LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Tietoturvan taso ja kehityskohteet

– Case Laurea Service Desk

Haaksivuori, Tuomas
Simonen, Erja

Laurea-ammattikorkeakoulu

Tietoturvan taso ja kehityskohteet – Case Laurea Service Desk

Haaksivuori Tuomas
Simonen Erja
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Huhtikuu, 2016

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittely

Haaksivuori Tuomas, Simonen Erja

Tietoturvan taso ja kehityskohteet – Case Laurea Service Desk

Vuosi 2016 Sivumäärä 31

Tämä opinnäytetyö on osa toimeksiantajan, Laurea-ammattikorkeakoulun, tietoturvakatsausta. Työn tavoitteena oli tehdä kattava katsaus Laurea Service Desk'in tietoturvan tasosta nykyhetkellä sisältäen parannusehdotukset mahdollisiin ongelmakohtiin.

Opinnäytetyön keskeisimpiä työvälineitä olivat Laurea-ammattikorkeakoulun omat aineistot tietoturvasta, tietojenkäsittelyn viitekehykset ja tehdyt kyselyt. Tutkimuksen kohteen Service desk'in tärkeimpiä työkaluja ovat: Service Manager Console, Active Directory sekä Keepass. Käyttäjätunnuksia käytetään useita erilaisia tilanteesta riippuen. Kaikilla eri käyttäjätunnuksilla on lisäksi omat salasanansa. Service desk'issä on tärkeää perehdyttää uudet harjoittelijat ja käyttää saatua tietoa tietoturvallisesti. Asiakaspalvelu ja asiakkaiden tunnistaminen ovat tärkeitä toimintoja. Asiakaspalvelussa on käytössä erilaisia tekniikoita ja ohjelmistoja. Tietoturvallisuudessa on tärkeää tietoturvatietoisuus ja – vastuullisuus, joka on saavutettavissa riittävällä tiedottamisella, koulutuksella ja perehdyttämisellä.

Tärkeimmiksi tuloksiksi nousivat Service Desk-tilojen epäkäytännöllisyys, salasanakäytänteiden tehostaminen, tietoturva-aineiston lisääminen perehdytykseen ja vastuuhenkilön nimeäminen tietoturva-asioihin liittyen.

Avainsanat: Tietoturva, Service desk, Help desk, Lähituki, Etätuki, Asiakaspalvelu, BSI, Katakri, Vahti

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology

Haaksivuori Tuomas, Simonen Erja

The Level of Information Security and Targets for Improvement – A Case of Laurea Service Desk

Year 2016 Pages 31

This thesis is a part of Laurea University of Applied Sciences information security overview. The primary goal is to become familiar with Service Desk's information security and the level the information security including the best ways of solving the possible problems.

The main tools for this thesis are the documents given by Laurea University of Applied Sciences, the frameworks of information technology and most importantly an inquiry. In the Service Desk, the main tools however are Service Manager Console, Active Directory and Keepass. Different types of usernames and passwords are used in different work situations. When a new trainee starts to work at the Service Desk, it is essential to familiarize him/her with his/her new job. In Laurea, there are many different methods that can be used to recognize the customer and customer service has a large role. Informing about information security is also a part of working at Laurea's Service Desk.

The most valuable results were that the Service Desk room is impractical, the password policy should be enhanced, interns training in the work should be provided with more information about information security and the person who is in charge of information security should be named more clearly.

Keywords: Information security, Service desk, Help desk, Onsite, Remote help, BSI, Katakri, Vahti

Sisällys

1 Johdanto

Opinnäytetyö on tutkimuksellinen työ ja se on toteutettu yhteistyössä Laurea-ammattikorkeakoulun, myöhemmin Laurea, Service desk'in kanssa. Tavoitteena on luoda laaja-alainen raportti tietoturvan nykytilanteesta, sen ongelmakohdista sekä antaa kehitysehdotuksia ongelmiin liittyen. Fyysisen tilan osalta keskitymme Leppävaaran toimipisteen Service desk'iin, sillä suurin osa työstä keskittyy sinne.

Laurean Service desk toteutetaan pääsääntöisesti harjoittelija voimin. Yhtäaikaisesti siellä työskentelee viidestä kuuteen harjoittelijaa ja heitä tukee 13 vakituista työntekijää. Harjoittelijat hoitavat 70–75 % kaikista työpyynnöistä. Service desk'in työtehtävät koostuvat puhelinpalvelusta, lähitukitilanteista sekä sähköpostitse tulevista työpyynnöistä eli tiketeistä. Jokaisesta työpyynnöstä kirjataan tiketti ja mikäli Service desk'in harjoittelija ei pysty hoitamaan tikettiä loppuun, se ohjataan asiantuntijoille. Työtehtävät ovat laadultaan erittäin monipuolisia pienistä salasanan uusimisista ja koneiden asennuksista kytkinkaappien kaapelointiin.

Pääasiallinen tutkimusongelma on, onko tietoturva tarvittavan korkealla tasolla Service desk'issä. Tätä tutkitaan perehtymällä mahdollisimman kokonaisvaltaisesti toimintaan ja mitä teoreettiset lähteet kertovat hyvistä menettelyistä. Tietoturvan jatkuva kehittyminen tekee aiheesta aina mielenkiintoisen ja ajankohtaisen. Tästä syystä on myös hyvä perehtyä, onko tietoturva tässä ympäristössä ajan tasalla.

Opinnäytetyö aloitetaan kertomalla välineistä, joita käytetään Service desk'in työssä sekä niiden merkityksestä. Tämän jälkeen edetään kronologisessa järjestyksessä käyttäjätunnuksiin, Service desk'in sisäiseen toimintaan, kuten perehdytykseen, asiakaspalveluun, tiedottamiseen sekä lopuksi annamme parannusehdotuksia.

2 Tutkimusvälineet

Leppävaaraan keskittyy Service desk'in puhelinpäivystys ja suuri osa lähitukitehtävistä, joten suurin osa harjoittelijoista työskentelee Leppävaarassa. Toinen kampus, jossa on vakituisesti harjoittelija paikalla, on Tikkurila. Siellä on yhdestä kahteen harjoittelijaa vakituisesti. Otaniemessä, Keravalla, Hyvinkäällä, Porvoossa sekä Lohjalla on harjoittelija paikalla vain tarvittaessa.

Itse työ aloitettiin tiiviissä yhteistyössä Laurean kanssa määrittelemällä työn raamit sekä tutkimusongelma. Tämän jälkeen keskitimme huomiomme teoriaan, jota saatiin lukuisista eri lähteistä ja tämän tutkimuksen pohjalta nousi esiin kysymyksiä. Saatujen tietojen pohjalta luotiin kaksi kyselyä. Lopputuloksena saimme kokonaisvaltaisen kuvan tietoturvallisuuden tilasta Laurean Service desk'issä sekä pystyimme antamaan parannusehdotuksia.

