VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Aleksi Karjalainen

YRITYKSEN TIETOTURVA

Liiketalous
2022

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Aleksi Karjalainen
Opinnäytetyön nimi	Yrityksen tietoturva
Vuosi	2022
Kieli	suomi
Sivumäärä	33
Ohjaaja	Antti Mäkitalo

Opinnäytetyössä tutkitaan tietoturvaa ja tietoturvauhkia nykypäivänä. Työn tarkoituksena on kertoa yrityksen tietoturvasta. Työssä käydään läpi tietoturvaa kokonaisuutena.

Opinnäytetyössä tutkitaan tietoturvan perusteita, osa-alueita, tietoturvan lainsäädäntöä, haittaohjelmia, hyökkäyksiä sekä yleisesti tietoturvan toteuttamista ja riskejä.

Opinnäytetyö pohjautuu paljolti teoriaan. Työssä kerrotaan tietoturvasta etenkin yrityksen näkökulmasta ja miten se on muuttunut lähivuosina. Tutkitaan myös yleisiä tietoturvauhkia yritykselle sekä yksityishenkilöille. Lopussa käydään läpi tietoturvan toteutusta ja riskejä.

Avainsanat tietoturva, tietoturvauhat, riskit, lainsäädäntö

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittely

ABSTRACT

Author	Aleksi Karjalainen
Title	Information Security of an Enterprise
Year	2022
Language	Finnish
Pages	33
Name of Supervisor	Antti Mäkitalo

The thesis examined information security and information security threats today. The objective of this was to study and describe about the information security of enterprises. The thesis covers information security as a whole.

The thesis examines the basics and aspects of information security, information security legislation, malware, attacks, and the technical implementation as well as risks of information security in general.

The thesis is largely based on theory. It examined information security, especially from the company's point of view, and how it has changed in the past decade. It also examines common security threats to businesses and individuals. At the end, the implementation and risks of data security are reviewed.

Keywords information security, security threat, risks, legislations

SISÄLLYS

KUVA- JA TAULUKKOLUETTELO

Kuvaotsikkoluettelon hakusanoja ei löytynyt.

1 JOHDANTO

Tietoturva on nykypäivänä yksi tärkeimmistä osista yrityksen toimintaa. Siitä huolehtiminen on etenkin yrityksille elintärkeää. Kaikki tulisi aina suunnitella pitäen tietoturva mielessä. Yritykselle tietoturvariskit voivat suurempia kuin yksityishenkilöille, ja ne voivat olla sisäisiä sekä ulkoisia. Yrityksen tietoturva suojaa myös asiakkaita ja heidän mahdollisesti arkaluontoisia tietojaan.

Opinnäytetyön aihe valittiin oman kiinnostuksen sekä lisäopin saamiksesi. Opinnäytetyöllä ei ole toimeksiantajaa. Työn kohderyhmänä on yritykset sekä osittain yksityishenkilöt. Työ on tutkimuksellinen perustuen kirjallisuus ja verkkolähteisiin.

Opinnäytetyön tarkoituksena on tutkia tietoturvaa, sen perusteita, osa-alueita, tietoturvan lainsäädäntöä sekä yleisiä tietoturvauhkia, haittaohjelmia, hyökkäyksiä ja riskejä. Lopuksi kerrotaan tietoturvan toteutuksesta sekä siihen kuuluvista toimista.

Työn tavoitteena on esitellä yrityksen tietoturvaa ja mitä siihen kuuluu. Työssä kerrotaan tietoturvasta kokonaisuutena sekä miten sitä voitaisiin toteuttaa yrityksessä.

2 TIETOTURVAN PERUSTEET

Tietoturvalla tarkoitetaan yleisesti teknisiä ja hallinnollisia tapahtumia, joilla pyritään suojaaman tiedon, palveluiden, tietojärjestelmien ja tietoliikenteen luottamuksellisuus, eheys ja saatavuus. Näistä puhuttaessa voidaan käyttää klassista CIA-mallia Confidentiality (luottamuksellisuus), Integrity (eheys) ja Availability (käytettävyys). Nykyisin tosin klassinen määrittely nähdään puutteellisena, koska siinä ei huomioida tiedon tuottajaa tai omistajan identiteettiä. Klassisen määritelmän rinnalle tämän myötä on luotu uusi laajennettu määritelmä, joka sisältää viisi osaa: Luottamuksellisuus, käytettävyys, eheys, kiistämättömyys ja pääsynvalvonta. (Hakala, Vainio, Vuorinen. 2006, 4-5.)

Tietoturvallisuus on osa jokapäiväisiä toimia yrityksessä. Se koostuu pienistä teoista ja toimista. Hyvä tietoturvallisuus on osa yrityksen kulttuuria, jolloin kaikki ymmärtävät ja huolehtivat tietoturvallisesta toiminnasta. Tietoturvallisuutta tulee toteuttaa lainsäädännön vaatimuksia ja rajoituksia huomioiden sekä vaatii yritykseltä määrätietoista otetta ja johtamista, jotta koko yrityksen henkilöstö takaa hyvän tietoturvallisuustason saavuttamisen ja ylläpidon. (Laaksonen, Nevasalo, Tomula. 2006, 17-18.)

2.1 Luottamuksellisuus, käytettävyys & eheys

Luottamuksellisuudella (confidentiality) tarkoitetaan, että tietojen ja erilaisten järjestelmien käyttö on sallittua vain niille, jotka ovat siihen oikeutettuja. Luottamuksellisuus pysyy, kun tiedot pidetään salassa heiltä, joille ne eivät kuulu. Luottamuksellisuuteen kuuluu siis kaikki eri käyttäjät, salasanat sekä fyysinen turvallisuus. (Hakala ym. 2006, 4.)

Käytettävyys (availability) takaa, että tietojärjestelmissä olevat tiedot ovat oikeassa muodossa ja mahdollisimman nopeasti saatavilla. Tämän lisäksi huolehditaan, että tieto- ja tietoliikennejärjestelmä laitteet ovat tehokkaita ja ohjelmistot soveltuvat järjestelmien tietojen käsittelyyn. Käytettävyydellä taataan

myös, että käyttäjä saa tiedot järjestelmästä itselleen sopivassa muodossa. (Hakala ym. 2006, 4-5.)

Eheys (integrity) tarkoittaa, että tiedot eivät saa muuttua, ellei niitä muuteta tarkoituksella henkilön toimesta, jolla on oikeus niitä muuttaa. Eheydellä taataan, että tiedot ovat tosia eivätkä sisällä virheitä. Tietojen ja järjestelmien tulee olla luotettavia, ajanmukaisia ja oikeita. Ne ei eivät saa muuttua mahdollisten haavoittuvuuksien takia. (Hakala ym. 2006, 4-5.)

2.2 Kiistämättömyys

Kiistämättömyydellä (non-repudiation) tarkoitetaan tietojärjestelmien kykyä tunnistaa ja tallentaa luotettavat käyttäjät ja heidän tietonsa. Kiistämättömyyteen pyritään, koska halutaan varmistaa tiedon alkuperä tai tietojen luvaton käyttö, jos harkitaan oikeudellisia toimenpiteitä käyttäjää vastaan. Kiistämättömyyteen pyritään käyttämällä mm. salausmenetelmiä ja tunnistusmekanismejä. (Hakala ym. 2006, 5.)

