liiketoiminnan harjoittamisen kannalta, sillä Suomen lait ja asetukset sekä EU velvoittavat yrityksiä huolehtimaan tietoturvallisuudestaan. Muiden yritysten, kuten toimittajien, alihankkijoiden ja yhteistyötahojen, kanssa tehdyt sopimukset velvoittavat yrityksiä huolehtimaan oman tietoturvansa lisäksi myös muiden tahojen ja asiakkaiden tiedoista. [2, s. 125–126.]

2.1 Fyysinen turvallisuus

Fyysinen turvallisuus takaa yritykselle häiriöttömän ja turvallisen toimintaympäristön ja toimii samalla perustana kaikille muille suojaustoimenpiteille, joilla tietoturvallisuutta voidaan ylläpitää. Jokainen yritys tarvitsee fyysiset tilat toimiakseen. Fyysistä tietoturvaa suunniteltaessa on tärkeää, että koko toimintaympäristön turvallisuustarpeita ja ratkaisuja arvioidaan kattavasti. [4, s. 125.]

Fyysinen tietoturva kattaa tietoturvan fyysisen osa-alueen, ja siihen kuuluvat muun muassa kulunvalvonta, kameravalvonta, muu tekninen valvonta ja vartiointi sekä palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunta [7]. Fyysisistä turvallisuusasioista huolehtiminen on tärkeää, sillä fyysinen turvallisuus on suoraan yhteydessä kyberturvallisuuteen [1, s. 31]; yritysrakennuksessa esimerkiksi ovien tarkoituksena on estää ja hidastaa luvaton kulkemista [8]. Ilman fyysistä turvallisuutta hallinnollisen ja teknisen tietoturvan saavuttaminen on lähes mahdotonta, eikä tietoturvallisuuden koskemattomuutta voida varmistaa [3, s. 177].

Yrityksen rakennuksen turvallisuutta käsiteltäessä tarkoituksena ei ole pyrkiä täysin estämään esimerkiksi murtovarkautta, sillä ei ole mahdollista täydellisesti estää murtautumista. Asiaa tarkasteltaessa lähdetään siitä olettamuksesta, että minne tahansa pystytään murtautumaan, jos murtautujalla on tarpeeksi suuri motiivi. Fyysisen turvallisuuden tarkoituksena onkin hidastaa murtautujaa tarpeeksi paljon niin, että murto ehdistään huomata ajoissa ja siihen voidaan reagoida. [8.]

Kulunhallinta on tärkeä yrityksen toimitiloihin liittyvä käsite. Kulunhallintaan liittyy vahvasti kulunvalvonta, jolla pyritään rajoittamaan ja valvomaan ihmisten liikkumista yrityksen tiloissa. Muita osa-alueita, jotka kuuluvat kulunhallintaan, ovat myös esimerkiksi kiinteistössä liikkumisen linjaukset, poliitikkojen, standardien sekä toimintaohjeiden

ylläpito ja kehittäminen, käytettävien kulunhallinnan toteutuskeinojen määrittely sekä näiden asioiden johtaminen. [3, s. 179–180.]

2.2 Hallinnollinen tietoturva ja henkilöturvallisuus

Hallinnollisella tietoturvalla pyritään kaikki yrityksen muut tietoturvallisuuden osa-alueet kokoamaan yhdeksi kokonaisuudeksi, jota voidaan helposti johtaa ja hallita, ja se luo edellytykset tietoturvallisuuden ylläpidolle ja kehittämiselle. Hallinnollinen tietoturvallisuus tarkastelee tietoturvallisuuden toimintapolitiikkaa, toiminnan linjauksia, toimintojen organisointia ja sijoitusta, johtamista ja resursointia sekä tietoturvallisuuden hoitoon liittyviä vastuita. [3, s. 18.]

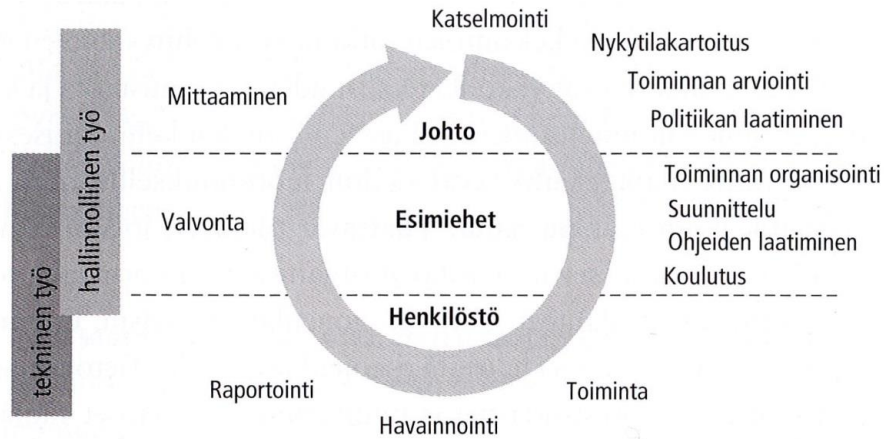
Turvallisuustoiminnan järjestäminen ja siihen liittyvien resurssien organisointi on yrityksen johdon lisäksi myös esimiesten ja keskijohdon tehtävä. Esimies voi esimerkiksi nimetä vastuuhenkilöt ja suunnitella raportointi- ja seurantajärjestelmät, joilla valvotaan toimintayksikön tavoitteiden saavuttamista. Turvallisuustoiminnan suunnitteluvaiheessa toimintamallit ja vastuu tietoturvan toteuttamisesta jaetaan ja tavoitteet sovitetaan yrityksen päivittäiseen toimintaan. [4, s. 121.]

Tietoturvallisuus tulee sisällyttää osaksi yrityksen johtamista ja työntekijöiden jokapäiväistä toimintaa. Asiat, joita tietoturvallisuudessa painotetaan, muovautuvat yrityksen toiminnan luonteen ja liiketoiminnan vaatimusten mukaan. Kaikki yritykset eivät esimerkiksi tarvitse suurta johtamisjärjestelmää tietoturvan hallinnointiin, kun taas joillekin yrityksille se voi olla elinehto ja menestystekijä. Tietoturvallisuus täytyy siis asettaa yrityksen vaatimuksiin nähden riittävälle tasolle. [4, s. 115–116.]

Tietoturvallisuuden tila paranee, kun yrityksen työntekijät toimivat ja käsittelevät tietoa tietoturvaohjeiden mukaisesti ja kun teknisellä suojauksella voidaan varmistaa, että myös yrityksen järjestelmät suojaavat tietoa oikein. Tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta varmistuminen kehittää samalla yrityksen toiminnan tasoa muutenkin kuin vain tietoturvan osalta. [4, s. 120.]

Tietoturvan hallinnointia voidaan myös kuvata maailmanpyöränä. Hallinnointi alkaa ylhäältä johdon toimenpiteistä, kehittyy sen jälkeen keskijohdon toimesta ja toteutuu työntekijöiden toiminnassa. Työntekijät raportoivat havaintonsa ja toimintansa keski-

johdolle, joka välittää ne taas ylimmälle johdolle. Lopuksi ylin johto analysoi, miten tietoturva on toteutunut asetettuihin tavoitteisiin verrattuna. [4, s. 122–123] Kuvassa 1 on havainnollistettu tietoturvan hallinnointiprosessia.



Kuva 1. Tietoturvan hallinnoinnin vaiheet [4, s. 120].

Henkilöturvallisuus on se tietoturvallisuuden osa-alue, joka pitää sisällään yrityksen tietojen ja tietojenkäsittelyn suojaamisen ihmisten tahallisesti ja tahattomasti aiheuttamia uhkia vastaan, ja se tarkastelee tämän lisäksi myös ihmisten tietoturvallisuutta varmistavaa toimintaa [3, s. 18–19]. Henkilöturvallisuudella tarkoitetaan siis työntekijöiden toiminnasta aiheutuvien ja heihin kohdistuvien tietoturvauhkien hallintaa [4, s. 138]. Henkilöturvallisuus kattaa yrityksen työntekijöiden lisäksi myös ulkopuoliset henkilöt ja vierailijat, ja henkilöturvallisuuteen liittyviä asioita käsitellään esimerkiksi uuden työntekijän rekrytoinnissa ja työsuhteen päättyessä [3, s. 18].

Tietoturvastandardit

Monet yleiset tietoturvastandardit ovat nykyään ISO-, eli International Organization for Standardization, standardeja. Standardeilla voi olla merkittävää vaikutusta esimerkiksi yritysten väliseen liiketoimintaan. Jos yritys noudattaa jotain tiettyä tietoturvastandardia, voidaan myös yrityksen kanssa yhteistyötä tekevää yritystä vaatia noudattamaan tietoturvallisuuden osalta samanlaista tasoa. Tällaisessa tapauksessa sopimukset saattavat velvoittaa yhteistyöyritystä hankkimaan kyseisen standardin tai muutoin noudattamaan standardin vaatimaa toimintamallia. [4, s. 85.] ISF, eli Information Security Forum, on myös tuottanut ilmaisen Standard of Good Practice for Information Security -standardin, joka on tarkoitettu kaikille yrityksille. ISF:n tietoturvastandardille ei voi ha-

kea sertifiointia, mutta sen avulla on mahdollista rakentaa sertifioitavissa oleva hallintajärjestelmä, joka täyttää ISO 27001 -standardin asettamat sertifiointiin liittyvät vaatimukset. [4, s. 90–91.]

Yrityksen on tarvittaessa mahdollista sertifioida tietoturvallisuuden hallintajärjestelmänsä ja siten osoittaa, että tuote tai toiminta täyttää sille asetetut vaatimukset. Sertifiointi vaatii muun muassa ISO 27001 -standardin vaatimusten täyttymistä. Sertifiointi ei ole välttämätöntä, ja monet sen tarjoamista hyödyistä voidaan saada myös pelkästään noudattamalla kyseessä olevan standardin vaatimuksia. Käytössä olevan standardin sertifiointista on kuitenkin höytyä mahdollisissa riitatilanteissa, joissa yritys saattaisi joutua osoittamaan, että sen toiminta on ollut tasoltaan standardin mukaista. [4, s. 105–109.]

2.3 Tekninen tietoturva

Hallinnollisten toimenpiteiden ja ohjeistuksen lisäksi tarvitaan myös teknisiä toimenpiteitä, jotta liiketoiminnan edellytyksiä voidaan pyrkiä edistämään. Tekninen tietoturva on järjestelmien teknisen toteutuksen turvallisuutta. Tietoturvan teknisellä toteuttamisella tarkoitetaan siis sellaisia ohjelmistoilla ja laitteilla tehtäviä toimia, joilla parannetaan tietoturvaa. [4, s. 172.]

Tietoverkkojen ja tietoliikenteen turvallisuus

Tietoliikenteen turvallisuus käsittelee yrityksen tietoverkkojen ja tietoliikenteen suojaamista niihin kohdistuvilta uhilta, ja sen tarkoituksena on pyrkiä turvaamaan tietoverkon jatkuva ja häiriötön toiminta myös ongelmatilanteissa. Tietoverkkojen turvallisuudella pyritään suojaamaan yrityksen tiedot, kun niitä lähetetään ja varastoidaan verkossa. Sen avulla pyritään siis erityisesti estämään tietojen päätyminen ulkopuolisten tahojen käsiin ja varmistamaan, että tiedot säilyvät eheinä ja luotettavina alkuperäisessä muodossaan. [3, s. 20.]

Palvelinten ja työasemien turvallisuus

Käyttöoikeuksien hallinta on hyvin tärkeä ja keskeinen tietoturvallisuuteen liittyvä osa, ja sen periaatteena on antaa käyttäjälle järjestelmiin ne oikeudet, joita hän tarvitsee

työtehtäviensä suorittamiseksi. Käyttöoikeuksien hallinta koostuu käyttöoikeuksien luonnista, muutoksista, poistosta ja seurannasta. [4, s. 151.]

Ohjelmistojen turvallisuus

Ohjelmistoturvallisuus tarkastelee yrityksellä käytössä olevien ohjelmistojen suojaamista ja niihin liittyvää lisensointia. Ohjelmistoturvallisuudella halutaan varmistaa muun muassa se, että ohjelmien lisenssit ja käyttöoikeudet ovat ajan tasalla ja että ohjelmistojen suojausominaisuudet vastaavat yrityksen vaatimuksia. [3, s. 21–22.]

Tietojen salaus

Tietojen salausta kutsutaan myös kryptografiaksi, ja sen tarkoitus on muuttaa tallennettava tai lähetettävä tieto sellaiseen muotoon, ettei kukaan ulkopuolinen, jolle tietoa ei ole tarkoitettu, pysty sitä lukemaan tai muokkaamaan. Tiedon salaus tehdään erilaisilla matemaattisilla salausalgoritmeilla. [6, s. 759–760, 765.]

3 Yritykseen kohdistuvat uhat

Kyberturvallisuuteen liittyviä uhkia tarkasteltaessa kannattaa ensin tarkastella kysymystä ”Miksi?”. Kysymys ”miksi?” määrittelee sen, kuinka tärkeää tietoturvallisuus on yritykselle, sekä esimerkiksi hyökkääjien motiivit. [3, s. 29–31; 9, s. 53.] Kysymyksiä ”mitä?” ja ”miten?” tarkastelemalla voidaan määrittää yrityksen toiminnan kannalta tärkeimmät suojaavat resurssit sekä käytännön suojausratkaisuja niiden suojaamiseksi [3, s. 29, 34–33].

Yritykseen kohdistuvat uhat voidaan jakaa seuraaviin ryhmiin: vahingossa syntyneet ja tarkoituksella aiheutetut uhat, passiiviset ja aktiiviset uhat, sisäiset ja ulkoiset uhat sekä ihmisen aiheuttamat ja luonnosta johtuvat uhat. Vahingossa syntyneet uhat voivat syntyä esimerkiksi ihmisen huolimattomuudesta tai osaamattomuudesta. Tarkoituksella aiheutetut uhat aiheutuvat ihmisen tahallisesta toiminnasta ja sille on jokin tietty motiivi. Passiivinen uhka ei aiheuta yritykselle välitöntä vahinkoa, ja se voi olla esimerkiksi vakoilua, jolla kerätään tietoa myöhempää tarkoitusta varten. Aktiivinen uhka aiheuttaa yritykselle välitöntä vahinkoa, ja se voi kohdistua esimerkiksi ihmiseen tai yrityksen tärkeään järjestelmään. Sisäiset uhat ovat yrityksen sisältä päin tietoturvallisuuteen

kohdistuvia uhkia ja aiheutuvat yleensä yrityksen omasta työntekijästä. Ulkoiset uhat kohdistuvat yritykseen sen ulkopuolelta, ja niiden aiheuttajia ovat esimerkiksi tietoverkkoon pyrkivä tunkeutuja, kilpaileva yritys tai valtiollinen tiedustelupalvelu. Ihmisen aiheuttamat uhat aiheutuvat ihmisen toiminnasta, ja ne voivat olla joko tahattomia tai tahallisia. Luonnosta aiheutuvat uhat ovat luonnon toiminnan aikaansaamia, ja niitä aiheuttavat esimerkiksi tulvat, metsäpalot ja myrskyt. [3, s. 34–37.]

Rikollisuus on merkittävä kyberturvallisuuden uhka, ja rikolliset pyrkivät lähes aina saamaan toiminnallaan taloudellista hyötyä [9, s. 39]. Kyberrikollisuudessa liikkuu Interpolin vuonna 2013 antaman tiedotteen mukaan enemmän rahaa kuin huumekaupassa. Vuonna 2012 amerikkalaispankeista ryöstettiin ”perinteisillä menetelmillä” 900 miljoonaa dollaria, kun kyberrikoksilla ryöstetty summa oli 12 miljardia dollaria. Samana vuonna 90 prosenttia Britannian suurista yrityksistä joutui kyberrikollisten hyökkäyksen kohteeksi. Kyberrikollisuus on siis miljardibisnes, ja FBI:n ja Interpolin mukaan se on myös tällä hetkellä kaikkein nopeimmin kasvava rikollisuuden muoto. [9, s. 39–40.] Taulukosta 1 nähdään, että kyberrikokset ovat yleistyneet myös Suomessa. Erityisesti tietomurrot ovat yleistyneet merkittävästi. Tietoverkkorikokset eivät kuitenkaan aina tule poliisin tietoon. [9, s. 41.]

Taulukko 1. Poliisin tilasto tieto- ja viestintärikoksista vuosilta 2004–2013 [9, s. 41].

Ilmoitettu kpl	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Viestintäsalaisuuden loukkaus	187	173	214	238	241	275	319	297	268	279
Viestintäsalaisuuden loukkauksen yritys	2	1	1	2	0	4	1	0	1	0
Törkeä viestintäsalaisuuden loukkaus	11	2	5	0	5	1	2	1	6	3
Salassapitorikos	24	17	29	33	31	35	40	57	45	48
Tietoliikenteen häirintä	31	44	45	42	42	41	36	32	50	93
Törkeä tietoliikenteen häirintä	2	5	1	3	4	8	3	4	7	13
Tietomurto	94	120	122	153	196	153	315	410	503	580
Tietomurron yritys	9	8	6	10	5	8	8	11	11	5
Törkeä tietomurto	-	-	-	-	-	-	-	8	14	5
Henkilörekisteririkos	27	41	28	27	24	42	40	91	148	119
Yhteensä	387	411	451	508	547	562	760	958	1053	1145

Tietoturvaan liittyviä yleisiä rikkomuksia ovat muun muassa tiedon varastaminen, rahan varastaminen, tiedon luvaton muuttaminen tai tuhoaminen, luvaton pääsy tietojärjestelmiin, haittaohjelmat ja niiden avulla saatava etähallinta sekä luvattoman tai laittoman materiaalin hallussapito [10, s. 25].