Opinnäytetyön tekemisen kannalta tärkeimpiä työkaluja olivat siis tietoturvallisuuden auditointityökalu viranomaisille eli Katakri, saksalainen IT-Grundschutz, Laurean omat aineistot tietoturvasta sekä kyselyt. Toteutimme kaksi erillistä teemakyselyä. Toinen oli suunnattu vakituiselle henkilöstölle kuten asiantuntijat ja ylläpitäjät ja toisessa kyselyssä keskityttiin enemmän harjoittelijoiden työtapoihin ja välineisiin. Tällä tavalla pyrittiin saamaan mahdollisimman laaja näkemys tietoturvallisuuden tilasta eri näkökulmista. Toteutusmuodoksi valittiin e-Lomake, sillä tämä ratkaisu todettiin parhaaksi opinnäytetyön tekijöiden kannalta. Katakri on puolustusministeriön johdolla yhdessä eri viranomaisten sekä elinkeinoelämän kanssa laatima kansallinen auditointikriteeristö, joka on myös saanut Yhdysvaltojen kansallisen turvallisuusviraston eli NSA:n yhteistyöryhmän hyväksynnän. Katakri on työkalu, jota voidaan käyttää, kun arvioidaan valitun kohdeorganisaation tietoturvallisuusjärjestelyjä viranomaisten salassa pidettävien tietojen käsittelemiseksi. Työkalu on jaoteltu kolmeen eri osaan, turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus. Tässä opinnäytetyössä hyödynnettiin enimmäkseen viimeistä osa-aluetta eli teknistä tietoturvallisuutta. IT-Grundschutz on Saksan Bundesamt für Sicherheit in der Informationstechnik'in, vapaasti suomennettuna kansallinen tietoturvallisuuden virasto, laatima viitekehys, joka koostuu moduuleista. Moduuli koostuu määritelmästä, riskiskenaariosta, uhkista sekä suojausmenettelyistä. Uhkat ja suojausmenettelyt on myös luetteloitu erikseen eri kategorioiden alle. IT-Grundschutz on erittäin monipuolinen työkalu tilanteiden arviointia varten. (Puolustusministeriö 2015, 3; National Security Agency 2011; Bundesamt für Sicherheit in der Informationstechnik 2013, 2-3.)

3 Service desk'issä käytettävät työtavat ja työkalut

Nykypäivänä yrityksissä tehdään paljon töitä tietokoneiden, tablettitietokoneiden ja puhelimien avulla, unohtamatta muita oheislaitteita, jotka ovat osa tai tukevat näitä laitteita. Näistä syistä yrityksissä ja organisaatioissa on välttämätöntä tuottaa tukitoimintoja näille laitteille ja niiden käyttäjille. Service desk'issä tukitoimintoja hoidetaan puhelinpalvelun, etätuen sekä lähituen kautta, jotta saadaan asiakkaalle mahdollisimman vaihtoehtoiset tavat ottaa yhteyttä ongelmansa tiimoilta ja saada ratkaisu niihin haluamallaan tavalla.

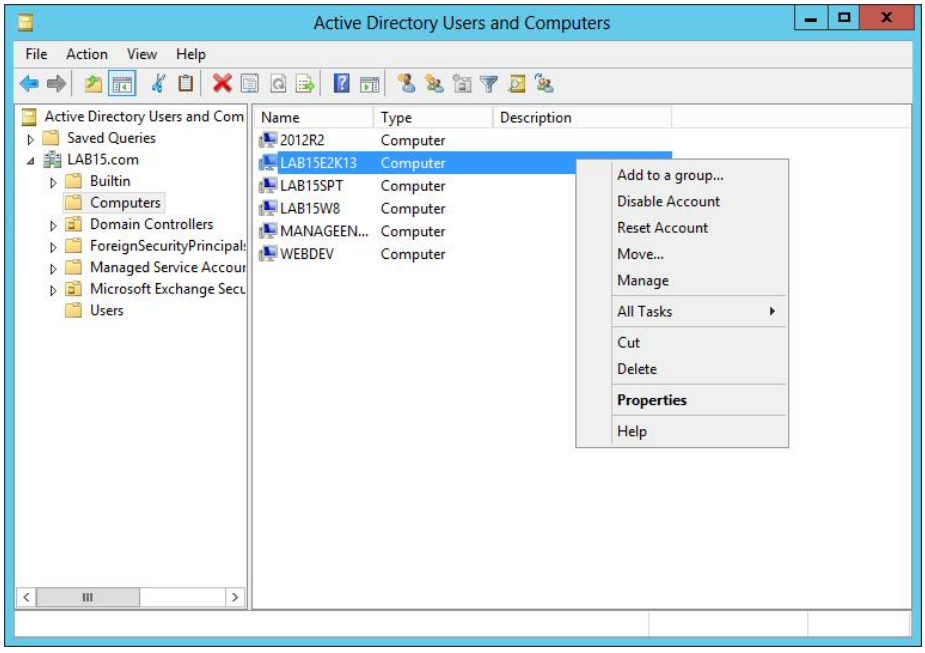
Laurea Service-Desk'in työntekijöillä on käytössään tietokoneet, jotka on varusteltu kahdella eri näytöllä samanaikaisten työtehtävien hoitamista varten. Lisäksi jokaisella työntekijällä on käytössä työpuhelin sekä Applen iPad.

3.1 Service Manager Console

Tärkein ohjelmisto työntekoon liittyen Service desk'issä on tikettijärjestelmä nimeltään Service Manager Console. Tikettijärjestelmään kirjataan puhelimitse tulleet työpyynnöt, etätukitilanteissa hoidetut työpyynnöt sekä lähitukitilanteissa hoidetut työpyynnöt, näiden lisäksi järjestelmä kirjaa itse tukipyynnöt, jotka ovat tulleet sähköpostin kautta Service desk'in osoitteeseen. Kaikki työt kirjataan järjestelmään, jotta asiantuntijat voivat seurata kuinka paljon työpyyntöjä tulee esimerkiksi kuukausittain, mistä aiheista näitä tulee eniten, kuka niitä ratkoo sekä missä tilanteessa keskeneräinen työ on. Tikettijärjestelmän avulla voidaan myös seurata työn laatua. Työn laadun seuranta on tärkeää, jotta palveluita osataan tulevaisuuden kannalta kehittää esimerkiksi tilanteessa, jossa tulisi paljon tukipyyntöjä liittyen salasanan vaihtamisongelmiin. Näinn voidaan luoda selkeämmät ohjeet isoimpiin ongelmakohtiin tai toisena esimerkkinä useat yhteydenotot jonkin ohjelmiston tietoturvaan liittyen.

3.2 Active Directory

Tikettijärjestelmän lisäksi työn tukena käytetään Microsoft Windowsin ohjelmistoa nimeltä Active Directory. Ohjelman käyttötarkoitus on hallinnoida käyttäjien oikeuksia, käyttäjäryhmiä sekä tietokoneiden saamia oikeuksia. Näin esimerkiksi voidaan hallinnoida eri kampuksien työntekijöiden oikeuksia verkon yli jaettuihin kansioihin. Hallinnointi on yleistä, sillä Laureassa on paljon harjoittelijoita, ketkä suorittavat projekteja tai harjoittelujaksoja opintoihin liittyen. Active Directory toimii myös niin sanottuna laiterekisterinä, sillä sinne viedään tiedot esimerkiksi henkilökunnan tietokoneista, niiden käyttäjistä ja mahdollisesta työtilasta. Active Directory'n avulla myös ryhmitellään tietokoneet eri kampuksille ja luokkiin, jolloin voidaan hallita tietokoneelle System Center Configuration Manager'in kautta asentuvia ohjelmia.