2.3 Pääsynvalvonta

Pääsynvalvonta (access control) tarkoittaa menetelmiä, joilla rajoitetaan yrityksen tietojenkäsittely laitteiston käyttöä. Pääsynvalvonta ei siis estä itse tietoihin pääsyä vaan se kuuluu luottamuksellisuuteen. Pääsynvalvonnan haavoittuvuuksilla on yhteys yrityksen tietoturvallisuuden osatekijöihin. Langattomien verkkojen yleistyttyä tulee huomioida pääsynvalvontaan kohdistuvat lisääntyneet uhat, sillä ulkopuoliset henkilöt saattavat yrittää murtautua niihin niiden helppouden ansiosta. (Hakala ym. 2006, 5-6.)

3 TIETOTURVAAN LIITTYVÄ LAINSÄÄDÄNTÖ

Lainsäädäntö asettaa yleisluontoisia velvoitteita yritykselle tietoturvallisuuden huolehtimiseksi, mutta yrityksen on tärkeää huomioida yksittäiset säädökset, jotka ohjaavat käytännön toteutusta. Lainsäädännön tarkoituksena on turvata tietoturvallinen yhteiskunta. Suomen laissa ei ole erillislakia, joka velvoittaisi pakolliseen tietoturvaan, mutta erillisiä lakeja ja säännöksiä on säädetty, jotta tietoturvallisuus ja yksityisyyden suojaaminen turvataan. Tässä työssä havainnollistetaan tietoturvan kannalta tärkeimmät lainsäädännölliset perusperiaatteet, joilla turvataan päivittäinen tietoturva työskentely. (Laaksonen ym. 2006, 18,21-22.)

Tietoturvan lainsäädäntö asettaa selkeät rajat tietoturvatoimenpiteille, jotka liittyvät tunnistamiseen tai viestien sisällön käsittelyyn. Lakien asettamien tietoturvavelvotteiden ja säännösten noudattaminen vaatii hyvää perehtymistä lainsäädäntöön. Yrityksen tietoturva on yleisesti hyvin hoidettu, jos yrityksessä noudatetaan lainsäädäntöä ja noudatetaan samoja käytäntöjä kuin muissa samanlaisissa hyvin johdetuissa ja asiaan perehtyneissä yrityksissä. (Laaksonen ym. 2006, 80-82.)

3.1 Kansallinen lainsäädäntö

Tietoturvallisuuteen liittyviä velvoitteita on sisällytetty useisiin lakeihin. Tämä kuitenkin tuo haasteita tietoturvatyön toteutumiselle. Tässä osiossa käymme lyhyesti läpi niitä.

3.1.1 Perustuslaki

Perustuslaki toimii Suomessa kaikkien lakien pohjana. Sillä pyritään turvaamaan kansalaisten perusoikeuksien toteutuminen, joihin kuuluu vahvasti yksityisyyden suojan turvaaminen. Perustuslain 10 § määrittelee yksityisyyden suojan seuraavasti: ”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun

luottamuksellisen viestin salaisuus on loukkaamaton.”(Suomen perustuslaki 1999/731 § 10). Käytännön työskentelyssä yksityisyyden suojan turvaaminen vaatii yritykseltä moninaisia toimia.

3.1.2 Laki viranomaisen toiminnan julkisuudesta (Julkisuuslaki)

Toiselta nimeltään julkisuuslaki, jota sovelletaan pääsääntöisesti viranomaisten toimintaan, tosin julkisuuslakia voidaan myös soveltaa yksityisellä sektorilla kuten yrityksissä. Julkisuuslaki käsittelee viranomaisten tietoaineistojen salausta, julkisuutta ja julkaisua. Julkisuusasetuksen mukaan tiedot tulee luokitella eri luokkiin viranomaisten omasta toimesta. Yritykset voivat käyttää samaa luokittelu menetelmää. Tiedot luokitellaan sen mukaan kuinka vaativia niiden käsittelyn ja suojauksen tietoturvavaatimukset ovat. Luokkajako tapahtuu kolmeen eri luokkaan: erittäin salaiset, salaiset ja luottamukselliset. Myös julkiselle tiedolle tulee olla oma luokkansa. (Laaksonen ym. 2006, 29-30.)

3.1.3 Tietosuojalaki

Tietosuojalaki on erityisesti tietoturvan kannalta tärkeä laki, kun käsitellään henkilötietoja. “Tällä lailla täsmennetään ja täydennetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta...” (Tietosuojalaki 2018/1050.) Tietosuojalaki täydentää EU:n yleistä tietosuoja-asetusta ja siinä säädetään poikkeuksia ja täsmennyksiä EU:n tietosuoja-asetukseen (Sulin 2019).

3.1.4 EU:n yleinen tietosuoja-asetus (GDPR)

Yleinen tietosuoja-asetus on luotu yhtenäistämään EU-maiden tietosuojaa koskevaa lainsäädäntöä. Asetuksen tarkoituksena on turvata, että jokaisella on oikeus yksityisyyteen ja henkilötietojensa suojaan. Asetus koskee kaikkia organisaatioita, jotka pitävät henkilödataa tai henkilörekisteriä. Yrityksen kannalta asetus velvoittaa asianmukaiseen dokumentointiin ja tämän lisäksi yrityksen pitää pystyä perustelemaan tietojen kerääminen, tallentaminen ja mihin tietoja

käytetään. Yrityksen tulee poistaa henkilötiedot, jos yrityksellä ei ole oikeuksia käsitellä niitä. Tarvittaessa yrityksen tulee pystyä keräämään kaikki tiedot yksittäisestä henkilöstä ja mahdollisesti poistamaan ne, jos henkilö näin haluaa. Lisäksi tietosuoja-asetus velvoittaa yrityksen nimeämään tietosuojavaltuutettu, joka huolehtii tietosuojalainsäädännön toteutumisesta. (Tietosuoja-asetus, Sulin 2017.)

3.1.5 Laki kansainvälisistä tietoturvallisuusvelvotteista

Lakia säädetään erityisesti viranomaisten toimissa kansainvälisten tietoturvasäännösten turvaamiseksi. Laki koskee pääasiassa viranomaisia, mutta erityistapauksissa sitä voidaan soveltaa myös elinkeinoharjoittajaan. (Laaksonen ym. 2006, 47-48.) “Lakia sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana.” (Laki kansainvälisistä tietoturvavelvoitteista 2004/588 § 1).

3.1.6 Laki yksityisyyden suojasta työelämässä

“Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä.” (Laki yksityisyyden suojasta työelämässä 2004/759 §1.) Lakia sovelletaan siis työntekijöiden henkilötietojen käsittelyyn, testeihin ja valvontaan. Tietoturvan kannalta etenkin työnantajalle tärkeää huomioda kyseinen laki. Työntekijöillä on oikeus yksityisyyteen työpaikalla sekä työnantajan työvälineitä käytettäessä, vaikka nämä kuuluvatkin työpaikan omaisuuteen. (Laaksonen ym. 2006, 49-50.)

Laki kattaa myös erilaiset työntekijöihin kohdistuvat valvonnat. Nämä koostuvat teknisestä valvonnasta kuten tietoverkkovalvonta, kameravalvonnasta ja kulunvalvonnasta. Työntekijöiden teknistä valvontaa voidaan harjoittaa monin eri keinoin, kunhan huomioidaan työntekijän oikeus yksityisyyteen. Kameravalvontaa

saa toteuttaa vain työnantajan tiloissa valvomaan muun muassa työntekijöiden turvallisuutta, tuotantoprosessien asianmukaiseen toimintaan sekä omaisuutta tai muita vaarantavaan toimintaan. Kulunvalvontaan kuuluu työntekijöiden liikkuminen työpaikalla, kuten portit ja ovet. Valvonnalla pyritään estämään asiaton pääsy työpaikan tiloihin. (Laaksonen ym. 2006, 50-54.)

