

## **Yksityisen syöpäsairaalan tietoturvakartoitus**

Martti Kitunen

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

2014



<b>Tekijä tai tekijät</b> Kitunen Martti	<b>Ryhmätunnus tai aloitusvuosi</b> 2012
<b>Opinnäytetyön nimi</b> Yksityisen syöpäsairaalan tietoturvakartoitus	<b>Sivu- ja liitesivumäärä</b> 45+9
<b>Opettajat tai ohjaajat</b> Petri Hirvonen, Ville Kanninen	
<p>Tämän opinnäytetyön aiheena oli kartoittaa yksityisen syöpäsairaalan tietoturvaluottu. Työssä haluttiin tuoda esille tietoturvaluottu sairaalan näkökulmasta. Tutkimuksen teoriaosuudessa osuudessa perehdyttiin tietoturvan osa-alueisiin ja -käsitteisiin. Työssä tarkasteltiin tietoturvaluottuuden merkitystä yrityksille, sekä mahdollisia tietoturvaluottuuhkia. Lisäksi käytiin läpi tietoturvan arviointiin käytettäviä teknisiä ratkaisuja.</p> <p>Tutkimuksen tavoitteena oli kartoittaa Docrateen tietoturvan nykytila ja saada selville mahdolliset yrityksen tietoturvaan liittyvät ongelmat. Tutkimuksessa pyrittiin löytämään mahdollisimman kattavia, helppokäyttöisiä ja uudelleenkäytettäviä tapoja tietoturvan kehittämiseen ja ylläpitoon.</p> <p>Tutkimus tehtiin toimeksiantona yksityiselle Docrates Syöpäsairaallalle. Docrateen tietoturvaluottu arvioitiin henkilöstö-, käyttö-, tietoliikenne-, laitteisto- ja ohjelmistoturvaluottuuden osalta. Arviointimenetelmiä oli yhteensä 12. Tutkimus sisälsi sekä teknisiä että silmämääräiseen havainnointiin perustuvia arviointimenetelmiä. Henkilökunnalle tehtiin tietoturvakysely ja lisäksi kahta yrityksen tietoturvan kannalta olennaista henkilöä haastateltiin. Jokaisesta menetelmästä tehtiin suppea riskiarvio ja tietoturvan nykytila arvioitiin näiden perusteella.</p> <p>Tuloksena tutkimuksesta Docrates sai selvityksen tietoturvaluottuensa nykytilasta. Selvitykseen kirjattiin puutteet ja haavoittuvuudet ja niihin annettiin korjausehdotuksia. Työssä kerättyjä tietoja voidaan jatkossa käyttää tietoturvan kehittämässä ja ylläpidossa.</p>	
<b>Asiasanat</b> tietoturva, tietoturvakartoitus, tietosuoja, haavoittuvuusskannaus, tietoturvaluottu	

<b>Author</b> Martti Kitunen	<b>Group or year of entry</b> 2012
<b>The title of thesis</b> Cyber security assessment for a private cancer center	<b>Number of report pages and attachment pages</b> 44+8
<b>Supervisor</b> Petri Hirvonen, Ville Kanninen	
<p>The subject of this bachelor's thesis was to assess the cyber security of a private cancer center. The main focus was on finding out the special cyber security needs of a hospital environment. The sections and concept of cyber security were studied in the public part of this thesis. The importance of cyber security and its possible threats for companies were also studied. In addition the technical solutions for evaluating cyber security were examined.</p> <p>The aim was to assess the present state of Docrates' cyber security and to find out possible issues concerning the cyber security of the company. This thesis includes comprehensive, easy to use and reusable ways to develop and maintain the cyber security.</p> <p>This study was made in assignment for Docrates Cancer Center. The cyber security was evaluated by personnel security, usage security, telecommunication security, hardware security and software security. In total 12 evaluation methods were used. The study included both technical and physical observations. A cyber security enquiry was made for the company's personnel and two company members were interviewed about the security facts. A narrow risk assessment was made of every 12 methods. The present state of the cyber security was evaluated with these assessments.</p> <p>As the result of this thesis Docrates received a thorough evaluation of the current state of their cyber security. The flaws and vulnerabilities were put on record and repair suggestions were given. The information collected in this thesis can be used on developing and maintaining the cyber security of Docrates.</p>	
<b>Key words</b> cyber security, cyber security assessment, data privacy, vulnerability scanning, information security violation	

# Sisällys

1. Johdanto .....	1
1.1 Tutkimusongelmat ja rajaukset.....	2
1.2 Tavoitteet.....	2
1.3 Käsitteet.....	2
2. Tietoturva.....	8
2.1 Tietosuoja .....	8
2.2 Tietoturvan merkitys.....	8
2.3 Tietoturvan tavoitteet .....	9
2.3.1 Eheys, käytettävyys ja luottamuksellisuus .....	9
2.3.2 Kiistämättömyys, todentaminen ja pääsynvalvonta .....	10
2.4 Tietoturvan osa-alueet .....	11
2.5 Tietoturva sairaalaympäristössä.....	14
2.6 Tietoturvaan liittyvä dokumentaatio .....	15
2.7 Tietoturvauhat .....	18
2.7.1 Henkilöstö tietoturvallisuuden uhkana .....	19
2.7.2 Langattomien verkkojen uhkatekijät.....	21
2.7.3 Haittaohjelman aiheuttama uhkaskenaario sairaalaympäristössä .....	22
2.7.4 Tietoturvaloukkaus.....	22
3. Tietoturvan arviointi .....	24
3.1 Tietoverkon sisäisen tietoturvallisuuden arviointimenetelmät .....	24
3.2 Tietoverkon ulkopuolisen tietoturvallisuuden arviointimenetelmät.....	25
3.3 Organisaation fyysisen tietoturvallisuuden arviointimenetelmät .....	26
3.4 Sovellukset tietoverkon ja -järjestelmien turvallisuuden arviointiin .....	27
3.4.1 OpenVAS .....	28
3.4.2 Nmap .....	29
3.4.3 Microsoft Baseline Security Analyzer (MBSA).....	31
4. Tietoturvakartoitus.....	32
4.1 Kohdeyritys .....	32
4.2 Riskien arviointi.....	33
4.3 Suunnittelu .....	33
4.3.1 Käytettävät arviointimenetelmät.....	35

4.3.2	Arviointimenetelmien painotus .....	39
4.4	Toteutus.....	40
5.	Pohdinta .....	41
5.1	Ajankäyttö .....	41
5.2	Menetelmävalinnat ja tutkimuksen luotettavuus .....	42
5.3	Tulosten hyödynnettävyys.....	42
	Lähteet.....	43
	Liitteet.....	1
Liite 1.	PowerShell – skripti.....	1
Liite 2.	Haastattelukysymyksiä talousjohtajalle.....	3
Liite 3.	Haastattelukysymyksiä tietohallintopäällikölle .....	5
Liite 4.	Tietoturvakysely .....	8
Liite 5.	Docrateen tietoturvakartoitus (Salattu) .....	9

# 1. Johdanto

Tietoturva puhututtaa nykyään paljon. Uutisista voi lähes viikoittain lukea tietoturvaan liittyviä otsikoita. Vaikka nykyään tietoturvan tärkeys tiedostetaan, se on silti aliarvostettu osa yritysten kokonaisturvallisuutta, eikä välttämättä toteudu käytännössä. Tiedon suojaamisen tärkeyttä ei ymmärretä, koska se ei ole tarpeeksi konkreettinen asia suojattavaksi. Asian tekee vaikeaksi se, että tietoturva on tasapainoilua turvallisuuden ja käytettävyyden kanssa. Lisäksi tietoturvan kehittämisestä ja ylläpidosta aiheutuneet kustannukset mietityttävät. Useimmiten käytettävyys painaa vaa'assa huomattavasti enemmän kuin tietoturvallisuus. Lisäksi käyttäjien asennoituminen vaikuttaa tietoturvallisuuteen. Tietoturvauhkia ei oteta tosissaan, käytetään heikkoja salasanoja tai ei käytetä niitä ollenkaan. Voidaan miettiä tilannetta, jossa yrityksen työntekijän puhelin varastetaan ja heikosti suojatut yrityksen arkaluontoiset tiedot päätyvät suoraan kolmannen osapuolen tietoon esimerkiksi sähköpostien muodossa. Usein edes henkilökohtaisten tietojen suojaaminen ei kiinnosta, vaan sama asenne toistuu niidenkin suojaamisessa. Tietoturva-asioista kiinnostutaan vasta kantapään kautta oppimalla.

Tämän opinnäytetyön aiheena on yksityisen syöpäsairaalan tietoturvakartoitus. Toimeksiantaja on Docrates Syöpäsairaala Oy. Tällä hetkellä Docrateella ei ole muodollista tietoturvasuunnitelmaa, vaikka tietoturvallisuus oli ratkaisevassa roolissa toimitiloja suunniteltaessa vuonna 2009. Docrates on yksityinen syöpäsairaala, minkä takia tietoturvasta huolehtiminen on erityisen tärkeää, jotta potilaiden tiedot olisivat turvassa. Tästä johtuen lähtökohdat tietoturvan osalta ovat huomattavasti paremmat kuin useissa muissa Pk-yrityksissä.

Tutkimus tehdään, jotta yrityksen tietoturvan nykytilasta saataisiin tarkempi kuva. Tutkimuksesta syntyvää dokumenttia voidaan jatkossa käyttää yrityksen tietoturvan kehittämisessä ja ylläpidon apuna. Dokumentti toimii keväällä 2014 suoritettavan tietoturvan itseauditoinnin osana.

## **1.1 Tutkimusongelmat ja rajaukset**

Tutkimus rajataan yrityksen tarpeiden mukaisesti. Se käsittelee tietoaaineisto-, henkilöstö-, laitteisto-, ohjelmisto- ja tietoliikenneturvallisuuksia.

Henkilöstöturvallisuuksia laajennetaan hieman käyttöturvallisuuden puolelle tietoturvakäyttämisen osalta. Tutkimus ottaa kantaa pintapuolisesti yrityksen ulkopuolella käytettäviin ohjelmistoihin, eli niin sanottuihin pilvipalveluihin.

Laitteistoturvalisuuksia käsitellään työasemien, kannettavien tietokoneiden, puhelinten, monitoimilaitteiden ja verkon aktiivilaitteiden osalta. Tietoliikenneturvallisuuksien fyysiseen puoleen, eli yrityksen toimitiloissa sijaitsevien laitteiden ja seinärasioiden liitännöihin otetaan tässä tutkimuksessa kantaa lähinnä pintapuolisesti. Palomuurin säännöksiin tai asetuksiin ei oteta kantaa, koska ne ovat aiemmin kartoitettuja.

Tutkimuksessa yritetään löytää mahdollisimman helppokäyttöisiä ja kattavia keinoja, joilla voidaan turvallisesti parantaa Docrateen tietoturvalisuuksia. Käytettävien keinojen tulee olla uudelleenkäytettäviä, jotta niitä voidaan hyödyntää vuosittain tietoturvalisuuksien tarkastamisessa.

## **1.2 Tavoitteet**

Opinnäytetyön tavoitteena on kartoittaa kohdeyrityksen tietoturvan nykytila ja sen puutteet, sekä antaa tämän perusteella kehitysehdotuksia tietoturvan parantamiseksi. Lopputuloksena yritys saa tämän hetkisen tietoturvatilanteen dokumentoituna kehitysehdotuksineen. Dokumenttia voidaan jatkossa käyttää tietoturvan ylläpidon ja kehittämisen apuvälineenä. Tavoitteena on oppia tietoturvaan liittyviä asioita mahdollisimman syvällisesti sekä teoriassa että käytännössä ja taata opinnäytetyön tekijälle edellytykset toimia tarvittaessa tieturvasta vastaavana asiantuntijana projektin jälkeen.

## **1.3 Käsitteet**

Aliverkotus

Verkon jakaminen ja eristäminen osiin

Asiakaslaite	Asiakaslaitteiksi luokitellaan työasemat, kannettavat tietokoneet ja matkapuhelimet
Auditointi	Arviointi tietyn menetelmän mukaan
Autentikoida	Tunnistautua
Avaintiedosto	Tiedosto, joka sisältää salatun tiivisteen toisen osan
Avoin lähdekoodi	Ohjelmalisenssi, joka tarjoaa käyttäjälle mahdollisuuden tutustua, muokata, kopioida ja levittää sekä alkuperäistä että muokattua versiota
Bruteforce	Automatisoitu kirjautumisyritys, jossa kirjautumista yritetään väkisin tietyn salasanalistan avulla, salasanoihin voidaan lisätä automaattisesti tiettyjä merkkijonoja
Dedikoitu	Yksilöity, tiettyyn käyttöön varattu
Etätyhjennys	Etänä olevaan mobiililaitteeseen voidaan lähettää käsky, joka tyhjentää laitteen oletusasetuksille
Haittaohjelma	Ohjelma, joka pyrkii vahingoittamaan käyttöjärjestelmää, sekä sen sovellusohjelmia
ICT-infrastruktuuri	Tietoverkon ja tietojärjestelmien kokonaisuus, joka toimii perustana muille IT-toimille
Konfiguroida	Määrittää asetukset ohjelmistoon tai laitteeseen
Koventaminen	Poistetaan ylimääräiset ominaisuudet käytöstä ja konfiguroidaan oletusasetukset turvallisiksi



Kytkin	Verkon aktiivilaite, joka yhdistää verkossa olevia laitteita
Linux	Avoimeen lähdekoodiin perustuva käyttöjärjestelmä tai sen ydin
Lisenssi	Ohjelmiston käyttöön oikeuttava sopimus
Loki	Paikka, johon kerätään tietoa järjestelmän tapahtumista
Mobiililaite	Matkapuhelin, tabletti tai kannettava tietokone
Monitoimilaite	Laite, joka yhdistää tulostimen, skannerin, faksin ja kopiokoneen
NLA	Verkkotason kirjautuminen (Network Level Authentication)
Paikantaminen	Käytetään matkapuhelinverkkoa tai satelliittia löytämään tietty kohde
Paketti	Internet-protokollan perusyksikkö, tietoverkkoon lähetetty tieto paketoitua ennen lähetystä
Palomuuuri	Verkkolaite, jolla suojataan tietoverkko ja rajoitetaan tietoliikennettä
Palvelin	Tietokone, joka tarjoaa erilaisia palveluita verkossa oleville asiakaslaitteille

Pilvipalvelu	Pilvipalvelu on verkon yli käytettävä palvelu, joka voi esimerkiksi olla sähköposti tai muu sovellus
PIN – koodi	Yleensä nelinumeroinen koodi, jolla avataan SIM-kortin suojaus
Pingaaminen	Tapa, jolla pyritään selvittämään, onko jokin laite tavoitettavissa verkon yli
Porttikohtainen todennus	Todennetaan verkkoon liitetyt laitteet
Potilassuhde	Sairaalan ja potilaan välinen luottamussuhde
Potilastieto	Potilaisiin liittyvä informaatio, kuten kuvat ja henkilötiedot
Ryhmäkäytäntö	Windows palvelimien ominaisuus, jolla Windows – työasemien asetuksia hallitaan keskitetysti
Salattu yhteys	Yhteys, jota ei voi salakuunnella
Sateenkaaritaulu	Tietokanta tai tiedosto, johon on syötetty salasanoja ja niitä vastaavia tiivistettä
SSH	Secure Shell on salattuun tietoliikenteeseen käytetty protokolla, jota käytetään yleensä nimensä mukaisesti komentorivipohjaisissa yhteyksissä, voidaan salata myös tiedonsiirtoyhteyksiä.
SSL	Secure Sockets Layerin avulla saadaan luotettava suojattu yhteys Internetin yli