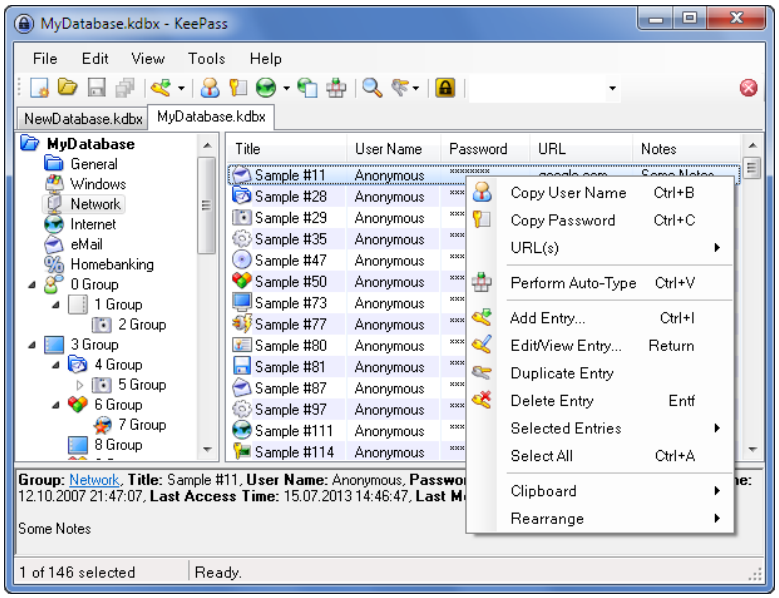


Kuva 1: Esimerkki Active Directoryn tietokoneet näkymästä

3.3 Keepass

Service desk'in työntekijät käyttävät työn tukena Keepass-ohjelmaa, mikä auttaa salasanojen hallinnassa, sillä tietoturvallisuussyistä jokaiseen palveluun pitää olla eri salasana. Kyseinen ohjelma helpottaa näiden muistamista sekä hallinnointia (Keepass 2016).

Keepass-ohjelma toimii siten, että sen tietokantaan syötetään kaikki tunnukset ja salasanat ja käyttäjän tarvitsee itse muistaa vain Master salasana päästäkseen tietokantaan käsiksi. Kuitenkin tietoturvallisuuden näkökulmasta käyttäjän täytyy olla erittäin huolellinen Master salasanansa kanssa. Mikäli salasana unohtuu, tietokantaan jossa salasanat ovat, ei enää pääse käsiksi.



Kuva 2: Keepass-ohjelman ulkoasu.

Erilaisten ohjelmistojen lisäksi työntekoa helpottamassa ovat Front desk-työpiste sekä erillinen asennuspöytä. Front-desk'in ensisijaiseksi tarkoitukseksi kuvattiin kyselyssä Service desk'in henkilökunnan työrauhan ja tietoturvallisuuden kasvattaminen sekä asiakkaiden huoltotoimenpiteiden ja ongelmien kartoitus. Asennuspöytä on tarkoitettu nimensä mukaisesti asennustöiden tekemiseen. Pöydälle mahtuu noin 4-5 kannettavaa tietokonetta, joka mahdollistaa monen asiakkaan palvelemisen yhdessä osassa Service desk'in tilaa.

Etätyöskentelyn mahdollistamiseksi Service desk'issä käytetään pääsääntöisesti TeamViewer ohjelmaa ja tämän lisäksi myös Remote Desktop ohjelmaa, mutta tämän käyttö on hieman vähäisempää. Etätyökalut ja niiden toiminta avataan tarkemmin myöhemmässä kappaleessa

4 Käyttäjätunnukset

Yleisiä periaatteita käyttäjätunnuksista viitekehykset kertovat hyvin kattavasti. Katakri kertoo vähimpien oikeuksien periaatteesta, joka pitää sisällään kaksi vaatimusta. Ensimmäinen määrää, että käyttäjille annetaan tiedot, oikeudet ja valtuudet niihin tietoihin, jotka ovat välttämättömiä työtehtävien suorittamiseksi. Toinen kertoo oikeushallinnalla toteutettavasta salassa pidettävän tiedon luvattomasta käytöstä tai muuttamisesta. IT-Grundschutz puhuu samasta asiasta ”Need-to-know” nimellä. Katakri työkaluna antaa esimerkkejä kuinka mainitut vaatimukset voidaan toteuttaa eri tietojen suojaustasoilla. Tärkeimmät Laureassa toteutuvat esimerkit ovat:

1. Käyttöoikeuksia määrittelee käyttäjille vain kampusten paikallinen ylläpitäjä.
2. Käyttöoikeuksia voi pyytää vain henkilöt, joilla on siihen oikeudet. Yleensä käyttäjän, kenelle oikeudet tulevat, esimies.
3. Jokaisesta oikeuspyynnöstä jää sähkököinen dokumentti tikettijärjestelmään.
4. Oikeudet tarkistetaan välittömästi, kun niihin tulee muutoksia.

Bundesamt für Sicherheit in der Informationstechnik (BSI) mainitsee kappaleessaan vastaavien esimerkkien lisäksi, kuinka on tärkeää tietää myös kuka voi hätätilanteessa antaa lisäoikeuksia. Tämä sama asia tuli kyselyssä esille osittain kysyttäessä käytettävistä tunnuksista ja niiden eroista, joten tämä asia on otettu Laureassa huomioon. Seuraavassa kappaleessa perehdymme enemmän tähän asiaan (Puolustusministeriö 2015, 38; Bundesamt für Sicherheit in der Informationstechnik 2013, 1295).

4.1 Hallinta ja käyttö

Service desk’issä vähimpien oikeuksien periaate toteutuu kaksien eri käyttäjätunnusten avulla, jotta yleisiin työtehtäviin ei tarvitse käyttää liian tehokkaita tunnuksia. Yleisissä työtehtävissä Service desk’issä käytetään henkilökuntatunnusta, joka on samanlainen tunnus kuin kaikilla Laurean henkilöstön jäsenillä. Haastattelussa kysyttiin kuka tunnuksen tilaa uudelle työntekijälle ja vastaus on uuden käyttäjän esimies. Hakemuksessa vaaditaan vähintään nimi, henkilötunnus, työsuhteen laatu sekä -kesto ja monesti myös muuta tietoa. Allekirjoitettu työsopimus on myös ehdoton edellytys käyttäjätunnuksen saamiseksi. Laurean henkilökunnan tietoturvaopas neuvoo käsittelemään tunnusta kuin omaa henkilökohtaista pankkikorttia, valitsemaan sille mahdollisimman vahvan salasanan, joka pitää sisällään kolmea eri merkkityyppiä. Tärkeä oppaan neuvo on, että jokainen käyttäjä on itse henkilökohtaisesti vastuussa omasta käyttäjätunnuksestaan sekä siihen liittyvästä salasanasta. Käyttäjätunnus pysyy samana koko työsuhteen ajan mahdollisesta nimenmuutoksesta huolimatta. Vain äärimmäisissä erikoistilanteissa voidaan käyttäjähallinnan harkinnan mukaan lähteä vaihtamaan käyttäjän

käyttäjätunnusta. Yleisesti käytäntönä on, että avioliitto tai avioero ei ole tarpeeksi väkevä syy tällaiselle toimenpiteelle. (Kysely 2016; Laurea 2015d, 2-3)

Service desk'in työntekijöillä on lisäksi käytössään henkilökohtainen järjestelmänylläpitäjätunnus. Tämän kaltainen tunnus on käytössä ainoastaan tietohallinnon työntekijöillä. Eräs vastaaja täsmensi kyselyssä, että on ehdottoman tärkeää Service desk'in harjoittelijan hahmottaa, milloin tulee käyttää henkilökuntatunnusta ja milloin järjestelmänvalvojan tunnusta. Tällä varmistetaan tietoturvaa sekä voidaan tilaisuuden vaatiessa tarkistaa mitä toimenpiteitä ja kuka on työn kohteena olevalle koneelle tehnyt.