3.1.7 Laki sähköisen viestinnän palveluista

Laki sähköisen viestinnän palveluista on hyvin laaja ja hieman epäselvä sekä kattaa paljon muutakin kuin tietoturvaan liittyviä kohtia. Laissa on monia eri tietoturvaan liittyviä huomioita, mutta ne ovat hyvin yksityis- ja tapauskohtaisia. Tietoturvan kannalta laissa säädetään viestintäverkkojen ja palveluiden turvallisuudesta sekä yksityisyyden suojaamisesta ja sähköisen viestinnän luottamuksellisuudesta (Laki sähköisen viestinnän palveluista 2014/917). Tärkeimpiä kohtia tietoturvan kannalta ovat § 349 sähköisen viestinnän tietosuojarikkomukset sekä luku 29 viestintäverkon ja viestintäpalvelun laatuvaatimukset.

3.1.8 Laki sähköisestä asioinnista viranomaistoiminnassa

Laki sähköisestä asioinnista viranomaistoiminnassa pyrkii parantamaan asiointia sekä tietoturvallisuutta viranomaistoiminnassa. “Laissa säädetään viranomaisten ja näiden asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa.” (Laki sähköisestä asioinnista viranomaistoiminnassa 2003/13 § 1.) Lakia sovelletaan sähköiseen aloitteiseen esimerkiksi tuomioistuin, syyte tai ulosotto asioissa. Lakia käytetään myös muussa viranomaistoiminnassa, mutta ei esimerkiksi esitutkinnassa tai poliisitutkinnassa. (Laki sähköisestä asioinnista viranomaistoiminnassa 2003/13.)

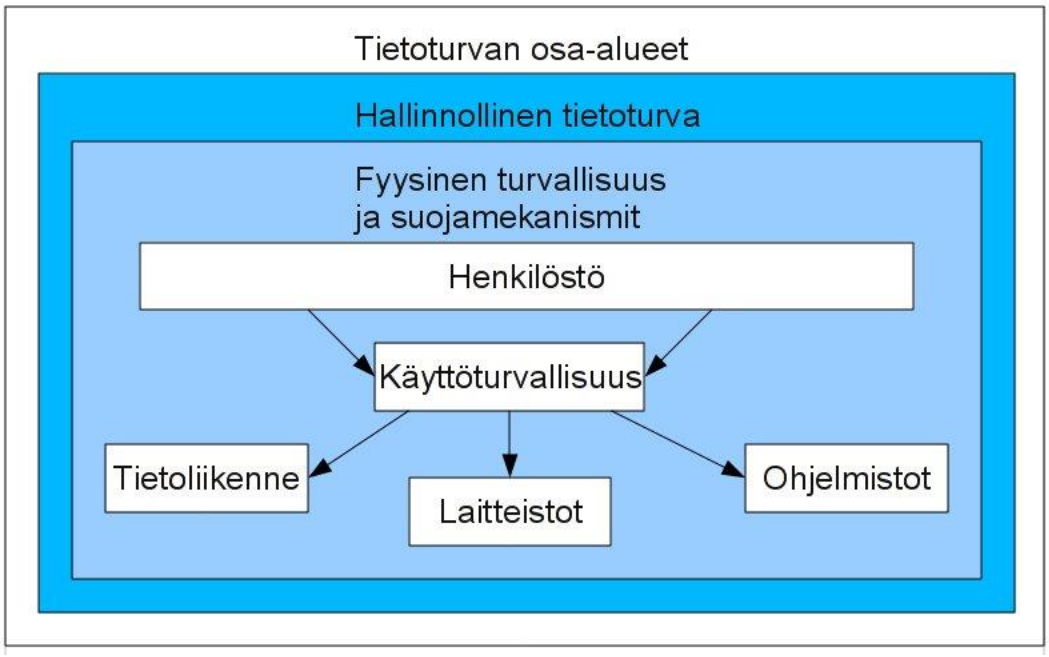
3.1.9 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista

“Tässä laissa säädetään vahvasta sähköisestä tunnistamisesta sekä tunnistuspalveluiden tarjoamisesta palveluntarjoajille, yleisölle ja toisille

tunnistuspalvelun tarjoajille.” (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 2009/617 § 1.) Laki siis säätelee vahvaa sähköistä tunnistautumista sekä sellaisten palveluiden tarjoamiasta. Laissa kerrotaan kuinka ja mihin tunnistautumispalveluita tulee käyttää ja keille niitä saa tarjota. Eritellään myös eri velvollisuuksia tietojen käsittelyyn ja vaatimuksiin. Vahvoja sähköisiä tunnistuspalveluita ovat muun muassa verkkopankkitunnukset sekä mobiilivarmenteet.

4 TIETOTURVAN OSA-ALUEET

Tietoturvallisuuden kokonaisuus halutaan usein pilkkoa helpommin käsiteltäviin osiin, joiden avulla myös laadittavat dokumentit ja niiden rakenne selkeytyy. Tavallisin tapa on jakaa tietoturvallisuus osa-alueisiin. (Hakala ym. 2006, 10-11.)



Kuvio 1. Tietoturvan osa-alueet kuvana.

4.1 Hallinnollinen tietoturva

Hallinnollinen tietoturva hallinnoi ja ohjaa tietoturvan muita osa-alueita. Se määrittää toimintalinjat, toimenpiteet ja periaatteet, joita käytetään organisaatiossa. Siihen kuuluu organisaation suhteet asiakkaisiin ja muihin ryhmiin, kuten viranomaisiin. Hallinnolliseen tietoturvaan kuuluu myös erilaiset yksityisoikeudelliset sopimukset kuten lisenssisopimukset, palvelusopimukset ja vaikutusten arviointi yrityksen tietoturvakäytäntöihin. Hallinnollisen turvallisuuden ylläpidosta vastaa yrityksen tietohallinto. (Hakala ym. 2006, 10-11.)

4.2 Fyysinen tietoturva

Toimitilojen ja laitteiden fyysinen suojaaminen. Laitteistotilojen, käyttötilojen, varastointitilojen, laitteiston ja arkistojen suojaus. Pyritään estämään tietojen tuhoutuminen, vahingoittuminen tai muuten vain vääriin käsiin joutuminen. Fyysinen tietoturva siis suojaa käytännön fyysisiltä uhilta kuten palo- ja vesivahingoilta. Fyysisen tietoturvan ylläpidosta vastaavat yleensä kiinteistönhuollon- ja vartioinnin ammattilaiset. Tietojenkäsittelyn ja tietohallinnon ammattilaisten tulisi kuitenkin osallistua fyysisen turvallisuuden suunnitteluun. (Hakala ym. 2006, 11.)

4.3 Laitteistoturvallisuus

Laitteiden kokoonpanoon ja kunnossapitoon liittyvät turvallisuustoimet. Laitteistoturvallisuuteen kuuluu kaikki yrityksen tietokoneet, puhelimet, tulostimet ja palvelimet sekä niiden käytettävyys, toiminta, kokoonpano, kunnossapito ja laadunvarmistus. Yrityksen tietohallinnon tulee siis pitää huoli, että laitteet ovat toimivia, huollettu ja selkeä kuva mitä laitteita yrityksellä on ja kuinka paljon. (Hakala ym. 2006, 12.)

4.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan tietojärjestelmissä käytettävien lisenssien ja ohjelmistojen hallinnointia. Siihen kuluu käyttöjärjestelmien, sovellusohjelmien ja tietoliikenneohjelmien suojaaminen ja päivittäminen sekä pääsynvalvonta, ohjelmistolisenssit, varmistus, loki, testaus ja valvonta-asiat. Ohjelmisto turvallisuudesta vastaa yrityksen tietohallinto. (Hakala ym. 2006, 11-12.)