3.1 Fyysiset uhat

Fyysiset uhat voidaan jakaa kolmeen kategoriaan: ulkoiset uhat, sisäiset uhat ja ihmisestä aiheutuvat uhat. Ulkoisia fyysisiä uhkia ovat esimerkiksi tulvat, ukkonen, maanjäristys, tuuli, jää ja tulipalo. Sisäisiä fyysisiä uhkia ovat esimerkiksi tulipalo, vesivuodot ja sähkökatkokset. Ihmisestä aiheutuvia uhkia puolestaan ovat esimerkiksi varkaus, vandalismi, sabotointi, vakoilu ja vahingot. [11.] Yrityksen tilat tulee suojata ainakin seuraavilta uhilta: varkaus, tulipalo, lämpötilan liian suuret muutokset, vesivahinko, kosteus, sähköhäiriö ja pöly [4, s. 126].

Kannettavien tietokoneiden ja laitteiden varkaudet ovat yleinen ongelma, ja ne eivät kohdistu pelkästään kannettaviin tietokoneisiin vaan myös niiden sisällä oleviin komponentteihin, kuten kiintolevyihin ja muistipiireihin. Varkaudet tapahtuvat myös usein päiväsaikaan silloin, kun yrityksen hälytysjärjestelmät on mahdollisesti kytketty pois päältä. [4, s. 126.]

3.2 Hallinnolliset ja henkilöturvallisuuteen liittyvät uhat

Yrityksen omistama tai hallitsema tieto on kiinnostavaa monellakin tavalla. Tiedon hankkimiseen tai tuhoamiseen johtavat motiivit voivat olla henkilökohtaisia, taloudellisia tai poliittisia. Yrityksen oman työntekijän syyt voivat esimerkiksi olla henkilökohtaisia. Hän saattaa kokea tulleen kohdelluksi huonosti, ja se voi laukaista halun vahingoittaa yrityksen tietoa. Rikollisten motiivit ovat yleensä taloudellisia. Heitä voivat kiinnostaa esimerkiksi yrityksen hallussa olevat henkilötiedot, joita voi muun muassa myydä roskapostittajille tai luottokorttitietoja väärinkäyttävälle taholle. Poliittiset motiivit voivat johtaa esimerkiksi innovaatioiden tai keksintöjen tutkimus- tai kehitystietojen varastamiseen. Valtiovallat voivat myös vakoilla teollisuus- ja tutkimustietoa ja käyttää sitä esimerkiksi aseellisuuden kehittämisessä. [4, s. 119.]

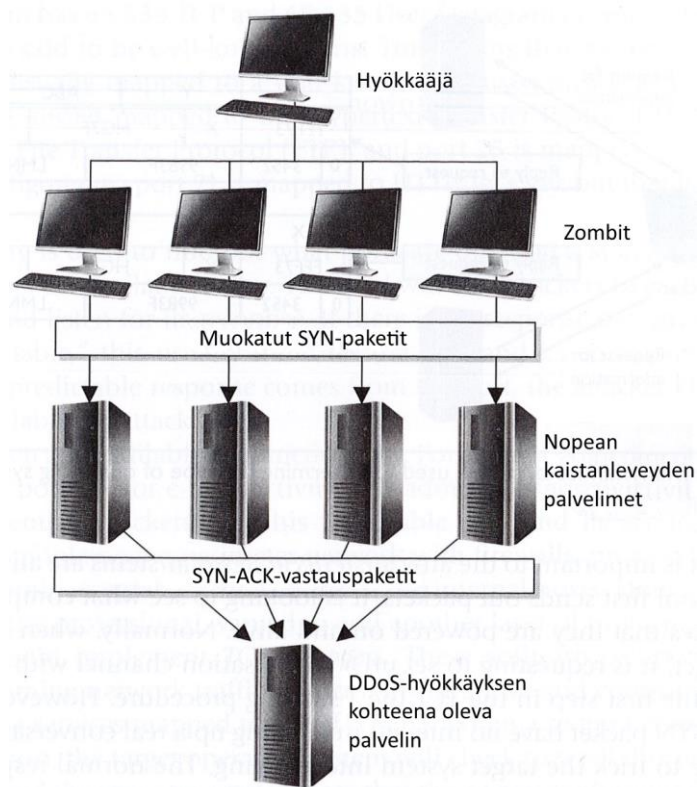
Henkilöturvallisuuden osalta tietoturvariskejä aiheuttavat esimerkiksi muutokset yhteiskunnassa, yrityksen kilpailutilanteen kiristyminen sekä tietojenkäsittelyyn osallistuvan henkilökunnan suuri määrä yrityksen sisällä ja sen ulkopuolella [4, s. 138].

Uuden työntekijän palkkaamiseen ja yhteistyökumppanin valintaan liittyy paljon erilaisia henkilöstöriskejä. Väärän henkilön palkkaaminen voi aiheuttaa suuria tietoturvahyökkäyksiä, kuten varkauksia ja sabotaasia. Vaikka työntekijä ei syyllistyisikään rikkomuksiin, aiheutuu väärän henkilön palkkaamisesta merkittäviä kuluja ja vaivaa yritykselle. Työntekijän virheellinen toiminta voi aiheuttaa tietoturvan kannalta riskejä ja kriittisiä tilanteita, ja tiedon luotettavuus voi kärsiä esimerkiksi, jos järjestelmään tai tietokantaan syötetään virheellistä tietoa. Myös yrityksen johto voi vaarantaa yrityksen maineen työnantajana, jos se toimii puutteellisesti esimerkiksi irtisanomistilanteessa. [4, s. 139, 143–144.]

3.3 Tekniset ja käytännön uhat

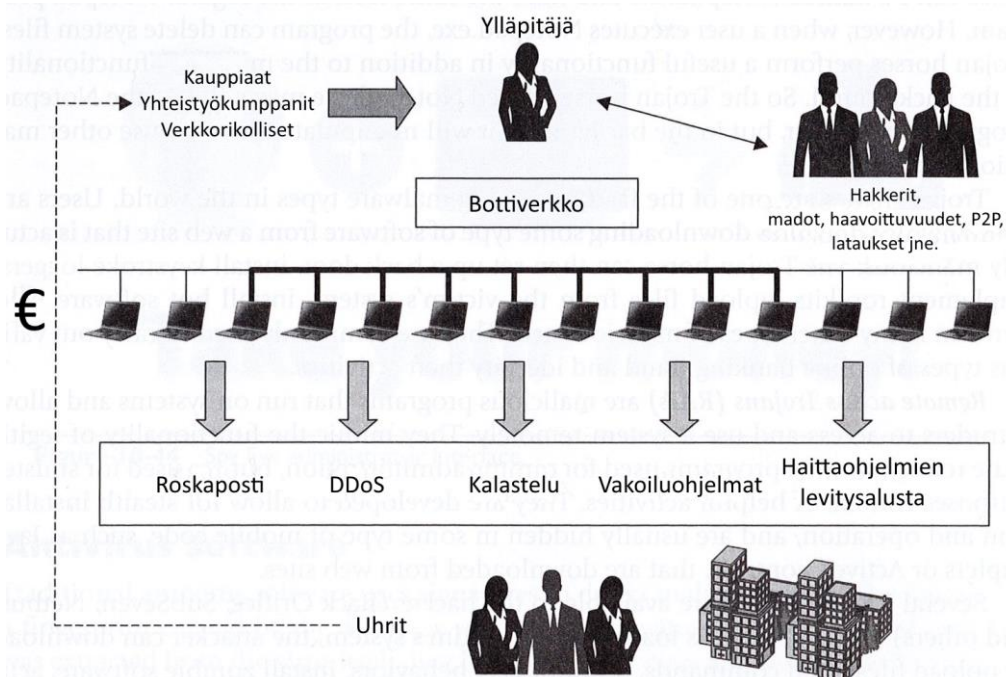
Tietoverkkouhat

Verkossa liikkuvia IP- eli Internet Protocol -paketteja voidaan kuunnella, muokata, uudelleenohjata ja väärentää, ja myös MitM-, eli man-in-the-middle, hyökkäykset ovat mahdollisia. Esimerkiksi jopa monien palomuurien sallimaa ICMP:tä, Internet Control Message Protocol, käyttävää ping-pakettia voidaan käyttää haitalliseen tarkoitukseen, ja sen sisällä voidaan esimerkiksi lähettää komentoja hyökkääjän tartuttamalle koneelle. MitM-hyökkäyksessä hyökkääjä asettuu huomaamattomasti kahden järjestelmän väliin ja pystyy näin kuuntelemaan kaiken liikenteen järjestelmien välillä. [6, s. 547, 585, 587 ja 1294.] DDoS-, eli distributed denial-of-service, palvelunestohyökkäyksillä voidaan esimerkiksi kuormittaa verkko niin, ettei verkko tai verkossa oleva palvelu enää toimi [12; 6, s. 1287]. Kuvassa 2 on havainnollistettu DDoS-hyökkäyksen toimintaperiaatetta, kun monta järjestelmää kohdistetaan häiritsemään hyökkäyksen kohdetta samanaikaisesti.



Kuva 2. Esimerkki DDoS-palvelunestohyökkäyksestä [6, s. 1287].

Palvelunestohyökkäykset voidaan suorittaa esimerkiksi botnetien, eli bottiverkkojen, avulla. Bottiverkko koostuu monista hyökkääjän tavalla tai toisella tartuttamista ja haltuunsa ottamista järjestelmistä eli zombeista, joita hyökkääjä pystyy ohjaamaan haluamallaan tavalla. Bottiverkossa saattaa olla jopa miljoona tartunnan saanutta zombia. Internetissä suoritetaan jatkuvasti skannauksia, joilla yritetään löytää lisää haavoittuvia kohteita. [6, s. 1204–1205, 1286–1287.] Kuvassa 3 on havainnollistettu bottiverkkojen toimintaa ja sitä, että ne koostuvat monista hyökkääjän haltuunsa ottamista järjestelmistä.



Kuva 3. Esimerkki bottiverkosta, jossa hyökkääjä ohjaa monia haltuunsa ottamia järjestelmiä samanaikaisesti [6, s. 1205].

Palvelimiin kohdistuvat uhat

Palvelimet tuottavat huomattavan määrän lämpöä, ja niihin voi tulla eheys- ja käytettävyyssongelmia, jos niiden sisäinen lämpötila nousee liian suureksi. Ongelmia voivat aiheuttaa myös liian alhainen tai korkea ilmankosteus sekä pöly ja muut ilman epäpuhtaudet. [5, s. 305.]

Web-palvelimiin tai niiden ohjelmistoihin kohdistuu muun muassa seuraavia uhkia: tiedon kerääminen, hallintayhteyksien hyväksikäyttö, autentikointiin ja pääsynvalvontaan

liittyvät uhat, haitalliset syötteet ja parametrit ja istuntojen hallintaan liittyvät uhat [6, s. 1158].

Tiedon keräämisen avulla pyritään löytämään hyökkäystä auttavaa tietoa, ja sitä voidaan kerätä myös hakukoneita käyttämällä ilman, että hyökkääjä on suoraan yhteydessä yrityksen web-palvelimeen. Hallintayhteyksiin voi liittyä haavoittuvuuksia ja puutteita, joiden avulla hyökkääjä voi hallita järjestelmää. Autentikointiin ja pääsynvalvontaan käytettävät tunnukset ja salasanat, joita käyttäjät käyttävät, voivat olla heikkoja, ja käyttäjät saattavat käyttää samoja tunnuksia rekisteröityessään eri palveluihin. Palvelimen ohjelmistolle voidaan myös syöttää haitallisia syötteitä ja parametreja. Hyökkääjä saattaa pystyä kiertämään syötteiden tarkistukseen liittyvät suojaukset ja esimerkiksi päästä käsiksi hakemistoihin, joihin ulkopuolisten ei kuuluisi päästä. Myös järjestelmien erilaiset puskurit voivat pitää sisällään ylivuodon mahdollistavia haavoittuvuuksia, joiden avulla hyökkääjä voi ylisuuren syötteen syöttämällä suorittaa järjestelmässä omaa koodiaan. Syötteisiin liittyy myös esimerkiksi SQL-injektio, jonka avulla voidaan manipuloida palvelimella olevia tietokantoja tai saada niistä sellaista tietoa, johon ei kuuluisi päästä käsiksi. Palvelimelle saatetaan myös pystyä tallentamaan haitallista JavaScript-koodia. Istuntojen hallintaan liittyvä session ID, jolla käyttäjän istunto tunnistetaan, saatetaan myös pystyä kopioimaan tai arvaamaan niin, että hyökkääjä saa käyttäjän istunnon haltuunsa. [6, s. 1158–1168.]

Myös DNS-, eli Domain Name System, palvelimien myrkyttäminen on mahdollista niin, että ne ohjaavat käyttäjän väärään IP-osoitteeseen [6, s. 272].

Työasemiin ja kannettaviin laitteisiin kohdistuvat uhat

Lähes kaikki kannettavat laitteet voidaan kytkeä yrityksen työasemiin käyttämällä USB- eli Universal Serial Bus -liitäntää. Esimerkiksi pelkässä kannettavassa musiikkisoittimessa on niin paljon tallennuskapasiteettia, että sille voi kopioida merkittävän määrän vaikka työasemalta löytyvää tietoa. Työntekijän on siis monessa tapauksessa teknisesti mahdollista viedä kaikki haluamansa tiedot ulkopuoliselle taholle. [4, s. 218.]

Kannettavia tietokoneita voidaan käyttää sekä yrityksen omassa että ulkopuolisessa verkossa, ja on mahdollista, että järjestelmä saa tartunnan vieraassa verkossa ollessaan. Kun tartunnan saanut kannettava tietokone kytketään yrityksen omaan verkkoon, on riskinä esimerkiksi se, että ulkopuolinen taho voi päästä saastuneelta koneelta kä-

siksi sisäverkon muihin kohteisiin tai että haittaohjelma pääsee leviämään yrityksen muihin järjestelmiin. [5, s. 137.] Kannettavia laitteita unohdetaan merkittäviä määriä esimerkiksi takseihin, ja työasema saatetaan myös varastaa tai ottaa mukaan työpisteeltä ilman lupaa. [4, s. 218–219; 3, s. 188.] On mahdollista, että työasema vioittuu tai vahingoittuu teknisen vian, toimintahäiriön tai virheellisen käytön vuoksi [3, s. 188].

Kuvassa 4 on esitelty esimerkkejä yritysten kyberomaisuudesta, joka saattaa vaarantua, jos yrityksen tietokoneisiin onnistutaan murtautumaan.



Kuva 4. Esimerkkejä kyberomaisuudesta, joka voi vaarantua tietokoneen välityksellä [9, s. 63].

Ohjelmistouhat

Yleisiä ohjelmistouhkia ovat esimerkiksi huonosti toteutetut ja päivittämättömät ohjelmistot ja käyttöjärjestelmät, sillä ne voivat sisältää haavoittuvuuksia [6, s. 26, 1081]. Myös päivitetty ohjelmistot saattavat sisältää niin sanottuja nollapäivähaavoittuvuuksia, jotka eivät ole yleisesti tiedossa ja joihin ei ole olemassa päivitystä [6, s. 1107]. Taulukossa 2 on esitelty vuoden 2015 viiden yleisimmän exploit kitin hyödyntämät viisitoista yleisintä haavoittuvuutta. Exploit kit on työkalu, jonka avulla hyökkääjä voi etsiä haa-

voittuvuuksia ja jonka avulla kohdejärjestelmään voidaan syöttää haitallista koodia. Taulukosta nähdään, että selainten Flash-laajennus on ollut usein hyökkäyksen kohteena. Taulukko perustuu F-Securen tekemään tunnistukseen. [13, s. 25, 29.]

Taulukko 2. Vuoden 2015 viiden yleisimmän exploit kitin hyödyntämät yleisimmät haavoittuvuudet [13, s. 29].

HAAVOITTUVUUDET		5 YLEISINTÄ EXPLOIT KITIÄ				
Ohjelma	CVE Nro	Angler	Neutrino	Nuclear	Magnitude	Rig
Flash Player	CVE-2015-0310	●				
Flash Player	CVE-2015-0311	●	●	●	●	●
Flash Player	CVE-2015-0313	●	●			
Flash Player	CVE-2015-0336	●	●	●	●	
Flash Player	CVE-2015-0359	●	●	●	●	●
Flash Player	CVE-2015-3090	●	●	●	●	●
Flash Player	CVE-2015-3105	●		●	●	
Flash Player	CVE-2015-3113	●	●	●	●	●
Flash Player	CVE-2015-5119	●	●	●	●	●
Flash Player	CVE-2015-5122	●	●	●	●	●
Silverlight	CVE-2015-1671	●			●	
Internet Explorer	CVE-2015-2419	●	●	●	●	●
Flash Player	CVE-2015-5560	●		●		
Flash Player	CVE-2015-7645	●	●	●	●	
Flash Player	CVE-2015-8446	●				

Ohjelmiin saattaa myös esimerkiksi jäädä niiden kehitysvaiheessa käytettyjä Maintenance hookeja, jotka ovat ohjelman takaovia ja mahdollistavat helpon pääsyn kooditasolle ohjelman sisällä. Joskus nämä kuitenkin unohdetaan poistaa valmiista versiosta, ja hyökkääjä voi löytää ne ja käyttää niitä haitalliseen tarkoitukseen. [6, s. 409.]

Haittaohjelmat

Haittaohjelmat sisältävät haitallista koodia, ja erilaisia haittaohjelmia ovat esimerkiksi virukset, madot, rootkitit, vakoiluohjelmat, troijalaiset hevokset ja logiikkapommit. Haittaohjelmat voivat levitä esimerkiksi sähköpostin, tiedostonjakamisen tai Internetistä tiedostojen lataamisen välityksellä. Hyökkääjä voi myös tahallisesti istuttaa haittaohjelmia järjestelmään. [6, s. 1197.]