Kolmas Service desk'issä käytettävä tunnus on paikallinen järjestelmänvalvojan tunnus. Paikallista järjestelmänvalvojantunnusta ei käytetä kuin tilanteissa, joissa konetta ei saada Laurean LAN, eli Local Area Network, verkkoon. Tällöin kone ei voi hakea Service desk'in työntekijän henkilökohtaisen ylläpitäjäntunnuksen tietoja nimipalvelimelta, joten on pakko käyttää paikallista tunnusta. Tämän kaltaisia tilanteita ovat etänä tehtävät ylläpitotoimet joissa käyttäjä ulkoverkossa ja tilanteet joissa konetta ei erilaisista mekaanisista syistä saada langalliseen verkkoon. Verkko saattaa olla koneen asetuksista poistettu käytöstä tai mahdollisesti verkkokortti on hajonnut. Paikallisen järjestelmänvalvojantunnuksen huonoja puolia ovat ne, ettei jälkikäteen voida todentaa kuka on koneelle asentanut tiedostoja sekä lisäksi salasanan huono vaihtuvuus. Kyselyssä tulee yksimielisesti vastauksista ilmi, ettei tätä salasanaa vaihdeta läheskään tarpeeksi usein. Tämä tunnus voidaan myös luokitella tietoturvariskiksi edellä mainitusta syystä. Paikallinen järjestelmänvalvojan tunnus on kuitenkin välttämätön pakko työn sujuvuudelle.

Henkilökunnan tietoturvaopas ohjeistaa kuinka toimia työsuhteen päättyessä. Koska käyttäjätunnukset ovat sidottuja työsuhteeseen, tunnukset suljetaan välittömästi työsuhteen päättymisen jälkeen. Sulkemista ennen tulee käyttäjän huolehtia mahdollisesta henkilökohtaisista tiedoistaan sähköpostissa tai verkkolevyasemilla. Tärkeämpää tunnuksen sulkeminen on kuitenkin tietoturvan kannalta, sillä organisaatioon kuulumaton henkilö ei näin pääse enää järjestelmiin ja mikäli työsuhde ei pääty rauhallisissa merkeissä käyttäjä saattaisi aiheuttaa suurtakin vahinkoa. (Laurea 2015d, 7; Kysely 2016)

4.2 Salasanakäytänteet

Salasanat ovat olennainen osa käyttäjätunnuksia ja niiden turvallisuutta ja siksi niiden tulee olla mahdollisimman vaikeasti murrettavia. Salasanojen vaihdon yleisissä Laurean ohjeissa kerrotaan vaatimukset henkilökunnan käyttäjätunnuksille. Perusehdot ovat, että salasanan tulee olla vähintään kahdeksan merkkiä pitkä sekä tulee sisältää kolmea eri merkkiluokkaa. Merkkiluokkia ovat pienet aakkoset, suuret aakkoset, numeraalit sekä erikoismerkit. Lisäksi

on erikoisehtoja kuten kielto käyttää salasanassa edes osaa käyttäjätunnuksesta eikä samaa salasanaa voi käyttää kahta kertaa peräkkäin. Salasana normaaleissa henkilökuntatunnuksissa vanhenee neljän kuukauden välein ja vanhenemisesta saa käyttäjä useita sähköpostimuistutuksia. Samoin kuten Microsoft artikkelissaan Vihjeitä vahvojen salasanojen ja tunnuslauseiden luomiseksi Laurea suosittelee käyttämään salasana eli tunnuslausekkeita. Vihje artikkelissaan Microsoft määrittelee mikä on tunnuslauseke. Tunnuslauseke luodaan käyttäjälle henkilökohtaisesta lauseesta, joka pitää sisällään numeraalin. Esimerkiksi käyttäjä voi käyttää lausetta ”Aloitin opiskelut Laureassa 2013 tammikuussa” tunnuslausekkeena. Tästä lauseesta otetaan sanojen ensimmäisiä sekä mahdollisesti viimeisiä kirjaimia ja luodaan salasana ”AnotLa13ta”. Vielä vahvemman salasanasta saa lisäämällä siihen erikoismerkkejä esimerkiksi ”AnotL@13t@” (Laurea 2015d; Microsoft 2016).

Työntekijöiden henkilökohtaiset järjestelmänvalvojantunnuksien salasanat ovat periaatteessa hyvin samanlaisia, mutta niiden turvallisuus vaatimukset ovat hiukan korkeammat. Salasanan tulee olla 10 merkkiä pitkä kyselyn mukaan ja tämä kerrotaan työsuhteen alussa, kun Service desk’in työntekijä saa kyseisen tunnuksen sekä vaihtaa salasanan ensimmäisen kerran. Henkilökohtaiset järjestelmänvalvojantunnuksen salasanat vanhenevat kolmen kuukauden välein ja oman kokemuksen mukaan tämän salasanan vanhenemisesta saa muistutusta muutoin, kun kirjautumalla koneelle kyseisellä tunnuksella ja Windowsin ilmoituskeskus kertoo salasanan vanhenemisesta.

5 Service desk’in sisäinen toiminta

Laurea Service desk’in tavoitteena on tehostaa ja auttaa tietotekniikkaan liittyvissä asioissa, sen henkilöstöä ja opiskelijoita, jotta opiskelu, opetus ja muut näihin liittyvät tukitoiminnot toimivat asianmukaisesti. Service desk’in palveluaika on arkisin normaaliin 8.00–16.00 toimistoaikaan sillä siihen aikaan pääsäännöllisesti tapahtuu kaikki opetustoiminta sekä henkilöstön työaika on sama. Service desk palvelee käyttäjiä puhelimitse, sähköpostitse, itsepalveluportaalin kautta tai palveluaikaan lähitukena. Näillä yhteydenottotavoilla saadaan toteutettua hyvä palvelun saatavuus. Saatavuus on tärkeää, sillä Service desk’in tavoitteena on palvella kyselyn mukaan noin 7500 opiskelijaa ja 500:a henkilöstön jäsentä mahdollisimman laadukkaasti kaikissa ongelmissa, jotka liittyvät Laurean tietokoneisiin. Service desk’issä työskentelee viidestä kuuteen harjoittelijaa, ketkä työskentelevät ensisijaisesti tikettien kanssa ja 14 vakituista työntekijää, ketkä ovat ylläpitäjiä ja eri osa-alueiden asiantuntijoita. Yhteydenottoja ja tikettejä tuleekin Service desk’iin noin 700–800 kuukaudessa (Laurea 2015b; Kysely 2016).

5.1 Perehdytys

Perehdyttäminen on tärkeä osa työtä ja sen kirjaaminen työturvallisuuslakiin (738/2002) korostaa tärkeyttä. Laissa määritellään, että työnantaja on velvollinen perehdyttämään uuden työntekijän esimerkiksi työhön, ihmisiin, tarvittaviin työvälineisiin sekä toimintatapoihin. IT-Grundschutz käsittelee asiaa ensimmäisessä henkilöstöön liittyvässä suojausmenettely osassa ensimmäisessä kappaleessa, joka on sisällöltään hyvin samanlainen kuin laki. Molemmat lähteet kertovat kuinka tärkeää on korkeatasoinen perehdytys. Tietojenkäsittelyalalla tämä tarkoittaa myös perehdyttämistä tietoturvaympäristöön, -sääntöihin sekä -organisaatioon. Hyvällä perehdytyksellä voidaan estää työntekijöiden virheellinen toiminta (Työturvallisuuskeskus 2003, 12; Bundesamt für Sicherheit in der Informationstechnik 2013, 2413)

Laureassa perehdytys yleisiin organisaatio asioihin tapahtuu lähimmän esimiehen toimesta perehdytysmateriaalien avulla, mitkä käydään läpi ensimmäisen kahden päivän aikana. Kuitenkin suurin osa työhön ja toimintatapoihin perehtymisestä tapahtuu vanhempien kollegojen toimesta. Uusi työntekijä seuraa heidän toimintaansa sekä aloittaa yksinkertaisimpien työtehtävien tekemisen heidän valvonnassaan. Perehtymiskausi on noin kahden viikon mittainen ennen kuin harjoittelijalla alkaa puhelinpäivystykset. Kuitenkin työn ja harjoittelun luonne on tyypiltään sellainen, että oppimista tapahtuu koko harjoittelujakson ajan. Tietoturvallisuuden kannalta haastavinta on perehdyttää harjoittelija turvallisiin käytänteisiin ja tietoturva koulutusta voisikin lisätä huomattavasti harjoittelujakson alkuun.