Sädehoito	Hoito, jossa käytetään ionisoivaa säteilyä, joka tuhoaa syöpäsoluja.
Sädehoitolaite	Laite, joka toteuttaa sädehoidossa tarvittavan säteilyn
Tarkistussumma	Koodinpätkä, josta voidaan todentaa, onko jokin tiedosto eheä
Tarkistussummavirhe	Kun lähetetty tieto ei ole eheää, saadaan tarkistussummavirheitä
Tiedon säilytysmedia	Erillinen laite johon tieto varastoidaan, esimerkiksi DVD – levy tai muistitikku
Tietojärjestelmä	Järjestelmä, jossa tietoa säilytetään ja tarjotaan käytettäväksi
Tietomurto	Suojatun laitteen, ohjelmiston tai verkon luvaton käyttö
Toimikortti	Sähköinen asiointikortti, jolla voidaan kirjautua esimerkiksi työasemalle kortin ja PIN -koodin yhdistelmällä.
Tulvittaminen	Lähetetään turhia paketteja toistuvasti, jotta saadaan jokin palvelu estettyä tai häirittyä
Työasema	Pöydällä kiinteästi oleva tietokone, jota käytetään työntekoon.
Varmuuskopiointi	Tietojen kopioiminen turvalliseen paikkaan säilytystä varten

Verkon aktiivilaite	Laite joka yhdistää verkkoja, laitteita tai rajoittaa verkon toimintaa
VLAN	Virtuaalinen lähiverkko
VPN	Salattu tunneliyhteys kahden pisteen välillä. Tunnelilla yhdistetään kaksi paikallisverkkoa
Välimieshyökkäys	Selaimen ja palvelimen välillä oleva kone kaappaa niiden välisen liikenteen ja esiintyy selaimelle palvelimena, kaappaajan tekemä sivu on yleensä tehty näyttämään oikealta.
Välityspalvelin	Välityspalvelimella voidaan suodattaa ja varastoida verkossa siirrettäviä tiedostoja
WLAN	Langaton lähiverkko

## **2. Tietoturva**

Tietoturva käsittää tietojen suojaamisen käytännön toimenpiteet, joilla pyritään turvaamaan käyttäjien tietosuojaa. Suojaustoimenpiteet varmistavat, että tiedon käsittely on luottamuksellista ja, että tieto pysyy koskemattomana. Lisäksi varmistetaan, että tieto on aina saatavilla oikeilla käyttöoikeuksilla silloin, kun sitä tarvitaan. Tietoturvan käytännön toimenpiteisiin kuuluu muun muassa tietoturvaohjelmistot, toimitilojen pääsynvalvonta, hallinto, vakuutukset, kouluttaminen ja jatkuvuussuunnittelu. Tietoturvan tärkein päämäärä on, että organisaation jatkuvuus on turvattuna, olosuhteista huolimatta. (Ylipartanen 2010, 18; Andreasson, Koivisto & Ylipartanen 2013, 32.)

### **2.1 Tietosuoja**

Tietosuoja liittyy vahvasti tietoturvaan ja yksityisyyteen. Sen tarkoituksena on suojata tiedon kohteen, eli henkilön yksityisyyttä. Se ottaa huomioon henkilön edut ja oikeusturvan, jotka ovat henkilötietoja koskevissa laeissa ja vaatimuksissa määriteltyjä. Pohjimmiltaan tietosuoja tarkoittaa siis henkilötietojen suojaamista. Lisäksi tietosuojasäädökset antavat viitekehyksen henkilötietorekisterien ylläpitäjille, siitä kuinka henkilötietoja tulee käsitellä. (Ylipartanen 2010, 18; Andreasson 2013, 14.)

Tietosuoja korostuu erityisesti terveydenhoito-alalla, jossa käsitellään potilastietoja. Tietosuoja ei ole pelkästään tiedon suojaamista, vaan sillä pyritään saavuttamaan esimerkiksi luottamuksellinen potilassuhde hoidosta vastaavien henkilöiden ja potilaan välille. Potilaan henkilökohtaisia asioita käsiteltäessä täytyy olla erityisen varovainen, ettei luottamuksellinen tieto joudu kolmannen osapuolen tietoon. Potilastietoja saa lukea vain potilaan hoitoon osallistuva henkilö. (Ylipartanen 2010, 24.)

### **2.2 Tietoturvan merkitys**

Suomen lainsäädännön mukaan, tietoturva ja tietosuoja on otettava huomioon organisaation päivittäisissä toiminnoissa. Niiden merkitys on suurempi kuin moni organisaatio tiedostaa. Usein asia tiedostetaan, mutta sille ei tehdä mitään sen työläyden

takia. Heikko tietoturva ei vaikuta pelkästään organisaatiossa säilytettyihin tietoihin. Se vaikuttaa suoraan yrityksen liiketoimintaan ja sen luotettavuuteen markkinoilla. Lisäksi siitä voi koitua organisaatiolle taloudellista tappiota. Pahimmassa tapauksessa organisaatio menettää maineensa huonosti hoidetun tietoturvan takia. Tietoturvan kehittämisen jatkuvuus on tärkeää, koska tietoturvat kehittyvät koko ajan. Hyvin hoidetussa organisaatiossa tietoturva on otettu huomioon liiketoimintaprosesseja suunniteltaessa, ja sitä kehitetään eteenpäin muun toiminnan mukana. (Andreasson 2013, 30; Laaksonen, Nevasalo & Tomula 2006, 19–20.)

### **2.3 Tietoturvan tavoitteet**

Tietoturvan päätavoitteena on varmistaa, että organisaatiossa olevat laitteet, tietokoneet ja niissä olevat ohjelmistot tekevät vain sen, mikä niille kuuluu. Tämä tarkoittaa käytännössä sitä, että tietojärjestelmän pitäisi olla suojattu mahdollisimman montaa tunnettua tai tuntematonta eri riskiä vastaan. Lisäksi tietojärjestelmien tulisi olla aina käytettävissä ja niissä olevat luottamukselliset tiedot tulisi aina olla saatavilla todennetuille käyttäjille. Tietoturvan tavoitteet voidaan jakaa kuuteen eri osaan: eheyteen, käytettävyyteen, luottamuksellisuuteen, kiistämättömyyteen, todentamiseen ja pääsynvalvontaan. (Ruohonen 2002, 2; Sarja 2005.)

#### **2.3.1 Eheys, käytettävyys ja luottamuksellisuus**

Eheyden tavoitteena on, että tietojärjestelmien tiedot pysyvät muuttumattomina, jos tiedon muokkaamiseen oikeutetut käyttäjät eivät ole niitä muokanneet. Huomioon otettavaa on, että tietokoneen tai ohjelmiston virhe saattaa aiheuttaa tiedon tahattoman muuttumisen. Tiedon eheys menetetään, jos luvaton taho pääsee muokkaamaan tietoa. (Ruohonen 2002, 3.)

Käytettävyys on tietoturvan tavoitteista käyttäjille näkyvin. Käytettävyyden tavoitteena on, että tietojärjestelmissä olevat tiedot ovat aina käyttäjien käytettävissä. Jos tieto on vaikeasti käytettävissä, käyttäjä saattaa pyrkiä kiertämään ongelman ratkaisulla, joka ei ole tietoturvallinen. Ylläpidolle tämä on vaikeimmin saavutettava tavoite.

Turvallisuuden ja käytettävyyden välille on tärkeää löytää sopiva tasapaino.

Käytettävyys tarkoittaa samaa kuin saatavuus tietoturvan näkökulmasta. (Ruohonen 2002, 3.)

Luottamuksellisuuden tavoitteena on taata, että tietojärjestelmässä oleviin tietoihin pääsevät käsiksi vain ne henkilöt, joilla on siihen käyttöoikeus. Jos ulkopuolinen tai käyttöoikeudeton taho pääsee käsiksi tietojärjestelmän tietoihin, joihin hänellä ei ole käyttöoikeutta, tietojärjestelmän luottamuksellisuus on menetetty. (Ruohonen 2002, 2.)

### **2.3.2 Kiistämättömyys, todentaminen ja pääsynvalvonta**

Aikaisemmin katsottiin, että eheys, käytettävyys ja luottamuksellisuus olivat riittävät tavoitteet tietoturvan määrittämisessä. Nykyään kuitenkin katsotaan, että kiistämättömyys, pääsynvalvonta ja todentaminen ovat olennaisia, jotta nämä kohdat voivat toteutua, sillä nuo kolme ensimmäistä kohtaa eivät huomioi tiedon muokkaajan tai omistajan henkilöllisyyttä. (Hakala, Vainio & Vuorinen 2006, 5.)

Kiistämättömyyden tavoitteena on, että kaikki tietojärjestelmän tapahtumat ovat luotettavasti jäljitettävissä. Tämä tarkoittaa käytännössä sitä, että tietojärjestelmän tapahtumista pidetään lokitiedostoa tai erillistä tietokantaa, johon tapahtumat tallentuvat. Tällä pyritään estämään väärinkäytökset esimerkiksi potilastietoja luvattomasti muuttaessa. Kun muutoksista jää jälki, niin väärinkäytökset vähentyvät. Kiistämättömyys menetetään, jos tiettyä tapahtumaa ei voida todentaa lokitiedoista jälkikäteen, oli kyseessä sitten väärinkäytös tai muu muutos. (Laakso 2010; Ruohonen 2002, 3.)

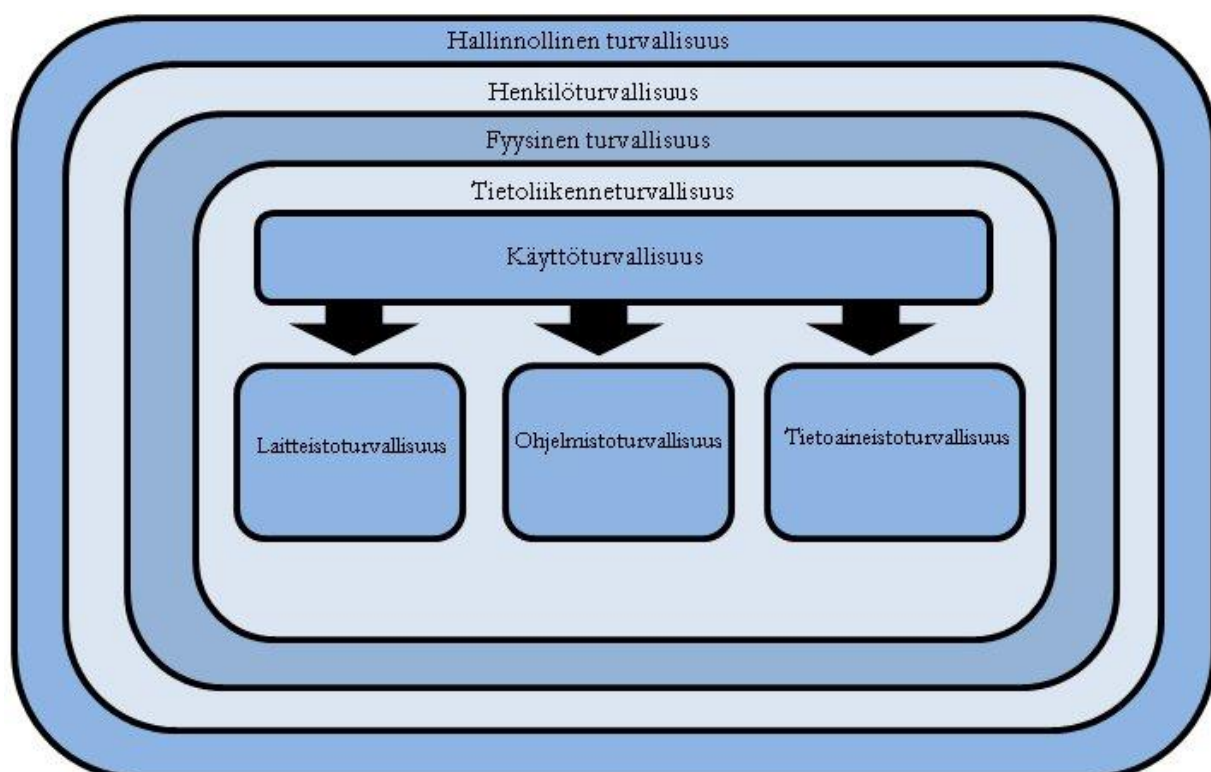
Todentamisen tavoitteena on varmistaa, että vain käyttöoikeudet omaava henkilö pääsee kirjautumaan tietojärjestelmän tiettyyn osaan. Todentaminen voidaan katsoa olennaiseksi osaksi luottamuksellisuuden varmistamista. Tietojärjestelmässä todennus suoritetaan useimmiten käyttäjätunnuksella ja salasanalla. Erilaisia todennusvaihtoehtoja on lukuisia ja vahvimmissa tapauksissa voidaan käyttää kahta eri tapaa. Hyvä esimerkki on sähköinen toimikortti, jossa vaaditaan kortin syöttäminen fyysiseen lukijaan ja siihen kuuluvaa PIN -koodia. Muita vaihtoehtoja ovat muuttuvat luvut, sormenjäljen tunnistaminen ja erilaiset avaintiedostot. Asianmukaisesti

todennettu käyttäjä pääsee kirjautumaan järjestelmään ja saa käyttöönsä hänelle tarkoitetut resurssit. (Laakso 2010.)

Pääsynvalvonta sisältää ne menetelmät, joilla rajoitetaan ICT-infrastruktuurin käyttöä. Pääsyn rajoittaminen tietoihin kuuluu taas luottamuksellisuuden piiriin. On tärkeää, että ICT-infrastruktuurin käyttöä rajoitetaan, jotta voidaan estää organisaation laitteiden ja tietoliikenneyhteyksien luvaton käyttö ja kuormitus. Jos tätä ei estetä, niin organisaation toiminnan kannalta olennainen tietoliikennekapasiteetti kärsii. Pahimmillaan tämä tarkoittaa, että työt keskeytyvät tai hidastuvat. Lisäksi luvaton käyttö altistaa tietojärjestelmän haittaohjelmille. Haittaohjelmat aiheuttavat luottamuksellisuus- ja eheysongelmia. Pääsynvalvonta kattaa sekä ulkopuolisen että organisaation oman henkilöstön. Lisäksi pääsynvalvontaan kuuluu käytön seuraaminen. Tietojärjestelmä pitää lokitiedostoa henkilöistä, jotka ovat käsitelleet tietojärjestelmässä olevia tiedostoja. (Hakala 2006, 5-6; Sarja 2005.)

## 2.4 Tietoturvan osa-alueet

Tietoturva jaetaan kahdeksaan osa-alueeseen. Alla oleva kuva (Kuvio 1.) pyrkii havainnollistamaan näiden osa-alueiden suhdetta toisiinsa.





Kuvio 1. Tietoturvan osa-alueet havainnollistettuna (Paavilainen 1998, 108.)

### **Hallinnollinen turvallisuus**

Hallinnollinen tietoturva on tietoturvan eri osa-alueiden johtamista ja kehittämistä. Hyvällä johtamisella varmistetaan, että kaikki osa-alueet ovat riittävän hyvällä tasolla. Tietoturvan johtamiseen liittyy tietoturvasuunnitelman ja -politiikan luominen sekä niiden ylläpito ja kehittäminen. Lisäksi hallinnolliseen tietoturvaan liittyy olennaisesti yhteydenpito turvallisuudesta vastaavien sisäisten ja ulkopuolisten osastojen kesken. Tietoturvakäytäntöjen suunnittelussa ja ylläpidossa on tärkeää huomioida erityisesti lainsäädännön ja erilaisten sopimusten vaikutus niihin. (Ruohonen 2002, 5; Hakala 2006, 10–11.)