4.5 Tietoaineiston turvallisuus

Tietoaineiston turvallisuudella tarkoitetaan sähköisten ja paperisten dokumenttien käsittely ja suojaaminen. Siihen kuuluu myös asiakirjojen, tiedostojen ja muiden tietoaineistojen tunnistaminen, säilyttäminen,

palauttaminen ja tuhoaminen. Tietoaineistoturvallisuudesta vastaa yleisesti yrityksen tietohallinto. (Hakala ym. 2006, 11.)

4.6 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan toimenpiteitä, joilla pyritään varmistamaan tietoverkon kautta välitettävien tietojen eheys, käytettävyys ja luottamuksellisuus. Tietoliikenneturvallisuudessa huolehditaan tiedonsiirtoratkaisujen eli lähi- ja laajaverkkoyhteyksien sekä muiden viestintäjärjestelmien turvallisuudesta. Tietoliikenneturvallisuudesta on vastuussa yrityksen tietohallinto. (Hakala ym. 2006, 12.)

4.7 Henkilöstöturvallisuus

Henkilöstöturvallisuuteen kuuluu toimet, joilla varmistetaan tietojärjestelmän käyttäjien toimintakyky sekä rajataan käyttäjien oikeuksia käyttää yrityksen tietoja ja järjestelmiä. Näihin kuuluvat mm. varamiesjärjestelyt, henkilöstön koulutus, vastuun ja oikeuksien jakaminen sekä mahdollisten taustatietojen selvittäminen. (Hakala ym. 2006, 11.)

4.8 Käyttöturvallisuus

Käyttöturvallisuudella varmistetaan henkilöstön turvalliset käyttöperiaatteet, käytettävien ohjelmiston koulutus ja osaaminen, käyttöympäristön ja varsinaisen tietojenkäsittelyn turvallisuuden valvonta ja virustentorjunta. Käyttöturvallisuuteen kuuluu myös palveluiden ulkoistamis- ja etäkäyttöön liittyvät periaatteet sekä poikkeusoloihin valmistautuminen.

5 YLEISIMMÄT HAITTAOHJELMAT JA HYÖKKÄYKSET

Datan määrä lisääntyy päivä päivältä, yritykseen voi päivittäin kohdistua useita tietoturvauhkia, joista suurin osa jää täysin huomaamatta. Yrityksen tietoturvasta puhuttaessa tulee huomioida yleisimmät uhat ja kuinka niiltä suojaudutaan. Mahdollisen tietomurron sattuessa on hyvä tietää mitä on tehtävissä. Kyseessä voi olla yrityksen maine sekä asiakkaiden luottamus. Yrityksen sisäinen tietoturvakoulutus tulisi olla kunnossa, suurin osa tietomurroista tapahtuu vahingossa tai tietämättömyyden takia.

Haittaohjelmilla tarkoitetaan ohjelmia ja sovelluksia, joiden tarkoituksena on aiheuttaa ei-toivottuja tapahtumia tietojärjestelmissä. Haittaohjelmiin luetaan myös tahattomasti haittaa aiheuttavat ohjelmat. Näiden lisäksi on myös muita ohjelmia tai vastaavia, jotka aiheuttavat ongelmia tai kuormitusta käyttäjälle tai tietojärjestelmälle. (Laaksonen ym. 2006, 163.)

5.1 Virus

Virus on yleensä pätkä koodia, joka liittää itsensä ohjelmaan ja käynnistyy kun kyseinen ohjelma tai tiedosto avataan. Tietokonevirus käyttäytyy kuin mikä tahansa muukin virus, eli pyrkii monistamaan itseään ja levittäytymään koneesta toiseen. Viruksen tunkeuduttua koneeseen se pystyy tekemään vaikka mitä hallaa koneelle, sen käyttäjille ja muille, jonka kanssa kone on yhteyksissä. Yleisimpiä on kuitenkin herkkäluonteisen tiedon varastaminen sekä tuhoaminen. Viruksen voi saada sähköpostista, pikaviesteistä tai internetistä ladatuista tiedostoista. Yrityksen näkökulmasta viruksen leviäminen voisi olla katastrofaalista, täten yrityksen henkilöstö tulisi ohjeistaa käyttämään työkoneita vain työhön ja suojautumaan haitallisilta sähköposteilta. (Baker 2021.)

5.2 Tietokonemato (Worms)

Tietokonemato kuten virus leviää koneesta toiseen, se ei kuitenkaan tarvitse ns. isäntäohjelmaa. Mato leviää yleensä huomaamatta sähköpostitse,

tietojenkalastelulla, haavoittuvaisten ohjelmien sekä internetin välityksellä kuten pikaviestinnän kautta. Se pystyy muokkaamaan tiedostoja tai jopa poistamaan niitä. Tietokonemadon saastuttamia koneita, joihin on avattu takaovi, voidaan käyttää mm. palvelunestohyökkäyksiin, tietojen varastamiseen tai käyttäjän kiristämiseen. (Baker 2021; Laaksoharju 2021.)

5.3 Mainosohjelma (Adware)

Mainosohjelmat ovat ohjelmia, jotka mainostavat käyttäjälle mainoksia selaimessa tai ponnahdusikkunoilla. Mainosohjelmat voidaan jakaa kahteen eri luokkaan: Lailliset mainosohjelmat ja ei-toivotut mainosohjelmat. Ne voivat kerätä tietoa käyttäjästä ja täten luoda kohdemainontaa. Käyttäjä voi vahingossa ladata mainosohjelman toisen latauksen yhteydessä tai klikkaamalla haitallista mainosta. Mainosohjelmat itsessään ovat vain mainoksia varten, mutta ne voivat hidastaa konetta sekä aiheuttaa tietoturvariskejä. (Baker 2021; Laaksoharju 2021.)

5.4 Troijalainen (Trojans)

Troijalainen on yksi yleisimpiä haittaohjelmia, niiden tarkoituksena on hämätä käyttäjää. Troijalainen naamioi itsensä tavalliseksi ohjelmaksi tai tiedostoksi ja avattaessa kyseisen ohjelman tai tiedoston päästää käyttäjä haittaohjelman koneellensa. Koneelle tunkeutumisen jälkeen troijalainen tekee samaa kuin mikä tahansa muukin haittaohjelma. Troijalainen voi ladata laitteelle uusia haittaohjelmia tai antaa pääsyn ei-toivotuille henkilöille. Yleisesti troijalaiset voivat olla mitä tahansa haittaohjelmia, jolloin ne ovat hyvin vaarallisia tietoturvalle. (Laaksoharju 2021.)

5.5 Näppäilytallennin (Keylogger)

Näppäilytallennin nimensä mukaisesti vakoilee käyttäjää seuraamalla näppäilynpainalluksia. Näppäilytallentimet eivät aina ole laittomia, niitä voidaan

käyttää teknisien ongelmien ratkomiseen tai työntekijöiden lailliseen silmällä pitoon. Näppäilytallentimet ovat laillisia, jos niiden käyttäjä omistaa laitteen, jolle se asennetaan. Ongelmana ovat henkilöt, jotka väärinkäyttävät näppäilytallentimia ja asentavat niitä laitteille, johon heillä ei ole oikeuksia sitä tehdä. Laitteen oikea käyttäjä voi olla täysin tietämätön kyseisen ohjelman olemassaolosta ja vahingossa luovuttaa kaiken näppäillyn tiedon kuten salasanat. Näppäilytallentimet voivat myös ottaa näyttökuvia, tallentaa vierailtuja nettisivuja, varastaa pankkitunnuksia, PIN-numeroita ym. Tämän jälkeen varastetut tiedot voidaan lähettää toiselle koneelle tai serverille, josta väärinkäyttäjä saa kyseiset tiedot itselleen. (Malwarebytes.)