5.2 Sähköisen tiedon käsittely

Sähköistä tietoa tulee käsitellä yhtä tarkkaan kuin kirjoitettua tietoa. Kuten IT-Grundschutz sekä Laurean Tietoturvaopas henkilöstölle kertovat, suojauksen perusasia on pitää huolta muistitikusta tai vastaavasta laitteesta, jos tietoja on sellaiselle tallennettu. Muistitikkua ei suositella tietojen tallennussijainniksi, sillä ne katoavat helposti tai rikkoontuvat lisäksi muistitikut ovat harvoin salattuja. Muistitikun kadotessa myös kaikki tiedot päätyvät erittäin suurella todennäköisyydellä vääriin käsiin varsinkin salaamattomalta muistitikulta. Toimistossa muistitikkua tulee IT-Grundschutz'in mukaan säilyttää samoin lukituissa kaapissa kuin paperistakin tietoa silloin kun muistitikku pitää sisällään luottamuksellista tai salaista materiaalia. Laurean henkilöstöllä on käytössään verkkolevyasemat tietojen tallennusta varten ja sinne tallentaessa ei tarvitse huolehtia tiedon fyysisestä katoamisesta. Tietoturvaopas neuvoo käyttämään tätä ensisijaisena tallennussijaintina, sillä verkkolevystä myös otetaan varmuuskopioita jolloin tiedon perus käytettävyys ja eheys säilyvät. Nykyään on käytössä myös mobiililaitteita ja näitä tietoturvaopas neuvoo suojaamaan samanlaisin keinoin kuin tietokoneita. Mobiililaitteeseen tulee aina asettaa näytönsuojakoodi, jotta laitetta ei pysty ulkopuolinen avaamaan, turhia yhteyksiä, kuten WLAN tai Bluetooth, ei tule olla käytössä, kun niitä ei tarvitse ja lisäksi tulee aina miettiä mitä ohjelmia mobiililaitteeseen asentaa. Bundesamt für Sicherheit in der Informationstechnik 2013, 1203; Laurea 2015d, 5-6)

Service desk'issä tietoa siirretään paljon suoraan henkilöltä toiselle suullisesti, joten on oltavana tarkkana, ketä tilassa on tällaisissa tapauksissa. Samoin sähköpostitse siirrettävän tiedon kanssa on oltava tarkka. Sähköpostit kulkevat verkossa täysin salaamattomina, joten niitä voi ulkopuolinen lukea välistä. Välistä lukemisen estämiseksi Laurea on ottamassa käyttöön sähköpostin salaustyökalun. Samoin tulee myös ottaa huomioon, millaista tietoa voidaan erilaisiin sijainteihin tallentaa. Mikäli Service desk'issä tulee käsiteltäväksi salassa pidettävää tietoa, kuten tietoturvallisuuteen liittyvää tietoa, sitä ei tule tallentaa julkisiin tallennuspaikkoihin, vaan Laurean omille palvelimille kuten aikaisemmin mainittiin.

5.3 Toimistokäyttäytyminen

Service desk'issä vierailee päivittäin useita Laurean henkilökunnan jäseniä sekä opiskelijoita ja tämän takia toimitilan tietoturvallisuus ja siihen liittyvä käyttäytyminen on äärimmäisen tärkeää. Valtiovarainministeriön henkilöstön tietoturvaohjeessa kehotetaankin noudattamaan seuraavia asioita tilan turvallisuuden suhteen;

- Tietokoneiden näytöt eivät saa olla suunnattuina asiakkaihin päin
- Huolehdi tietokoneiden, USB-tikkujen, paperisten asiakirjojen asianmukaisesta säilytyksestä
- Salassa pidettävä tieto ei saa olla esillä muun muassa Front desk- tai asennuspöydillä
- Eksyneiden / vieraiden ohjaaminen oikeaan paikkaan, asiattomilta pääsy kielletty

Toimistotilan yleinen siisteys on siis avainasemassa tietoturvallisuuden näkökulmasta, asiattomille ei saa antaa mahdollisuutta arkaluontoisten tai salassa pidettävien tietojen urkintaan. Valtiovarainministeriön toimitilojen turvallisuusohjeessa sanotaan, että tärkeimpiä IT-laitetilaa koskevia riskejä ovat muun muassa tietoturvaloukkaus ja tietovarkaus. Tätä voidaan myös soveltaa hyvin Service desk'in tilaan, sillä tilassa on lukuisia tietokoneita, oheislaitteita sekä tallennusvälineitä, joita pahimmassa tapauksessa epäsiisteyden takia voidaan varastaa, tarkastella ilman lupaa tai käyttää tarkoituksellisesti väärin, näiden seikkojen takia tavaroiden oikeaoppinen suojaaminen ja säilöminen sekä yleisen siisteyden ylläpito ovat hyvin tärkeitä (Valtionvarainministeriö 2013a, 34; Valtiovarainministeriö 2013b, 55).

Service desk'issä työtehtäviin liittyy paljon muistettavaa ja näitä asioita voi kirjoittaa muun muassa muistilapuille ylös, ottaen huomioon tiedon vakavuuden. Suotavaa olisi kuitenkin käyttää vihkoa tai jotain vastaavaa tiedon ylläpitämiseen liittyen, sillä muistilaput voivat unohtua esimerkiksi asennuspöydälle, joka taas aiheuttaa epäsiisteyttä sekä mahdollisesti tiedon vuodattamista sellaisille henkilöille kenelle asia ei kuulu. Mikäli harjoittelija käyttää esimerkiksi vihkoa tietojen ylläpitämiseen, sitä on helpompi kantaa mukana aina kun siirtyy työpisteeltä toiselle.

Yleisen siisteyden lisäksi toimistokäyttäytyminen on iso osa niin normaalia työntekoa kuin asiakaspalvelutilanteita. Itse asiakaspalvelutilanteita ja niiden hyviä piirteitä käsitellään lisää luvussa kuusi. Suositeltavaa olisi, että harjoittelija pysyy selvillä siitä, että ketä tilassa on silloin kun ottaa asian puheeksi, jota jonkun ulkopuolisen ei kuulu tietää.