### **Henkilöstöturvallisuus**

Tietojärjestelmät tulee suojata henkilöstön aiheuttamia uhkia vastaan. Uhat ovat usein vahinkoja, ja ne johtuvat yleensä huonosta tietoturvakoulutuksesta. Uhkia vastaan varaudutaan rajaamalla eri tietojärjestelmiin pääsy sopivin käyttöoikeuksin. Hyvä tapa on antaa henkilölle vain ne oikeudet, jotka hän tarvitsee työnsä suorittamiseen. Tahallisesti aiheutettuja uhkia vastaan varaudutaan jo rekrytointivaiheessa tarkistamalla henkilöiden taustatiedot. (Ruohonen 2002, 5.) Alaluvussa 2.7.1 on kerrottu tarkemmin henkilöstön aiheuttamista tietoturvauhista.

### **Fyysinen turvallisuus**

Fyysinen tietoturva liittyy ensisijaisesti toimitilojen suojaamiseen. Näissä toimitiloissa sijaitsevat muun muassa yrityksen tietojärjestelmät. Fyysisen tietoturvan tavoitteena on estää luvattomia henkilöitä pääsemästä käsiksi yrityksen tietojärjestelmiin tai muihin tietoaineistoihin. Etenkin palvelimet ovat tärkeitä fyysisesti suojattavia kohteita, mutta väärään paikkaan jätetty muistitikkukin voi aiheuttaa yrityksen tietojen päättymisen väärin käsiin. (Ruohonen 2002, 4.)

## **Tietoliikenneturvallisuus**

Tietoliikenteen sisäinen ja ulkoinen häiriötön käyttö on tärkeää organisaation toiminnan kannalta. Tietoliikenneturvallisuudella varmistetaan, että liikenne on suojattu luvattomilta käyttäjiltä tai ohjelmilta. Turvallisuutta voidaan parantaa monilla eri teknisillä keinoilla. Tähän lukeutuvat esimerkiksi palomuurit, välityspalvelimet sekä salatut yhteydet, kuten VPN tai SSH. Lisäksi turvallisuutta voidaan parantaa aliverkottamalla tai käyttämällä virtuaalisia verkkoja (VLAN), jolloin verkot on eristetty toisistaan. (Ruohonen 2002, 4.)

## **Käyttöturvallisuus**

Tietojärjestelmiä täytyy käyttää hyvien tietoturvakäytäntöjen mukaisesti. Tämä pyritään huomioimaan käyttöturvallisuudessa. Käyttöturvallisuus liittyy henkilöstöturvallisuuteen, sillä usein käyttäjät ovat tietojärjestelmien turvallisuuden heikoin lenkki. Esimerkkinä voidaan mainita huonosti valitut salasanat tai muunlaiset huolimattomat käyttötavat. Tietoturvakoulutuksen puute johtaa usein käyttöturvallisuuden huononemiseen. Yksinkertaiset salasanat on helppo murtaa. (Ruohonen 2002, 5.)

Käyttöturvallisuuteen kuuluu päivittäinen tietoturvallinen tietotekniikan käyttö, tiedon käsittely ja käytön tukeminen. Lisäksi tietojärjestelmien turvalliset ylläpito- ja kehittämistoimenpiteet ovat osa käyttöturvallisuutta. (Sosiaali- ja terveysministeriö 2007, 33.)

## **Laitteistoturvallisuus**

Laitteistoturvallisuudella tarkoitetaan työasemien, kannettavien tietokoneiden, älypuhelinien, monitoimilaitteiden sekä verkon aktiivilaitteiden suojaamista. Laitteistoturvallisuus toteutetaan osittain fyysisellä tasolla esimerkiksi varkauksien estämiseksi. Lisäksi laitteisiin pääsy pyritään estämään salasanoin sekä esimerkiksi levyn salauksella. (Ruohonen 2002, 5.)

## **Ohjelmistoturvallisuus**

Ohjelmistoturvallisuus kattaa varusohjelmistot, käyttöjärjestelmät, sovellusohjelmat ja tietoliikenneohjelmat. Tarkoituksena on taata näiden turvallinen ylläpito ja hallinta. Kokonaisuuteen kuuluvat ohjelmistojen pääsynvalvonta, tunnistaminen, tarkkailu, eristäminen ja lokien kerääminen. Lisäksi ohjelmistojen laadusta ja turvallisuudesta huolehtiminen on tärkeää. Palveluja ulkoistettaessa pitäisi pyrkiä saavuttamaan nämä samat asiat. (Sosiaali- ja terveysministeriö 2007, 36.)

Tärkeä osa ohjelmistoturvallisuutta on lisenssien ylläpito ja hallinta. Jos tietoturvaohjelmistojen lisenssit vanhentuvat, niin koko organisaatio saattaa jäädä ilman sovellustason turvaa. Lisäksi suuret organisaatiot, kuten Microsoft saattavat tehdä yllätystarkastuksia, joilla varmistetaan, että organisaation lisenssit ovat ajan tasalla ja laillisesti hankittuja. (Ruohonen 2002, 4.)

## **Tietoaineiston turvallisuus**

Tietoaineiston turvallisuus tarkoittaa tietojärjestelmissä olevien tietojen suojaamista. Tietojen turvallista käsittelyä parannetaan pitämällä huolta säännöllisestä varmuuskopioinnista sekä määrittämällä sopivia käyttöoikeuksia tiedostojen käyttöä varten. Lisäturvaa saadaan käyttämällä tietoturvaohjelmia. (Ruohonen 2002, 4.)

Näillä toimenpiteillä turvataan tiedon säilytys, varmistaminen ja palauttaminen. Lisäksi tietoaineiston hävittäminen täytyy hoitaa turvallisesti, jottei esimerkiksi tiedon säilytysmediaan jäisi jälkiä hävitetyistä materiaalista. Tähän voidaan vielä lisätä tulostetut paperiversiot, joiden käsittelyssä täytyy olla huolellinen. (Hakala 2006, 11.)

### **2.5 Tietoturva sairaalaympäristössä**

Sairaaloissa, kuten muissakin organisaatioissa tietoturva on otettava huomioon päivittäisessä toiminnassa. Erona esimerkiksi liikeyrityksiin on se, että sairaaloissa käsitellään potilastietoja, jotka voivat olla erittäin arkaluontoisia. Tämän takia sairaaloilla on suurempi vastuu hyvästä tietoturvasta kuin muilla organisaatioilla. On erityisen tärkeää, että aiemmin mainitut tietoturvan tavoitteet ovat kunnossa, sillä potilaista

kirjatut tiedot vaikuttavat heidän hoitoihinsa. Jos potilastiedot muuttuvat tai katoavat hallitsemattomasti niin potilaan terveys voi olla uhattuna. (Paavilainen 2013, 2.)

Potilastiedot eivät ole ainoa asia, jotka sairaalassa täytyy suojata luotettavasti. Vaikeimpia sairauksia, kuten esimerkiksi syöpää diagnosoidaan ja hoidetaan erilaisilla kuvantamis- ja hoitolaitteilla. Nykyaikaiset kuvantamis- ja hoitolaitteet ovat lähes poikkeuksetta tietokoneohjattuja. On huomioitava, että nämä laitteet ovat yhteydessä tietoverkkoon siinä, missä tavallinen työasemakin ja alttiita samoille uhille. Erona kuitenkin on, että hoitolaitteissa ei ole erillisiä tietoturvaohjelmia tai automaattisia tietoturvapäivityksiä, kuten työasemissa. (Paavilainen 2013, 6-7.)

Laitteet tarvitsevat tietoliikenneyhteyttä muun muassa tietojen lähettämiseksi kuva-arkistoon sekä potilastietojen lukemiseksi potilastietojärjestelmästä. Tietoliikenneyhteyttä voidaan tarvita esimerkiksi tarkasti lasketun sädehoidon 3D-annossuunnitelman syöttämiseksi sädehoitolaitteeseen. Hoitolaitteet ovat sairaalan kriittisimpiä laitteita, joten on erityisen tärkeää, että nämä laitteet ovat asianmukaisesti suojattuina. (Paavilainen 2013, 7.)

Potilastietoihin ja potilaan hoitoihin liittyvät tietojärjestelmät ja laitteet voidaan eristää muusta tietoliikenteestä esimerkiksi luomalla niille oman dedikoidun virtuaaliverkon (VLAN), joka suojataan erillisellä palomuurilla. Lisäksi voidaan estää muiden, kuin sallittujen laitteiden liittyminen verkkoon ottamalla porttikohtainen todentaminen käyttöön (802.1X). (Paavilainen 2013, 8.)

## **2.6 Tietoturvaan liittyvä dokumentaatio**

Tietoturvan ylläpidon ja kehittämisen kannalta on tärkeää, että siitä on laadittu dokumentteja. Tietoturvaan liittyviä keskeisiä dokumentteja ovat tietoturvapolitiikka, tietoturvasuunnitelma, tietoturvaohje sekä jatkuvuus- ja toipumissuunnitelma. (Hakala 2006, 32–56.)

## **Tietoturvapoliittikka**

Tietoturvapoliittikasta sovitaan organisaation ylimmän johdon kesken ja siitä luodaan kirjallinen dokumentti. Se on organisaation tärkein tietoturvaan liittyvä dokumentti, jonka tehtävä on ohjata tietoturvakäytäntöjä ja tietoturvallisuusprosessia.

Suunnitteluvaiheessa johto hyväksyy käytännöt, joilla tietoturvan haluttu taso saadaan aikaiseksi. (Hakala 2006, 7.)

Tietoturvapoliittikka kuvaa yleisellä tasolla liiketoiminnan eri osa-alueiden edellyttämiä tietoturvan tarpeita ja vaatimuksia. Lisäksi kuvataan menetelmät, joilla haluttuun tietoturvasuoritusasteeseen päästään kullakin osa-alueella sekä niiden hallinnointi ja kehittäminen.

Tietoturvapoliittikka laaditaan kerrallaan viideksi vuodeksi, joskus jopa kymmeneksi vuodeksi, mutta se tarkistetaan vuosittain. Lyhyempi aikaväli on usein järkevämpi, koska tietoturvatilat kehittyvät jatkuvasti. Samasta syystä dokumentista tehdään yleisluontoinen, jotta tietoturvapoliittikka soveltuu joustavasti uusiin uhkakuvuihin.

Dokumentista täytyy käydä ilmi, että tietoturvan johtamiseen ja kehittämiseen on oikeasti sitouduttu. Ilman sitoutumista sitä on turha tehdä. Tietoturvapoliittikka kirjoitetaan niin, että yrityksen työntekijät ymmärtävät sen sisällön. Se ei saa sisältää sellaista tietoa, joka antaa informaatiota mahdollisen tietomurron tekijälle. Dokumentti on julkinen ja se voidaan antaa tiedoksi työntekijöille, yhteistyökumppaneille sekä asiakkaille. Tällä tavoin lisätään sidosryhmien luottamusta organisaatiota kohtaan tietojenkäsittelyn saralla. Tarkemmat käytännöt ja tekniset ratkaisut kuvataan liitteissä, jotka eivät ole julkisia. (Hakala 2006, 7-9.)

Tietoturvasuunnitelma pitää sisällään ne menetelmät ja käytännöt, joilla tietoturvasuoritusasteeseen halutaan päästä. Työmenetelmät ja tietotekniset ratkaisut kirjataan yksityiskohtaisesti ylös jokaista tietojärjestelmää varten. Tietoturvasuunnitelma pohjautuu tietoturvapoliittikan linjauksista. Suunnitelma luodaan lyhyemmäksi ajaksi, kuin tietoturvapoliittikka. Suositeltu aika on kahdesta viiteen vuotta. Organisaatiossa tapahtuvat tietojärjestelmämuutokset ja uudet hankinnat täytyy aina käydä läpi tietoturvan osalta. Tämän vuoksi tietoturvasuunnitelmaa täytyy tarkistaa vuosittain. (Hakala 2006, 9.)

## **Tietoturvasuunnitelma**

Tietoturvasuunnitelma pitää sisällään ne menetelmät ja käytännöt, joilla tietoturvasuoritusasteeseen halutaan päästä. Työmenetelmät ja tietotekniset ratkaisut kirjataan yksityiskohtaisesti ylös jokaista tietojärjestelmää varten. Tietoturvasuunnitelma pohjautuu tietoturvapoliittikan linjauksista. Suunnitelma luodaan lyhyemmäksi ajaksi, kuin tietoturvapoliittikka. Suositeltu aika on kahdesta viiteen vuotta. Organisaatiossa tapahtuvat tietojärjestelmämuutokset ja uudet hankinnat täytyy aina käydä läpi tietoturvan osalta. Tämän vuoksi tietoturvasuunnitelmaa täytyy tarkistaa vuosittain. (Hakala 2006, 9.)

Tietoturvasuunnitelmaa ylläpitää ja kehittää organisaation turvallisuudesta vastaavat henkilöt yhdessä tietohallinnon ja ICT-asiantuntijoiden kanssa. Tietoturvasuunnitelma on aina luottamuksellinen. (Hakala 2006, 9.)

### **Tietoturvaohje**

Tietoturvaohje muodostetaan tietoturvasuunnitelman pohjalta. Ohje on yleensä mahdollisimman lyhyt ja käytännönläheinen, jotta käyttäjät ymmärtäisivät sen. Vaikeasti ymmärrettävä ja monisivuinen ohje ei motivoi käyttäjiä sisäistämään sitä. Ohjeita voi olla useita, yksi kullekin tietojärjestelmälle tai liiketoimintaprosessille. Hyvään ohjeistukseen kuuluu selitys siitä, että minkä takia sitä tulisi noudattaa. Ohjeen merkitys käyttäjän päivittäiseen työhön kannattaa tuoda selkeästi esille. Tietoturvaohjeet ovat organisaation sisällä säilytettäviä luottamuksellisia dokumentteja. (Hakala 2006, 10.)

### **Jatkuvuus- ja toipumissuunnitelma**

Jatkuvuus- ja toipumissuunnittelun lähtökohtana on keskeytys-vaikutusanalyysin luominen. Siinä määritellään järjestelmäkohtaisesti tavoitteet käytettävyydelle, palvelutasovaatimukset sekä sallitut kestot häiriöille. Tuloksena saadaan tärkeysluokitukset järjestelmille ja toiminnoille. Toipumissuunnitelma pitää sisällään ohjeistuksen häiriöiden kirjaamis-, havaitsemis- sekä korjausmenettelyille. Tehtävät ja niiden vastuut jaetaan nimetyille henkilöille. Lisäksi vastuuhenkilöille kirjataan varahenkilöt. Poikkeustilanteista selviämistä auttaa esimiesten etukäteen miettimä ja hyvin delegoitu tilannejohtaminen. (Sosiaali- ja terveysministeriö 2007, 35.)

Organisaation jatkuvuussuunnitelma tehdään, jotta yrityksen tärkeät liiketoimintaprosessit olisi turvattu sekä normaalitilanteessa että häiriötilanteessa ja häiriön jälkeen. Jatkuvuussuunnitelma on suunnitelma tietojenkäsittelyn ja tiedonsiirron jatkumiselle erilaisten häiriötilanteiden varalta. Jatkuvuussuunnitelma ei kuitenkaan ota huomioon normaalitoiminnan aikana tehtäviä huoltotoimenpiteitä, jotka kuitenkin edistävät jatkuvuutta. (Laaksonen 2006, 227.)