5.6 Piilohallintaohjelma (Rootkit)

Piilohallintaohjelmasta puhuttaessa tarkoitetaan ohjelmaa tai ohjelmia, jotka piiloutuvat koneelle kumoten tai välttäen suojamekanismit, jonka jälkeen hyökkääjä voi ottaa koneen haltuunsa etäohjauksella. Piilohallintaohjelmat antavat hyökkääjälle järjestelmänvalvojan-tason oikeudet käyttöjärjestelmään, jolloin hyökkääjä voi asentaa lisää haittaohjelmia, varastaa herkkäluontoisia tietoja, vakoilla käyttäjää sekä deaktivoida viruksentorjunnan. Piilohallintaohjelmat ovat erityisen ovelia piiloutuessa koneelle. Ne ovat vaikeita havaita ja voivat sivuuttaa tai kiertää suojamekanismit, tehden niistä huomaamattomia. Piilohallintaohjelmiin voi kuulua myös takaovi-pääsy, jolloin pystytään kiertämään todennukset ja luvaton etäkäyttö tai tunkeutuminen on mahdollista. (Malwarebytes.)

5.7 Vakoiluohjelma (Spyware)

Vakoiluohjelma on haittaohjelma, joka kerää tietoa käyttäjästään kuten vieraillut nettisivut, lataukset, maksutiedot, käyttäjätunnukset, salasanat ja sähköpostit. Vakoiluohjelma siis pyrkii vakoilemaan ja valvomaan käyttäjää huomaamatta. Ohjelman päästyä koneelle se pyörii taustalla salassa käyttäjältä keräten tietoja ja valvomalla käyttäjän toimia. Vakoiluohjelma siis pyrkii vakoilemaan ja valvomaan

käyttäjää huomaamatta. Vakoiluohjelmia on monia erilaisia kuten näppäilytallentimet, pankkitrojalaiset ja salasanan kaappaajat. (Malwarebytes.) Nykypäivänä vakoiluohjelmat pystyvät muuhunkin kuin vakoiluun, kuten hidastamaan laitetta ja yhteyttä sekä lataamaan lisää haittaohjelmia.

5.8 Verkkourkinta (Phishing)

Verkkourkinnalla tarkoitetaan tietojenkalastelua. Tarkoituksena on hämätä tai huijata uhreja uskomaan hyökkääjiä luotettaviksi tahoiksi ja täten luovuttamaan arkaluonteisia tietojaan tai rahaa hyökkääjälle. Kalastelu voidaan yleisesti jakaa kolmeen osaan: lähettäjä, viesti ja määränpää. Tarkoituksena on esittää luotettavaa tai tuttua lähdettä, jolloin uhri hämääntyy ja luottaa viestin lähettäjään ja sisältöön. Viestin sisältö voi vaihdella linkin painalluksesta aina rahan lähettämiseen, mutta yleisesti asialla on kiire ja täten lähettäjä haluaa uhrilta nopeaa toimintaa, jolloin uhri voi pelästyä ja toimia hätäisesti välttääkseen mahdolliset seuraukset. Tietojenkalastelu ei välttämättä vaadi minkäänlaista teknistä osaamista, joka tekee siitä erittäin vaarallisen ja tehokkaan oikeissa käsissä. (Malwarebytes.) Tietojenkalasteluja on eri typpisiä, vaihdellen kuinka kalastelu on toteutettu. Esimerkkinä spear phishing eli kohdennettu tietojenkalastelu pienempään kokonaisuuteen kuten yksittäinen henkilö tai yritys.

5.9 Palvelunestohyökkäys (Denial-of-Service(DDoS))

Palvelunestohyökkäys on kyberhyökkäys palveluun tai nettisivulle. Hyökkäyksen tarkoituksena on ylikuormittaa palvelu tai verkkosivu lähettämällä samanaikaisesti suuria määriä dataa eri lähteistä. Palvelun tai sivun ylikuormittuessa kaikki resurssit menevät hukkaan ja oikeat käyttäjät eivät pääse läpi. Riippuen hyökkäyksen kestosta ja koosta, voivat hyökkäykset olla vahingoltaan pienestä häiriöstä aina pysyvään vahinkoon asti. Palvelunestohyökkäys toimii kuten edellä mainittiin, mutta sen toteuttamiseen käytetään yleensä ns. Bottiverkkoa, jolla hyökkäys voidaan toteuttaa. Bottiverkko koostuu yleensä saastuneista koneista, jotka luovat verkoston saastuneiden koneiden välillä. Hyökkääjät käyttävät ja

ohjaavat niitä sitten laajamittaisissa hyökkäyksissä. Bottiverkon koneet pyörittävät koneilla ohjelmia, jotka toistavat automaattisia skriptejä. (Malwarebytes.)

5.10 Väliintulohyökkäys (Man-in-the-middle Attack)

Väliintulohyökkäys on kyberhyökkäys, jossa hyökkääjä pystyy tunkeutumaan ja salakuuntelemaan viestintää kahden osapuolen välissä, täten nimetty väliintulohyökkäys. Hyökkäyksen tarkoituksena on kerätä tietoa osapuolista, kuten henkilökohtaisia tietoja tai salasanoja sekä pankkitietoja. Yleisesti hyökkäykset ovat kohdistettuja yksittäisiin henkilöihin, mutta myös yritykset ovat mahdollisia kohteita. Hyökkäykset toteutetaan yleisesti Software-as-a-Service(SaaS) ohjelmilla, kuten viestintä- tai etätyöohjelmat. Hyökkäys tapahtuu kahdessa eri osassa. Ensiksi suoritetaan yhteyden sieppaus, jossa hyökkäjä pääsee verkkoon käsiksi ja ottaa käyttöön tietojenkeräysohjelman, jolla kerää tiedot salakuunnellakseen. Tiedon varastamisen jälkeen tapahtuu salauksen purku, jotta kerätty tieto on luettavaa hyökkääjälle. Saatua tietoa voi sitten käyttää uhria vastaan tai identiteettivarkauksiin. (Crowdstrike 2022.)

6 RISKIT & TIETOTURVALLISUUDEN SEURANTA

Riskit ovat osa liiketoimintaa ja tietojenkäsittelyä. Niihin voidaan vaikuttaa sekä todennäköisyyksiä voidaan pienentää. Riskeihin tulee varautua huolella, huomioiden riskit joihin varaudutaan ja mihin päätetään olla varautumatta. (Hakala ym. 2006, 90.)

6.1 Riskien hallinta

Riskien hallinnannalla pyritään havaitsemaan ja hallitsemaan yrityksen toimintaan kohdistua riskejä. Tietoturvallisuuden testaamisella pyritään havaitsemaan tietoturvan heikot kohdat ja tietoturva toteutuksien toimivuus. (Laaksonen ym. 2006, 150.) Yritys voi myös yrittää hallita osaa riskeistä, jolloin ne voidaan ulkoistaa siirtämällä niitä yrityksen ulkopuolelle. On kuitenkin muistettava, että ulkoistettu riski on yhtä vakava hoitamattomana kuin se olisi omassa yrityksessä. (Hakala ym. 2006, 90.)