Toimistokäyttäytymisessä on myös toinen puoli—se miten käyttäytyy työtovereilleen eikä pelkästään asiakkaille. Hyvät käytöstavat ovat tärkeitä Service desk'issä työskenteleville, sillä siellä sekä vakituinen henkilökunta että harjoittelijat tekevät tiivistä yhteistyötä. Tämä tarkoittaa sitä, että puhelinpäivystäjällä ei ole juurikaan omaa tilaa toimia ja keskittyä asiakaspalveluun, varsinkin jos taustalla on liikaa häiriötekijöitä. Tällaisissa tilanteissa muiden harjoittelijoiden kuuluisi osata lukea tilannetta ja käyttäytyä siten, että puhelinpäivystäjä saa työlleen tarvittavan rauhan ja pystyy pitämään kiinni laadukkaasta asiakaspalvelusta. Lisäksi myös tästä syystä on tärkeää pyrkiä rajaamaan lähitukea hakevat käyttäjät Front desk puolelle.

6 Asiakaspalvelu

Harjoittelijan työkuvaa varten ei vaadittu aiempaa työkokemusta muun muassa asiakaspalvelu tai IT-alan työtehtävistä, mutta kyseiset taidot laskettiin hakijan eduksi, ainoina selkeinä vaatimuksina hakijalle oli asetettu suomen ja englannin kielitaito.

Service desk'issä työtä tehdessä tärkeintä asiakaspalvelutehtävien suorittamisessa oli positiivinen asenne sekä hyvä ongelmanratkaisukyky, jotta sujuva ja asianmukainen palvelu saatiin toteutettua alusta loppuun.

6.1 Service desk'in tilassa

Hyvän asiakaspalveluhenkilön tunnusmerkkejä ovat muun muassa seuraavat piirteet:

- Ystävällinen asiakkaille
- Iloinen ja ulospäin suuntautunut
- Sopeutunut hyvin työyhteisöön
- On toimelias ja idearikas
- On yhteistyö- ja edustuskelpoinen (Lehtonen, Pesonen, Toskala 2002, 60)

Service desk'issä asiakaspalvelua toteutetaan monen eri kanavan kautta, käytössä ovat sähköpostitse luodut tukipyynnöt, puhelimitse tehdyt yhteydenotot, lähituki tilanteet missä asiakas

tulee suoraan Service desk'in tiloihin ongelmansa kanssa tai työntekijä vierailee asiakkaan tiloissa. Kun asiakaspalveluun käytetään useita erilaisia kanavia, pitää pystyä huolehtimaan yhtenäisestä asiakaspalvelun laadusta ja niiden työtehtävien tietoturvatasosta.

Tärkeää asiakaspalvelussa on luoda asiakkaalle useita vaihtoehtoisia yhteydenottotapoja, jotta asiakas löytää niiden joukosta itselleen sopivimman. Tämän lisäksi useiden kanavien käyttö ennaltaehkäisee muun muassa jonottamisen aikaa esimerkiksi puhelimitse. Mikäli palvelua joutuu jonottamaan kauan, se nähdään usein huonona asiakaspalvelukokemuksena tai toinen huono vaihtoehto on se, että asiakkaalle ei anneta vaihtoehtoja siihen, miten hän voisi ottaa yhteyttä tukeen (Call Waves 2015).

Kiireettömissä tapauksissa asiakkaat voivat ottaa yhteyttä IT-tukeen sähköpostitse, tällöin järjestelmä luo automaattisesti sähköpostiviestistä tukipyynnön, joka on helppo ottaa järjestelmästä työn alle parhaana mahdollisena hetkenä. Puhelinvaihteeseen soittaessa asiakas saa akuutteihin tilanteisiin apua hyvinkin nopeasti, sillä Laureassa puhelin palvelussa käytetään vaihdepalvelua, joka mahdollistaa oikean henkilön tavoittamisen, eikä asiakasta pompotella henkilöltä toiselle (Call Waves 2015).

Lähituen kautta voidaan tarjota sellaista apua, jota ei voida esimerkiksi hoitaa etäyhteyden kautta tai mikäli asia on kiireellinen, lähituki tilanteet hoidetaan joko Service desk'in tiloissa tai asiakkaan luona.

Parhaan asiakastyytyväisyyden takaa kommunikointi, joka pitää sisällään seuraavat asiat,

- Asiakasta kuunnellaan
- Asiakkaan ongelmiin paneudutaan
- Osoitetaan palveluvalmiutta
- Etsitään ratkaisuja asiakkaan ongelmiin
- Asiat sanotaan kielellä ja käsitteillä, joita asiakas varmasti ymmärtää
- Kommunikoinnin ansiosta asiakkaan kuva yrityksestä asiantuntevana ja luotettavana paranee (Lehtonen ym. 2002, 96)

Lähituki ja tikettijärjestelmän tukipyyntötilanteissa asiakkaan kanssa on helppo kommunikoida, mutta asiakaspalvelun laadunvarmistaminen puhelimitse on hieman haastavampaa. Puhelimessa toimivalle työntekijälle hyviä muistettavia asioita ovat muun muassa,

- Keskittyy sanojen ääntämiseen (selkeys ja luontevuus)
- Äänessä on vaihtelevaa sävelkulkua
- Puhenopeuden huomioiminen

- Tärkeiden seikkojen tai sanojen painotus
- Älä kiirehdi asian suhteen
- Älä syö mitään asiakaspalvelutilanteessa (Heikkinen 2013)

6.2 Asiakkaan tunnistaminen

Suuren asiakasmäärän vuoksi Service desk työssä on erittäin tärkeää asiakkaan tunnistaminen varsinkin, kun asiaa tarkastellaan tietoturvallisuuden näkökulmasta, oli sitten kyseessä etätuki tai lähituki tehtävät. Tukitehtävissä tehdään muun muassa asennuksia tai päivityksiä vain ja ainoastaan asiakkaan henkilökohtaiseen työtietokoneeseen tai yleisen tilan tietokoneeseen, eli esimerkiksi kollega ei voi tuoda tietokonetta toisen henkilön puolesta asennusta tai päivitystä varten IT-tukeen. Asiakkaan tunnistamiseen on olemassa muutamia eri tapoja lähituki sekä etätuki tilanteissa, joita käsitellään tarkemmin jälkimmäisissä kappeleissa.

6.3 Lähitukitilanteet Service Desk'in tilassa

Service desk tilassa hoidettujen lähitukitilanteiden kanssa tulee olla tarkkana, sillä itse toimistotilat ovat hieman epäkäytännölliset ja tämän vuoksi on olemassa myös tietoturvariski. Ongelmaksi koettiin omien havaintojen myötä sekä kyselyn perusteella harjoittelijoiden työpisteiden sijainti, sillä nämä tietokoneet ovat sijoitettu tilaan siten, että toimistoon tuleva asiakas saattaa nähdä harjoittelijan näytön ja sillä käsiteltävänä olevia tietoja astuttuaan toimistotilaan, vaikka matkaa ovelta työpisteille on hieman. Työpisteen tietokoneilla voi mahdollisesti esiintyä hyvin arkaluontoista materiaalia, joten tällainen tilanne on aina huomioon otettava riski. Kyseinen tilanne voidaan luokitella tietojen urkinnaksi ja sitä kautta pahimmillaan sen levittämiseen, oli kyseessä tahaton tai tahallinen tapaus. Niin kuin Laurean tietotekniikkapalveluiden käyttösäännöissäkin kohdassa 5.6 sanotaan, että muille ihmisille kuuluvien tietojen urkinta näiden hyväksikäyttö tai talteenotto ja levitys on ehdottomasti kielletty.

Lähitukeen tulevien asiakkaiden palveleminen pitäisi tapahtua aina ensisijaisesti Front-desk pöydän luona, joka sijaitsee heti toimistotilan oven vieressä. Kyseisen vastaanottopöydän luona on tarkoitus tehdä ensimmäinen kartoitus asiakkaan palvelemisen tilanteesta sekä henkilöllisyyden todentamisesta. Tämän jälkeen asiakkaan kanssa voidaan muun muassa siirtyä asennuspöydän luo, joka sijaitsee Front desk'in vieressä tai tarpeen mukaan asiakkaan tiloihin, mikäli hänellä ei ole tietokonetta mukanaan.