Toipumissuunnitelma tehdään, jotta liiketoimintaprosessien palautuminen olisi mahdollisimman nopeaa erilaisten häiriötilanteiden jälkeen. Toipumissuunnitelma on

osa jatkuvuussuunnitelmaa. Se sisältää ohjeet toiminnan jatkamisesta ja paluusta normaalitilaan, katastrofista toipumiseen sekä varajärjestelmien vaatimukset. Liiketoimintaprosessien eri osa-alueille määritetään vastuut ja tehtävät valmiuden luomiseksi. Lisäksi luodaan ohjeet toiminnasta poikkeustilanteessa. Toipumissuunnitelma ei rajoitu pelkästään tietojärjestelmien toipumiseen. (Laaksonen 2006, 227–228.)

Tietojärjestelmän näkökulmasta toipumissuunnitelman tavoitteena on saada tietojärjestelmä takaisin toimintakuntoon mahdollisimman nopeasti. Yleisiä syitä tietojärjestelmän palauttamiseen ovat levyrikko ja tietomurrot. Toipumissuunnitelman tavoitteisiin kuuluu, että kun tietoja menetetään, niin menetykset olisivat mahdollisimman vähäiset. Lisäksi on tärkeää, että palautettu järjestelmä ei sisällä uuden tietomurron mahdollistavia ohjelmia tai asetuksia. Näin varmistetaan, että tietomurto ei toistu. (Ruohonen 2002, 9.)

Jatkuvuus- ja toipumissuunnitelma tehdään ensisijaisesti liiketoiminnan häiriöttömän toiminnan turvaamiseksi ja sen palauttamiseksi normaalitilaan. Tietojärjestelmät ovat osa liiketoimintaan kuuluvia liiketoimintaprosesseja, ja ne ovat tärkeässä roolissa, sillä nykyään tietotekniikalla on merkittävä rooli organisaation liiketoiminnassa. Jatkuvuus- ja toipumissuunnitelma ovat tietoturvallisuuden kannalta tärkeässä asemassa, sillä ne pitävät sisällään tietoturvan kaikki osa-alueet. Suunnitelmia luodessa täytyy ottaa huomioon organisaation maantieteellinen sijainti ja ympäristö sekä organisaation toiminnan luonne ja laajuus. (Laaksonen 2006, 228.)

## **2.7 Tietoturvaohjeet**

Tietoturvaohjeita on monenlaisia. Osa uhista johtuu käyttäjistä, kun taas osa aiheutuu tietojärjestelmien heikosta suojauksesta. Nykyään lähes kaikki palvelut ovat saatavilla Internetin kautta. Näin ollen näihin kaikkiin palveluihin on mahdollista yrittää tietomurtoa tai aiheuttaa muunlaista vahinkoa, ja mikä pahinta, tämä kaikki tapahtuu etäältä. Hieman uudempana uhkana voidaan mainita viime vuosina yleistyneet älypuhelimet. Älypuhelin sisältää pahimmillaan koko käyttäjän elämänsä aikana tallennetut tiedot, kuvat, sähköpostit ja kalenterimerkinnät. Useimmiten älypuhelimien

tietoturvaa ei oteta huomioon juuri ollenkaan. PIN -koodiksi on jätetty oletus 1234 tai 0000, eikä suojakoodi ole käytössä ollenkaan. Paremmat kooditkin ovat toki murrettavissa, mutta niillä saadaan aikaa esimerkiksi puhelimen sijainnin paikantamiseksi tai etätyhjennyksen suorittamiseksi.

Nämä uhkatekijät täytyy ottaa huomioon palvelujen tietoturvaa suunniteltaessa. Tarvitaan siis teknisiä ratkaisuja, joilla voidaan ennaltaehkäistä näitä uhkia. Lisäksi käyttäjien tiedottaminen ja kouluttaminen tietoturvallisuuden osalta edesauttaa tietoturvallisuuden toteutumista. (Andreasson, Koivisto 2013, 202–203.)

### **2.7.1 Henkilöstö tietoturvallisuuden uhkana**

Tietoturvan heikoin lenkki on usein organisaation henkilöstö. Usein henkilöstö ei ole kiinnostunut tietoturva-asioista. Tietoturvakoulutuksia ei järjestetä tarpeeksi usein ja tietoturva-asioista tiedotetaan harvoin. Pahimmassa tapauksessa organisaation luotettu työntekijä saattaa aukaista kolmannelle osapuolelle pääsyn tietojärjestelmiin edes ajattelemtta asiaa sen enempää. Turvallisuusjärjestelmistä tulee hyödyttömiä, kun käyttäjä avaa tietojärjestelmään pääsyn ulkopuoliselle. (Laaksonen 2006, 252–253.)

Tietoturvauhkia syntyy erityisesti silloin, kun työntekijälle ei ole annettu riittävää koulutusta käyttöjärjestelmän ja ohjelmistojen käyttöön. Tällöin työntekijän tietotaito ja siihen liittyvä osaaminen ei ole tietoturvallisuuden vaatimusten tasolla. Osa työntekijöistä saattaa olla huolimattomia tietoja käsitellessään, koska he eivät ymmärrä tiedon suojaamisen tärkeyttä käytännön tasolla. Tietoturvan osalta tehdään tahattomia virheitä, ja joskus tietoturva-asioista ollaan yksinkertaisesti tietämättömiä. Lisäksi työasemille asennetaan niihin kuulumattomia ohjelmia, jotka voivat sisältää haittaohjelmia. (Sosiaali- ja terveysministeriö 2007, 16; Mikael Mäki 2007.)

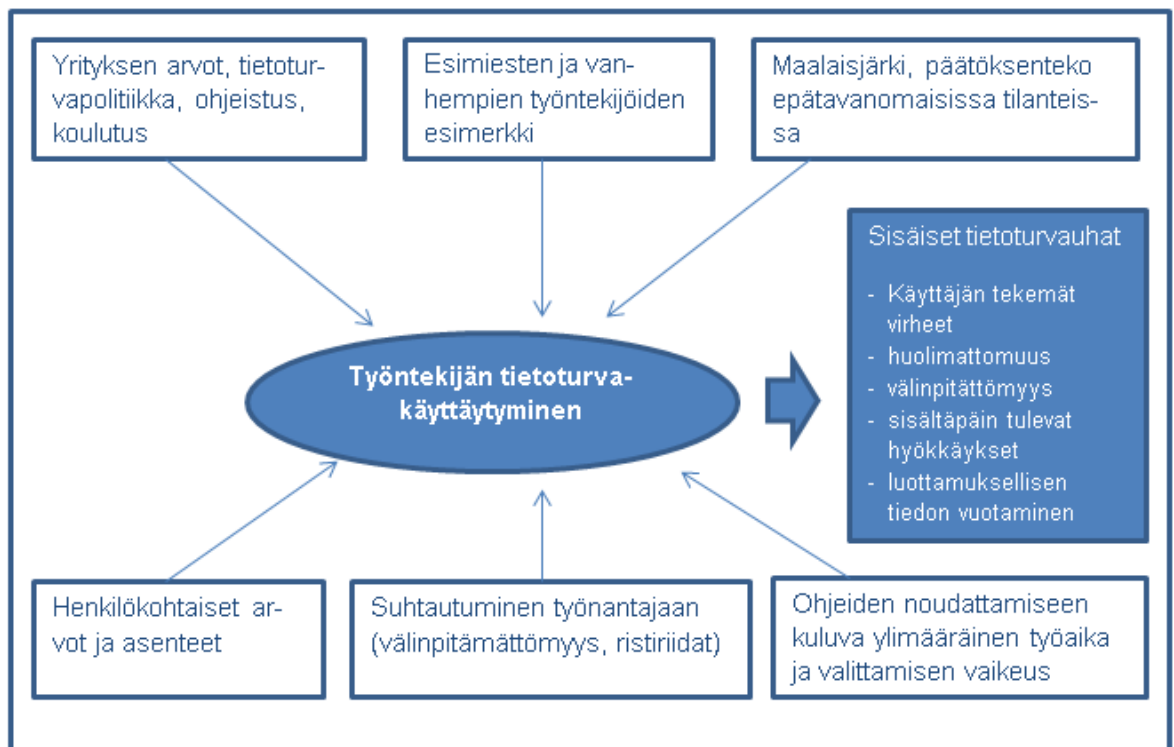
Edellä mainittujen uhkien takia organisaation henkilöstöä tulisi kouluttaa säännöllisesti, jotta organisaation tietoturva pysyisi kunnossa. On tärkeää, että organisaation sosiaalinen ilmapiiri edesauttaa tietoturvan huomioon ottamista. Henkilöstöä koulutettaessa oikeanlainen motivointi on tärkeää. Positiiviset kannustimet asioiden sisäistämiseksi sekä käytännön esimerkit osana koulutusta vievät asiaa eteenpäin.



Henkilöstölle voidaan esimerkiksi näyttää koulutuksessa, miten sateenkaaritaulu käytännössä toimii ja miten sanakirjan sanoihin perustuvat salasanat murtuvat sekunneissa. Lisäksi voidaan näyttää, miten suojaamattomalta Internet-sivustolta saadaan käyttäjätunnukset selväkielisenä liikennettä kuuntelemalla. (Laaksonen 2006, 253–255.)

Työntekijät täytyy myös kouluttaa ottamaan työympäristö huomioon. Tämä tarkoittaa sitä, että asiakkaat eivät saa nähdä yrityksen tai tietosuojan alaisia tietoja tietokoneen näytöltä tai mistään muualtakaan. Tulostimet ja faksit täytyy sijoittaa niin, että ulkopuoliset eivät pääse niihin käsiksi. Lisäksi samat asiat on otettava huomioon silloinkin, kun niistä puhutaan ääneen. (Sosiaali- ja terveysministeriö 2007, 16.)

Koulutuksessa on tärkeää korostaa asiaa arkipäivän esimerkeillä. Kun säännöt ja ohjeet saavat käytännön merkityksen, tulee asioiden oppimisesta parhaassa tapauksessa mielenkiintoista, eivätkä ne tunnu turhilta hidasteilta. Alla olevassa kuvassa (Kuvio 2.) havainnollistetaan, mitkä asiat vaikuttavat työntekijän tietoturvakäyttäytymiseen. Kaikkien ei tarvitse kuitenkaan alkaa tietoturva-asiantuntijoiksi, vaan riittää, että ymmärtää tietoturvariskit ja niiden merkityksen omassa päivittäisessä työssään. (Laaksonen 2006, 253–255.)



Kuvio 2. Työntekijän tietoturvallisuuskäyttäytymiseen vaikuttavat asiat. (Laaksonen 2006, 249.)

### 2.7.2 Langattomien verkkojen uhkatekijät

Langattomiin verkkoihin liittyy useita uhkatekijöitä, koska verkkoliikenne tapahtuu langattomasti, eikä verkko näin ollen rajoitu pelkästään organisaation toimitiloihin. Osa uhista kohdistuu suoraan käyttäjiin ja osa suoraan IT-infrastruktuuriin. (Thomas 2005, 295.)

Käyttäjiin kohdistuvat uhat toteutuvat useimmiten siten, että käyttäjä liittyy julkisesti saatavilla olevaan langattomaan verkkoon. Julkisissa salaamattomissa verkoissa on aina riskinä, että kolmas osapuoli nauhoittaa verkkoliikennettä, ellei liikennettä ole eristetty muista asiakaslaitteista. Tätä käyttäjä ei kuitenkaan voi tietää, joten riski on aina olemassa. Käytännössä käyttäjien selaimeen syöttämät salasanat ovat suoraan luettavissa nauhoituksista, mikäli käytetty yhteys ei ole salattu. Toinen esimerkki on, että käyttäjä lähettää luottamuksellisen sähköpostin salaamattomana edellä mainitussa verkossa. Tällöin viestin voi lukea kuka tahansa tarvittavan tietotaidon omaava henkilö. IT-infrastruktuuriin kohdistuvat uhat koskevat langattomaan verkkoon murtautumista tai siihen kohdistuvaa palvelunestohyökkäystä. (Thomas 2005, 295–298.)

Murtautumiseen saatetaan käyttää esimerkiksi Linux -järjestelmässä käytettävää AirSNORT -nimistä ohjelmaa. Ohjelmalla voidaan kaapata paketteja langattomasta verkosta ja murtaa verkon salaus. Tähän riittää yleensä viidestä kuuteen miljoonan paketin kaappaaminen. Pakettien kaappaamisen nopeus riippuu kyseisen verkon liikennemäärästä. Salauksen murtuminen on luonnollisesti kiinni käytettävästä salauksesta sekä salausavaimen pituudesta ja monimutkaisuudesta. (Thomas 2005, 316–317.)

Jos mahdollinen hyökkääjä ei saa langattoman verkon salausta murrettua, hän saattaa yrittää estää muita käyttämästä sitä. Tällaisia palvelunestohyökkäyksiä voidaan toteuttaa langattomasti tulvittamalla verkko uudelleenautentikointipyynnöillä (deauthentication attack). Käytännössä tämä tarkoittaa sitä, että langattomaan verkkoon yhteydessä olevat

asiakaslaitteet menettävän yhteyden siihen ja saavat virheilmoituksen epäonnistuneesta autentikaatiosta. Yhteyden saaminen on mahdollista vasta, kun palvelunestohyökkäys päättyy. (Thomas 2005, 297; Stuart Compton 2007.)

### **2.7.3 Haittaohjelman aiheuttama uhkaskenaario sairaalaympäristössä**

Nykyään sairaaloiden toiminnan keskeinen osa on tietoinfrastruktuurin toimivuus. Hoitolaitteita ohjataan tietoteknisesti ja potilasjärjestelmät ovat suurimmaksi osaksi sähköisiä. Yksi pahimmista uhkaskenaarioista on tilanne, jossa sairaalan työasemien ja palvelimien tietoturvaohjelmistot on jätetty päivittämättä, kokonaan asentamatta tai niissä on toimintahäiriö. Tässä tilanteessa, mikä tahansa haittaohjelma voi levitä vapaasti sairaalan tietoverkoissa. Riittää, että yksi henkilö liittyy suojaamattomaan työasemaan saastuneen muistitikun, joka on saatu esimerkiksi ulkomailla pidetyssä konferenssissa.

Sairaalan toiminta lamaantuu tai keskeytyy, kun haittaohjelma on levinnyt verkon kaikkiin työasemiin ja pahimmassa tapauksessa sairaalan hoitolaitteisiin. Saastuneita työasemia ei voi käyttää esimerkiksi potilastietojen käsittelyssä, koska tietojen luottamuksellisuudesta tai eheydestä ei ole takeita. Työasemien uudelleenasetus kestää viikkoja, eikä niitä voi liittää verkkoon, ennen kuin ollaan varmoja, että verkossa ei ole yhtään saastunutta konetta jäljellä. (Paavilainen 2013, 3.)