6.2 Riskikartoitus

Yrityksen riskeistä voidaan tehdä kartoitus, jos tietojärjestelmien dokumentointi on kattava ja rakenteeltaan hyvä. Kartoitukseen olisi hyvä osallistua yrityksen eri henkilöstöryhmät, jotta riskit ja uhkat tulevat laajasti huomioitua ja pystytään hyödyntämään kaikkien osallisten asiantuntemus, tämän lisäksi miellekartat riskienkartoituksen tekemisessä on hyvä apuväline. Riskikartoituksessa tulisi selvittää aiemmin esiintyneet ongelmat sekä miettiä potentiaalisia riskejä, joita ei ole vielä syntynyt, mutta ovat mahdollisia. Riskikartoituksessa on hyvä toteuttaa riskiluokitus, jonne kriteerien perusteella voi sijoittaa jo aiemmin ilmenneet sekä potentiaaliset tulevat riskit. (Hakala ym. 2006, 80-81.)

6.3 Riskien arviointi

Riskien ja uhkien selvittämisen jälkeen arvioidaan riskit. Arvioinneissa tulee huomioida riskien mahdolliset vaikutukset yritykseen ja sen toimintaan sekä

kuinka todennäköisiä riskit oikeasti ovat. Riskit arvioidaan lähtökohtaisesti, kuinka vakavaa vahinkoa ne voisivat aiheuttaa yrityksen eheyteen, käytettävyyteen ja luottamuksellisuuteen. Tarkastellaan myös riskien vahinkojen vakavuutta ja niiden todennäköisyyksiä. Mitä vakavampi ja todennäköisempi, sitä enemmän siihen tulee varautua. (Hakala ym. 2006, 81.)

6.4 Riskeistä toipuminen ja seuranta

Vaikka suunnitelma riskeiltä suojautumiseen olisi hyvä, se ei takaa riskitöntä lopputulosta. Riskien hallinnassa ei pyritä täydelliseen riskittömyyteen, vaan asetetaan tavoitteita pienempiin jäännösriskeihin. Yrityksen olisi kannattavaa laatia erillinen toipumissuunnitelma, jossa ohjeistetaan miten toimia riskien tullessa toteen. Suunnitelmassa käsitellään muun muassa, kuinka riskien realisoituminen havaitaan, onko tapahtuneella vaikutusta muihin yrityksen tietojärjestelmiin, keitä tiedotetaan tapahtuneesta sekä mitä välittömiä ja välillisiä vaikutuksia tapahtumalla on. (Hakala ym. 2006, 98.)

Turvallisuuden ylläpito edellyttää yritykseltä tämän tietoturvallisuuteen vaikuttavien tapahtumien seurantaa sekä tallentamista. Osa riskeistä on voinut jäädä huomaamatta tai riskeihin varautuminen ei ollut tarpeeksi tehokasta. Yrityksen turvallisuuden suunnittelu ja kehittäminen edellyttää huomioimaan aiemmin tapahtuneet tietoturvallisuuteen liittyvät riskit. Tietoturvan seuranta edellyttää koko yrityksen henkilöstön paneutumista seurantaan sekä raportoimaan havainnoistaan. (Hakala ym. 2006, 101-102.)

7 TIETOTURVAN TOTEUTUS

Tässä kappaleessa käydään lyhyesti läpi yrityksen tietoturvan toteutusta. Kappale käsittelee mitä kaikkea tulee huomioida kun suunnitellaan yrityksen tietoturvaa. Tietoturvan toteutus on tekninen ja käytännöllinen osa yrityksen tietoturvaa. Hyvin toteutettuna se suojaa itse yritystä, sen henkilöstöä sekä asiakkaita.

7.1 Identiteetti- ja käyttöoikeuksien hallinta

Identiteettihallinnalla tarkoitetaan varmistamista, että ainoastaan valtuutetuilla henkilöillä on oikeus käsitellä tietoja ja järjestelmiä, joihin heidät on valtuutettu. Käyttöoikeuksienhallinta kuuluu identiteettihallintaan. Käyttöoikeudet koostuvat käyttöoikeuksien luonnista, muutoksista, poistosta ja seurannasta. (Laaksonen ym. 2006, 173.)

Käyttöoikeuksien hallinnan tärkein tehtävä on hallita käyttöoikeuksia, jolloin käyttäjät saavat ne oikeudet, joita he tarvitsevat työtehtävissään. Hallintaan kuuluu myös oikeuksien poistaminen välittömästi niiden tarpeellisuuden loputtua. (Laaksonen ym. 2006, 151.)

Käyttöoikeuksien hallinta edellyttää käyttäjältä oman henkilökohtaisen tunnuksen, jolla kirjaudutaan työasemalle. Käyttäjän tunnistaminen toteutetaan yleensä käyttäjätunnuksella ja todennetaan salasanalla tai toimikortilla. Annetut tiedot tarkistetaan niitä valvovalla järjestelmällä. (Hakala ym. 2006, 124.)

7.2 Tietojen salaus

Salauksen tavoitteena on varmistaa tietojen luottamuksellisuus. Salausta käyttävien ohjelmien avulla pystytään varmistamaan tietojen eheys sekä järjestelmän ja käyttäjän välisen tiedon kiistämättömyys. Salattujen yhteyksien käyttö on suotavaa esimerkiksi, kun työntekijät käyttävät etäyhteyttä yrityksen tietojärjestelmiin. Lisäksi salaus on tärkeää, kun suojataan yrityksen kriittistä tietoa tai salaisten sähköpostien ja liitetiedostojen lähettämisessä. (Laaksonen ym.

2006, 195-196.) Tietojen salaus kattaa myös kiintolevyjen, ylläpitoyhteyksien ja sähköpostin salauksen.

7.3 Sähköpostin suojaaminen

Sähköposti on yksi yleisimmistä tavoista saada haittaohjelma koneelle. Yrityksen työntekijät voivat käyttää sähköpostia päivittäin, jolloin sähköposti ja sillä lähetetyt sekä tulevat viestit tulee suojata hyvin. Sähköpostia voidaan käyttää myös etäyhteyksien kautta. Etäyhteyden käytössä esimerkiksi kotona luettuja sähköpostien lukuun ei saa käyttää POP3- tai IMAP4-protokollia, jos yhteys ei ole salattu. Sähköpostia luettaessa etäyhteydellä tulisi käyttää VPN-yhteyttä tai webmailin HTTPS-yhteyttä. Kyseinen pätee ainoastaan yrityksen sisäiseen viestien lähettämiseen postipalvelimen ja sähköposti sovelluksen välillä. Yritysten välinen sähköpostiliikenne tulee salata käyttäen muita keinoja. Sähköpostien liitetiedostot on helppo salata esimerkiksi tekemällä niistä salattuja purettavia tiedostoja. Tämä tekee niistä tosin ohjelmatiedostoja, jolloin palomuurit ja sähköpostin suodatusohjelmat eivät päästä niitä läpi, myös exe-tiedostojen avaaminen sähköpostista tulisi herättää hälytysmerkkejä käyttäjässä itsessään. (Laaksonen ym. 2006, 197.)