Service desk'in tiloissa työskentelee harjoittelijoiden tukena yksi asiantuntija, jonka läsnäolo saattaa ajoittain aiheuttaa ongelmia Front desk'in käyttöön liittyen, sillä monet työntekijät ovat hyviä tuttuja asiantuntijan kanssa ja tulevat kysymään ongelmiinsa apua ensisijaisesti

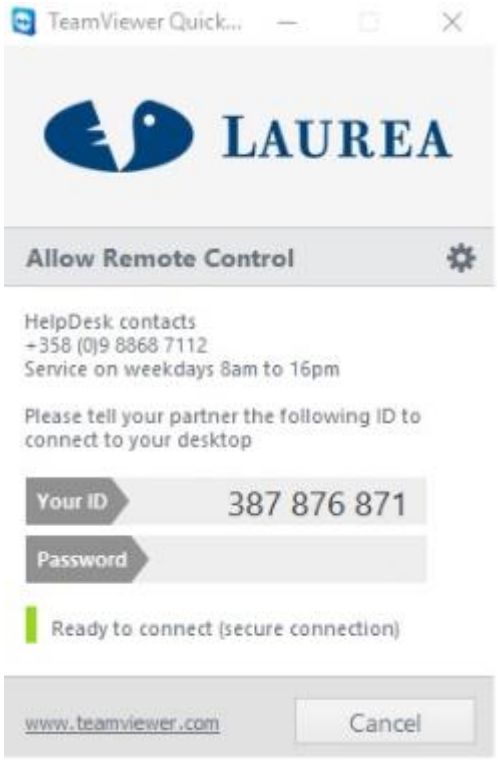
häneltä. Kyseinen tilanne voi aiheuttaa edellä mainittuun toimistotilan epäkäytännöllisyyteen liittyen tietoturvauhkia, sillä asiakkaat, jotka tulevat tapaamaan asiantuntijaa voivat automaattisesti lähteä tavoittelemaan asiantuntijaa, jolloin muuan muassa harjoittelijoiden esillä olevat työt voivat näkyä asiakkaalle. Asiakas voidaan tunnistaa muutamalla eri tavalla, joita ovat tunnistaminen tutuksi henkilöksi jo etukäteen, kysymällä henkilökorttia, asiakkaan nimeä tai käyttäjätunnusta.

Mikäli työtehtävänä on lähitukitehtävä ilman asiakkaan läsnäoloa (Tikettijärjestelmästä omaan jonoon otettu tehtävä), oikean kohdekoneen voi paikantaa työtilasta kysymällä itse asiakkaalta esimerkiksi puhelimitse missä hänen tietokoneensa sijaitsee tai hyödyntämällä ID-numerosarjaa, joka löytyy jokaisesta Laurean tietokoneesta. ID-numerosarja antaa yksilöllisen nimen tietokoneelle, jotta se on helppo paikantaa muiden tietokoneiden joukosta. Lähitukitehtävän voi myös hoitaa Remote desktopin avulla, mikäli tiedetään, että asiakas ei ole sillä hetkellä tietokoneella.

6.4 Etäyhteys ja käytettävät työkalut

Etätyöskentely lisääntyy koko ajan yrityksissä ja tämä tarkoittaa sitä, että ohjelmien on toimittava myös ympäri maailman tarpeen vaatiessa. Etätöiden lisääntyminen luo tarpeen erilaisten päivityksien ja asennuksien tekemiselle etänä, jotta työlle tarvittavat ohjelmistot toimivat. Asennus ja päivitystöitä varten on olemassa muutamia erilaisia ohjelmistoja niin yrityksien sisäverkossa kuin julkisiin verkkoihin.

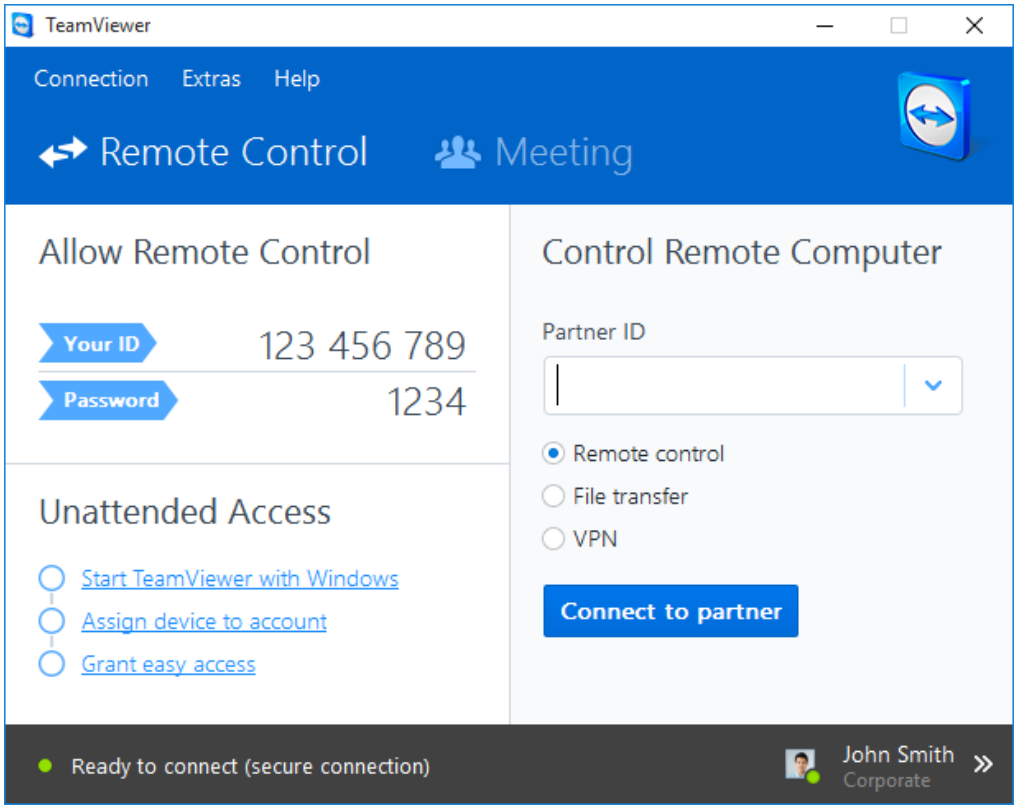
TeamViewer ohjelmistoa käytetään Laureassa ja ei mikään ihme, sillä se on maailman johtavimpia näytön jakamisen mahdollistamia ohjelmistoja. Tämän lisäksi ohjelmisto on ammattitaitoisesti tehty ja suojattu. Tietoturvallisuus on erityisen tärkeää, kun tehdään etäasennuksia tai muita korjaustoimenpiteitä eri verkossa, etteivät tiedot pääse matkan varrella tuntemattomien käsiin. TeamViewer käyttää yhteyksien salauksessaan tämän hetkisen tekniikan varminta salausta, joka koostuu RSA julkisesta/yksityisestä avainsalausprotokollasta sekä AES-256 bittisestä istuntosalauksesta. Tietoturvallisuuden lisäksi ohjelman käyttö on tehty helpoksi asiakkaan näkökulmasta. Quick support mahdollistaa etäyhteysohjelman käytön ilman asennuksia, sen ulkoasun voi räätälöidä oman yrityksen logolla sekä tervehdystekstillä, jos tämän tyylinen tilanne nähdään tarpeelliseksi, aiheeseen liittyvä kuva alla (TeamViewer 2016a; TeamViewer 2016b; TeamViewer 2016c)



Kuva 3: TeamViewer, ulkoasu asiakkaalle

TeamViewer yhteys luodaan Service desk'in ja asiakkaan tietokoneiden välille käyttäen kyseistä ohjelmaa ja tämän lisäksi Service desk'in työntekijä tarvitsee kohdekoneelta ID-numerosarjan ja tämän jälkeen myös asiakkaan istuntosalasanan. Kyseisten toimenpiteiden jälkeen asiakkaan tietokoneelle ilmestyy ikkuna, jossa kysytään vielä lupaa luoda yhteys tietokoneiden välille. Näiden tietoturvallisuustoimien jälkeen Service desk'issä työskentelevä henkilö pääsee muun muassa tekemään asennustöitä kohdekoneelle.