### **2.7.4 Tietoturvaloukkaus**

Tietoturvaloukkauksella tarkoitetaan, että organisaatiossa säilytettyä tietoa on päätenyt kolmannen osapuolen käyttöön. Lisäksi tietojenkäsittelyn estäminen tai sen vaikeuttaminen sekä tahattomasti että tahallisesti lasketaan tietoturvaloukkaukseksi. Tietoturvaloukkausten suojaksi on olemassa rikoslain suoja. Tämän takia jokainen loukkaustapaus tulee käsitellä vähintään organisaation sisäisin kurinpitomenettelyin. Vakavimmissa tapauksissa loukkauksesta tulee ilmoittaa viranomaisille. Tietoturvaloukkaukset täytyy aina saattaa sekä organisaation johdon että tietoturvasta vastaavan henkilön tietoon. Tietoturvaloukkausten sanktiot on määriteltävä valmiiksi

organisaation tietoturvapoliitikassa, jotta asian käsittely olisi selkeää ja ymmärrettävää.  
(Sosiaali- ja terveysministeriö 2007, 43–44.)

### **3. Tietoturvan arviointi**

Ennen kuin tietoturvaa voidaan alkaa kehittämään, tarvitaan kattava arviointi nykytilasta ja kehitystarpeista. Tietoturvan arviointi on ensiaskel kohti parempaa tietoturvaa, mutta se ei silti saisi olla kertaluonteista. On tärkeää, että tietoturvaa arvioidaan vähintään kerran vuodessa, koska esimerkiksi vuoden päästä tietoturvauhat saattavat olla täysin erilaiset. Yleisesti katsotaan, että tietoturvan arvioijan tulisi olla ulkopuolinen tekijä, jotta arvio olisi rehellinen ja objektiivinen. Ulkopuolista tekijää käytettäessä, organisaation täytyy selvittää mahdollisimman tarkasti arvioinnin tekijän menettelytavat ja arviointiprosessi. Lisäksi aikaisemmilta asiakkailta tulee pyytää referenssit. (Thomas 2005, 366–367.)

Tietoturvan arviointitapoja on erilaisia. Yleensä ne jaetaan verkon sisäisiin ja ulkoisiin haavoittuvuuksiin sekä fyysisen turvallisuuden arviointiin. Tämän lisäksi arvioidaan onko verkkoon tunkeuduttu sisältä tai ulkoa. (Thomas 2005, 367.)

#### **3.1 Tietoverkon sisäisen tietoturvallisuuden arviointimenetelmät**

Verkon sisäiset tietoturvauhat johtuvat usein puutteellisesti asennetuista verkon aktiivilaitteista, vanhentuneista ohjelmistoista sekä hyvien tietoturvakäytäntöjen puuttumisesta. Arviointia suoritettaessa tulisi miettiä, että mitkä puutteista aiheuttavat vahingossa syntyneitä uhkia, ja mitkä edesauttavat tahallisesti tehtäviä tietomurtoja. (Thomas 2005, 367.)

Sisäinen arviointi suoritetaan nimensä mukaisesti paikanpäällä. Siinä tulee keskittyä tietoturvakäytäntöihin ja -menettelytapoihin sekä verkossa oleviin laitteisiin ja sovelluksiin liittyviin sisäisiin riskeihin. (Thomas 2005, 368.)

Lopputuloksena syntyy dokumentti, joka sisältää käytetyt arviointimenetelmät, tehdyt toimenpiteet, yksityiskohtaisen luettelon haavoittuvuuksista ja luettelomaisesti tiedot kaikista tietojärjestelmistä. Dokumentti kuvaa selkeästi verkon rakenteen ja haavoittuvimmat pisteet. Lopussa esitellään arvioinnissa löytyneet uhat ja annetaan

niihin parannusehdotuksia. Sisäiseen arviointiin kuuluvat seuraavat toimenpiteet. (Thomas 2005, 368–369.)

- Organisaation dokumentoiman sisäiseen tietoverkkoon liittyvän informaation koostaminen
- Tutustutaan tietoturvamenetelmiin ja käytäntöihin
- Tietoverkon kartoittaminen ja loogisen kuvan muodostaminen siitä
- Verkon laitteiden ja sovellusten tekninen tunnistelu
- Verkon laitteiden ja sovellusten haavoittuvuusskannaus
- Verkon kuuntelu liikennevirtojen tunnistamiseksi, jotta erotetaan tavallinen liikenne haitallisesta
- Analysoidaan haavoittuvuudet erilaisin luotettaviksi todetuin työkaluin
- Löydettyjen haavoittuvuuksien tarkistaminen, jotta erotetaan väärät hälytykset oikeista
- Etsitään tietojärjestelmiä, joissa on heikot käyttäjätodennusmenetelmät
- Tarkistetaan, että salasanojen vaihtamisväli on riittävän lyhyt
- Etsitään turvattomat langattomat verkot
- Raportoidaan löydetty asiat ja ehdotetaan niihin parannuksia

### **3.2 Tietoverkon ulkopuolisen tietoturvallisuuden arviointimenetelmät**

Verkon ulkoisiin uhkiin kuuluu paljon samoja elementtejä kuin sisäisiin uhkiinkin, kuten esimerkiksi puutteellisesti asennetut verkon aktiivilaitteet, vanhentuneet ohjelmistot sekä heikot tietoturvakäytännöt. Mahdollisiin uhkiin voidaan lisätä pilvipalvelut, jotka ovat usein web-pohjaisia. (Thomas 2005, 369.)

Tietoverkon ulkoisen turvallisuuden arviointi suoritetaan paikoissa, joissa on liityntäpisteitä organisaation verkkoon. Näitä ovat Internet-yhteydet, langattomat verkot, puhelinjärjestelmät sekä muut etäpisteet. Muu etäpiste voi esimerkiksi olla toinen organisaatio, josta kulkee VPN -yhteys arvioitavaan organisaatioon. Ulkoiseen arviointiin kuuluvat seuraavalla sivulla olevat toimenpiteet. (Thomas 2005, 369–370.)

- Organisaation dokumentoiman ulkoiseen tietoverkkoon liittyvän informaation koostaminen
- Verkosta julkisesti saatavilla olevien tietojen selvittäminen
- Tietoverkon kartoittaminen ulkopuolelta ja loogisen kuvan muodostaminen
- Ulkopuolisen kartoituksen vaikutus palomuriin ja sen lokeihin
- Verkon laitteiden ja sovellusten tekninen tunnustelu ulkoverkon puolelta
- Verkon laitteiden ja sovellusten haavoittuvuusskannaus ulkoverkon puolelta
- Langattoman verkon testaaminen toimitilojen ulkopuolelta, mikäli nähdään tarpeelliseksi
- Verkon kuuntelu liikennevirtojen tunnistamiseksi, jotta erotetaan tavallinen liikenne haitallisesta
- Analysoidaan haavoittuvuudet erilaisin luotettaviksi toimitilojen työkaluin
- Löydettyjen haavoittuvuuksien tarkistaminen, jotta erotetaan väärät hälytykset oikeista
- Etsitään ulkopuolisia tietojärjestelmiä, joissa on heikot käyttäjätodennusmenetelmät
- Raportoidaan löydetty asiat ja ehdotetaan niihin parannuksia

### **3.3 Organisaation fyysisen tietoturvallisuuden arviointimenetelmät**

Fyysistä turvallisuutta arvioidaan toimitilojen havainnoinnilla. Havainnointikierröksellä on hyvä olla mukana joku tietohallintoon kuuluva henkilö sekä organisaation turvallisuudesta vastaava henkilö. Löydetty havainnot kirjataan ylös. Kierroksella on tärkeää käydä läpi ainakin kriittisten tietojärjestelmien laitetilat, työasemat, tietojen varmistus-, tuhoamis- ja säilytystilat, tietovälinekaapit sekä tietoliikenteen solmukohtat. Näiden paikkojen havainnoinnilla saadaan kokonaiskuva fyysisestä tietoturvallisuudesta. (Porvari 2014, 186.)

Kirjatuista havainnoista saadaan dokumentti, joka sisältää lisäksi arviointimenetelmät, tehdyt toimenpiteet ja suositukset löydettyjen ongelmakohtien korjaamiseksi kustannustehokkaasti. Arviointiin liittyvät seuraavat toimenpiteet. (Thomas 2005, 371–372.)

- Toimitilojen sisäänkäyntien ja niihin liittyvien turvajärjestelmien tarkastaminen (kulkuluvat, valvontakamerat ja asiakkaiden vastaanottopisteet)
- IT-laitteiden ja – resurssien sekä paperiarkistojen fyysisten suojausmenetelmien tarkastaminen.
- Henkilökunnan tietoturvakäyttäytymisen seuranta
- Fyysisen tiedon hävittämispisteiden tarkastaminen
- Annetaan suositukset löydettyjen turvallisuusuhkien korjaamiseksi
- Tiedon varmuuskopioinnin ja tärkeiden tietojen säilytysmenetelmien tarkastaminen
- Selvitetään käytännöt vieraiden vastaanottamiseen ja liikkumiseen organisaation toimitiloissa.
- Selvitetään menettelytavat tunkeilijoita kohdatessa

### **3.4 Sovellukset tietoverkon ja -järjestelmien turvallisuuden arviointiin**

Tutkimusta varten otettiin tarkasteluun kolme ilmaista ja mahdollisimman hyvin toimivaa tietoturvan arviointisovellusta, jotka kattaisivat yhdessä sekä Windows että Linux – käyttöjärjestelmät.

Valitettavasti haavoittuvuudet ovat osa jokaista sovellus- ja laitejärjestelmää. Tietoturva-aukot tai virheellisesti asennetut järjestelmät altistavat järjestelmät hyökkäyksille. Haavoittuvuuksia hyödynnetään sekä kaupallisista että henkilökohtaisista motiiveista. Vaikka tietojärjestelmään murtautuminen on teknisesti haastavaa, onnistuneita yrityksiä on ollut tarpeeksi. Tämän vuoksi tietoturva-aukkoja ja haavoittuvuuksia tulisi etsiä ja testata ennakkoidusti. Tähän tarkoitukseen on useita kalliita kaupallisia tuotteita, mutta siihen löytyy myös loistavia avoimen lähdekoodin ilmaisia ratkaisuja, joilla päästään hyvin tuloksiin. Suosituista ja toimivista verkon turvallisuuskannereista voidaan mainita muun muassa Nmap ja OpenVAS. (LINUX for You 2012.)

On huomionarvoista muistaa, että lähes kaikissa organisaatioissa on käytössä Microsoftin Windows – käyttöjärjestelmä. Windowsin tietoturvapäivitykset ovat yksi olennainen osa sen tietoturvaa. Vaikka edellä mainitut avoimen lähdekoodin sovellukset etsivät haavoittuvuuksia ja paljastavat verkossa olevat työasemat ja palvelut,



niin Windowsin tietoturvapäivityksiä tai ylläpitäjien määrää ne eivät paljasta. Sitä varten Microsoftilla on olemassa oma työkalu tätä varten, joka on nimeltään Microsoft Baseline Security Analyzer. (WindowsITPro 2013.)

### **3.4.1 OpenVAS**

OpenVAS (Open Vulnerability Assessment System) on ilmainen avoimeen lähdekoodiin perustuva ohjelmien viitekehys, joka sisältää useita palveluja ja työkaluja, jotka toimivat yhdessä. Ohjelmaa on kehitetty Nessus – nimisen ohjelman pohjalta, joka on nykyään kaupallinen. Ohjelmakokonaisuus sisältää perusteellisen haavoittuvuuskansienetsintäskannerin sekä haavoittuvuuden hallintaratkaisun. Ratkaisun eri osat keskustelevat keskenään SSL -salatun yhteyden kautta. OpenVAS – haavoittuvuuskannetta käytetään selainpohjaisella Greenbonen Security Assistant – käyttöliittymällä, joka näkyy kuvassa 3. (Kuvio 3.)

Skanneriin päivitetään päivittäin eri puolilla maailmaa tehtävät haavoittuvuustarkastusten tulokset (NVT), joita skanneri käyttää tunnistena etsiessään uusia haavoittuvuuksia. Vuonna 2013 näitä oli yhteensä 33000. OpenVAS on laajimmin käytetty avoimen lähdekoodin haavoittuvuuskannetta. Sitä käyttää ja kehittää maailmanlaajuisesti ihmisiä tietoturva-asiantuntijoista yksittäisiin käyttäjiin. (Greenbone 2013; OpenVAS 2013.)

Greenbone Security Assistant Logged in as Admin **martti** | Logout  
Sat Mar 8 14:58:50 2014 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Tasks 1 - 1 of 1 (total: 1) No auto-refresh No overrides

Filter: apply\_overrides=0 rows=10 first=1 sort=name

Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		
<a href="#">Network security assessment</a>	1 %	0					


(Applied filter: apply\_overrides=0 rows=10 first=1 sort=name)

**Welcome dear new user!**

To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon .



**Quick start: Immediately scan an IP address**

IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the details icon and review the results collected so far.

Kuvio 3. Greenbonen toimittama OpenVAS – hallintaliittymä

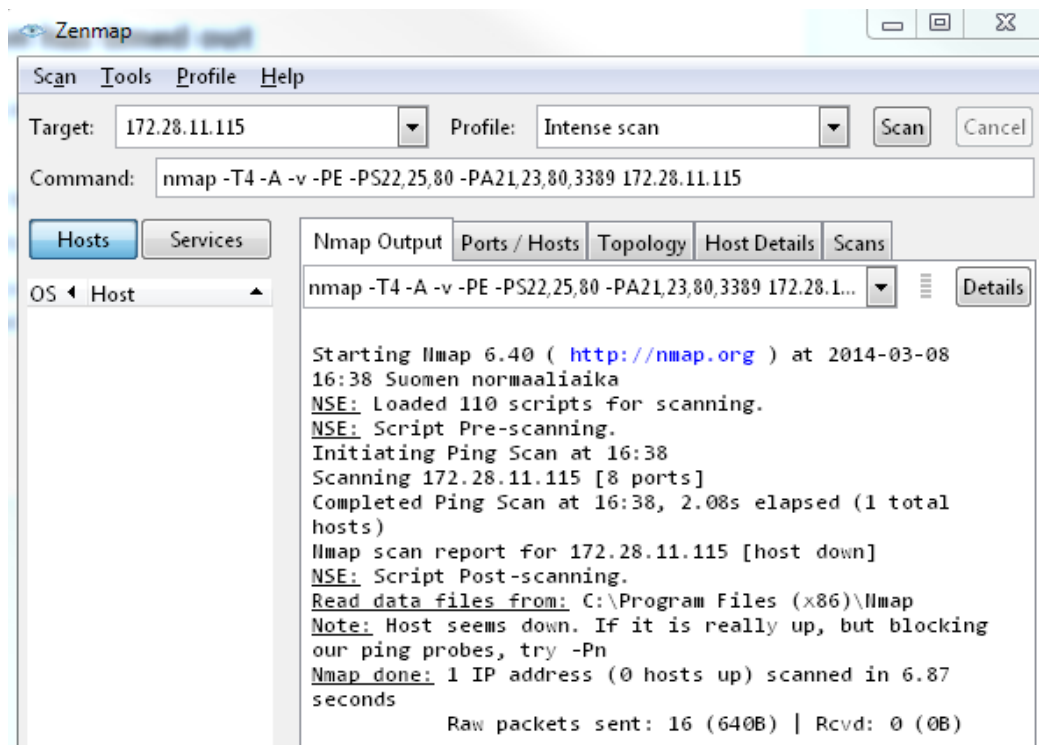
### 3.4.2 Nmap

Nmap (Network Mapper) on ilmainen avoimeen lähdekoodiin perustuva ohjelma, jolla voidaan tarkastella tietoverkkoa ja tehdä turvallisuusauditointia. Se on tunnettu ammattilaisten käyttämä työkalu, jonka avulla voidaan kartoittaa tietoverkossa olevia laitteita ja tarkastaa niissä olevat palvelut (portit), käyttöjärjestelmät sekä käynnissäoloaika. Lisäksi voidaan saada tietoja palomuurin toiminnasta ja toimintatavasta. (Lyon 2014.)