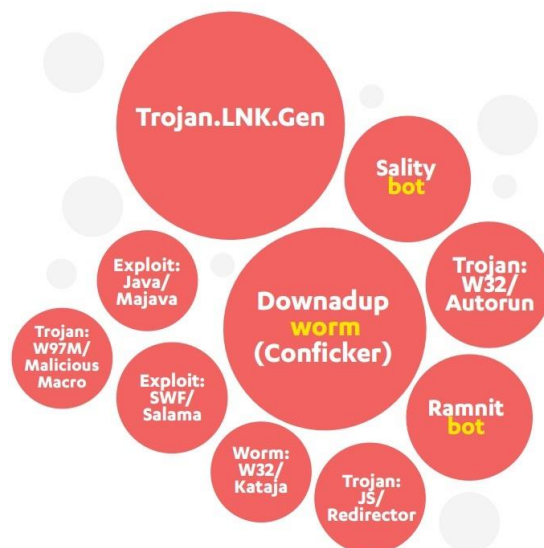
Virukset ovat haitallisia ohjelmia, jotka tartuttavat ohjelmistoja. Virus tekee itsestään kopioita ja lisääntyy liittämällä niitä muihin tiedostoihin. Mato eroaa viruksesta siten, että se on täysin itsenäinen ohjelma, joka pystyy levittämään kopioita omatoimisesti itsestään tarttumatta muihin tiedostoihin. Rootkit on joukko työkaluja, jotka hyökkääjä voi piilottaa haltuun ottamaansa järjestelmään myöhempää käyttöä varten. Rootkitin tarkoitus on antaa hyökkääjälle pääkäyttäjätason pääsy järjestelmään, ja se pitää yleensä sisällään takaoven, jonka kautta konetta voidaan hallita. Rootkit voidaan piilottaa esimerkiksi järjestelmän ytimeen, eli kerneliin, tai jopa firmwareen, joka sijaitsee piirin pyyhkiytymättömässä muistissa. Firmwareen piilotettua rootkitiä on vaikea havaita, sillä se ei näy ohjelmistojen eheyttä varmistavissa tarkistuksissa ja se voi järjestelmän käynnistyessä latautua muistiin jo ennen käyttöjärjestelmää ja muita suojaustyökaluja. Vakoiluohjelma on sellainen haittaohjelma, joka kerää järjestelmästä arkaluonteista tietoa, mutta se voi myös kerätä esimerkiksi käyttäjän selaushistoriaa kohdistettua mainontaa varten. Troijalaiset hevoset tekeytyvät näyttämään toisilta ohjelmilta, mutta sisältävät kopioidun ohjelman lisäksi haitallisia, taustalla toimivia ominaisuuksia. [6, s. 1206.]

Kuvassa 5 on esitetty vuoden 2015 yleisimmät uudet ja uniikit haittaohjelmaperheet. Pallon koosta nähdään haittaohjelmaperheen yleisyys, eli mitä suurempi pallo on, sitä yleisempi haittaohjelmaperhe on ollut prosentuaalisesti kaikkiin tunnistettuihin haittaohjelmiin nähden. Tilastot perustuvat F-Securen tekemään tunnistukseen. [13, s. 12.]



Kuva 5. Vuoden 2015 yleisimmät uniikit haittaohjelmaperheet [13, s. 12].

Kuvassa 6 on esitetty vuoden 2015 yleisimmät vanhat haittaohjelmaperheet ja yleisluonteiset haittaohjelmat. Kaikkia haittaohjelmia ei tunnisteta kuuluvaksi tiettyyn haittaohjelmaperheeseen, vaan ne tunnistetaan yleisten samankaltaisuuksien perusteella. Myös tämä tilasto perustuu F-Securen tekemään tunnistukseen. [13, s. 13.]



Kuva 6. Vuoden 2015 yleisimmät vanhat haittaohjelmaperheet ja yleisluonteiset haittaohjelmat [13, s. 13].

Tallennettuun dataan liittyvät uhat

Yrityksillä on paljon arvokasta tietoa. Esimerkiksi liikesalaisuuksia, tarjouskilpailutietoja, tuotetietoja ja asiakastietoja voidaan myydä eteenpäin varastetun tiedon kauppapaikoilla. [9, s. 35, 42.] Myös salattuihin tietoihin kohdistuu monia uhkia, ja salaus voidaan yrittää purkaa eri tavoin. Suurin osa salausalgoritmeista voidaan purkaa, jos käytössä on riittävästi aikaa, resursseja ja motivaatiota. [6, s. 865, 759.] Varmuuskopiot voivat myös tuhoutua niin, että ne menetetään [3, s. 227].

Muut tekniset ja käytännön uhat

Yksi perinteinen tekninen uhka on esimerkiksi salasanoihin ja pääsynvalvontaan liittyvä sanakirjahyökkäys, jolla pyritään löytämään oikea salasana erilaisia sanakirjoja hyödyntämällä. Hyökkäystä varten tehdyt sanakirjat sisältävät monia yleisesti salasanoina käytettyjä sanoja tai merkkiyhdistelmiä, joita käyttämällä pyritään laskennallisesti löytämään oikea salasana. Jos oikea salasana löytyy, voi hyökkääjä tämän jälkeen käyttää sitä päästäkseen sisään hyökkäyksen kohteena olevaan järjestelmään. Monet järjestelmät rajoittavat salasanojen arvauskertoja, mutta hyökkäys voidaan tehdä myös kaapatun salasanatiedoston avulla täysin järjestelmästä erillään. [6, s. 269.]

Brute force -hyökkäys liittyy sanalistahyökkäyksen tavoin salasanoihin. Tässä hyökkäyksessä pyritään laskennallisesti käymään kaikki erilaiset merkkivaihtoehdot läpi, jotta oikea salasana löytyisi. Sanalistahyökkäys ja brute force -hyökkäys voidaan myös yhdistää, jolloin hyökkäyksestä tulee tehokkaampi. [6, s. 270.]

Käyttäjän tunnukset voidaan myös saada selville, jos järjestelmä on tartutettu ohjelmalla, joka tallentaa käyttäjän kirjautuessaan syöttämät tiedot. Tällainen ohjelma voi esimerkiksi esittää aitoa kirjautumisikkunaa vastaavan ruudun, johon käyttäjä tietämättään syöttää tunnuksensa. Ohjelma voi tämän jälkeen antaa virheilmoituksen ja sulkeutua, ja käyttäjä luulee tehneensä kirjoitusvirheen ja syöttää tämän jälkeen tunnukset uudelleen aitoon kirjautumisikkunaan. [6, s. 270.]

Eräs hyvin yleisesti käytetty huijaustapa on phishing eli tietojenkalastelu, joka on käyttäjän manipulointitekniikka. Sen avulla yritetään saada muun muassa henkilötietoja, tunnuksia ja salasanoja, luottokorttinumeroita ja pankkitietoja. Käyttäjää voidaan yrittää huijata antamaan tietonsa esimerkiksi huijaussähköposteja tai -sivustoja käyttämällä.

Huijauksilla saatuja tietoja voidaan myös käyttää identiteettivarkauksen tekemiseen. Identiteettivarkauksessa sen tekijä esittää toista henkilöä ja voi esimerkiksi tehdä ostoksia uhrin nimissä. [6, s. 271–272.]

4 Fyysinen suojautuminen

Toimitilaturvallisuudelle erittäin tärkeitä osa-alueita ovat kulunhallinta ja palosuojaus, mutta tärkeää on myös esimerkiksi varmentaa sähkönsaanti ja tarvittaessa suojata tilat sähköisiä ja magneettisia häiriöitä vastaan [3, s. 177]. Fyysinen toimintaympäristö tulee arvioida säännöllisesti, kun tehdään riskikartoitusta. Kaikki korjaus- ja kehitysehdotukset tulee kirjata, minkä jälkeen korjaukset on mahdollista toteuttaa esimerkiksi yleisten rakennus- ja korjaushankkeiden yhteydessä. [4, s. 125.]

Vakuutusyhtiöiden vakuutuskirjojen vaatimuksia noudattamalla pystytään suojaamaan tietoturvan kannalta oleellisia fyysisiä kohteita. Vakuutuskirjojen vaatimukset voivat myös toimia hyvänä lähtökohtana yrityksen jatkuvuussuunnitelman kannalta mahdollisten kriisien varalle. [4, s. 127.]

4.1 Fyysiset alueet

Riippuen toiminnan luonteesta yrityksen kannattaa jakaa fyysiset tilansa eritasoisiksi alueiksi. Alueiden sisäänkäynteihin voidaan laittaa kulkuvalvonta, jolla kontrolloidaan, ketkä pääsevät alueelle sisään. [14, s. 6.] Alueet voidaan jakaa esimerkiksi seuraaviin ryhmiin: ei-tärkeä tila, tärkeä tila ja erittäin tärkeä tila. Tärkeysluokituksen tarkoituksena on tunnistaa toimitilojen tärkeys yrityksen toiminnalle, ja sen avulla kullekin toimitilalle voidaan toteuttaa oikeanlaajuiset suojaukset. Kaikki yrityksen tilat eivät vaadi samantasoista suojausta, ja se pitää ottaa huomioon, kun suojausta toteutetaan. Yleensä esimerkiksi tuotekehitystilat, tietoteknisten laitteiden tilat ja hallinnolliset tilat vaativat korkean tason suojausta. Tärkeysluokitus kannattaa laatia kaikille toimitiloille, joissa käsitellään yrityksen toiminnan kannalta merkityksellistä tietoa. [3, s. 177–178.]

4.2 Kulunvalvonta

Kulunvalvonta toteutetaan mekaanisilla tai sähköisillä lukituksilla. Mekaaninen lukitus toteutetaan lukoilla, jotka avataan mekaanisilla, esimerkiksi Abloy-, avaimilla. Sähköinen lukitus toteutetaan esimerkiksi työntekijöille annettavilla avainkortteilla, jotka määrittelevät kulkuoikeudet. Oviin laitetaan tällöin lukijat, joilla avainkortti luetaan, ja ovi avautuu, jos henkilöllä on kulkuoikeudet oveen. Sähköinen kulunvalvonta on mekaanisia lukkoja joustavampi, koska sen avulla kulkuoikeudet voidaan määrittellä joustavasti. Jos mekaaninen avain katoaa, joutuu yritys usein vaihtamaan lukot väärinkäytösten estämiseksi. Sähköinen avain voidaan ottaa helposti pois käytöstä, mikä ei aiheuta ylimääräisiä kustannuksia. [3, s. 180.] Yrityksen tulee myös pitää kirjaa avaimista ja valvoa, kenelle niitä luovutetaan ja että ne palautetaan asianmukaisesti. Avaimet, jotka eivät ole käytössä, tulee säilyttää lukitussa avainsäilytys- tai kassakaapissa. [4, s. 126.]

4.3 Videovalvonta

Videovalvonnan avulla voidaan seurata tapahtumia yrityksen toimintaan liittyvissä kohteissa. Tyypillisesti videovalvonta on käytössä ympäri vuorokauden, mutta se voidaan myös ajastaa toimimaan vain tietynä aikana. Videovalvonnasta saatava kuva voidaan sekä tallentaa että sitä voidaan valvontapisteessä katsella monitorista. Paras tulos saavutetaan pitämällä kamerat jatkuvasti käytössä ja tallentamalla ja varastoimalla videokuvat riittävän pitkäksi ajaksi. Tallennukset voidaan esimerkiksi säilyttää muutama viikon ajan, minkä jälkeen tallennustila voidaan käyttää uudelleen. Voimassa oleva lainsäädäntö voi asettaa vaatimuksia videovalvonnan käytölle, joten se pitää myös huomioida videovalvontaa toteutettaessa. Lakien vaikutus videovalvontaan tulee tarkistaa jo ennen, kuin se otetaan käyttöön. Säädökset voivat esimerkiksi vaatia, että kohteissa täytyy olla selkeät merkinnät videovalvonnan käytöstä. [3, s. 180.]

4.4 Murtosuojaus

Pääsyn laittiloihin tulee olla valvottu kaikkina aikoina, eli valvonnan tulee olla käytössä toimitilojen ollessa auki ja myös silloin, kun ne ovat kiinni [4, s. 126]. Yrityksen tilat voidaan suojata murtosuojauksella, jonka yleisiä toteutustapoja ovat mekaaninen lukitus, sähköinen murtosuojausjärjestelmä ja tilojen fyysiset rakenteelliset ratkaisut. Mekaani-

silla lukituksilla tehtyjä perussuojaustoimia voidaan täydentää sähköisellä murtosuojausjärjestelmällä, joka koostuu keskusyksiköstä ja siihen yhteydessä olevista antureista tai ilmaisimista. Järjestelmä voi käyttää esimerkiksi liikeilmaisista, lämpöilmaisista, magneettikoskettimista, paineilmaisista ja ääni-ilmaisista. Ilmaisimet voidaan yhdistää murtosuojausjärjestelmän keskukseseen langallisesti tai langattomasti, ja ne lähettävät keskukselle tiedon ympäristössä tapahtuvista muutoksista. Keskus voi tiedot tulkituaan tehdä hälytyksen esimerkiksi vartiointiliikkeelle. [3, s. 182.]

4.5 Palo- ja vesisuojaus

Palosuojauksella pystytään suojaamaan yrityksen käytössä olevat toimi- ja tuotantotilat palovahinkoja vastaan. Kiinteistöjen rakennemääräykset ja vakuutusyhtiöiden vaatimukset asettavat myös edellytyksiä paloturvallisuudelle. Automaattinen palohälytysjärjestelmä on yksi yleisimmin käytetyistä palosuojausmenetelmistä. Järjestelmän ilmaisimet tarkkailevat lämpötilaa tai savun määrää ja ovat yhteydessä keskusyksikköön, joka tulkitsee ilmaisimien lähettämät tiedot ja tekee tarvittaessa niiden perusteella hälytyksen. [3, s. 183.] Laitetiloihin ei saa päästä savua, sillä se voi vahingoittaa laitteita tai tallennusmedioita. Järjestelmän tulee tehdä lämpötilan kohoamisesta hälytys jo ennen, kuin kriittinen lämpötila ylittyy. Laitetilassa tulee olla myös riittävän tehokas ilmastointi, joka pitää lämpötilan haluttujen rajojen sisällä. Ilmastointia toteutettaessa kannattaa ottaa huomioon myös mahdolliset tulevat laitehankinnat niin, että ilmastointi on riittävän tehokasta myös tarpeen kasvaessa. [4, s. 127.] Automaattinen palohälytysjärjestelmä on edullinen, ja se olisi syytä olla käytössä yrityksen kaikissa toimi- ja tuotantotiloissa [3, s. 183].

Toinen yleisesti käytetty palosuojausmenetelmä on automaattinen sammutusjärjestelmä, joka pyrkii sammuttamaan alkaneen tulipalon. Sammutusaineena voidaan käyttää vettä, paloa tukahduttavia kaasuja tai vaahtoa. Tässäkin järjestelmässä on ilmaisimet, jotka tarkkailevat ympäristöä tulipalon varalta ja lähettävät ympäristöstä tietoa, jonka perusteella sammutus voidaan käynnistää. Automaattinen sammutusjärjestelmä on kallis, joten se sopii parhaiten sellaisten kohteiden suojaamiseksi, joissa palo täytyy saada rajattua tai sammutettua mahdollisimman nopeasti. Sammutusjärjestelmällä suojattuja kohteita voivat olla esimerkiksi tehtaiden tuotantolinjat, suuret materiaalivarastot ja tietokonesalit. [3, s. 183–184.]

Vesivahinko on tulipalon ohella toinen varsin yleinen yritysten kärsimä vahinko. Laitetiloissa ei saa olla vesiputkia, sillä ne voivat aiheuttaa vuodon laitetilassa tai sen yläpuolella. Laitetilaan voidaan myös rakentaa välipohja, joka parantaa suojaa vesivahinkoja vastaan. [4, s. 127.]

4.6 Muut fyysiset suojaustoimenpiteet

Pölyn muodostumista voidaan estää säännöllisellä siivouksella, ja esimerkiksi laitetilassa pölyä voidaan ehkäistä rajoittamalla laitetilän käyttöä. Laitetilaa ei tule myöskään käyttää muuhun tarkoitukseen, esimerkiksi varastona tai työskentelytilana. [4, s. 127.]

Yrityksen tietoturvallisuuteen voidaan joissain tilanteissa vaikuttaa myös esimerkiksi kiinteistön sähkönsyötön varmentamisella, tilojen suojaamisella sähkömagneettisia ja mikroaaltopulsseja vastaan ja tilojen äänieristämällä. [3, s. 184.]

Sähkönsyötön varmistamisella voidaan varmentaa tärkeimmissä laitetiloissa olevien laitteiden toiminta virtakatkoksen aikana. Sähkönsyötön varmentaminen voidaan toteuttaa joko katkeamattoman virransyöttöjärjestelmän eli UPS-laitteiston tai polttomootorilla toimivan voimageraattorin avulla. Ne kumpikin toimivat automaattisesti niin, että kun sähkönsyöttö häiriintyy tai tulee virtakatkos, ne siirtyvät käyttämään akuista tai generaattorista tulevaa varavirtaa. [3, s. 185.] Sähköhäiriöt voivat myös rikkoa laitteita, ja laitteet tulee suojata jännitepiikeiltä käyttämällä ylijännitesuojaa. Sähköverkkoon voi syntyä jännitepiikkejä esimerkiksi ukkosesta. Ylijännitesuojien ja UPS-laitteistojen toimivuus tulee testata säännöllisesti. [4, s. 127.]