7.4 Henkilöstön koulutus

Yrityksen johdon tehtävä on näyttää ja saada henkilöstö ymmärtämään tietoturvan laiminlyönnistä aiheutuvat uhat ja riskit sekä hyvän tietoturvallisuuden hyödyt. Yrityksen tietoturvan hallinta vaatii ymmärrystä yrityksen kulttuurista ja kuinka henkilöstö suhtautuu eri toimintamalleihin. Ymmärrys koostuu siitä, kuinka henkilöstö sisäistää ja noudattaa malleja sekä henkilöstön motivaatio noudattaa annettuja ohjeita. Yrityksen tietoturvapolitiikka ja ohjeistus ovat peruspilareina henkilöstön toimintatavoille. Tietoturvallisuuteen vaikuttavat hyvät rutiinit tietoturvallisessa toiminnassa sekä muun johdon ja henkilöstön esimerkit. Turvallisuuden toimintamallit ja ohjeen tulee olla

yhdenmukaisia sekä uusien työntekijöiden rekrytoinnin käytännöt linjassa tietoturvamallien kanssa. (Laaksonen ym. 2006, 248-250.)

Henkilöstön koulutuksesta vastaa yrityksen johto. Johdon tavoitteena on saada työntekijät motivoitumaan ja toimimaan halutulla tavalla, jotta tietoturvaa ei laiminlyödä. Henkilöstö tulee kouluttaa noudattamaan tietoturvapolitiikkaa, johon kaikki perustuu. (Laaksonen ym. 2006, 254.)

7.5 Virustorjunta

Virustorjunta on vanhimpia tietoturvallisuuden teknisiä toimenpiteitä sekä varmasti myös tunnetuin niistä. Hyvin toteutettu ja huolellinen virustorjunta ei kuitenkaan aina takaa tietoturvallisuutta. Tietoturvan toteuttamiseksi vaaditaan paljon lukuisia toimenpiteitä. Luonnollisesti virustorjunta ei pysty estämään kaikkia uhkia tietoturvalle. Virustorjunnalla on myös omat heikot kohtansa. (Laaksonen ym. 2006, 202-203.)

Virustorjunta kattaa työasemat, palvelin ja tuotannolliset järjestelmät sekä selainliikenteen. Työasemien virustorjunta on yleisesti hoidettu hyvin. Työasema virustorjunnan suurimpia haasteita ovat etä- ja kotikäytön työasemat. (Laaksonen ym. 2006, 204.) Etenkin nykypäivänä etätyön lisääntyessä, on tärkeää muistaa myös etätöissä käytettävien työasemien virustorjunta sekä muut tietoturvasuojat.

7.6 Verkon suojaus

Tietoverkon suojaus on tärkeä osa yrityksen tietoturvaa. Sen toteuttamiseen on monia eri keinoja ja sovelluksia. Huolellisesti toteutettu verkon looginen rakenne on tärkeää sekä tietoturvan että itse käytettävyyden kannalta. Myös lainsäädäntö asettaa omat linjaukset verkon suojaamiseen ja valvontaan. Laki yksityisyyden suojasta työelämässä kattaa sähköpostien ja tietoverkkojen valvonnan. (Laaksonen ym. 2006, 181-182.)

Verkon looginen rakenne tulisi toteuttaa hyvin, jolloin verkon laajentaminen on helppoa tulevaisuudessa. Näin ollen yrityksen verkko tulee erottaa muista verkoista, kuten internetistä tai palveluntarjoajan verkosta palomuurilla. Tämän lisäksi yrityksen sisäinen verkko kannattaa jakaa pienempii osiin yleisen toimivuuden ja tietoturvan takia. Yleisesti verkko jaetaan eri laitteille ja toiminnoille niiden tietoturvaluokituksien tai vaatimuksien mukaan. (Laaksonen ym. 2006, 182-184.)

7.7 Palomuurit

Palomuurien tehtävänä on pitää ei-halutut tahot poissa ja suojata hyviä. Tekniikan ja liiketoiminnan kehittyessä on myös tietoverkkojen rakenne sekä käyttötavat muuttuneet, jolloin tämä ei välttämättä pidä enää paikkaansa. Syitä muutokseen ovat: langattomat verkot, etätyö ja siihen liittyvät laitteet, liiketoimintamallit ja sovellusten digitalisoituminen sekä verkostoituminen. Yleisesti turvallisuusuhat kattavat nykyään isomman osan kuin vain verkon sekä yrityksen verkko ja käyttöjärjestelmä suojaukset ovat hyvällä mallilla. Vaikka palomuurien suojausalue on pienentynyt ei niiden merkitys ole vähentynyt. Nykyään palomuureilta edellytetään enemmän toiminnallisia ominaisuuksia, kuten sovellustason suojausta. (Laaksonen ym. 2006, 186-187.)

7.8 Varmistuskäytännöt ja varmuuskopiointi

Yrityksen tiedon ollakseen luottamuksellista ja eheää se tulee varmistaa ja kopioida mahdollisten yllättävien tilanteiden varalta. Varmistuskäytännöillä pyritään varmistamaan tiedon säilyvyys. Varmuuskopiointi tarkoittaa kopioita tietokoneen tai palvelimen tiedoista, joka päivittyy mahdollisimman usein uusimpaan versioon. Tallennuksen sijainti tulisi olla muu kuin alkuperäisen tiedoston. Varmuuskopiointi on helppo tapa suojata tieto mahdollisten tietomurtojen tai onnettomuuksien kannalta. (Laaksonen ym. 2006, 170-171.) Nykyisin varmuuskopiointi tehdään pääosin pilvipalveluihin, jolloin tieto on entistä paremmassa turvassa kuin fyysisellä levyllä.

7.9 Pilvipalvelut

Pilvipalvelut ovat verkossa käytettäviä palveluita, ohjelmistoja tai muuta tietoa. Kun pilveen tallentaa jotain, se ei tallennu omalle koneelle tai yrityksen palvelimelle, vaan pilvipalvelun tarjoavan yrityksen palvelimelle. Pilveä käytetään tyypillisesti verkossa, jolloin siihen pääsee käsiksi omalta tai yrityksen koneelta sekä mobiililaitteilta. Käytännössä sen käyttämiseen tarvitset ainoastaan laitteen jossa on internet. (Kangasniemi, Lintulahti 2017).

Nykypäivänä yhä useampi yritys siirtyy käyttämään pilvipalveluita osana yrityksen muuta IT-puolta. Etenkin IT-yritykset hyötyvät pilvipalveluista. Ne ovat myös helppokäyttöisiä ja kustannustehokkaita. Niiden käyttö tulisi olla aina ensisijainen vaihtoehto. Pilvessä voidaan käsitellä ei-julkista tietoa, kunhan tietoturva on hoidettu oikein. Pilvipalvelut tuovat etenkin lisää turvaa yrityksen tietoturvalle ja tietosuojalle, kun ne on ulkoistettu ja palveluntarjoaja huolehtii pilven tietoturvasta. Pilvipalveluiden uhat ja riskit ovat samoja kuin fyysisen konesalin. (Kauppi 2019.)

Käyttäjälle pilvipalvelut eivät muuttaisi arkea paljoa, ainakaan huonommaksi. Käyttäjät voivat tehdä töitä tästä lähtien etänä sekä milloin vain haluavat. Yrityksen työntekijät voisivat siirtyä etätöihin, jos työnkuva tämän sallii. Käyttäminen olisi helppoa joko kotikoneelta tai työkannettavalta. Teknologisesta näkökulmasta pilvipalveluiden käyttö on järkevää. Niiden ansiosta palvelut ja ohjelmistot olisivat kaikki tallessa samassa paikassa, ilman erillisiä yrityksen sisäisiä palvelimia. Laitteiden hajoaminen tai väärinkäyttö ei olisi enää huoli yritykselle, jolloin tietoturva paranisi.