Skannauksen lopputuloksena saadaan lista skannatuista kohteista mahdollisimman kattavilla tiedoilla, riippuen tosin käytetystä skannaustavasta ja asetuksista. Kohteet listataan taulukossa, josta voi tarkastella isäntäkohtaisia lisätietoja, joita ovat isännän DNS-nimi, IP -osoite, MAC -osoite, avoimet portit, käytetyt protokollat ja palvelut, sekä käyttöjärjestelmän versio. (Lyon 2014.)

Avoimista porteista ilmoitetaan tila, joka on joko "open", "closed", "unfiltered" tai "filtered". "Open" -tila tarkoittaa, että portti on auki. "Closed" -tila tarkoittaa, että portti on kiinni. "Unfiltered" -tila tarkoittaa, että Nmap saa vastauksen skannauksiinsa, muttei pysty päättelemään, että onko portti auki vai ei. "Filtered" -tila tarkoittaa, että palomuri, pakettisuodatin tai muu este verkossa estää skannauksen. (Lyon 2014.)

Nmap tehtiin alun perin suurten verkkojen nopeaa luotausta varten, mutta se toimii yhtäläillä yksittäisiä koneita luodattaessa. Nmap on saatavilla Linux-, Windows- ja Mac OS X -käyttöjärjestelmiin. Sitä voi käyttää graafisesti tai komentoriviltä. Käytössä on huomioitava, että Nmapin tekemä porttiskannaus voidaan luokitella tietomurroksi, joten ohjelman käyttämisessä on oltava tarkkana. (Lyon 2014.) Seuraavalla sivulla on kuva (Kuvio 4.) Nmap – ohjelman graafisesta käyttöliittymästä.



Kuvio 4. Nmap – ohjelman graafisen apuohjelman Zenmapin käyttöliittymä

### 3.4.3 Microsoft Baseline Security Analyzer (MBSA)

Microsoftin omalla turvallisuustarkastusohjelmalla pystytään tarkistamaan esimerkiksi koko toimialueen työasemien tietoturvapäivitysten tila. Työasemilla olevia päivityksiä verrataan suoraan Windows Updatesta löytyviin tuoreisiin päivityksiin. Lisäksi se tunnistaa yleisimmät konfiguraatio -virheet, kuten heikot ylläpitäjän salasanat, verkkojaot sekä palomuurin tilan. Uusin versio toimii Windows 7 -käyttöjärjestelmässä sekä sitä uudemmissa Windows -työasema- ja palvelin -käyttöjärjestelmissä. Sovellusta voidaan käyttää sekä graafisesta käyttöliittymästä (Kuvio 5.) että komentoriviltä. (WindowsITPro 2013.)

Microsoft  
Baseline Security Analyzer

### Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: localhost

IP address:

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

- Check for Windows administrative vulnerabilities
- Check for weak passwords
- Check for IIS administrative vulnerabilities
- Check for SQL administrative vulnerabilities
- Check for security updates
- Configure computers for Microsoft Udate and scanning prerequisites
- Advanced Update Services options:
  - Scan using assigned Windows Server Update Services(WSUS) servers only
  - Scan using Microsoft Update only
  - Scan using offline catalog only

Learn more about [Scanning Options](#)

Kuvio 5. Microsoft Baseline Security Analyzer – ohjelman käyttöliittymä

## 4. Tietoturvakartoitus

Tietoturvakartoitusta tehtäessä on hyvä edetä suunnitelmallisesti. Aluksi määritetään kohteet, jotka ovat oleellisia tietoturvan kannalta. Tämän jälkeen mietitään tavat, joilla näistä voidaan kerätä analysoitavaa tietoa. Lopuksi suunniteltu kartoitus toteutetaan ja tulokset analysoidaan. Analyysin perusteella annetaan kehitysehdotuksia. Koska kysymys on tietoturvasta, pahimmat tietoturvaongelmat pyritään korjaamaan välittömästi niiden löydyttyä.

Tämän tietoturvakartoituksen tavoitteena on selvittää kohdeyrityksen tietoturvan nykytila ja puutteet tutkimuksen rajauksen puitteissa. Selvityksen perusteella löytyneistä puutteista annetaan kehitysehdotuksia tietoturvan parantamiseksi. Tarkoitus on, että työssä tehtyä suunnitelmaa voidaan hyödyntää jatkossakin tietoturvan ylläpidossa ja kehittämisessä. Tutkimuksen kehitystehtävänä on löytää uudelleen käytettäviä menetelmiä tietoturvan kehittämiseen, arviointiin ja ylläpitämiseen.

Työn päämenetelmänä on empiirinen eli selvitystyyppinen tutkimus. Tietoa kerätään tutkimalla ja testaamalla kohdeyrityksen järjestelmiä sekä silmämääräisellä havainnoinnilla. Lisäksi tietoturvan nykytilaa selvitetään haastatteluilla ja henkilökunnalle tehtävällä kyselytutkimuksella.

### 4.1 Kohdeyritys

Tämä opinnäytetyö tutkii Docrates Syöpäsairaalan tietoturvallisuutta. Docrates toimii terveydenhuollon alalla. Se on suomalaisomistuksessa oleva yksityissairaala, joka on erikoistunut syöpäsairauksien diagnostiikkaan, lääke- ja sädehoitoon sekä syövän seurantaan. Docrates on perustettu vuonna 2007 ja se sijaitsee Helsingin Jätkäsaarella Crusellin sillan kupeessa. Muita toimipisteitä ei tällä hetkellä ole. Docrates on Suomen suurin terveydenhoitopalveluiden vientiyritys.

Tällä hetkellä yritys työllistää vakinaisesti tai osa-aikaisesti 47 henkilöä. Näihin kuuluu muun muassa lääkäreitä, hoitajia, farmaseutteja, fyysikoita, IT-ammattilaisia sekä muita

hallinnollisia työntekijöitä. Lisäksi yritys hyödyntää ammatinharjoittajalääkäreitä, joita on 20. (Docrates Syöpäsairaala 2014.)

## 4.2 Riskien arviointi

Riskien arvioinnissa päätettiin käyttää valtionvarainministeriön tekemää riskiarviointitaulukkoa (Taulukko 1.). Taulukossa seurausten vakavuudelle ja uhan todennäköisyydelle on kolme eri tasoa. Seurausten vakavuutta arvioidaan tasoilla vähäinen, vakava ja erittäin vakava. Uhan todennäköisyyttä arvioidaan tasoilla alhainen, keskimääräinen ja korkea. Riski arvioidaan määrittelemällä riskin seurausten vakavuus vaakariviltä, jonka jälkeen määritetään riskin todennäköisyys pystysarakkeesta. Riski katsotaan näiden kohtien leikkauspisteessä olevasta arvosta. Riskitasoja on yhteensä viisi. Näitä ovat "sietämätön riski", "merkittävä riski", "kohtalainen riski", "vähäinen riski" ja "merkityksetön riski". Tuloksia tarkasteltaessa ilmoitetaan riskin kriittisyys. Kriittisyys ilmaistaan edellä mainituilla riskitasoilla.. Riskitaulukko on suuntaa antava, ja korjaustoimenpiteet on syytä päättää tapauskohtaisesti. (Valtionvarainministeriö 2003, 43.)

Taulukko 1. Riskiarviointitaulukko (Valtionvarainministeriö 2003, 43.)

Kriittisyys		Seurausten vakavuus		
		Vähäinen	Vakava	Erittäin vakava
Uhan todennäköisyys	Korkea	Kohtalainen riski	Merkittävä riski	Sietämätön riski
	Keskimääräinen	Vähäinen riski	Kohtalainen riski	Merkittävä riski
	Alhainen	Merkityksetön riski	Vähäinen riski	Kohtalainen riski

## 4.3 Suunnittelu

Tietoturvakartoitusta suunniteltaessa hyödynnettiin sekä työssä esiteltyä teorian tietoa että tekijän IT-alan kokemusta. Nämä vaikuttivat myös arviointimenetelmien valintaan. Suunnittelun alussa selvitettiin, että mitkä ovat ne kohteet, joiden tietoturvallisuutta halutaan arvioida. Tämä opinnäytetyö oli rajattu koskemaan henkilöstö-, laitteisto-, ohjelmisto-, tietoaineisto- ja tietoliikenneturvallisuutta, joten kohteet ja menetelmät valittiin näiden perusteella. Alla on selvitys siitä, mitä näihin osa-alueisiin kuuluu.

## **Tietoaineistoturvallisuus**

Tietoaineistoturvallisuuden arvioinnissa päätettiin tarkastaa tekniset varmuuskopiointiratkaisut sekä kahden käytetyimmän verkkojaon hakemistojuuren pääsyoikeudet. Tietoaineiston käsittelyä selvitetään henkilöstölle tehtävässä kyselytutkimuksessa.

## **Henkilöstöturvallisuus**

Henkilöstöturvallisuuden osalta tarkkaillaan henkilökunnan päivittäistä tietoturvakäyttäytymistä. Käyttäytymistä arvioidaan tekemällä kyselytutkimus sekä päivittäisellä havainnoinnilla. Kyselytutkimus lähetetään koko henkilökunnalle. Vastaanottajia on 47. Kyselyn vastausprosentin tavoitteeksi asetetaan 75 prosenttia. Havainnoinnissa keskitytään yleisilmeeseen, eikä arvioinnissa keskitytä yksittäisiin henkilöihin, vaan kokonaisuuteen. Havainnoinnin tulokset kirjataan anonyymisti. Tämän lisäksi haastatellaan tietohallintapäällikköä ja talousjohtajaa.

## **Laitteistoturvallisuus**

Laitteistoturvallisuutta tutkitaan tekemällä tarkastuksia kohdeyrityksen IT-laitteisiin ja niiden suojaamiskäytäntöihin. Tarkastetaan muun muassa, että verkon aktiivilaitteet on kovernettu. Tarkastusten lisäksi henkilökunnan henkilökohtaisten laitteiden turvallisuutta selvitetään kyselytutkimuksella.

## **Ohjelmistoturvallisuus**

Ohjelmistoturvallisuuden osalta tarkastetaan, että käyttöjärjestelmien päivitykset ovat ajan tasalla. Tarkastetaan myös pahimmat konfigurointivirheet. Yrityksen käyttämistä sisäisistä ja ulkoisista pilvipalveluista tehdään lyhyt katsaus turvallisuuden saralta.

## **Tietoliikenneturvallisuus**

Tietoliikenneturvallisuutta tarkastellaan erilaisilla verkon skannausohjelmilla sekä kohdeyrityksen sisäverkosta että ulkoverkosta. Tutkitaan, että minkälaisia palveluita

verkossa olevilla laitteilla on avoinna, ja että mitä asioita yrityksestä voidaan saada selville Internetin kautta tehtävillä skannauksilla.

### **4.3.1 Käytettävät arviointimenetelmät**

Edellä mainitut viisi osa-aluetta sisällytettiin 12:sta eri arviointimenetelmään. Jokaisessa arviointimenetelmässä kerrotaan, että mihin osa-alueisiin kyseinen arviointi liittyy. Lisäksi kerrotaan tarkemmat tiedot arviointimenetelmästä sekä sen tavoitteista.

Verkkojen skannauksissa päätettiin tehdä kompromissi ja jättää hoito- ja kuvantamislaitteisiin liittyvien laitteiden tiukemmin suojatut verkot skannaamatta, jotta välttyttäisiin mahdollisilta ongelmilta. Olisi ollut mahdotonta arvioida etukäteen, että miten esimerkiksi verkossa kiinni oleva PET-TT -laite olisi reagoanut skannauksiin. Tästä ei ollut aiempaa tutkimustietoa saatavilla. Tämän lisäksi skannaamatta jätettiin langaton vierasverkko, koska haluttiin kunnioittaa asiakkaiden yksityisyyttä. Pahimmassa tapauksessa asiakkaan tietoturvaohjelmisto olisi ilmoittanut tietoturvapoikkeamasta, joka olisi tullut Docrateen sisäverkosta. Tämä olisi voitu luokitella tietoturvaloukkaukseksi, josta kerrottiin alaluvussa 2.7.4. Seuraavaksi tarkastellaan arviointimenetelmiä. Arviointimenelmien otsikot on numeroitu ja niihin viitataan jälkikäteen numeroiden perusteella.

#### **1. Porttiskannaus**

Nmap – sovelluksella on tarkoitus tehdä selvitys verkosta löytyvistä työasemista, palvelimista sekä avoimista porteista ja palveluista. Tavoitteena on saada selville verkossa mahdollisesti esiintyviä uhkia. Skannaustulosten perusteella saadaan tieto muun muassa siitä, että onko verkkoon liitetyillä laitteilla sellaisia portteja auki verkkoon päin, jotka ovat tunnetusti haavoittuvia tai haittaohjelmien käyttämiä. Lisäksi selvitetään samat asiat ulkoverkon puolelta. Tämä menetelmä kuuluu tietoturvan osa-alueista tietoliikenneturvallisuuteen. Ohjelman tarkempi esittely ja toiminnallisuus löytyvät alaluvusta 3.4.2.



## **2. Haavoittuvuusskannaus**

Haavoittuvuusskannaus tehdään teoriaosuuden alaluvussa 3.4.1 esitellyllä OpenVAS – sovelluksella. Tietoturvan osa-alueista se kuuluu tietoliikenne- ja ohjelmistoturvallisuuteen. Tavoitteena on löytää Docrateen tietoverkossa olevista laitteista ja ohjelmistoista haavoittuvuuksia, joista voidaan lopuksi antaa sekä korjaus että kehitysehdotuksia.

## **3. Monitoimi- ja verkon aktiivilaitteiden tarkastaminen**

Tätä menetelmää käytetään yhdessä menetelmän 1. ja 2. kanssa. Menetelmä kuuluu tietoturvan osa-alueista tietoliikenne- ja laitteistoturvallisuuteen. Aluksi tarkastetaan manuaalisesti, että onko laitteisiin asetettu salasana, ja että onko salasana niin sanottu vahva salasana. Salasanojen vahvuus saadaan kysymällä asiaa tietohallintopäälliköltä. Tämän lisäksi katsotaan, että onko käytetty yhteysmuoto salattu. Lopuksi tarkastetaan Nmap -ja OpenVAS – sovellusten raporteista, että mitä portteja kyseisillä laitteilla on auki, ja mitkä ovat niiden mahdolliset haavoittuvuudet. Tavoitteena on selvittää, että ovatko monitoimi- ja verkon aktiivilaitteet konfiguroitu turvallisiksi.

## **4. Pintapuolinen tarkastus yrityksen käyttämiä pilvipalveluita varten**

Tämä tarkastusmenetelmä on nimensä mukaisesti suppea. Menetelmällä tarkastetaan, että käytetäänkö pilvipalveluja suojatun yhteyden kanssa (SSL) vai ei. Tavoitteena on selvittää yrityksen käyttämien pilvipalveluiden turvallisuus loppukäyttäjän kannalta. Lisäksi tarkastetaan, että palveluissa vaaditaan tarpeeksi monimutkaisia salasanoja, ja että niitä pitää vaihtaa tietyin väliajoin. Muut tehdyt havainnot kirjataan ylös. Tämä menetelmä kuuluu tietoturvan osa-alueista ohjelmistoturvallisuuteen.