Sähkömagneettiset ja mikroaaltopulssit voivat tuhota tietokonelaitteiden virtapiirejä tai häiritä niiden toimintaa, sillä pulssit kehittävät piireihin voimakkaan sähkövirran. Voimakas EMP, eli Electromagnetic Pulse, voi esimerkiksi syntyä ilmakehässä tapahtuvasta ydinräjähdyksestä ja kulkeutua tuhansia kilometrejä ilmakehää pitkin. Tällaisia sähkömagneettisia pulsseja vastaan voidaan suojautua EMP-suojan avulla, joka on suljettu metallihäkki. Suojattavat laitteet laitetaan EMP-suojan sisään. EMP-pulsseja todennäköisempi uhka ovat suurvaltojen kehittämät mikroaaltoaseet, joilla tietotekniset laitteet voidaan lamauttaa. Tällaisia aseita vastaan voidaan suojautua vastaavanlaisilla tekniikoilla kuin sähkömagneettisia pulsseja vastaan. [3, s. 185.]

Yrityksen toimi- ja tuotantotilat voidaan suojata äänieristyksellä. Äänieristys estää luottamuksellisten keskustelujen kuuluminen seinien läpi toisiin kerroksiin tai tiloihin. Eristys toteutetaan lisäämällä seiniin tarvittava määrä äänieristemateriaalia, joka estää äänen kuuluminen huoneen ulkopuolelle. [3, s. 185.]

5 Hallinnollinen suojaava toiminta

Yllättävät tilanteet, jotka uhkaavat tiedon luottamuksellisuutta, saatavuutta tai eheyttä, häiritsevät yrityksen toimintaa ja johtuvat monenlaisista syistä. Jatkuvuussuunnittelun avulla tietoturva uhkaavat tilanteet voidaan selvittää, jotta syy voidaan korjata tai vahingot estää tulevaisuudessa. Se vaatii normaaliajan ja toipumissuunnitelman lisäksi myös kriisiajan johtamista. Tietoturvan hallinnointi perustuu nykytilakartoituksiin ja toiminnan arviointiin ja sen vertaamiseen tavoitteisiin, vaatimuksiin ja muihin vastaaviin yrityksiin tai organisaatioihin. [4, s. 119, 121.]

Tietoturvariskejä tulee hallita usealla eri yritystasolla. Yrityksen johdon tulee tiedostaa tietoturvauhat ja riskit. Esimiesten tulee ainakin teoreettisella tasolla hallita sellaiset tietoturvallisuuteen liittyvät tilanteet, jotka tulevat vastaan päivittäisessä työssä. Myös työntekijöiden täytyy ymmärtää yrityksen tiedon arvo sekä tietoturvapoliittika ja toimintaohjeet, jotta he osaavat toimia oikein yllättävissäkin tilanteissa. [4, s. 120.]

Yrityksen tulee laatia tietoturvaohjelma, jolla määrätään tietoturvaan liittyvät periaatteet ja toimintalinjat, joita tulee noudattaa. Se on kokonaisuus, joka muodostuu turvallisuus-toiminnan järjestelyistä, henkilöstön tehtävistä ja vastuista sekä ohjeistuksesta, koulutuksesta ja valvonnasta. Tietoturvaohjelman ei tarvitse olla laaja, mutta sen tulee sisältää tietoturvallisuuteen liittyvien toimintatapojen keskeiset linjaukset. Tietoturvatointenpiteiden tulee olla huolellisesti suunniteltuja, ettei yritys joudu ongelmatilanteessa vastuuseen tietoturvatointenpiteiden seurauksena. Tietoturvakäytäntöjen tulee myös ottaa huomioon viestinnän luottamuksellisuus, yksityisyydensuoja ja sananvapauden asetamat vaatimukset. [4, s. 128.]

Tietoturvan suunnitteluun tulee ottaa mukaan myös suorittavan portaan työntekijöitä, jotta he voivat sisäistää tietoturvakäytännöt ja sen tavoitteet mahdollisimman hyvin. Tietoturva saadaan näin tekemällä jatkuviksi ja konkreettisiksi toimintatavoiksi päivittäisessä työnteossa. Jos tavoitteet eivät ole riittävän konkreettisia, henkilöstö ei näe nii-

den vaikutusta päivittäisessä työnteossaan. Tavoitteet tulee jakaa lyhyen ja pitkän aikavälin tavoitteiksi ja yhdistää yrityksen muihin tavoitteisiin. [4, s. 122, 128.]

Koulutus, perehdytys ja tiedottaminen ovat keskeisiä asioita tietoturvallisuudessa, ja niiden avulla työntekijöiden toimintatavat saadaan turvallisemmiksi ja paremmin tavoitteiden mukaisiksi. Tietoturvakoulutus kannattaa yhdistää muuhun koulutukseen, jolloin työntekijät ymmärtävät paremmin, että tietoturvallisuus on kiinteä osa jokaisen työnkuvaa. Yrityksen johdon tulee asettaa tietoturvan päämäärät ja vaatimukset, seurata osaamista, jakaa käytettäviä resursseja ja päättää koulutukseen liittyvistä mittaus- ja raportointitarpeista. [4, s. 122.]

Yrityksen kaikilla johtajilla tulee olla näkemys tietojen suojaustarpeesta, tietoriskeistä ja tietoriskien hallinnan ja siihen liittyvän työn laajuudesta. Johdolla tulee olla kuva siitä, miten ja mihin suuntaan tietoturvallisuutta täytyy kehittää. Tietoturvallisuuteen liittyvää vastuuta ei voi siirtää muille, mutta sen toteuttamisen voi delegoida eteenpäin. Johdon on kuitenkin varmistuttava siitä, että yritys toimii tietoturvapoliittikan mukaisesti. Johdon keskeisiä tehtäviä ovat osallistuminen riskianalyysiin, tavoitteen asettaminen pohjautuen nykyiseen arvioon tietoturvariskeistä, tietoriskien hallinnoinnin suunnittelu ja toiminnan suunnan näyttäminen, tietämyksen hankkiminen lakien, sidosryhmien ja asiakkaiden tietoturvavaatimuksista, tietoturvallisuuden painotuksista päättäminen ja riittävien resurssien varaaminen ja varmistaminen sekä tietoturvapoliittikan noudattamisen seuraaminen. [4, s. 130.]

5.1 Liiketoiminnan jatkuvuuden turvaaminen

Jatkuvuus- ja toipumissuunnitelmien laatimisella voidaan saavuttaa taloudellisia säästöjä. Toimintakatkoksista saattaa aiheutua huomattavia kustannuksia, ja katkojen määrää voidaan pystyä vähentämään jatkuvuutta edistävillä toimilla. Tietyillä toimialoilla jatkuvuus- ja toipumissuunnitelman laatiminen on pakollista. Tällaisia yrityksiä ovat esimerkiksi Rahoitustarkastuksen valvonnan alla olevat yritykset, joita ovat muun muassa pankit ja rahastoyhtiöt. Myös liiketoiminnan luonne voi vaatia jatkuvuuden turvaamista, esimerkiksi toiminnot, joiden katkoksista aiheutuu välitöntä vaaraa ihmisen terveydelle tai hengelle, ovat tällaisia. [4, s. 229.]

Jatkuvuussuunnitelma

Jatkuvuussuunnitelman tarkoituksena on turvata yrityksen tärkeiden prosessien jatkuminen kaikissa tilanteissa. Sen pyrkii turvaamaan jatkuvuuden normaalitilanteissa, häiriötilanteissa ja niiden jälkeen. Valtionhallinnon tietoturvakäsitteistön määritelmän mukaan jatkuvuussuunnitelmassa on suunniteltu se, miten tietojenkäsittely ja tiedonsiirto turvataan niin, että ne voivat jatkua häiriöiden aikana ja niiden jälkeen. [4, s. 227.]

Jotta jatkuvuussuunnitelman tekeminen olisi mahdollista, tulee yrityksen tietää, mitkä liiketoiminnan osa-alueet ovat sille kaikkein tärkeimmät ja mitä prosesseja, toimintoja, tehtäviä, tietoja ja resursseja niihin liittyy. Tulee myös tietää, kuinka pitkät toiminnan kestoajat sallitaan ja mitkä osa-alueet täytyy pitää toiminnassa keinolla millä hyvänsä. Tässä arvioinnissa auttaa myös tärkeysluokittelu. [3, s. 268–269.]

Jatkuvuussuunnittelu ei ole kertaluontoista, vaan se on jatkuva prosessi, jota pitää ylläpitää. Se vaatii muun muassa säännöllistä testaamista ja dokumentointia sekä suunnitelmien ylläpidon seuranta. [4, s. 228–229.]

Toipumissuunnitelma

Liiketoiminnan toipumissuunnitelman tarkoituksena on mahdollistaa yrityksen tärkeiden prosessien riittävän nopea toipuminen häiriötekijöistä ja jatkuminen niiden jälkeen. Valtionhallinnon määritelmän mukaan toipumissuunnitelma on jatkuvuussuunnitelman osa, joka sisältää ohjeet katastrofista toipumiseen, toiminnan jatkamisesta ja paluusta normaaliin toimintaan. Se määrittelee tärkeille tietojärjestelmille varajärjestelmävaatimukset, vastuut ja toimet valmiuden luomiseksi sekä antaa ohjeet toiminnasta poikkeustilanteissa. Toipumissuunnitelmaa tarvitaan siis erityisesti silloin, kun on tapahtunut jokin, mikä vakavasti häiritsee tai estää normaalin liiketoiminnan. [4, s. 227, 234.]

Jatkuvuussuunnitelman tapaan myös toipumissuunnitelma on jatkuva prosessi. Toipumissuunnittelu liittyy jatkuvuussuunnitteluun, ja sen ylläpitäminen sisältää samankaltaisia toimenpiteitä. [4, s. 228–229.]

5.2 Riskianalyysi ja tietoturvallisuuden testaaminen

Riskienhallinnalla pyritään havaitsemaan ja hallitsemaan yrityksen toimintaan kohdistuvia riskejä, ja se voidaan jakaa kahteen vaiheeseen: riskikartoitukseen ja riskien arviointiin [4, s. 150; 5, s. 80]. Riskianalyysien ja murtotestausten avulla voidaan mitata miten hyvin yrityksen prosessit toimivat. Tietoturvallisuuden testaamisella pyritään havaitsemaan tietoturvaan liittyvät heikkoudet ja testaamaan käytössä olevien suojaustoimenpiteiden toimivuus sekä havaitsemaan puutteet niiden toiminnassa. Murtotestauksella mitataan siis sitä, tuottavatko prosessit laadukasta tulosta. Laadukas lopputuote tarkoittaa järjestelmiä, joita murtotestauksessa ei pystytä murtamaan. [4, s. 279, 150.]

Riskikartoituksessa tulee käsitellä yritykseen kohdistuvia uhkia nykytilanteessa ja myös tulevaisuuden mahdollisesti mukanaan tuomia uusia uhkia [5, s. 80]. Jotta riskikartoitus saataisiin tehtyä mahdollisimman laajasti ja totuudenmukaisesti, tulee sen tekemiseen osallistua henkilöitä yrityksen eri toiminnoista [4, s. 121]. Riskianalyysiltä voidaan odottaa parempia tuloksia sen mukaan, kuinka laajasti eri henkilöstöryhmät osallistuvat kartoitukseen [5, s. 80]. Eri toiminnoissa tietoturvallisuuteen liittyvät riskit voivat olla erilaisia, ja näin niitä saadaan käsiteltyä eri näkökulmista, jotta kaikki potentiaaliset riskit ja uhat saataisiin huomioitua [4, s. 121; 5, s. 80]. Näkökulmia ja mielipiteitä voidaan tuoda esille esimerkiksi työryhmissä, joiden valmisteluun kannattaa käyttää riittävästi aikaa ja tarvittaessa myös ulkopuolisten asiantuntijoiden apua [4, s. 121].

Riskien arviointi tehdään sen jälkeen, kun riskianalyysi on saatu valmiiksi ja riskit ja uhat on selvitetty. Riskien arvioinnissa keskeistä on arvioida riskien vaikutukset yrityksen toimintaan ja niiden toteutumistodennäköisyys. [5, s. 81.] Vaikutusten arvioinnissa tulee ottaa huomioon suojattavan kohteen tärkeys, jotta voidaan arvioida, kuinka vakavia vahinkoja luottamuksellisuuteen, eheyteen tai saatavuuteen kohdistuvat riskit voivat toteutuessaan yritykselle aiheuttaa. Voidaan laskea riskikerroin, joka koostuu riskin toteutumisesta aiheutuvien vahinkojen suuruuden ja toteutumistodennäköisyyden suhteesta. Riskikertoimen perusteella voidaan nähdä, mihin riskeihin on tärkeää varautua. Riskiin varaudutaan arvioimalla riskin toteutumisesta syntyvien vahinkojen ja riskiä vastaan suojautumisen aiheutuvien kustannusten suhdetta. [6, s. 74–78; 5, s. 81.] Yleensä riskiin ei kannata varautua, jos siihen varautumisen kustannukset ovat riskin toteutumisesta aiheutuvia kustannuksia suuremmat [6, s. 74].

Riskien arvioinnin ja tietoturvallisuuden testaamisen tulee olla säännöllistä ja johdonmukaista, ja niille tulee olla vastuulliset suorittajat. Analyyseistä ja tuloksista tulee antaa raportti kaikille niille tahoille, joita analyysi koskettaa. Merkittävät havainnot tulee raportoida yrityksen johdolle, joka voi niiden pohjalta tehdä toiminnan kehittämiseen liittyviä päätöksiä. Riskianalyysin merkittävistä tuloksista voidaan myös tarvittaessa tehdä yhteenveto, joka osoittaa jokaiselle riskille tai puutteelle omistajan, jonka vastuulla riskin hallinta on. Toimenpiteiden toteutumista voidaan myös seurata säännöllisesti. [4, s. 150.]

5.3 Henkilöturvallisuuden suojaus

Yrityksen jokaisen työntekijän tulee omalta osaltaan huolehtia tietoturvapoliittikan tavoitteiden saavuttamisesta. Työntekijän on osallistuttava yrityksen tietoturvallisuuskoulutuksiin ja aktiivisesti sovellettava tietoturvaohjeita ja -toimintatapoja käytännön työtehtäviin. Työntekijöiden tulee suhtautua yrityksen tietoon ohjeiden mukaan ja olla huolellisia tietojenkäsittelyssä. Työntekijöiden keskeisiä tehtäviä ovat tiedon luokittelu ja käsittely ohjeiden mukaisesti, luokitellun tiedon käsittely, siirtäminen ja säilyttäminen ohjeiden mukaisesti, omien salasanojen hallinta ja turvallinen käyttö, ohjeiden noudattaminen, varahenkilön tiedottaminen ja koulutus sekä heikkouksien ja puutteiden raportointi sovittuja raportointimenetelmiä käyttäen. [4, s. 137.]

Työntekijöiden rekrytoinnissa esimiehen ja henkilöstöhallinnon vastuulla on selvitystyön tekeminen. Ennen sopimuksen allekirjoittamista tulee varmistua henkilön taustoista. Yritys voi taustatarkastuksen avulla vähentää uuden henkilön palkkaamiseen liittyviä riskejä ja saada kuvan siitä, miten hyvin henkilö voi sopeutua yrityksen kulttuuriin. [4, s. 139.] Työnhakijan henkilötiedot tulee ensisijaisesti kerätä työnhakijalta itseltään. Tiedon hakeminen työnhakijasta hakukoneiden avulla, eli niin sanotusti googlaamalla, on työelämän tietosuojalain (759/2004) 4 §:n ja henkilötietolain (523/1999) 5 §:n, 6 §:n ja 9 §:n pääsäännön vastaista ja laitonta, jos tällaista tietoa kerätään, talletetaan tai muuten käytetään työnhakijaan liittyvässä päätöksenteossa. Jos työntekijään liittyvää tietoa halutaan kerätä muualta kuin työnhakijalta itseltään, täytyy työnhakijalta pyytää tähän suostumus. [15.] Ansioluettelon totuudenmukaisuus tulee varmistaa, ja työnhakijalta on hyvä pyytää työtodistukset niistä työpaikoista, joissa hän on työskennellyt aiemmin. Työnhakijaan liittyvien henkilötietojen totuudenmukaisuudesta ja ajantasaisuudesta on

syötä varmistua myös siksi, että työnhakijalla on lainmukainen oikeus tulla arvioiduksi oikeiden ja asiaankuuluvien tietojen perusteella. [4, s. 140.]

Tarvittaessa työnhakijasta voidaan myös hänen suostumuksellaan teettää suojelupoliisin avulla turvallisuus selvitys. Turvallisuus selvitys voidaan tehdä kolmessa eri laajuudessa, joista suppea selvitys riittää tavallisen yrityksen tarpeisiin. Suppean selvityksen tarkoituksena on selvittää, voidaanko työnhakijalle myöntää oikeus luottamuksellisen tiedon käsittelyyn ja pääsyyn tietojenkäsittelytiloihin. Tällaisia tietoja ja tiloja ovat sellaiset tiedot ja kohteet, joilla on huomattavaa merkitystä valtion turvallisuudelle tai julkiselle taloudelle. Turvallisuus selvitys voidaan tehdä myös silloin, kun henkilö voi vaarantaa yksityistä arvokasta liike- tai ammattisalaisuutta. Kaikista palkattavista ei kannata pyytää suojelupoliisin turvallisuus selvitystä. Tarvittaessa voidaan selvittää myös työntekijän luottotiedot. [4, s. 140–141.]