Yrityksen kannalta pilvipalvelut ovat nykypäivänä itsestäänselvyys. Hyödyt ovat suuremmat kuin mahdolliset haitat. Kannattavuudeltaan helppokäyttöisyys, etäkäyttö, käyttäminen eri laitteilta sekä palveluiden edullisuus ovat kaikki hyviä syitä käyttää pilvipalveluita. Jokaisen yrityksen tulee kuitenkin miettiä oman yrityksen kohdalla, onko pilvipalveluiden riskit hyötyjä suuremmat.

8 POHDINTA & YHTEENVETO

Yrityksen tietoturva ja tietoturva itsessäänkin on kehittynyt paljon viime vuosikymmenellä. Digipalvelut, teknologia ja tietoturvauhat kasvavat, joten myös tietoturvan tulee kehittyä. Nykyään ei riitä pelkästään oma suojaus, vaan kaikkien tulee turvata suojauksensa ja tietoturvansa. Tietoturvassa nähdään yleensä vain haittapuolet ja uhat kuten hyökkäykset ja tietomurrot, mutta hyvin toteutettu ja toimiva tietoturva avaa mahdollisuudet uuden teknologian ihmeelliseen maailmaan. Tietoturva on oleellinen osa yrityksen toimivuutta ja ilman sitä se olisi avoin hyökkäyksille ja väärinkäytölle. Se antaa luottamusta ja turvaa yrityksen toimintaan ja palveluihin.

Opinnäytetyö esittelee tietoturvaa yrityksille. Työssä käydään läpi tietoturvaa kokonaisuutena ja pyritään luomaan lukijalle hyvä ja realistinen kuva tietoturvasta. Työssä käytetyt lähteet ovat luotettavia ja edelleen ajankohtaisia. Työhön sisällytettiin tietoturvan pääkohdat ilman tarkempaa syventymistä, välillä vain aihetta hipaisten, mutta kuitenkin tuoden sen esiin ja kertomalla pääpiirteet. Parannettavaa työssä voisi olla syventyminen tiettyihin alueisiin, kuten tietoturvan toteutus ja tietoturvan tekniset osat, jolloin lukija saa kattavamman kuvan, kuinka tietoturva toteutetaan. Halusin sisällyttää etenkin haittaohjelmat ja hyökkäykset työhön, koska ne ovat aiheena kiinnostavia. Työ onnistui hyvin ja siitä tuli sellainen kuin halusinkin.

Työn aikana opin paljon uutta tietoturvasta ja etenkin tietoturvaan liittyvästä lainsäädännöstä. Aiheen valitsin lisäopin toivossa, jota tuli paljon. Etenkin nykypäivänä 2022 ymmärtää ja arvostaa hyvää kyberturvallisuutta. Työssä ei tullut suurempia ongelmia, vaikka aihe muuttui hieman projektin aikana sekä oma kiinnostus projektin sisältöön muuttui. Projektin aikatauluttaminen sujui kohtalaisen hyvin.

LÄHTEET

Baker, K.2021. THE 11 MOST COMMON TYPES OF MALWARE. Crowdstrike. Viitattu 20.3.2022. https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/.

Crowdstrike. WHAT IS A MAN IN THE MIDDLE (MITM) ATTACK?. 2022. Viitattu 25.4.2022. https://www.crowdstrike.com/cybersecurity-101/man-in-the-middle-mitm-attacks/.

Hakala, M., Vainio, M., Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Dodenco Finland Oy. Jyväskylä.

Kangasniemi, H., Lintulahti, M. 2017. Mikä on pilvipalvelu?. Elisa. Viitattu 15.5.2022. https://elisa.fi/ideat/mika-on-pilvipalvelu/.

Kauppi, J. 2019. Pilven tietoturva, hyödyt ja haitat. Leijona Security. Viitattu 14.5.2022. https://www.leijonasecurity.fi/2019/09/18/pilven-tietoturva-hyodyt-ja-haitat/.

Kyberturvallisuuskeskus. Pilvipalveluiden turvallisuus. Viitattu 6.5.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf.

Kyberturvallisuuskeskus. Tietoturva. Viitattu 19.3.2022. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva.

L 11.6.1999/731 Suomen perustuslaki. Finlex. Viitattu 15.4.2022. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731.

L 13.8.2004/759 Laki yksityisyyden suojasta työelämässä. Finlex. Viitattu 25.4.2022. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759.

L 21.5.1999/621 Laki viranomaisen toiminnan julkisuudesta. Finlex. Viitattu 16.4.2022. https://www.finlex.fi/fi/laki/ajantasa/1999/19990621.

L 24.1.2003/13 Laki sähköisestä asioinnista viranomaistoiminnassa. Finlex. Viitattu 27.4.2022. https://www.finlex.fi/fi/laki/ajantasa/2003/20030013.

L 24.6.2004/588 Laki kansainvälisistä tietoturvallisuusvelvoitteista. Finlex. Viitattu 19.4.2022. https://www.finlex.fi/fi/laki/ajantasa/2004/20040588.

L 7.11.2014/917 Laki sähköisen viestinnän palveluista. Finlex. Viitattu 26.4.2022. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917.

L 7.8.2009/617 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista. Finlex. Viitattu 26.4.2022. https://www.finlex.fi/fi/laki/ajantasa/2009/20090617.

Laaksoharju, S. 2021. Haittaohjelmat pähkinänkuoressa – tunnistatko erilaiset haittaohjelmat toisistaan? Itewiki. Viitattu 21.3.2022. https://www.itewiki.fi/blog/2021/02/haittaohjelmat-pahkinankuoressa-tunnistatko-erilaiset-haittaohjelmat-toisistaan/.

Laaksonen, M., Nevasalo, T., Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Edita Publishing Oy. Helsinki.

Malwarebytes. Ddos. Viitattu 4.4.2022. https://www.malwarebytes.com/ddos.

Malwarebytes. Keylogger. Viitattu 23.3.2022. https://www.malwarebytes.com/keylogger.

Malwarebytes. Phishing. Viitattu 31.3.2022. https://www.malwarebytes.com/phishing.

Malwarebytes. Rootkit. Viitattu 27.3.2022. https://www.malwarebytes.com/rootkit.

Malwarebytes. Spyware. Viitattu 29.3.2022. https://www.malwarebytes.com/spyware.

Malwarebytes. What is a botnet?. Viitattu 4.4.2022. https://www.malwarebytes.com/botnet.

Opiskelijan digitaidot. Tietoturvan periaatteet. Viitattu 19.3.2022. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-1-tietoturvan-ja-tietosuojan-perusteet/tietoturvan-edellytykset/.

Sulin, I. 2017. Yleinen tietosuoja-asetus. Kuntaliitto. Viitattu 24.4.2022. https://www.kuntaliitto.fi/yleiskirjeet/2017/yleinen-tietosuoja-asetus.

Sulin, I. 2019. Tietosuojalaki. Kuntaliitto. Viitattu 24.4.2022. https://www.kuntaliitto.fi/laki/julkisuus-ja-tietosuoja/tietosuoja-asetus/tietosuojalaki.

Tietojesiturvaksi. Tietoturvan osa-alueet. Viitattu 19.3.2022. https://tietojesiturvaksi.fi/tietoturvasuunnitelma/tietoturvan-osa-alueet.

Tietosuoja-asetus. EU:n uusi tietosuoja-asetus koskettaa lähes jokaista yritystä ja yhdistystä. Viitattu 24.4.2022. https://www.tietosuoja-asetus.org/.

Tietoturvariskienarviointi. Tietoturvariskit ja niiden arviointi. Viitattu 23.3.2022 https://www.tietoturvariskienarviointi.fi/.

VirtuaaliAMK. Tietoturvan osa-alueet. Viitattu 19.3.2022. http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html.