## **5. Havainnointikierros toimipisteen tietokoneiden käyttötiloihin**

Tarkastuksen yhteydessä selvitetään, löytyykö tietokoneiden välittömästä läheisyydestä käyttäjätunnuksia kirjattuna paperilapulle tai luottamuksellisia tietoja selkeästi esillä. Samalla tarkastetaan tietosuojaroskisten tilanne sekä tilaan pääsy. Tavoitteena on

selvittää henkilökunnan tietoturvakäyttäytymistä. Tämä menetelmä kuuluu henkilöstöturvallisuuteen.

## **6. Mobiililaitteiden turvallisuus**

Mobiililaitteiden turvallisuutta selvitetään menetelmän 10. kyselytutkimuksessa ja haastatteluin. Mobiililaitteiden turvallisuudesta selvitetään hyvien PIN- ja suojakoodien käyttö. Kannettavien tietokoneiden osalta selvitetään, että onko tietokoneen kovalevy salattu. Lisäksi selvitetään käytössä olevien mobiililaitteiden etätyhjennysmahdollisuudet varkaustilanteissa. Tavoitteena on selvittää, että onko mobiililaitteiden käyttö hyvien turvallisuusperiaatteiden mukaista. Tämä menetelmä kuuluu laitteisto- ja henkilöstöturvallisuuteen.

## **7. Windows -ja Linux -palvelimien turvallisuushavainnointi**

Tarkastetaan palvelimista manuaalisesti, että ne ovat tietoturvan osalta konfiguroitu oikein. Tämä tehdään niin, että käydään Windows- ja Linux -palvelimille tehdyt tarkistuslistat läpi. Tavoitteena on löytää selviä virheitä, jotka voidaan korjata pienellä vaivalla. Tarkistuslistoilla selvitetään alla olevat asiat. Tämä menetelmä kuuluu tietoturvan osa-alueista ohjelmistoturvallisuuteen.

### Windows

- Onko palomuuuri päällä?
- Onko palomuuuri konfiguroitu?
- Onko tietoturvaohjelmisto asennettu?
- Onko palvelimella ylimääräisiä käyttäjätilejä?
- Onko etäyhteys on kovennettu? (NLA)
- Onko tietoturvapäivityksiä asentamatta?
- Tarkastetaan asennetut ylimääräiset sovellukset

### Linux

- Onko pääkäyttäjän (root) etäkirjautuminen otettu pois käytöstä? (SSH)

- Onko root – käyttäjä poistettu käytöstä?
- Onko turvallisempi julkisen avaimen -menetelmään perustuva kirjautuminen käytössä? (SSH)
- Onko turvattomampi salasanakirjautuminen käytössä? (SSH)
- Onko palomuuuri päällä?
- Onko palomuuuri konfiguroitu?
- Onko tietoturvapäivityksiä asentamatta?
- Onko palvelimella ylimääräisiä käyttäjätilejä?

## **8. Microsoft Baseline Security Analyzer**

Tällä menetelmällä tarkastetaan työasemien tietoturvapäivitysten ajantasaisuus, sekä mahdolliset konfigurointivirheet. Tavoitteena on saada tiedot kaikista toimialueen Windows -työasemista tekemällä etäskannaus, jotta säästettäisiin aikaa. Menetelmää voidaan näin hyödyntää jatkossakin. Tämä menetelmä kuuluu tietoturvan osa-alueista ohjelmistoturvallisuuteen. Ohjelman esittely löytyy alaluvusta 3.4.3.

## **9. Kahden eniten käytetyn verkkojaon oikeuksien tarkastaminen**

Tätä menetelmään varten luotiin liitteenä 1. oleva PowerShell – skripti, jolla voidaan puoliautomaattisesti tarkastaa kahden eniten käytetyn verkkojaon juurihakemistojen käyttöoikeudet. Skripti tulostaa hakemistojen käyttöoikeudet CSV -tiedostoon, josta niitä on helppo tarkastella. Lopputulos käydään läpi tietohallintopäällikön kanssa. Samalla selviää, että onko jollain vahingossa käyttöoikeudet johonkin hakemistoon, vaikka ei pitäisi olla. Tämä menetelmä kuuluu tietoturvan osa-alueista tietoaineistoturvallisuuteen.

## **10. Tietoturvakysely ja haastattelut**

Haastatellaan yrityksen tietohallintopäällikköä ja talouspäällikköä. Haastattelun kysymykset löytyvät liitteistä 2. ja 3. Tavoitteena on, että haastatteluilla saadaan kuva yrityksen tietoturvan nykytilasta. Haastatteluissa on kysymyksiä tämän tietoturvakartoituksen kaikista osa-alueista. Haastattelujen lisäksi tehdään

tietoturvakysely yrityksen henkilöstölle, jolla pyritään selvittämään yrityksen henkilöstön tietoturvakäyttäytymistä.

## 11. Varmuuskopiointiratkaisujen tarkastaminen

Tarkastetaan yrityksen käyttämä varmuuskopiointimenetelmä ja siihen liittyvät toimenpiteet yhdessä tietohallintopäällikön kanssa. Tavoitteena on varmistaa, että käytetty menetelmä on varma ja turvallinen sekä toimii mahdollisessa tietojenmenetys – tilanteessa. Tämä menetelmä kuuluu tietoturvan osa-alueista tietoaineistoturvallisuuteen.

## 12. Tietoturvaohjelmistopalvelimen tarkastaminen

Tässä menetelmässä tarkastetaan keskitetyn tietoturvahallintaohjelmiston hallinnan kautta, että mikä tilanne kohdeyrityksessä on haittaohjelmien ja virusten suhteen. Lisäksi tarkastetaan, että kuinka herkästi järjestelmä ilmoittaa tietoturvapoikkeamista järjestelmän ylläpitäjille. Tavoitteena on, että kaikki tietoturvallisuuteen liittyvät poikkeamat ilmoitetaan yrityksen IT-henkilöstölle. Tämä menetelmä kuuluu tietoturvan osa-alueista ohjelmistoturvallisuuteen.

### 4.3.2 Arviointimenetelmien painotus

Suunnittelussa haluttiin tarkastella eri arviointimenetelmien painotusta eri osa-alueiden välillä. Osa arviointimenetelmistä sisältyi useampaan osa-alueeseen. Teknistä osa-aluetta painotettiin hieman enemmän, kuten taulukosta 2 näkyy.

Taulukko 2. Tietoturvakartoituksen painotus

<b>Tietoturvan osa-alue</b>	<b>Käytetyt menetelmät</b>
Tietoaineisto	9, 10, 11
Henkilöstö	5, 10, 6
Laitteisto	3, 10, 6
Ohjelmisto	2, 4, 7, 8, 10, 12
Tietoliikenne	1, 2, 3, 10

#### 4.4 Toteutus

Tietoturvakartoitus toteutettiin suunnitelmassa esiteltyjä menetelmiä käyttäen. Toteutus aloitettiin testaamalla tutkimusmenetelmissä esiteltyjä ohjelmia. Niiden toiminta optimoitiin tutkimuksen tavoitteita silmällä pitäen.

Ohjelmilla saatiin selville yrityksen teknisen tietoturvan taso. Tietoturvakyselyllä (Liite 4.) ja haastatteluilla (Liitteet 2. ja 3.) saatiin selville yrityksen tietoturvatietämys ja -käytännöt. Samalla selvisi henkilöstön tietoturvakäyttäytyminen. Havainnointikierros ja loput menetelmät yhdistämällä saatiin kattava näkemys yrityksen tietoturvan nykytilasta. Tulosten perusteella annettiin kehitysehdotuksia.

## 5. Pohdinta

Opinnäytetyön tekeminen avasi näkemystä tietoturvan osalta. Tutkimustyö tietoturvan parissa oli erittäin mielenkiintoista. Työtä tehdessä oppi laajasti tietoturvan periaatteita ja tietoturvan kartoituksessa tarvittavia asioita. Löydetyt tietoturvaongelmat olivat mielenkiintoisia, eikä niitä olisi ennen aiheeseen perehtymistä tullut edes ajateltua.

Aihe ei ollut tekijälle entuudestaan niin tuttu kuin sen ehkä olisi pitänyt olla, joten aiheen valinta oli hyvä. Sitä varten oli pakko opiskella lisää. Opinnäytetyötä varten oli käyty kolme tietoturvakurssia, mutta työtä tehdessä huomasin, että kurssit olivat vain pintaraapaisu aiheeseen. Aiheeseen perehdyttäessä uutta tietoa tuli koko ajan vastaan ja siitä löytyi asioita, joita ei tämän tutkimuksen puitteissa ehtinyt selvittämään. Aiheen opiskelu ja siihen syvällisempi perehtyminen tulee jatkumaan tämän opinnäytetyön valmistuttua.

Työ opetti paljon tietoturvallisuudesta. Tietoturvallisuuden periaatteet ovat nyt selvillä ja tekijällä on nyt edellytykset tietoturvan parissa työskentelyyn sekä opitun hyödyntämiseen käytännössä.

Tutkimus rajattiin vain viiteen tietoturvan osa-alueeseen käytössä olevan ajan vähyyden vuoksi. Jotta tutkimuksesta olisi saatu vielä kattavampi, tulisi kolme viimeistä tietoturvan osa-aluetta tutkia. Nämä olivat fyysinen-, hallinnollinen ja käyttöturvallisuus. Jatkossa voitaisiin tutkia tarkemmin muita tietoturvallisuuden teknisiä arviointimenetelmiä.

### 5.1 Ajankäyttö

Ajankäytöllisesti työ ei onnistunut suunnitellusti. Teoriaosuuden tekemiseen oli varattu liian vähän aikaa ja se valmistui kaksi viikkoa myöhässä. Ohjausryhmän kokoukset pidettiin suunnitelman mukaisesti. Tutkimusta tehdessä kävi ilmi, että tekijällä on vielä kehitettävää ajan käytön hallinnassa sekä projektityöskentelyssä aikataulun mukaisesti. Ajankäytön ongelmista huolimatta työ valmistui määräaikaan mennessä.

## 5.2 Menetelmävalinnat ja tutkimuksen luotettavuus

Tutkimusongelmana oli löytää helppokäyttöisiä, uudelleenkäytettäviä, turvallisia ja kattavia menetelmiä tietoturvan kehittämiseksi ja ylläpitämiseksi.

Suurin osa menetelmävalinnoista oli onnistuneita ja niistä saadut tutkimustulokset olivat mielestäni luotettavia. Sekä haastatteluja että kyselytutkimusta analysoidessa ja verratessa muihin käytettyihin menetelmiin huomattiin, että asiat kohtaavat. Tekijä työskentelee itse kohdeyrityksessä. Tämän takia ei voida sanoa täysin varmasti, että kaikki löydökset olisivat objektiivisia. Voidaan kuitenkin todeta, että tietoturvan kartoittamista ei häiritty millään tavalla, vaan tarvittavaan tietoon päästiin käsiksi. Opinnäytetyön sidosryhmät olivat yhteistyökykyisiä.

Työssä olisi voitu selvittää tasapuolisemmin valittuja tietoturvan osa-alueita. Työ painottui hieman enemmän tekniseen kuin havainnolliseen ja fyysiseen puoleen. Ajan käyttöön olisi voitu myös kiinnittää enemmän huomiota. Suurin haaste työtä tehdessä oli se, että tekijä oli osittain samanaikaisesti töissä Docrateen IT-tuessa. Tämä haittasi aika ajoin keskittymistä tutkimuksen tekemiseen. Tutkimus saatiin kuitenkin suunniteltuun päivämäärään mennessä valmiiksi.

## 5.3 Tulosten hyödynnettävyys

Tutkimuksesta saadut tulokset dokumentoitiin tarkasti. Dokumentointi tehtiin niin, että tietoturvaan liittyviä epäkohtia voidaan korjata ja kehittää suoraan sen pohjalta. Käytännössä tulokset ovat suoraan yrityksen hyödynnettävissä ja niistä on helppo lähteä miettimään tietoturvan jatkokehittämistä löydettyjen ongelmakohtien perusteella. Lisäksi tutkimuksen teoriaosuus saattaa auttaa tietoturvan tärkeyden ymmärtämisessä ja huomioon ottamisessa.

## Lähteet

Andreasson, A., Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tietosanoma. Helsinki.

Andreasson, A., Koivisto, J., Ylipartanen, A. 2013. Tietosuojavastaavan käsikirja. Tietosanoma. Helsinki

Compton, S. 2007. 802.11 Denial of Service Attacks and Mitigation. Luettavissa: <http://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108>. Luettu 8.3.2014.

Docrates Syöpäsairaala 2014. Docrates Syöpäsairaala. Luettavissa: <http://www.docrates.com/fi/docrates>. Luettu 12.2.2014.

Greenbone 2013. OpenVAS. Luettavissa: <http://www.greenbone.net/technology/openvas.html>. Luettu 25.2.2014.

Hakala, M., Vainio, M., Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Docendo. Jyväskylä.

Laakso, M. 2010. Todentaminen ja kiistämättömyys. Luettavissa: <http://www.tietoesiturvaksi.fi/content/todentaminen-ja-kiist%C3%A4m%C3%A4tt%C3%B6myys>. Luettu 13.1.2014.

Laaksonen, M., Nevasalo, T., Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Edita. Helsinki.

LINUX For You 2012. Top 10 Security Assessment Tools. Luettavissa: <http://www.linuxforu.com/2012/02/top-10-security-assessment-tools/>. Luettu 26.2.2014.



Lyon, G. 2014. Nmap Reference Guide. Luettavissa:  
<http://nmap.org/book/man.html>. Luettu 25.2.2014.

Mäki, M. 2007. Työntekijä pahin tietoturvauhka pk-yrityksessä. Luettavissa:  
<https://ssl.ttlry.fi/tutkimus/pk-tietoturvatutkimus>. Luettu 4.2.2014.

OpenVAS 2013. About OpenVAS. Luettavissa: <http://www.openvas.org/about.html>.  
Luettu 25.2.2014.

Paavilainen, J. 1998. Tietoturva. Suomen ATK-kustannus Oy. Espoo.

Paavilainen, J. 2013. Kyberturvallisuus sairaalaympäristössä. STM valmiusseminaari.  
Luettavissa:  
[http://www.stm.fi/c/document\\_library/get\\_file?folderId=7705948&name=DLFE-26627.pdf](http://www.stm.fi/c/document_library/get_file?folderId=7705948&name=DLFE-26627.pdf). Luettu 26.1.2014.

Porvari, P. 2014. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Unigrafia. Espoo.

Ruohonen, M. 2002. Tietoturva. Docendo. Jyväskylä.

Sarja, J. 2005. Turvallista matkaa. Luettavissa:  
<http://www.verkkopedagogi.net/vanhat/fi/sisalto/materiaalit/tietoturva/luku016e4a.html?C:D=419124&selres=419124>. Luettu 17.2.2014.

Sosiaali- ja terveysministeriö 2007. Tietoturvallisuussuunnitelman laatiminen. Opas sosiaali- ja terveydenhuollon toimintayksiköille. Luettavissa:  
[http://www.stm.fi/c/document\\_library/get\\_file?folderId=28707&name=DLFE-3722.pdf&title=Tietoturvallisuussuunnitelman\\_laatiminen\\_\\_Opas\\_sosiaali\\_\\_ja\\_terveydenhuollon\\_toimintayksikoille\\_fi.pdf](http://www.stm.fi/c/document_library/get_file?folderId=28707&name=DLFE-3722.pdf&title=Tietoturvallisuussuunnitelman_laatiminen__Opas_sosiaali__ja_terveydenhuollon_toimintayksikoille_fi.pdf). Luettu 16.1.2014.