Työsuhteissa tulee pitää huolta siitä, että luottamukselliset ja salaiset tiedot eivät päädy sellaisten ihmisten tietoon, jotka eivät ole niihin oikeutettuja. Henkilöille, joille halutaan antaa oikeus luottamuksellisiin tietoihin, tulee laatia salassapitosopimukset. Salassapitosopimusten tarkoitus on suojata yrityksen kannalta kriittiset tiedot niin, ettei luottamuksellinen tieto pääse kulkeutumaan sopimuskumppaneilta eteenpäin myös työsuhteen päättymisen jälkeen. Työsuhteen päättyessä sellaiset työntekijästä kerätyt henkilötiedot pitää tuhota, jotka ovat yritykselle tarpeettomia. [4, s. 141–142, 144.]

6 Tekniset ja käytännön suojaustoimenpiteet

6.1 Tietoverkkojen suojaus

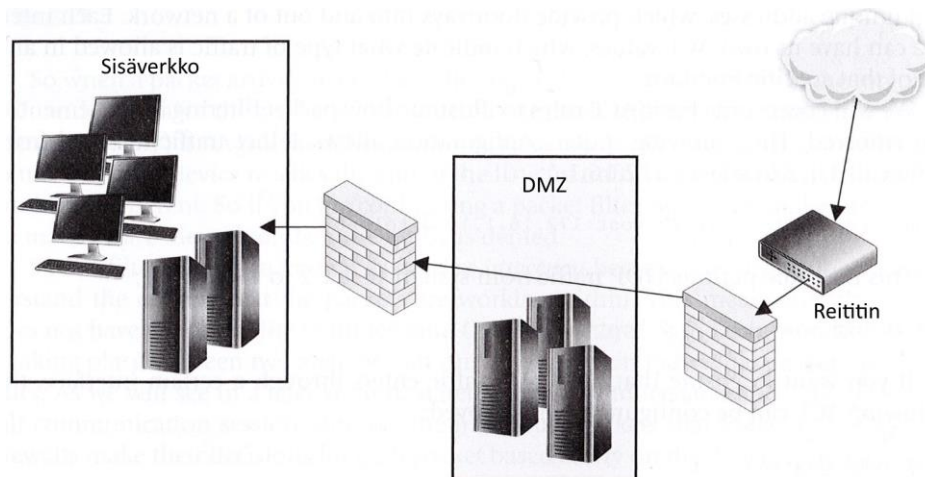
Tietoverkossa suoritettavia tietoturva toimenpiteitä saa yleensä suorittaa vapaasti silloin, kun ei käsitellä henkilötietoja, tunnistamistietoja, paikkatietoja tai muita vastaavia, joiden avulla yksittäinen henkilö voidaan tunnistaa. On myös huomioitava, että tietoverkon valvonnan tulee kohdistua ensisijaisesti vain yrityksen omiin tietojärjestelmiin ja yrityksellä on sähköisen viestinnän tietosuojalain (SVSTL) 19 §:n nojalla velvollisuus huolehtia työntekijöidensä paikkatietojen ja tunnistamistietojen tietoturvasta. Yritys on siis velvollinen toteuttamaan tietoverkkonsa sellaiseksi, että nämä suojatut oikeudet toteutuvat. [4, s. 185.] Jos Internet-yhteyden saatavuus on tärkeää, kannattaa yritykselle

lä olla varayhteys, joka otetaan käyttöön pääyhteyden katketessa [6, s. 910, 926 ja 941–942].

Tietoverkkojen looginen rakenne ja DMZ

Olennaista tietoverkon suojaamisessa on verkon huolellinen suunnittelu. Hyvin suunniteltu verkko on sekä helpommin laajennettava että suojattava. Lähes itsestään selvä toimenpide on erottaa yrityksen verkko Internetistä palomuurin avulla. Yrityksen sisäinen verkko kannattaa lisäksi jakaa pienempiin osiin, mikä parantaa verkon toimivuutta ja turvallisuutta. Kaikki erilliset toiminnot ja laitteet, joilla on erilaiset tietoturva-vaatimukset, kannattaa jakaa osiin ja niille tulee varata omat verkkoalueet. Järjestelmien tärkeysluokittelu helpottaa tietoverkon suojaamista. Verkon rakenteen tulee vastata käyttötarkoitusta ja myös esimerkiksi verkon hallinnalla ja langattomilla verkoilla tulee olla omat verkkoalueensa. Sisäverkon jakaminen voidaan toteuttaa VLAN-, eli Virtual Local Area Network, verkkojen avulla. Virtuaaliverkot parantavat verkon tietoturvaa rajaamalla liikenteen erillisten virtuaaliverkkojen sisälle. Korkean tietoturvallisuuden saavuttamiseksi eri verkon osat voidaan lisäksi erottaa toisistaan palomuurien avulla. [4, s. 182–183.]

Sellaiset palvelimet, joihin tulee saada yhteys yrityksen ulkopuolelta, kannattaa eristää omaksi DMZ-, eli Demilitarized Zone, alueeseen niin, että ne ovat erillään yrityksen sisäverkosta. DMZ-verkossa oleviin järjestelmiin pääsee käsiksi ulko- ja sisäverkosta, mutta siitä ei pysty luomaan yhteyksiä sisäverkkoon. [16; 6, s. 628–629.] DMZ-verkossa olevien järjestelmien tulee olla kovetettuja, ja sen yhteydessä on yleistä käyttää myös IDS-, eli Intrusion Detection System, järjestelmää [6, s. 629]. Kuvassa 7 on havainnollistettu DMZ:n toimintaa, kun se sijoitetaan sisäverkon ja Internetin väliin.



Kuva 7. DMZ sijoitetaan yrityksen sisäverkon ja Internetin väliin, ja se eristetään molemmista palomuuureja käyttämällä [6, s. 629].

Tietoverkkojen hallinta

Kaikkien verkkokomponenttien ja palomuurien konfigurointi ja hallinta tulee tehdä erityistä huolellisuutta noudattaen. Verkonhallintaan kannattaa käyttää omaa verkko-osiota, joka on varattu tähän tarkoitukseen, ja hallinta tulee estää muista verkoista. Kytkimillä tulee olla IP-osoite ainoastaan hallintaan käytetyssä VLAN-verkossa, ja kytkimien tulee sallia yhteydet itseensä vain sallituilla yhteysprotokollilla tietyistä IP-osoitteista. Hallintaverkkoon ei siis saa päästä muista verkoista, ja hallintatyöasemat tulee myös suojata hyvin. Kaikkia laitteita tulee hallita salattuja yhteysprotokollia käyttäen, ja käytöstä pitää poistaa sellaiset protokollat, jotka ovat tiedetysti murrettavissa. Hallintayhteyksien salaaminen on hyödyllistä, sillä kun yhteydet ovat salattuja, ulkopuoliset tahot tai yrityksen työntekijät eivät voi esimerkiksi kaapata verkkoliikenteestä ylläpitäjien salasanoja ja murtautua järjestelmiin niiden avulla. [4, s. 183–184, 197.]

Verkkokaapeleissa kannattaa käyttää värikoodausta, jonka avulla esimerkiksi hallintaverkko, varmistusverkko ja normaaliverkko voidaan selkeästi erottaa toisistaan. Samaa värikoodausta kannattaa käyttää myös verkkolaitteiden porteissa. Värikoodien käytöllä voidaan vähentää virheellisiä kytkentöjä. [4, s. 184.]

Palomuurit

Palomuurilla voidaan estää ulkopuolisten tahojen pääsy verkkoon tai verkon tarjoamaan tiettyyn palveluun. Esimerkiksi pakettisuodatinpalomuurit estävät ja sallivat lii-

kennettä lähde- ja kohdeosoitteiden ja porttinumeroiden perusteella. [5, s. 187.] Yrityksen kannattaa ottaa käyttöön DPI-, eli Deep Packet Inspection, tekniikkaa tukeva palomuuuri, joka yhteyksien suodattamisen lisäksi tutkii pakettien sisällön. Tällä tavalla palomuurissa voidaan esimerkiksi toteuttaa virustentorjunta, kun palomuuuri pystyy tutkimaan liikenteen sisältöä. [17.] DPI:n suhteen tulee kuitenkin huomioida se, että se ei kykene tutkimaan salatun liikenteen sisältöä. Tarvittaessa salattu liikenne voidaan palomuurissa purkaa ja salata uudelleen, jolloin liikenteen tutkiminen on mahdollista. [4, s. 195.]

Yritys voi tarvittaessa ottaa sellaisen palomuurin tai verkkojärjestelmän käyttöön, joka pyrkii tunnistamaan saastuneet laitteet ja suodattamaan tavallisesta poikkeavan ja haitallisen liikenteen yrityksen sisäverkossa [5, s. 137]. UTM-, eli Unified Threat Management, järjestelmät yhdistävät useita eri turvallisuusominaisuuksia niin, että niitä kaikkia voidaan hallinnoida yhdessä samasta järjestelmästä. Ne pyrkivät siis keskittämään ja yksinkertaistamaan verkon turvallisuuden hallintaa. UTM-järjestelmä voi pitää sisällään esimerkiksi palomuurin, IDS- ja IPS-, eli Intrusion Prevention System, järjestelmän, antivirusjärjestelmän, roskapostin ja verkkosisällön suodattimet, VPN-, eli Virtual Private Network, toiminnot ja QoS-, eli Quality of Service, ominaisuudet. [18; 6, s. 656.] VPN on salattu ja turvallinen tunneli, joka voidaan muodostaa epäluotettavan verkon läpi. QoS:n avulla kaistankäyttöä voidaan hallita ja priorisoida. [6, s. 702, 680.] Palomuurin käyttöjärjestelmä tulee pitää ajan tasalla, sillä niistäkin voi löytyä haavoittuvuuksia. Hyvällä ja päivitetyllä palomuuriratkaisulla voidaan suojata myös haavoittuvaisia IoT-laitteita, kun ne ovat yhteydessä Internetiin suojatun palomuurin kautta [19].

IPS ja IDS

Tunkeutumisen havaitsemiseen ja estämiseen on olemassa järjestelmiä. IDS pyrkii havaitsemaan tunkeutumisesta, ja IPS pyrkii havaitsemisen lisäksi myös estämään ne. Ne on tarkoitettu valvomaan verkkoa ja verkossa olevien laitteiden verkkoliikennettä ja estämään haitallisia tapahtumia. Järjestelmien toiminta perustuu verkon normaalin tietoliikenteen määrittämiseen, hyökkäysmallien kuvaamiseen, tietoliikenteen poikkeamien tunnistamiseen ja poikkeamien aiheuttamiin hälytyksiin tai automaattiseen pääsykontrollien toteuttamiseen. IPS- ja IDS-järjestelmien käyttöönotto tulee tehdä harkiten, ja niiden käyttöönottoprosessiin tulee varata riittävästi aikaa järjestelmien säätämistä varten. Olennaista on saada järjestelmä säädettyä niin, että väärin hälytyksien määrä saadaan alhaiseksi ilman, että merkittäviä tekijöitä jää havaitsematta. Myös järjestelmi-

en seurantaan ja operointiin tulee varata riittävästi resursseja. Verkon turvallisuudesta vastaavien henkilöiden on myös mahdollista saada näillä järjestelmillä hyödyllistä tietoa verkon ja järjestelmien tilasta sekä verkkoliikenteestä. [4, s. 190–191.]

6.2 Palvelinten suojaus

Palvelinhuoneiden ilman laatuun on kiinnitettävä huomiota. Tilaan tulee tarvittaessa asentaa erillinen ilman jäähdytys ja kostutus. Tällaiset koneelliset ilmastointiratkaisut usein myös suodattavat ilmaa epäpuhtauksista. [5, s. 305.] Palvelinlaitteet tulee nostaa pois lattiatasosta, sillä se ehkäisee vesivahinkoja ja pölyn kertymistä laitteisiin [4, s. 127].

Yrityksen kannattaa myös huomioida tuhoeläinten mahdollisuus. Laitetiloihin voidaan tarvittaessa laittaa muurahaisrasiat, jotka estävät, että muurahaiset eivät pesiydy laitteisiin ja aiheuta toimintahäiriöitä. Myös jyrsijät saattavat päästä laitetiloihin ja rikkoa verkko- ja muita kaapeleita. Niiltä voi yrittää suojautua esimerkiksi ilmastointikanavien metallisilla suojaverkoilla. [5, s. 306.]

Palvelinlaitteiston tulee olla vikasietoisempaa kuin työasemien, ja sen toimintaa voidaan varmistaa esimerkiksi käyttämällä useita virtalähteitä, kiintolevyjä, muistipiirejä, tuulettimia ja muita komponentteja niin, että ne otetaan käyttöön, kun käytössä olevaan komponenttiin tulee vikaa. Palvelin voidaan myös tarvittaessa kahdentaa kokonaan. Näillä toimenpiteillä laiteviat eivät helposti häiritse tai pysäytä palvelimen toimintaa. Erityisesti levyasemat kannattaa toteuttaa vikasietoisesti esimerkiksi RAID-levyjärjestelmää käyttäen niin, ettei kiintolevyn vioittuminen aiheuta tietojen menetystä. [5, s. 140–141.]

Web-, sähköposti- ja DNS-palvelimet ovat esimerkkejä sellaisista palvelimista, jotka kannattaa yleensä sijoittaa omaan DMZ-verkkoonsa [6, s. 629]. DNS-palvelin kantaa jakaa kahteen osaan niin, että DMZ:ssa sijaitseva palvelin käsittelee ulkoisen verkon DNS-kyselyt ja sisäverkossa sijaitseva palvelin käsittelee sisäverkon DNS-kyselyt. Näin sisäverkossa sijaitsevat järjestelmät eivät näy hyökkääjälle, jos Internetiin yhteydessä olevaan DMZ:ssa sijaitsevaan DNS-palvelimeen murtaudutaan. [6, s. 596.]

6.3 Työasemien ja kannettavien laitteiden suojaus

Käyttöoikeuksien lisäämis- tai muutospyyntöjä varten kannattaa tehdä lomake tai sovellus, jolla käyttöoikeuksiin liittyviä muutoksia voidaan pyytää. Hyväksytyt käyttöoikeuksien muutospyyntöt tulee arkistoida keskitetysti esimerkiksi käyttäjän nimen mukaan. Käyttöoikeuksien hallinta kannattaa yhdistää henkilöstöhallinnan kanssa niin, että esimerkiksi työntekijän työsuhteen päätyminen ilmoitetaan automaattisesti käyttöoikeuksien hallinnasta vastaaville. Käyttöoikeudet kannattaa myös tarkistaa säännöllisesti, esimerkiksi joitakin kertoja vuodessa. Tarkastuksessa käyttöoikeudet käydään läpi henkilöhallinnon listan kanssa, johon on koottu yrityksessä töissä olevat henkilöt ja ulkopuoliset konsultit. [4, s. 151–152.] Käyttöoikeuksien hallinta liittyy myös ohjelmistojen suojaukseen [5, s. 126].

Kuten sivun 15 taulukosta nähtiin, selainlaajennusten käyttöä tulee rajoittaa [13]. Lisäksi kannettavien laitteiden katoamisten ja työasemien varkauksien varalta on tärkeää, että kiintolevyt ja tärkeät tiedot ovat huolellisesti salattuja [4, s. 218–219]. Tietokoneiden ohjelmalliset suojausmekanismit kiertävää DMA-, eli Direct Memory Access, hyökkäystä vastaan voidaan suojautua esimerkiksi BIOS-salasanaa käyttämällä ja ottamalla DMA:n mahdollistavat liitännät, kuten Firewire, Thunderbolt ja ExpressCard, kokonaan pois käytöstä [20].

Tietokoneita tulisi käyttää langallisilla näppäimistöillä ja hiirillä tai sellaisilla langattomilla syötelaitteilla, jotka käyttävät AES-, eli Advanced Encryption Standard, salausta. Langattomia syötelaitteita, jotka eivät käytä kunnollista salausta, voidaan esimerkiksi kuunnella ulkopuolisten toimesta. [21.]

6.4 Ohjelmistojen suojaus

Ohjelmistoturvallisuuden tärkeitä suojausmenetelmiä ovat muun muassa ohjelmiston pääsynvalvonta, ohjelmiston tapahtumatietojen seuranta, varmuuskopiointi, asianmukainen ohjelmistodokumentaatio, asianmukaisesti laaditut ylläpito- ja huoltosopimukset ja rekisteröityjen ohjelmistojen käyttö [3, s. 226].

Tietoturvan kannalta on tärkeää, että yrityksen käytössä olevien ohjelmien tietoturvaaukkoja, haavoittuvuuksia tai muita riskejä seurataan. Seurannassa auttaa yrityksen

käytössä olevista ohjelmistoista koottu ohjelmistorekisteri. Yrityksen kannattaa antaa tietoturva-aukkojen seuranta yrityksen jonkin tahon hoidettavaksi ja päättää, mistä tietolähteistä uusia tietoturva-aukkoja seurataan. Hyviä tietolähteitä voivat olla esimerkiksi listat, joita CERTit, eli Computer Emergency Response Teamit, ylläpitävät. Myös toimintatavat uusien tietoturva-aukkojen tai ohjelmistopäivitysten osalta tulee sopia. [4, s.156.]

Virustorjunta tulee olla otettu käyttöön kattavasti. Työasemilla ja palvelimilla tulee olla asennettuna asianmukaiset virustorjuntaohjelmistot. Vaikka virustorjuntaohjelmiston käyttö on välttämätöntä, ei sen käyttö yksin riitä takaamaan riittävää tietoturvallisuutta. Yrityksen tietoturvasta vastaavien täytyy siis ymmärtää, että virustorjuntaohjelmistojen lisäksi vaaditaan myös lukuisia muita teknisiä ja käytännön toimenpiteitä. Virustorjunnan kannalta kannattaa huolehtia muun muassa seuraavista toteutuksista: toiminta virustartuntatapauksissa, työasemien virustorjunta, palvelimien virustorjunta, etä- ja mobiililaitteiden virustorjunta, tuotannollisten järjestelmien virustorjunta, siirrettävien medioiden, kuten USB-muistien, käsittely ja suojaus. [4, s. 203–205.]