Suvilehto, J. 2011. Tietoturva. Luettavissa: <http://www.cse.tkk.fi/fi/opinnot/T-110.1100/2011/luennot-files/05.Tietoturva.pdf>. Luettu 14.3.2014.

Thomas, T. 2005. Verkkojen tietoturva. Edita. Helsinki.

Ylipartanen, A. 2010. Tietosuoja terveydenhuollossa. 3. uudistettu painos. Tietosanoma Oy. Helsinki.

WindowsITPro 2013. Microsoft Baseline Security Analyzer 2.3 Adds Support for Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2.

Luettavissa: <http://windowsitpro.com/security/microsoft-baseline-security-analyzer-23-adds-support-windows-8-windows-81-windows-server-20>. Luettu 8.3.2014.

# Liitteet

## Liite 1. PowerShell – skripti

```
# Skriptin lähteitä:
# http://mywinsysadm.wordpress.com/2011/08/17/powershell-reporting-ntfs-permissions-of-windows-file-shares/
# http://mywinsysadm.wordpress.com/2011/08/17/powershell-execution-of-scripts-is-disabled-on-this-system/
# http://technet.microsoft.com/en-us/library/ee692801.aspx
# http://blogs.technet.com/b/heyscriptingguy/archive/2013/06/26/powertip-use-a-powershell-command-to-get-user-name-and-domain.aspx

# Skriptin ajamiseksi skriptien ajon täytyy olla päällä. Tilanteen voit tarkastaa komennolla: "Get-ExecutionPolicy"
# ajo-oikeudet voit asettaa komennolla "Set-ExecutionPolicy RemoteSigned". Alkutilanteeseen päästää komennolla "Set-ExecutionPolicy Restricted"

# Skripti kysyy käyttäjältä hakemiston, jonka alikansioiden oikeudet se tarkastaa, seuraavaksi kysytään tiedostonimi, johon tulokset tulostetaan.
# Tallennusmuoto on CSV, jotta tuloksia voidaan suoraan tarkastella Excelissä.

# Määritetään muuttujat

$starkastettavaPolku = Read-Host "Syötä hakemisto, josta oikeudet tarkistetaan. Esim. C:\ tai C:\Users"
$stallennusTiedosto = Read-Host "Syötä nimi tiedostolle, johon raportti tallennetaan"
$ilmoitus = "Tämä skripti tallentaa $starkastettavaPolku -alihakemistojen oikeudet c:\$stallennusTiedosto.csv -tiedostoon"
$stiedote = "Alla $starkastettavaPolku -alihakemistojen oikeudet"
$ilmoitus

# Viedään määritetyn alihakemiston hakemistot taulukkoon

[Array] $alihakemistot = Get-ChildItem -path $starkastettavaPolku -force | Where {$_.PSIsContainer}

# Lasketaan alihakemistojen määrä

$hakemistojenMaara = $alihakemistot.Count

# Määritetään lisää muuttujia mm. kellonaika ja päivämäärä, sekä skriptin ajanut käyttäjä muodossa domain/user

$pvm = Get-Date -format d.M.yyyy
$klo = Get-Date -format t
$skayttaja = whoami
$tyhjaTila = ""
$saikaLeima = "Tämän raportin loi $skayttaja $pvm klo $klo. Hakemistoja yhteensä: $hakemistojenMaara"
$erotin
="*****"

# Tulostetaan päivämäärä ja aika, sekä tiedoston luonut käyttäjä tiedostoon. Tulostetaan myös hakemisto, josta oikeudet on katsottu, sekä erottimet ja tyhjät rivit

$saikaLeima | Out-File -append "C:\$stallennusTiedosto.csv"
$tyhjaTila | Out-File -append "C:\$stallennusTiedosto.csv"
$stiedote | Out-File -append "C:\$stallennusTiedosto.csv"
$tyhjaTila | Out-File -append "C:\$stallennusTiedosto.csv"
```

```
$erotin | Out-File -append "C:\$tallennusTiedosto.csv"  
$tyhjaTila | Out-File -append "C:\$tallennusTiedosto.csv"
```

```
# Käydään $alihakemistot sisältävä taulukko läpi Foreach -silmukalla ja listataan niiden oikeudet tiedostoon rivi riviltä
```

```
ForEach ($hakemisto in [Array] $alihakemistot) {
```

```
    $muotoiltuPolku = (Convert-Path $hakemisto.pspath)
```

```
    $listaa = ("Polku: $muotoiltuPolku")
```

```
    $listaa | format-table | Out-File -append "C:\$tallennusTiedosto.csv"
```

```
    Get-Acl -path $muotoiltuPolku | Format-List -property AccessToString | Out-File -append  
"C:\$tallennusTiedosto.csv"
```

```
    } # Päätetään Foreach -silmukka
```

```
# Tulostetaan loppuun erotin-viiva tiedoston päättymisen merkiksi
```

```
$erotin | Out-File -append "C:\$tallennusTiedosto.csv"
```

## Liite 2. Haastattelukysymyksiä talousjohtajalle

1. Kuinka usein varmuuskopionauhoja vaihdetaan tai pitäisi vaihtaa?
2. Kuinka usein varmuuskopionauhoja viedään esimerkiksi pankin tallelokeroon? (turvalliseen paikkaan yrityksen ulkopuolelle)
3. Varmuuskopiointinauhoja säilytetään melko avoimella paikalla serverihuoneessa. Kenellä kaikilla on huoneeseen pääsy?
4. Onko yrityksellä valmiita käytäntöjä tietomurtojen tai tietoturvaloukkausten käsittelyyn (sekä sisäisiin että ulkoisiin)?
5. Miten varmistetaan, että rekrytoitava työntekijä on luotettava?
6. Onko Docrateen johto sitoutunut tietoturvan kehittämiseen ja ylläpitoon?
7. Onko tietoturva-asioista tehty ohjeita eri tilanteisiin?
8. Onko tietoturvapoliittikka voimassa? Onko se julkinen?
9. Onko ohjelmistojen ja laitteiden asentamiselle selkeät periaatteet, kenellä on oikeus tehdä niitä?
10. Onko tietosuojaroskisten tyhjennyksestä käytäntöä? Esimerkiksi kuinka usein ne tulisi tyhjentää?
11. Kuinka tarkasti potilastietojen- ja asiakirjojen käsittelyä on ohjeistettu?
12. Mikä on yrityksen käytäntö byod:n osalta (bring your own device)?
13. Miten varmistutaan, että entinen työntekijä ei pääse tietojärjestelmiin? Onko prosessi suunniteltu?
14. Milloin yrityksessä on viimeksi pidetty tietoturvakoulutus?
15. Mikä on käytäntö vierailijoiden osalta? Täytyykö heillä olla aina saattaja vai saako vierailija kulkea omin päin?
16. Onko yritystä vastaan koskaan tehty tietomurtoa tai tietoturvaloukkausta. Jos on, miten asia on hoidettu?

17. Miten tietosuojajäte käsitellään.
18. Luokitellaanko yrityksessä käsiteltäviä tietoja?
19. Säilytetäänkö tietosuojanalaista sähköistä ja fyysistä tietoa asianmukaisesti?
20. Onko tietosuojanalaisten materiaalien käsittelystä tulostus- tai kopiointiohjeistusta?
21. Onko yrityksellä jatkuvuussuunnitelmaa?
22. Entä toipumissuunnitelmaa?
23. Onko tietoturvan toteuttamiseen varattu riittävästi resursseja?
24. Onko yrityksessä käytössä ns. puhtaanpöydän politiikka?
25. Onko tämä laajennettu koskemaan myös näyttöjä?
26. Tarkastetaanko henkilöiden antamien tietojen oikeellisuus työhaastattelussa?
27. Tehdäänkö henkilöille turvallisuus selvitys työhönoton yhteydessä?
28. Saavatko uudet työntekijät riittävän tietoturvakoulutuksen tietojärjestelmien käyttöön?
29. Tehdäänkö työntekijöiden kanssa sopimus tietojärjestelmän tunnuksia vastaan?
30. Sisältääkö sopimus tietojärjestelmän käyttö säännöt?
31. Onko yrityksen avainhenkilöstölle olemassa varahenkilöt?
32. Järjestetäänkö yrityksessä säännöllistä tietoturvakoulutusta?
33. Varmistetaan työsuhteen päättyessä, että henkilö ei pääse käsiksi yrityksen tietojärjestelmiin?
34. Onko työasemien ja laitteiden käyttötilat suojattu ulkopuolisten pääsystä vastaan?
35. Onko henkilökunta tietoinen tietosuoja- ja tietoturvavastuusta?

### Liite 3. Haastattelukysymyksiä tietohallintopäällikölle

1. Kuinka usein varmuuskopionauhoja vaihdetaan tai pitäisi vaihtaa?
2. Kuinka usein varmuuskopionauhoja viedään esimerkiksi pankin tallelokeroon?
3. Onko tietoturva-asioista tehty ohjeita eri tilanteisiin?
4. Onko kannettavissa tietokoneissa levyn salaus?
5. Onko ohjelmistojen ja laitteiden asentamiselle selkeät periaatteet, kenellä on oikeus tehdä niitä?
6. Kuinka usein työasemien salasanoja vaihdetaan?
7. Mikä on yrityksen käytäntö byod:n osalta (bring your own device)?
8. Milloin yrityksessä on viimeksi pidetty tietoturvakoulutus?
9. Onko yritystä vastaan koskaan tehty tietomurto tai tietoturvaloukkaus. Jos on, miten asia on hoidettu?
10. Onko yrityksen sisäinen verkko eristetty Internetistä palomuurilla?
11. Entä langaton verkko?
12. Seurataanko verkon liikennettä esimerkiksi lokien avulla?
13. Tuleeko tietoturvapoikkeamista ilmoitus ylläpidolle?
14. Käytetäänkö verkon- ja palvelimien hallinnassa suojattuja yhteyksiä?
15. Onko verkon aktiivilaitteet kovennettu?
16. Onko langattomat verkot suojattu?
17. Todennetaanko käyttäjät ennen sisäverkkoon pääsyä?
18. Onko porttikohtainen todentaminen käytössä?
19. Käytetäänkö uusien laitteiden asennuksessa tarkistuslistaa, jonka avulla varmistutaan, että tietoturva-asetukset ovat kunnossa?
20. Onko yrityksessä käytössä aktiivinen virustorjuntajärjestelmä?
21. Saako ylläpito ilmoituksen virustartunnoista?

22. Onko laitteiden ja palvelimien lokien hallinta ja seuranta keskitetty?
23. Onko tietoverkon rakenne dokumentoitu?
24. Miten mobiililaitteiden ja tallennusmedioiden turvallisuus varmistetaan?
25. Jos jokin näistä esimerkiksi varastetaan, miten varmistetaan, että tieto ei päädy kolmannelle osapuolelle?
26. Onko tietosuojanalaisen materiaalien käsittelystä tulostus- tai kopiointiohjeistusta?
27. Ovatko käytetyt salausratkaisut ajantasaisia ja riittävän turvallisia?
28. Onko yrityksellä jatkuvuussuunnitelmaa?
29. Entä toipumissuunnitelmaa?
30. Onko etätyöskentely mahdollista tietoturvallisella tavalla?
31. Onko etätyöskentely koulutettu tietoturvallisuuden osalta?
32. Tehdäänkö verkkoon säännöllisiä haavoittuvuusskannauksia, jotta varmistutaan, ettei tunnettuja heikkouksia ole?
33. Korjataanko tietoturvapoikkeamat ja -uhat heti?
34. Onko tietoturvan toteuttamiseen varattu riittävästi resursseja?
35. Onko yrityksessä käytössä ns. puhtaanpöydän politiikka?
36. Onko tämä laajennettu koskemaan myös näyttöjä?
37. Huolehditaan säännöllisestä varmuuskopioinnista?
38. Saavatko uudet työntekijät riittävän tietoturvakoulutuksen tietojärjestelmien käyttöön?
39. Tehdäänkö työntekijöiden kanssa sopimus tietojärjestelmän tunnuksia vastaan?
40. Järjestetäänkö yrityksessä säännöllistä tietoturvakoulutusta?
41. Tiedotetaan henkilöstölle uusista yritystä koskevista tietoturvauhista?
42. Varmistetaan työsuhteen päättyessä, että henkilö ei pääse käsiksi yrityksen tietojärjestelmiin?
43. Onko työasemien ja laitteiden käyttötilat suojattu ulkopuolisten pääsyä vastaan?



44. Onko henkilökunta tietoinen tietosuoja- ja tietoturvavastuusta?
45. Onko työasemilla työn kannalta turhia sovelluksia?
46. Tarkastetaanko näitä?
47. Ylikirjoitetaanko laitteiden tallennustila, jos laite joutuu huoltoon tai se poistetaan käytöstä?
48. Onko palvelimissa virustorjuntaohjelmisto käytössä?
49. Entä palomuuuri?
50. Onko työasemissa virustorjuntaohjelmisto käytössä?
51. Entä palomuuuri?
52. Käyttääkö yritys vain laillisia ohjelmistoja?
53. Onko yrityksessä roskapostisuodatus käytössä?
54. Onko eri käyttötarkoituksiin asennettu eri selaimia?
55. Hallitaanko selainten asetuksia keskitetystä esimerkiksi ryhmäkäytännöillä?

#### Liite 4. Tietoturvakysely

1. Käytätkö työpuhelimesiasi PIN -koodia? (PIN -koodi on yleensä nelinumeroinen koodi, jota kysytään puhelinta käynnistäessä. PIN -koodi avaa SIM-kortin lukituksen ja mahdollistaa muun muassa puhelut)
2. Käytätkö työpuhelimesiasi suojakoodia? (Suojakoodi on yleensä viisinumeroinen koodi, jota kysytään, kun näyttö laitetaan päälle.)
3. Onko työpuhelimesi PIN- tai suojakoodi jokin seuraavista: 1234, 4321, 0000, 12345,54321 tai oma syntymäpäivä?
4. Muodostuuko salasanasi jostain sanakirjasta löytyvästä salasanasta ja sen numero- ja merkkiyhdistelmästä? (Esimerkiksi TyöSalasana984# tai WorkMate468#)
5. Käytätkö samaa salasanaa tai sen muunnosta kaikissa palveluissa?
6. Säilytätkö käyttäjätunnuksia selväkielisenä paperilla?
7. Entä selväkielisenä sähköisessä muodossa?
8. Otatko huomioon ympäristön, kun puhut yrityksen sisäisistä asioista tai potilastiedoista?
9. Lukitsetko työhuoneesi kun poistut lounaalle tai muulle pidemmälle käynnille?
10. Lukitsetko työasemasi/kannettavasi, kun poistut huoneestasi?
11. Lähetätkö potilastietoja sähköpostitse?
12. Entä tekstiviestitse?
13. Tiedätkö, mitä eroa on verkkosivun osoitteen edessä olevalla http:llä tai https:llä?
14. Käytätkö työpuhelinta/kannettavaa ilmaisissa langattomissa verkoissa? Esimerkiksi kahvilan WLAN -verkkoa.
15. Oletko saanut tietoturvakoulutusta Docrateella?
16. Tiedätkö, kenelle tietoturva- tai tietosuojapoikkeamista ilmoitetaan?
17. Tiesitkö, että henkilötietoja tai muuta salassa pidettävää tietoa ei saa välittää internetissä suojaamattomana?
18. Tiedätkö, mitä edellisessä kysymyksessä mainittu suojaus tarkoittaa, ja miten voit sen tarkistaa?

Liite 5. Docrateen tietoturvakartoitus (Salattu)