Windows-järjestelmien turvallisuutta voidaan parantaa ottamalla käyttöön Microsoftin kehittämä EMET eli Enhanced Mitigation Experience Toolkit. EMET parantaa järjestelmässä käytettävien ohjelmien turvallisuutta suojaamalla niiden käyttämää muistia ja auttaa suojautumaan myös uusia tunnistamattomia uhkia ja haittaohjelmia vastaan. Ohjelmat tulee kuitenkin tällöin testata, jotta voidaan varmistaa, että ne toimivat ja ovat yhteensopivia EMET:n kanssa. [22, 23.]

Työasemien käyttöjärjestelmät tulee kovettaa niin, että käyttöjärjestelmän turhat palvelut poistetaan käytöstä. Tämä pienentää hyökkäyspinta-alaa ja parantaa samalla suorituskykyä. [4, s. 215–216.] Työasemissa tulee käyttää pelkästään yrityksen hyväksymiä ohjelmia [2, s. 167]. Käyttöjärjestelmät tulee myös säätää keräämään riittävästi hyödyllisiä lokitietoja, jotka voidaan esimerkiksi tallentaa turvallisesti erilliselle lokipalvelimelle. [4, s. 216]

Ohjelmiston pääsynvalvonta on myös yksi ohjelmistojen perussuojausmenetelmä. Pääsynvalvonnalla pyritään estämään ulkopuolisten henkilöiden pääsy tietojärjestelmiin. Tavallinen keino toteuttaa pääsynvalvonta on kysyä käyttäjältä käyttäjätunnus ja salasana. Mikäli käyttäjällä ei ole tunnuksia, hän ei pääse sisälle järjestelmään. [3, s. 226.]

Monet ohjelmat keräävät tapahtumatietoja, eli lokitietoja, toiminnastaan. Yleensä kerätäviä lokitietoja ovat esimerkiksi autentikointitiedot, joista voidaan nähdä, kenen käyttäjätunnuksella ja mihin aikaan järjestelmään on kirjaututtu. Lokitietoja keräämällä pyritään tallentamaan tärkeitä järjestelmän toimintaan liittyviä tapahtumia, jotta väärinkäytös- tai vikatilanteita voitaisiin tutkia ja selvittää. [3, s. 226–227.]

Ohjelmilla on yleensä käyttöohjeet ja dokumentteja, jotka kuvaavat ohjelmiston toimintaa. Ohjelmistodokumentoinnin tarkoituksena on auttaa yritystä esimerkiksi virhetilanteiden selvityksessä, jotta voitaisiin selvittää, mitä on tapahtunut ja miten ongelma voidaan korjata. Ohjelmistodokumentoinnista on yritykselle hyötyä silloin, kun se on ajan tasalla ja riittävän kattava sellaisten ohjelmistojen osalta, joihin sitä tarvitaan. [3, s. 227–228.]

Ohjelmistotkin saattavat jossain vaiheessa vikaantua, ja yrityksellä voi tällaisten tilanteiden varalta olla ylläpito- ja huoltosopimukset [3, s. 228].

Yrityksen käyttämien ohjelmien tulee olla laillisesti hankittuja, ja niihin täytyy olla käyttöoikeus niin, ettei yritystä voida syyttää ohjelmien luvattomasta käytöstä [3, s. 228]. Esimerkiksi ISO 27001 -standardi vaatii IT-omaisuusrekisterin laatimista ja ylläpitoa, joten yrityksen kannattaa laatia prosessi lisenssien hallintaa varten. Käytössä olevat ohjelmat ja ohjelmalisenssit tulee inventoida säännöllisesti, ja uudet hankitut ohjelmistot tulee päivittää lisenssirekisteriin. Käyttämättömien ja vanhojen ohjelmistojen paikannus ja käytöstä poistaminen voidaan antaa esimerkiksi tietohallinnon vastuulle. Ohjelmistorekisterin ylläpidolla on mahdollista saavuttaa myös merkittäviä kustannussäästöjä. [4, s. 153.]

6.5 Datan suojaus ja varmuuskopiointi

Tietojen salauksella voidaan varmistaa tietojen luottamuksellisuus [4, s. 195]. Siitä huolimatta, että suurin osa salausalgoritmeista on lopulta purettavissa, voidaan salauksella salata tiedot niin, että salauksen purkaminen vie hyökkääjän näkökulmasta liikaa aikaa ja resursseja [6, s. 759]. Yrityksen tietojenkäsittelyyn liittyvässä ohjeistuksessa ja luokitelussa kannattaa ottaa kantaa siihen, miten ja mitkä tiedot tulee salata. Esimerkiksi salaiseksi luokitellun tiedon lähettämisen ja tallentamisen kannattaa olla sallittua ainoastaan salattuna. Salattuja yhteyksiä kannattaa käyttää esimerkiksi seuraavissa käyttö-

tarkoituksissa: kaikki etäyhteydet, yritykselle kriittisen tiedon suojaaminen, järjestelmien ylläpitoon ja hallintaan käytetyt yhteydet, www-pohjaiset järjestelmät, jotka sisältävät käyttäjän tunnistautumisen tai joissa tehdään tilauksia ja tärkeä tiedonsiirto, joka tapahtuu ei-luotetussa verkossa. Lisäksi salausta kannattaa käyttää myös työasemien ja kannettavien tietokoneiden kiintolevyjen salaamisessa, tiettyjen sähköpostiviestien ja liitetiedostojen lähetyksessä ja tietojen varastoinnissa. [4, s. 195–196.] Esimerkiksi etäyhteydet tulee hoitaa VPN-yhteyttä käyttäen, jonka avulla yrityksen verkkoon päästään ulkopuolelta turvallisesti [5, s. 284].

Kiintolevyjen ja massamuistien salaamisella voidaan suojata yrityksen tiedot niin, että ulkopuoliset tahot eivät pääse niihin käsiksi esimerkiksi varkaustapausten yhteydessä. Jos kiintolevy on salaamaton, päästään tietoihin helposti käsiksi esimerkiksi kytkemällä kiintolevy toiseen tietokoneeseen. [4, s. 196.] Salaus voidaan toteuttaa TPM-, eli Trusted Platform Module, järjestelmää käyttämällä, jolloin salaus on luotettavampaa. TPM on emolevyllä sijaitseva piiri, joka tekee tietojen lukemisesta vaikeaa ilman käyttäjän tunnistautumista. Kiintolevyn salausavain tallennetaan piirille turvallisessa muodossa niin, että kiintolevyä on hyvin vaikea lukea myös tietokoneen ulkopuolella esimerkiksi toisella tietokoneella. Kiintolevyjen salaus korostaa myös varmuuskopioiden tärkeyttä, sillä tietokoneen rikkoutuessa tiedot saatetaan menettää esimerkiksi TPM:ää käytettäessä. [6, s. 843.]

Varmuuskopiointi on yksi yleisimpiä tietojen perussuojaustekniikoita. Varmuuskopiointilla pyritään varmistumaan siitä, että yrityksellä on olemassa ajan tasalla olevat varakopiot kaikista tärkeistä ohjelmistoista ja tiedoista. Tietojen vaurioituessa ja tuhoutuessa tiedot voidaan palauttaa varmuuskopioiden avulla. Varmuuskopiointi voi olla sekä automatisoitua että manuaalista käyttäjän itsensä tekemää. Varmuuskopiointi kannattaa kuitenkin toteuttaa automaattisesti, jolloin käyttäjän ei itse tarvitse siitä huolehtia. Varmuuskopiointi kannattaa tehdä riittävän usein, ja varmuuskopiot kannattaa säilyttää fyysisesti eri paikassa kuin varsinaiset tiedot, jotta onnettomuustilanteessa varmuuskopiot eivät tuhoutuisi. [3, s. 227.] Säilytystila kannattaa suojata hyvin tulipalo- ja vesivahingoilta [5, s. 146].

6.6 Muut tekniset ja käytännön suojaustoimenpiteet

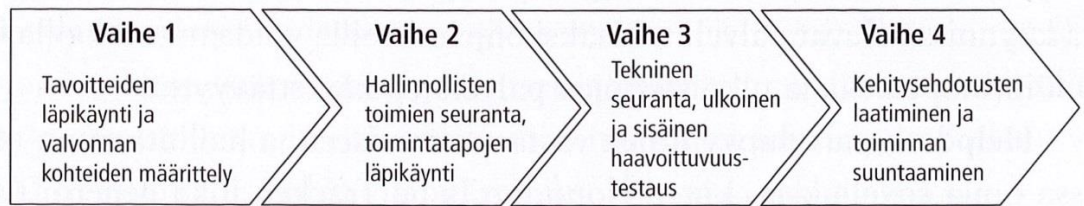
Maasta tai julkisista tiloista löydettyä USB-muistia ei tule kytkeä yrityksen järjestelmiin. Se saattaa sisältää haittaohjelman, joka tartuttaa tietokoneen, johon USB-muisti kytkeään. [2, s. 174.]

Yrityksen järjestelmissä tulee käyttää riittävän vahvoja salasanoja, ja ne tulee vaihtaa uusiin säännöllisin väliajoin. Vahvoja salasanoja käyttämällä ja salasanojen uusimisella voidaan suojautua esimerkiksi sanalista- ja brute force -hyökkäyksiä vastaan. [6, s. 194–195; 2, s. 179–180.]

Langattomat verkot tulee mielellään salata WPA2-, eli Wi-Fi Protected Access 2, salauksella käyttämällä. Vanhaa WEP-salauksella ei tule käyttää lainkaan, sillä se ei ole turvallinen. [6, s. 718–720, 722–723.] Jos esimerkiksi pienellä yrityksellä on käytössään langaton tukiasema, joka tukee WPS-, eli WiFi Protected Setup, suojausta, tulee WPS ottaa pois käytöstä, sillä langaton verkko voidaan yleensä helposti sen avulla murtaa [24].

7 Järjestelmien valvonta ja poikkeamiin reagointi

Tietoturvallisuutta tulee valvoa samalla tavoin kuin yrityksen muutakin toimintaa. Tietoturvan valvonnassa keskitytään saavutetun suojaustason seuraamiseen, jotta voidaan varmistua tietoturvan riittävydestä ja siitä, että toimintaa kehittyy oikeaan suuntaan. Valvonnalla ja mittaamisella voidaan kerätä tietoa mahdollisista puutteista ja heikkouksista, ja sillä voidaan pyrkiä löytämään kehityskohteita tietoturvassa. Valvonta koostuu yrityksen oman toiminnan valvomisesta ja ulkopuolisen toimintaympäristön tarkkailusta. Valvonnan tulee olla julkista, ja sen tulee ottaa huomioon myös lainsäädännön sille asettamat vaatimukset. Myös ulkoistettujen järjestelmien osalta lopullinen valvontavastuu on ulkoistajalla eikä palveluntarjoajalla. [4, s. 261, 263 ja 268.] Kuvassa 8 on havainnollistettu tietoturvallisuuden seurannan vaiheita.



Kuva 8. Tietoturvallisuuden seurantaan liittyvät vaiheet [4, s. 266].

Sisäisessä valvonnassa tulee tarkkailla ainakin seuraavia osa-alueita: pääsynvalvonta, verkkoliikenteen valvonta, käytön valvonta, muutoshallinta ja järjestelmäkehitys. Pääsynvalvonta sisältää sekä loogiset että fyysiset pääsykontrollit. Verkkoliikenteen valvonnassa tarkkaillaan tietoliikennehäiriöitä, virusten leviämistä, palvelunestohyökkäyksiä ja tunkeutumisyriä. Käytön valvonta puolestaan sisältää laiminlyöntien, varkauksien, tietovuotojen, kapasiteetin riittävyyden, laitteiden rikkoutumisen, ohjelmavirheiden ja tietoturva-aukkojen valvontaa. Muutoshallinnalla valvotaan järjestelmiin ja laitteisiin tehtäviä muutoksia, ja järjestelmäkehitys tarkkailee järjestelmien päivitysten ja uusien ominaisuuksien testausta ja käyttöönottoa. [4, s. 264.]

Ulkopuolisen toimintaympäristön valvonta koostuu tietoturvahäiriöiden ja tietoturvallisuuden vaikuttavien muutosten tarkkailusta. Muun muassa Viestintäviraston CERT-ryhmä pitää kirjaa tietoturva-vaivoista ja tiedottaa niistä. Myös virustorjuntaohjelmien ja palomuurivalmistajien verkkosivuilta löytyy ajankohtaista tietoa tietoturvahäiriöistä. [4, s. 265.]

Turvallisuustason mittaamisella pyritään siis löytämään kaikki nykyiset ja uudet tietoturva-aukot, saamaan vertailuaineistoa tilanteen kehittämiseksi, priorisoimaan hankintapäätöksiä, kohdistamaan korjaavat toimenpiteet oikein, kouluttamaan henkilökuntaa, vakuuttamaan sidosryhmät, lisäämään tuottavuutta ja ylläpitämään kilpailukykyä, vaikuttamaan yrityksen imagoon positiivisesti ja selvittämään, mitkä investoinnit ovat olleet kannattavia. [4, s. 269.]

Tietoturvallisuuden seuranta, valvonta ja mittaaminen ovat varsin tehottomia ilman asianmukaista raportointia ja korjaavia toimenpiteitä. Tietoturvallisuuden seuranta harjoitetaan yrityksen kaikilla tahoilla, ja havaintojen raportoimiseksi tulee olla omat kanavat. Raportoinnin osalta on hyvä määrittää menettelytavat, joita noudatetaan, mutta ne eivät saa olla liian raskaita, niin että havainnoinnille ei muodostu esteitä. [4, s. 281.]

Tietoturvahavaintoihin ja poikkeamiin vastaamisella pyritään poistamaan uhka yrityksen tietoteknisestä ympäristöstä, minimoimaan vahingot ja palauttamaan yrityksen normaali toiminta mahdollisimman nopeasti [10, s. 25]. Tietoturvaan liittyvät ongelmatilanteet ovat sellaisia, jotka rikkovat tiedon tai järjestelmän eheyttä, luotettavuutta tai saatavuutta [25, s. 91]. Oikeanlaisella reagoinnilla voidaan hyökkäystapauksesta säilyttää todistusaineistoa, joka auttaa tekijän jäljittämässä ja vahinkojen kartoituksessa [4, s. 185].

7.1 Järjestelmien valvonta

Järjestelmiä tulee auditoida säännöllisesti, eli esimerkiksi järjestelmien asetuksia tulee verrata vaatimusmäärittelyyn, asennusdokumentaatioon ja muihin dokumentoituihin muutoksiin. Auditointi voidaan suorittaa ja tietoturvan kannalta oleelliset tiedot kerätä ohjelmallisia työkaluja käyttäen, mutta se voidaan tehdä myös manuaalisesti, jos työasemien määrä on riittävän vähäinen. [4, s. 216.]

Järjestelmien seurannassa käydään läpi tunnettuja haavoittuvuuksia, joita järjestelmät sisältävät. Uusia haavoittuvuuksia löydetään jatkuvasti, joten yrityksen tulee valvontamekanismillaan pystyä päivittämään järjestelmät vastaamaan uusia tietoturvavaatimuksia. Järjestelmien seurannan tulee olla jatkuvaa, sillä yksittäinen tietoturva-auditointi kertoo tietoturvan tason vain kyseisellä ajanhetkellä. Haavoittuvuustestaus on myös yksi osa tietoturvallisuuden seuranta. [4, s. 266.]

Tietoverkon valvonta

Yritys saattaa esimerkiksi joutua tilanteeseen, jossa se epäilee, että tietoverkkoon on tunkeuduttu. Tällaisessa tilanteessa tulee reagoida siten, että mahdolliset tunkeutumisyritykset saadaan dokumentoitua ja tallennettua niin, että viranomaistutkinnassa ja siitä mahdollisesti seuraavassa oikeudenkäynnissä on riittävästi todistusmateriaalia. Jos yritykselle on selvää, että kyseessä on rikos, tulee viranomaisiin ottaa välittömästi yhteyttä. Yrityksellä itsellään ei ole oikeutta suorittaa riittäväntasoisia tutkintaa siitä, onko rikos tai väärinkäyttö tapahtunut tai mistä tietojärjestelmään on tunkeuduttu. [4, s. 185.]

7.2 Tietoturvapoikkeamiin vastaaminen ja reagointisuunnitelma

Se, mitä tietoturvapoikkeamilla tarkoitetaan, voi vaihdella sen mukaan, miten yritys on ne määritellyt. Yritys joutuu siis määrittelemään, mitä siihen kohdistuvat tietoturvapoikkeamat ovat. Niillä voidaan esimerkiksi tarkoittaa sellaisia teknisten laitteiden tietoturvaan liittyviä ihmisen toiminnasta aiheutuvia tapauksia, joilla pyritään aiheuttamaan vahinkoa. IR, eli Incident Response, on koordinoitu ja johdonmukainen tapa vastata tietoturvapoikkeamiin. Se kattaa joukon erilaisia toimenpiteitä, joilla pyritään löytämään ratkaisu havaittuun tietoturvapoikkeamaan. IR voi pitää sisällään esimerkiksi seuraavanlaisia toimenpiteitä: tietoturvapoikkeaman varmistaminen, tietoturvauhan eristäminen, tapauksen laajuuden arviointi ja dokumentointi, epäjohdonmukaisen reagoinnin ehkäisy, tapaukseen liittyvien varmojen tietojen ja tosiasioiden kerääminen, yritykseen tai sen toimintaan kohdistuvan vahingon tai häiriön minimointi, tavallisen toimintatason palauttaminen, yrityksen julkisen tiedottamisen hallinta ja saastuneen järjestelmän puhdistus ja uusilta hyökkäyksiltä puhdistaminen. IR-ryhmä koostuu yleensä tutkintaa tekevästä ryhmästä, korjaavia toimenpiteitä tekevästä ryhmästä ja julkista kuvaa hallitsevasta ryhmästä. Tutkintaa tekevä ryhmä tutkii, mitä on tapahtunut, ja kartoittaa vahinkoja. Korjaavia toimenpiteitä tekevä ryhmä estää hyökkääjän pääsyn järjestelmiin ja pyrkii suojaamaan järjestelmät. Julkista kuvaa hallitseva ryhmä puolestaan kommunikoi yrityksen johdon, työntekijöiden, yhteistyökumppaneiden tai julkisten tahojen kanssa. [10, s. 4–6.]

Valmistautuminen

Reagointisuunnitelman, liite 1, ensimmäinen vaihe on valmistautuminen. Valmistautumisessa on kyse resurssien organisoinnista oikeisiin tietoturvan kannalta oleellisiin kohteisiin ja toimintamallien päättämisestä. Yrityksellä tulee olla selkeät säännöt siitä, mitä valvotaan ja miten valvonta toteutetaan niin, että lain asettamat vaatimukset esimerkiksi yksityisyyden suhteen toteutuvat. [26, s. 17–20.] Lainsäädäntö asettaa vaatimuksia siis sen suhteen, miten todistusaineistoa voidaan hyökkäystilanteessa kerätä. Sellaisessa tapauksessa, jossa yrityksellä on syytä epäillä, että hyökkäyksessä on tapahtunut rikos, tulee viranomaisiin ottaa nopeasti yhteyttä. Poliisi tekee lopullisen ja riittäväntasoisin rikostutkinnan siitä, onko rikosta tapahtunut ja mistä tietojärjestelmään kohdistunut tunkeutuminen on tehty, eikä yrityksellä ole oikeutta tutkintaa tehdä. [4, s. 185]. Yritys voi kuitenkin valmistautumalla ja omalla reagoinnillaan pienentää hyökkäyksestä aiheutuvia haittoja ja kerätä tarpeellista todistusaineistoa [27; 4, s. 185].

Tunnistaminen

Reagointisuunnitelman toinen vaihe on tunnistaminen. Tämän vaiheen kannalta on oleellista, että yrityksen työntekijät on koulutettu havaitsemaan poikkeamia tai ongelmia ja ilmoittamaan ne tietoturvapoikkeamista vastaavalle taholle. IR-ryhmän tulee tämän jälkeen arvioida, onko kyseessä hyökkäys tai muu tietoturvaa rikkova tapahtuma ja kuinka laajasta tapahtumasta on kysymys. [26, s. 24.] Tutkinnassa voidaan käyttää hyödyksi lokitiedostoja, virheilmoituksia ja IDS-järjestelmistä ja palomuurista saatavaa tietoa. Kerätyt tiedot voivat myös olla hyvää todistusaineistoa mahdollista rikostutkintaa varten. [28, s. 5–6.] Pelkkien haittaohjelmien löytämiseen ei kannata keskittyä. Jos esimerkiksi hyökkääjä on päässyt sisälle verkkoon ja hänellä on hallussaan salasanoja, ei hän tarvitse haittaohjelmia päästäkseen käsiksi järjestelmiin, jotta hän kykenee varastamaan tietoa. [10, s. 33.] Yrityksen kannattaa myös dokumentoida, mitä toimenpiteitä tehdään ja kuka toimenpiteet suorittaa [28, s. 6]. Jos epäillään rikosta, tulee viranomaisiin ottaa yhteyttä [4, s. 185]. Tapahtuman laajuuden arviointi on tärkeää, jotta oikea määrä resursseja ja henkilökuntaa voidaan kohdistaa ongelman ratkaisemiseen. Yksinkertainen vakoiluohjelma saatetaan pystyä hoitamaan pelkän yhden työntekijän voimin, mutta erittäin suuren ongelman hoitamiseen saatetaan pahimmillaan tarvita yrityksen kaikki resurssit estämään, ettei ongelma tuhoa yrityksen toimintaa täysin. [26, s. 24.] Yrityksen tulee myös arvioida, kannattaako ongelman korjaaviin toimenpiteisiin ryhtyä nopeasti vai onko hyödyllisempää kerätä ongelmasta enemmän tietoa ja tehdä harkittuja päätöksiä ongelman korjaamiseksi [10, s. 32].

Eristäminen

Reagointisuunnitelman kolmas vaihe on eristäminen. Tässä vaiheessa kannattaa tehdä yhteistyötä yrityksen johdon kanssa, sillä IR-ryhmällä ja yrityksen johdolla saattaa olla eriävät näkemykset siitä, kuinka järjestelmien käyttöä kannattaa rajoittaa. On tärkeää samanaikaisesti sekä minimoida riskejä että pystyä ylläpitämään yrityksen toimintaa. On kuitenkin muistettava, että jos kyseessä on vakava tapaus, voidaan nopealla reagoinnilla lyhentää sitä aikaa, joka hyökkääjällä tai haittaohjelmalla on käytettävissä verkossa leviämiseen. Kannattaa myös arvioida, onko toimenpiteisiin ryhtyvällä henkilöllä riittävä ymmärrys ja osaaminen järjestelmän käytön suhteen. On mahdollista, että toimenpiteistä aiheutuu enemmän haittaa kuin hyötyä, jos esimerkiksi käyttöjärjestelmää tai reititintä konfiguroidaan ilman täyttä ymmärrystä siitä, mitä tehdyt muutokset saattavat järjestelmässä saada aikaan. [26, s. 27.]

Eristämisellä ei yleensä tarkoiteta järjestelmän sammuttamista, joka saattaa olla jopa haitallinen toimenpide esimerkiksi todistusaineiston keräämisen kannalta [26, s. 27]. Jos järjestelmä sammutetaan, sen muistista saattaa pyyhkiytyä haittaohjelman tai hyökkäyksen tutkinnan kannalta tärkeää tietoa [10, s. 137]. Eristämisen tarkoitus on mahdollistaa järjestelmän käyttö hyvään tarkoitukseen samalla, kun hyökkääjä tai haittaohjelma eristetään. Tätä tehdessä toimenpiteet kannattaa dokumentoida, mikä auttaa tekemään parempia päätöksiä. [26, s. 27–28.] Eristäviä toimenpiteitä voivat olla esimerkiksi järjestelmän paikkaaminen, eristäminen verkosta käyttämällä palomuureja tai VLAN:eja, verkkoliitännän kytkeminen pois päältä tai verkkokaapelin irrottaminen [26, s. 28; 28, s. 7].

Puhdistaminen

Reagointisuunnitelman neljäs vaihe on puhdistaminen. Kun on mahdollisesti saatu selville, mistä ja miten hyökkäys tai haittaohjelma on päässyt sisään, ja järjestelmät ovat hallinnassa ja voidaan olla riittävän varmoja siitä, että ongelma ei pääse enää leviämään, voidaan aloittaa järjestelmien varmuuskopiointi [26, s. 29, 31; 28, s. 7]. Varmuuskopioinnilla tarkoitetaan tässä yhteydessä todistusaineiston keräämistä, ja se tulee tehdä lain asettamien vaatimusten puitteissa [28, s. 7; 4, s. 185]. Jokaisen järjestelmän kohdalla tulee arvioida, mitä tietoa siitä kannattaa kerätä [10, s. 37]. Tartunnan saaneista järjestelmistä voidaan esimerkiksi ottaa todistusaineistoa keräävät imaget, eli järjestelmävedokset, siihen tarkoitetulla työkalulla. Tällaiset todistusaineistoa keräävät työkalut tallentavat koneen tilan silloin, kun ne ovat saastuneet. Näistä järjestelmävedoksista saatavaa tietoa voidaan hyödyntää myöhemmin rikostutkinnassa tai reagointisuunnitelman viimeisessä oppimisvaiheessa. [28, s. 7; 4, s. 185–186.] Kun todistusaineistoa on saatu kerättyä riittävästi, voidaan järjestelmät puhdistaa [28, s. 7]. Puhdistuksella tarkoitetaan kaikkien hyökkäyksestä tai haittaohjelmasta aiheutuneiden jälkien hävittämistä, ja se voi vaatia monia erilaisia toimenpiteitä. Yksinkertaisessa tapauksessa voi riittää, että järjestelmä puhdistetaan antivirusohjelmalla. Monimutkaisemmassa tapauksessa voidaan järjestelmä joutua palauttamaan varmuuskopioita käyttämällä. Pahassa tapauksessa, esimerkiksi jos rootkit-ohjelma on ottanut järjestelmän haltuunsa tai jos käyttöjärjestelmän eheyttä on rikottu, voidaan käyttöjärjestelmä joutua asentamaan kokonaan uudelleen luotettavaa asennusmediaa käyttäen, ennen kuin järjestelmään voidaan taas luottaa. Uudelleenasetaminen on helpompaa, jos yrityksellä on järjestelmästäan järjestelmävedosvarmuuskopio, jonka avulla järjestelmä voidaan suoraan asentaa aikaisempaan ja valmiiseen toimivaan tilaan. [26, s. 29–30.]

Puhdistamisen jälkeen järjestelmät tulee paikata, ettei hyökkäys onnistuisi tai haittaohjelma tarttuisi uudelleen. Jos päivitystä tai paikkaa ei ole saatavilla tai sitä joudutaan odottamaan, tulee mahdollisilta uusilta hyökkäyksiltä suojautua palomuuria tai IPS-järjestelmää käyttämällä. [26, s. 30.]

Palautuminen

Reagointisuunnitelman viides vaihe on palautuminen. Tämän vaiheen tarkoituksena on puhdistamisen jälkeen palauttaa järjestelmät tuotantoympäristöön. Järjestelmät tulee palauttaa tuotantoympäristöön niin, ettei alkuperäinen ongelma pääse uusiutumaan. Järjestelmät tulee testata ja varmentaa, ennen kuin ne otetaan uudelleen käyttöön, ja niitä tulee valvoa käyttöönoton jälkeen. Valvonnalla pyritään varmistumaan siitä, ettei tartuntaan tai hyökkäykseen viittaavia asioita ilmene uudelleen. [28, s. 8.]

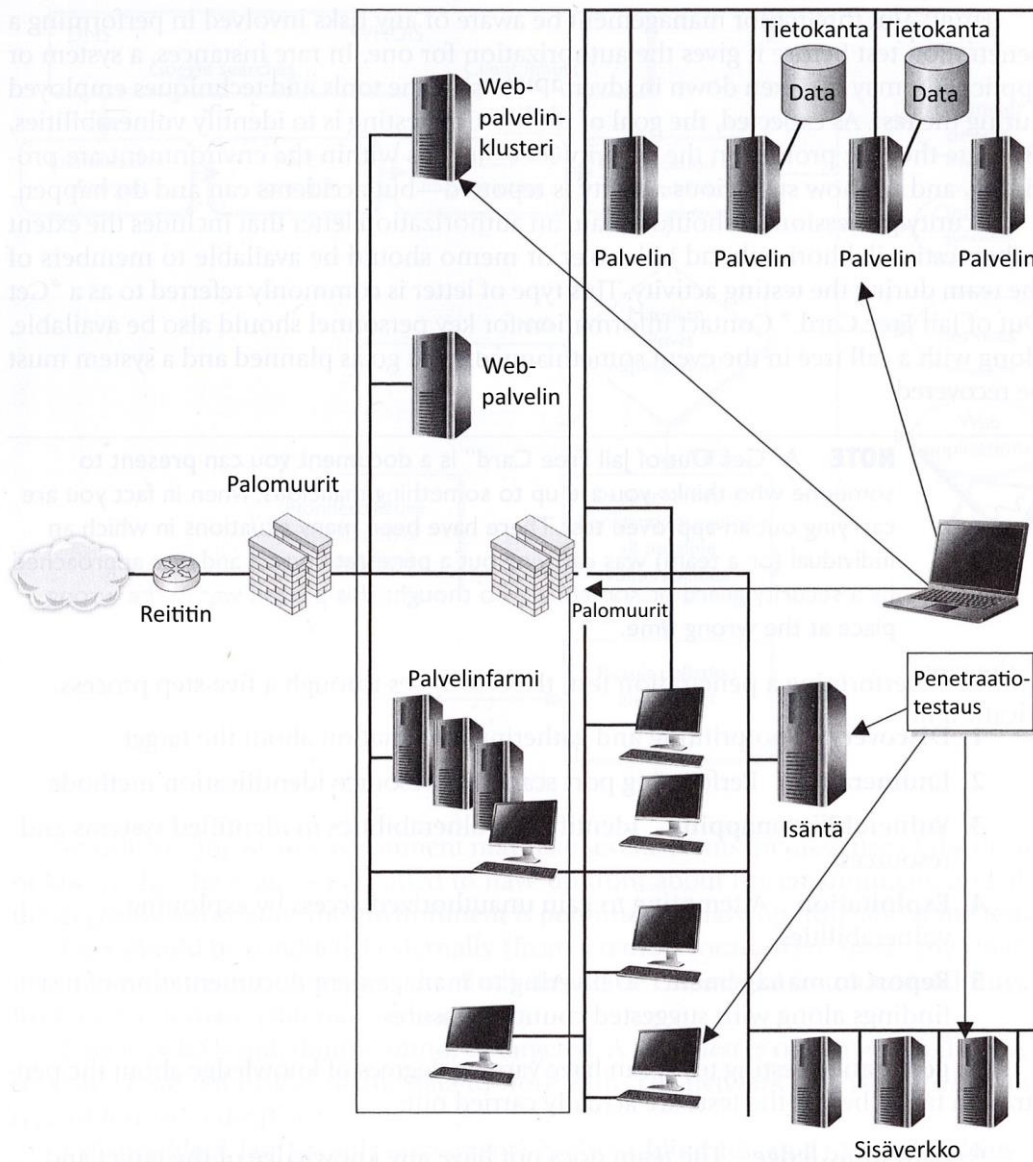
Oppiminen

Reagointisuunnitelman kuudes vaihe on oppiminen. Tämän vaiheen tarkoituksena on oppia tapahtuneesta, jotta vastaavanlaisia tapauksia varten voidaan varautua entistä paremmin tulevaisuudessa. Kaikki sellainen dokumentointi, joka on jäänyt puutteelliseksi, tulee viimeistellä. Tapauksen perusteella voidaan myös luoda dokumentaatiota, jonka avulla työntekijöitä voidaan kouluttaa tai josta voidaan muuten hyötyä vastaavanlaisen tilanteen tullen myös tulevaisuudessa. Tapauksesta tehty yhteenveto voi sisältää esimerkiksi seuraavat asiat: milloin ongelma havaittiin ensimmäisen kerran ja kuka sen havaitsi, ongelman laajuus, miten ongelma eristettiin ja hävitettiin, järjestelmien palauttamisessa tehdyt toimenpiteet, osa-alueet, joissa ongelmaa käsitellyt taho oli tehokas, ja osa-alueet, joita tulee kehittää. [28, s. 9.]

8 Penetraatiotestaus

Penetraatiotestaus on yrityksen tietojärjestelmien murtotestausta, ja sen avulla on tarkoitus varmistua järjestelmien turvallisuudesta [4, s. 279]. Penetraatiotestauksessa yritetään tarkoituksella murtautua järjestelmiin käyttäen samoja keinoja, joita myös rikolliset voivat käyttää [6, s. 194]. Penetraatiotestauksen tarkoituksena on varmistaa, että kyberturvallisuuden prosessit toimivat ja tuottavat laadukasta lopputuotetta eli turvallisia järjestelmiä [4, s. 279]. Tietoturvuutteita yritetään löytää ja korjata, ennen

kuin niitä mahdollisesti hyväksikäytetään haitalliseen tarkoitukseen [6, s. 194]. Kuvassa 9 on havainnollistettu, kuinka penetraatiotestausta voidaan soveltaa yrityksen eri järjestelmiin.



Kuva 9. Penetraatiotestaus [6, s. 1299].

Insinööriyössä suoritettu penetraatiotestaus tehtiin kahteen yritykseen julkisen Internet-yhteyden välityksellä, ja testauksessa keskityttiin erityisesti testaamaan yritysten palomureja ulkoverkosta tulevia uhkia vastaan. Palomureja tutkittiin muun muassa erilaisilla porttiskannauksilla.

8.1 Sopimusten laatiminen ja esityö

Ennen testausta on tärkeää laatia sopimukset yritysten kanssa. Testauksesta tehdään tällä tavalla laillinen toimeksianto, ja testaajalle annetaan kirjallinen lupa järjestelmien testausta varten. Jotkin testauksessa käytetyistä menetelmistä ovat ilman lupaa suoritettuina laittomia, minkä takia on erittäin tärkeää, että kirjallinen lupa on toimintaa varten tehty. Sopimuksista tulee käydä ilmi testausajankohta ja se, mitä testauksessa tul- laan tekemään. Tarpeellista on myös määritellä vahinkojen korvausvastuu mahdollisten vahinkojen varalle.

Insinööriytyö aloitettiin vierailemalla murtotestausprojektissa mukana olevissa yrityksis- sä. Tapaamisten aikana haastateltiin yritysten henkilökuntaa ja kyseltiin yritysten käy- tössä olevia järjestelmiä ja käytäntöjä. Kyselemällä kerättiin tietoa testausta varten se- kä kartoitettiin yritysten senhetkistä tietoturvaa. Keskusteluissa esiin tulleet asiat kirjat- tiin muistiin. Testaus myös esiteltiin yrityksille niin, että yrityksillä oli tapaamisen jälkeen yleisluonteinen kuva siitä, mitä testauksessa tehdään ja mitä sillä pyritään saavutta- maan. Tapaamisten yhteydessä yrityksille annettiin myös testausta varten allekirjoitet- tavaksi sopimukset, jotka yritykset toimittivat allekirjoitettuina takaisin.

Vierailuilla kierrettiin myös yritysten fyysiset työ- ja tuotantotilat. Kierrosten aikana kiin- nitettiin erityistä huomiota turvallisuuteen liittyviin asioihin, joita ovat esimerkiksi esillä olevat laput, joihin on kirjoitettu salasanoja. Havainnoista otettiin myös valokuvia, ellei valokuvien ottamista ollut tietyistä kohteista kielletty.

8.2 Testauksessa käytetyt työkalut

Testaus tehtiin Kali Linuxin versiolla 1.0.9. Kali on penetraatiotestaukseen ja tietoturva- auditointiin erikoistunut Linux-jakelu, jossa erilaisia testaukseen liittyviä työkaluja on valmiiksi asennettuina [29]. Testauksessa käytetyistä työkaluista tärkein oli Nmap, josta oli käytössä versio 6.47. Nmap on yleinen verkkoskannaustyökalu [30, s. 34]. Verkkos- kannaus on prosessi, jolla verkosta etsitään aktiivisia laitteita ja niihin liittyvää tietoa [30, s. 2]. Nmap kertoo avoimien porttien lisäksi tietokantansa perusteella myös sen, mihin avoimeksi todettua porttia yleensä käytetään [30, s. 101]. Löydettyjen avoimien porttien takana olevista palveluista voidaan saada lisää tietoa versioita tunnistavalla

skannauksella, ja Nmap pystyy tunnistamaan myös käyttöjärjestelmien versioita [30, s. 110–112]. Liitteessä 2 on esitetty Nmapin yleisten optioiden ja parametrien käyttö.

8.3 Testaus ja sen vaiheet

Yritystapaamisissa tiedusteltiin käytössä olevia järjestelmiä ja ohjelmia. Yrityksiltä saatiin myös julkiset IP-osoitteet, joiden avulla skannaus voitiin tehdä oikeaan kohteeseen. Tiedustelu pyrittiin tekemään monipuolisesti niin, että yritysten toiminnasta saatiin mahdollisimman selkeä kuva myöhempää raportointia varten.

Ongelmakohtien etsintä ulkoverkosta päin

Ennen testausta otettiin yhteys verkko-operaattoriin, jonka verkosta testaus aiottiin tehdä. Verkko-operaattorille ilmoitettiin muun muassa tehtävästä porttiskannauksesta. Yhteydenotossa kerrottiin, mistä on kyse, ja myös mainittiin, että skannaukseen on lupa. Yhteydenotto tehtiin ensin puhelimitse, minkä jälkeen myös kirjallinen ilmoitus lähetettiin sähköpostitse osoitteeseen abuse@sonera.fi, joka on tarkoitettu muun muassa tietoturvaloukkausilmoituksia varten. Kun operaattoria oli informoitu, suoritettiin yritysten julkisille IP-osoitteille porttiskannaukset.

Porttiskannaukset suoritettiin Nmapilla. Testauksesta ylläpidettiin dokumentaatiota, ja kaikki toimenpiteet sekä niiden suoritusajat kirjattiin. Löydettyjä avoimia portteja tutkittiin myös palveluntunnistuksella, joka pyrkii tarkemmin päättelemään, mikä palvelu tai ohjelma avoimen portin takana on.

Porttiskannaus tehtiin sekä Nmapin oletusskannauksella, joka skannaa portit 1–1024 ja ”services”-tiedostossa määritellyt portit, että skannaamalla koko porttialue 1–65535.

Tietoturvan parannusehdotusten ja testaustulosten raportointi

Yrityksille kirjoitettiin raportit, joissa annettiin parannusehdotuksia tietoturvan kannalta ja esiteltiin penetraatiotestauksen tulokset. Testaustulokset koottiin raporttiin testauksessa tehdyn dokumentaation pohjalta. Salassapidettävät raportit ovat liitteinä 3 ja 4. Niitä ei yritysten pyynnöstä voida julkisessa insinööriyössä esittää.

9 Yhteenveto

Insinööriyöni tarkoituksena oli selvittää pienten ja keskisuurten yritysten kyberturvallisuutta monipuolisesti ja suorittaa insinööriyön tilaamille yrityksille penetraatiotestaus. Onnistuin mielestäni erittäin kattavasti kokoamaan pk-yritysten näkökulmasta oleellista kyberturvallisuuteen liittyvää tietoa ja sen perusteella antamaan yrityksille ehdotuksia tietoturvallisuuden parantamiseksi. Penetraatiotestauksella onnistuttiin myös selvittämään, miten yritysten palomuurit reagoivat ulkoverkosta tuleviin uhkiin ja miten niiden turvallisuutta voitaisiin parantaa.

Insinööriyölle asetetut tavoitteet saavutettiin onnistuneesti, ja yritykset saivat tietoturvallisuuden liittyviä parannusehdotuksia. Yritykset näkivät testaustulosten perusteella myös, miten niiden käytössä olevat palomuurit näkyvät ulkomaailmalle ja miten ne reagoivat testaukseen.

Aiheeseen tutustuessani huomasin, että kyberturvallisuuden liittyvät uhat ja erityisesti rikollisuus on kehittynyt viime vuosina huomattavasti. Yllätyin, että kotimaisten lähteiden osalta lähdeaineistoa joutui etsimään osittain jopa varsin vanhoista teoksista. Joitakin pk-yritysten tietoturvallisuuden liittyviä osa-alueita oli vanhoissa suomalaisissa teoksissa esitelty uudempia yksityiskohtaisemmin. Kyberturvallisuuden liittyvät tekniset yksityiskohdat muuttuvat tekniikan kehittyessä nopeasti, ja esimerkiksi järjestelmien suojaamiseen liittyvää ajankohtaista lähdeaineistoa joutui teosten lisäksi etsimään myös Internetistä.

Insinööriyön aihe oli hyvin laaja, mutta mielestäni onnistuin rajaamaan sen tiiviiksi ja selkeäksi kokonaisuudeksi. En halunnut pienentää aihealuetta liikaa, sillä pyrkimykseni oli kuvata kyberturvallisuuden kokonaisuutta mahdollisimman kattavasti ja monipuolisesti. Halusin, että insinööriyö hyödyttäisi projektissa mukana olleiden yritysten lisäksi myös mahdollisimman montaa muuta yritystä. Insinööriyö selvittää lukijalle myös peruskäsitteitä, ja se on kirjoitettu niin, että sitä voivat lukea kaikki kyberturvallisuudesta kiinnostuneet.

Kyberturvallisuuden perehtymätöntä lukijaa saattaa yllättää, että kyberturvallisuus ei ole pelkästään haittaohjelmilta suojautumista ja suojautuminen vaatii monia muitakin suojaustoimenpiteitä. Hyökkääjällä on etulyöntiasema puolustautuvaan tahoon nähden,

sillä hyökkääjän täytyy löytää vain yksi aukko suojauksessa, kun puolustajan tulee puolestaan yrittää pitää kaikki järjestelmänsä aukottomina.

Kyberturvallisuus ja siihen liittyvä tietoturva ovat nykyään, ja ovat myös lähimenneisyydessä olleet, yrityksille erittäin tärkeitä asioita, sillä ne mahdollistavat yritysten liiketoiminnan nykyisessä tietojärjestelmien verkostoimassa yhteiskunnassa. Uskon, että kyberturvallisuuden merkitys kasvaa jatkuvasti myös tulevaisuudessa, kun tietoverkkoon liitettävien laitteiden määrä lisääntyy entisestään.

Lähteet

- 1 Limnell, Jarno; Majewski, Klaus; Salminen, Mirva. 2014. Kyberturvallisuus. Jyväskylä: Docendo.
- 2 Rousku, Kimmo. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Talentum Media.
- 3 Miettinen, Juha E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari.
- 4 Laaksonen, Mika; Nevasalo, Terho; Tomula, Karri. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Edita Publishing.
- 5 Hakala, Mika; Vainio, Mika; Vuorinen, Olli. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.
- 6 Harris, Shon. 2013. CISSP all-in-one exam guide. McGraw-Hill Education.
- 7 Vahti 2007. 2009. Verkkodokumentti. Valtionvarainministeriö. <<https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus>>. Päivitetty 10.9.2009. Luettu 29.11.2015.
- 8 Olzak, Tom. 2012. Physical Security: Managing the Intruder. Verkkodokumentti. InfoSec Institute. <<http://resources.infosecinstitute.com/physical-security-managing-intruder/>>. 18.12.2012. Luettu 29.11.2015.
- 9 Peltomäki, Juha; Norppa Kati. 2015. Rikos meni verkkoon. Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum Media.
- 10 Luttgens, Jason T.; Pepe, Matthew; Mandia, Kevin. 2014. Incident Response & Computer Forensics. Third Edition. McGraw-Hill Education.
- 11 Physical Security Threats and Controls. 2008. Verkkodokumentti. BestInternet-Security. <<http://www.bestinternetsecurity.net/28/physical-security-threats-and-controls.html>>. 17.3.2008. Luettu 12.1.2016.
- 12 Rouse, Margaret. 2013. Distributed denial-of-service attack (DDoS). Verkkodokumentti. TechTarget. <<http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack>>. May 2013. Luettu 12.3.2016.
- 13 Threat Report 2015. 2016. Verkkodokumentti. F-Secure. <https://www.f-secure.com/fi_FI/web/press_fi/news/news-archive/-/journal_content/56/1082194/1551411?p_p_auth=Wi3o5eID&refererPlid=1090668>. 2016. Luettu 10.3.2016.

- 14 Guil, Felicitas. 2003. Computer Rooms – Meet the physical security measures. Verkkodokumentti. SANS Institute. <<https://www.giac.org/paper/gsec/2892/computer-rooms-meet-physical-security-measures/104866>>. April 2003. Luettu 11.1.2016.
- 15 Tietosuojavaltuutetun päätös. 2006. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <<http://www.tietosuoja.fi/fi/index/ratkaisut/henkilotietojenkeramineninternetistahak.html>>. 27.1.2014. Luettu 1.3.2016.
- 16 Stoddard, Donald; Thomas, Thomas M. 2012 Network Security First-Step: Firewalls. Verkkodokumentti. Cisco. <<http://www.ciscopress.com/articles/article.asp?p=1823359&seqNum=5>>. 8 February 2012. Luettu 3.3.2016.
- 17 Dubrawsky, Ido. 2010. Firewall Evolution - Deep Packet Inspection. Verkkodokumentti. Symantec. <<http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection>>. Updated 2 November 2010. Luettu 3.3.2016.
- 18 Rouse, Margaret. 2014. Unified threat management (UTM). Verkkodokumentti. TechTarget. <<http://searchmidmarketsecurity.techtarget.com/definition/unified-threat-management>>. June 2014. Luettu 10.3.2016.
- 19 3 Ways to keep hackers out of your smart home. 2015. Verkkodokumentti. F-Secure. <<https://iot.f-secure.com/2015/08/18/3-ways-to-keep-hackers-out-of-your-smart-home/>>. 18 August 2015. Luettu 10.3.2016.
- 20 Tsang, Derek. 2015. Best Practices for Mitigating DMA Attacks. Verkkodokumentti. WinMagic. <<http://www.winmagic.com/blog/2015/09/01/best-practices-for-mitigating-dma-attacks/>>. 1 September. 2015. Luettu 13.3.2016.
- 21 Goodin, Dan. 2015. Meet KeySweeper, the \$10 USB charger that steals MS keyboard strokes. Verkkodokumentti. Ars Technica. <<http://arstechnica.com/security/2015/01/meet-keysweeper-the-10-usb-charger-that-steals-ms-keyboard-strokes/>>. 13 January 2015. Luettu 13.3.2016.
- 22 Hoffman, Chris. 2014. Quickly Secure Your Computer With Microsoft's Enhanced Mitigation Experience Toolkit (EMET). Verkkodokumentti. How-To Geek. <<http://www.howtogeek.com/190590/quickly-secure-your-computer-with-microsofts-enhanced-mitigation-experience-toolkit-emet/>>. 6 June 2014. Luettu 22.3.2016.
- 23 Enhanced Mitigation Experience Toolkit. Verkkodokumentti. Microsoft. <<https://technet.microsoft.com/en-us/security/jj653751>>. Luettu 22.3.2016
- 24 Hoffman, Chris. 2013. Wi-Fi Protected Setup (WPS) is Insecure: Here's Why You Should Disable It. Verkkodokumentti. How-To Geek.

- <http://www.howtogeek.com/176124/wi-fi-protected-setup-wps-is-insecure-heres-why-you-should-disable-it/>. 24 November 2013. Luettu 14.3.2016.
- 25 Defranco Joanna F. 2014. What Every Engineer Should Know About Cyber Security and Digital Forensics. Taylor & Francis Group.
- 26 Pokladnik, Mason. 2007. An Incident Handling Process for Small and Medium Businesses. Verkkodokumentti. SANS Institute. <<https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791>>. 2007. Luettu 8.3.2016.
- 27 Rouse, Margaret. 2014. Incident response plan (IRP). Verkkodokumentti. Tech-Target. <<http://searchsecurity.techtarget.com/definition/incident-response-plan-IRP>>. February 2014. Luettu 8.3.2016.
- 28 Kral, Patrick. 2012. Incident Handler's Handbook. Verkkodokumentti. SANS Institute. <<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>>. 2012. Luettu 9.3.2016.
- 29 What is Kali Linux ? Verkkodokumentti. Offensive Security. <<http://docs.kali.org/introduction/what-is-kali-linux>>. Luettu 14.3.2016.
- 30 Orebaugh, Angela; Pinkard, Becky. 2008. Nmap. In the Enterprise. Your Guide to Network Scanning. Elsevier.

Reagointisuunnitelma

1. Valmistautuminen: Työntekijät koulutetaan reagoimaan tietoturvaan liittyviin poikkeamiin nopeasti ja oikein, jos niitä ilmenee [27, s. 2; 26, s. 17–18].
2. Tunnistaminen: Tutkitaan, onko havaitussa tapahtumassa kyse oikeasta tietoturvapoikkeamasta tai hyökkäyksestä ja kuinka suuresta ongelmasta on kyse [27, s. 5–6; 26, s. 24].
3. Eristäminen: Minimoidaan hyökkäyksestä aiheutuvat vahingot ja eristetään uhka niistä järjestelmistä, joita hyökkäys koskettaa, ettei lisää vahinkoja pääse syntymään [27, s. 6–7; 26, s. 27–28].
4. Puhdistaminen: Tutkitaan, miten hyökkäys on syntynyt ja poistetaan saastuneet järjestelmät tuotantoympäristöstä. Tämän jälkeen järjestelmät puhdistetaan. [27, s. 7–8; 26, s. 29–30.]
5. Palautuminen: Puhdistetaan saastuneet järjestelmät ja varmistetaan, että niistä ei aiheudu uhkaa, kun ne kytketään uudelleen tuotantoympäristöön [27, s. 8; 26, s. 32].
6. Oppiminen: Tapaus dokumentoidaan ja analysoidaan niin, että siitä voidaan oppia ja sen avulla voidaan mahdollisesti parantaa reagointia tuleviin tietoturvaan liittyviin poikkeuksiin [27, s. 9; 26, s. 32–34].

Nmapin yleiset optiot

```
# nmap
Nmap 4.50 (http://insecure.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -PN: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO [protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
  --traceroute: Trace hop path to each host
  --reason: Display the reason a port is in a particular state
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=safe,intrusive
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
    directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
```

--script-trace: Show all data sent and received

--script-updatedb: Update the script database.

OS DETECTION:

-O: Enable OS detection

--osscan-limit: Limit OS detection to promising targets

--osscan-guess: Guess OS more aggressively

TIMING AND PERFORMANCE:

Options which take <time> are in milliseconds, unless you append 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).

-T[0-5]: Set timing template (higher is faster)

--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes

--min-parallelism/max-parallelism <time>: Probe parallelization

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies probe round trip time.

--max-retries <tries>: Caps number of port scan probe retransmissions.

--host-timeout <time>: Give up on target after this long

--scan-delay/--max-scan-delay <time>: Adjust delay between probes

FIREWALL/IDS EVASION AND SPOOFING:

-f; --mtu <val>: fragment packets (optionally w/given MTU)

-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys

-S <IP_Address>: Spoof source address

-e <iface>: Use specified interface

-g/--source-port <portnum>: Use given port number

--data-length <num>: Append random data to sent packets

--ip-options <options>: Send packets with specified ip options

--ttl <val>: Set IP time-to-live field

--spooof-mac <mac address/prefix/vendor name>: Spoof your MAC address

--badsum: Send packets with a bogus TCP/UDP checksum

OUTPUT:

-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename.

-oA <basename>: Output in the three major formats at once

-v: Increase verbosity level (use twice for more effect)

-d[level]: Set or increase debugging level (Up to 9 is meaningful)

--open: Only show open (or possibly open) ports

--packet-trace: Show all packets sent and received

--iflist: Print host interfaces and routes (for debugging)

--log-errors: Log errors/warnings to the normal-format output file

--append-output: Append to rather than clobber specified output files

--resume <filename>: Resume an aborted scan

--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML

--webxml: Reference stylesheet from Insecure.Org for more portable XML

--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:

-6: Enable IPv6 scanning

-A: Enables OS detection and Version detection, Script scanning and Traceroute

```
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
```

EXAMPLES:

```
nmap -v -A scanme.nmap.org
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -PN -p 80
```

SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES [30, s. 88–92].

Yritys X:n tietoturvaraportti ja testaustulokset (salainen)

Yritys Y:n tietoturvaraportti ja testaustulokset (salainen)