TeamViewer'in omien tietoturvallisuusseikkojen lisäksi täytyy kuitenkin muistaa asiakkaan tunnistaminen ennen etäyhteyden luomista, jotta varmistutaan siitä, että kenelle sen hetkistä toimenpidettä ollaan tekemässä. Asiakkaan tunnistamisen ja yhteyden luomisen jälkeen Service desk harjoittelija voi vielä tarkistaa asiakkaan henkilöllisyyden muun muassa käynnistävalikon kautta, sillä sen avaamalla näkee, kuka on sillä hetkellä kirjautuneena tietokoneelle. Näin saadaan varmuus siitä, että asennusta ollaan tekemässä yhteyttä ottaneen henkilön tietokoneeseen.



Kuva 4: TeamViewer, Service Desk'in näkymä

Kokemuksien mukaan TeamViewer ei kuitenkaan ole täysin vakaa, nimittäin yhteysongelmia voi ilmetä satunnaisesti, sillä ohjelma toimii ulkoisten välityspalvelimien kautta. Tämä voi hankaloittaa työntekijän asennustöitä varsinkin, jos puhelinyhteys on katkaistu asiakkaan ja Service desk'in välillä. Tällainen tilanne on täysin normaali, sillä puhelinpäivystäjän on otettava jatkuvasti uusia yhteydenottoja jos hän on sen hetkinen puhelinpäivystäjä. Uutta yhteyttä ei voida luoda, mikäli se katkeaa, koska TeamViewer luo jokaista istuntoa varten uuden istuntosalasanan, joka taas lisää turvallisuutta (TeamViewer, 2016c).

Yhteysongelmien lisäksi TeamViewer'issä voidaan törmätä käytönaikaisiin ongelmiin, tällä tarkoitetaan etäyhteyden luomisen jälkeen tapahtuvaa tietokoneen käyttöä. Ohjelma on varsin hyvä sen takia, että asiakas voi oppia itse uusia asioita samalla kun Service desk'in työntekijä tekee toimenpiteitä tietokoneelle, sillä asiakas näkee koko ajan mitä hänen koneelleen tehdään. Huono puoli tässä on se, että samanaikaisesti asiakas voi ohjata näppäimistöä ja hiirtä aivan normaalisti yhteyden aikana, joten on äärimmäisen tärkeää, että asennusta tai muuta ylläpitotehtävää hoitava henkilö kertoo asiakkaalle, ettei näin saa tehdä. Tietokoneelle voidaan olla kirjauduttu etäyhteyden kautta esimerkiksi järjestelmänylläpitotunnuksin, jolloin normaalin käyttäjän tekemillä virheillä voi olla suuret vaikutukset. Laureassa harjoittelijat tekevät asennus ja päivitystyöt aina järjestelmänylläpitotunnuksilla, sillä normaalit henkilökuntatunnukset eivät riitä tällaisiin toimenpiteisiin.

Kyselystä ilmeni etätyökaluihin liittyen myös haaste Service desk'in työntekijöitä kohtaan, mikä liittyy yksityisyydensuojaan. Asiakkaalla voi olla etäyhteyttä luodessa sellaisia töitä esillä, joita hän ei välttämättä halua näyttää ulkopuolisille, tämän takia on erittäin tärkeää varmistaa asiakkaalta puhelimessa, ettei hänellä ole mitään henkilökohtaista esillä ja vasta sen jälkeen voidaan luoda yhteys kohdekoneelle turvallisesti.

Remote desktop on ohjelma, joka mahdollistaa etäyhteyden kahden Windows-tietokoneen välille, näiden koneiden tulee olla kuitenkin samassa verkossa sekä virta kytkettynä, jotta yhteys pystytään muodostamaan (Microsoft 2016c).

Yhteyden muodostamiseksi täytyy tietää kohdekoneen eli sen tietokoneen nimi tai IP-osoite johon ollaan ottamassa sillä hetkellä yhteyttä (Microsoft 2016b).

Laureassa Remote desktop ohjelmaa käytetään mahdollisuuksien mukaan esimerkiksi huoltotoimenpiteitä varten. Ohjelmaa ei aina kuitenkaan voida hyödyntää, sillä se toimii vain koneen ollessa lähiverkossa sekä käynnissä. Täytyy myös huomioida, että järjestelmä automaattisesti kirjaa ulos koneella mahdollisesti työskentelevän käyttäjän. Tämä saattaa johtaa tallentamattomien tietojen menetykseen. Tällaiset tilanteet voidaan kiertää esimerkiksi varmistamalla Laurean tilanvaraus ohjelman kautta, että onko kyseisessä tilassa opetusta ja tämän jälkeen yhteys voidaan luoda ilman, että siitä aiheutuisi haittaa muille käyttäjille. Toinen vaihtoehto on tarkistaa tila henkilökohtaisesti ja tämän jälkeen luoda yhteys kohdekoneeseen.

Remote desktop on varsin kätevä ja turvallinen ohjelma asennuksien tekoa varten, mikäli työntekijä muistaa yllämainitut ohjeet yhteyttä luodessa. TeamViewer'iin verrattuna kyseinen ohjelma on tietoturvallisuudenkin näkökulmasta parempi vaihtoehto, sillä se toimii Laurean omassa verkossa, eikä täten käytä lainkaan julkisia verkkoja. TeamViewer'in hyvät puolet ovat sen nopeus ja helppokäyttöisyys varsinkin puhelinpäivystäjän näkökulmasta, sillä työ on ajoittain todella nopeatempoista ja vaatii täten nopeita otteita työhön.

7 Yleisistä tietoturvariskeistä tiedottaminen

Seuraavissa luvuissa tullaan käsittelemään tiedottamista Laureassa, niin sisäistä tiedottamista kuin kaikille Laurean käyttäjille suunnattua tiedottamista. Näkökulmaan otetaan mukaan myös tietoturvallisuus ja sen tuomat mahdollisuudet ja riskit tiedottamiseen liittyen. Laureassa ulkoisesta tiedotus- ja suhdetoiminnasta päättää rehtori/toimitusjohtaja ja sisäisestä ja ulkoisesta strategisesta viestinnästä sekä media- ja sidosryhmäsuhteista on vastuussa viestintäjohtaja (Laurea 2015d).

Nykymaailma on täynnä erilaisia tietoturvauhkia, joita vastaan pitäisi osata taistella. Internet ja erilaiset viestintäratkaisut esimerkiksi sähköposti ja pikaviestintäohjelmat ovat hyviä työvälineitä, mutta niissä itsessään ei välttämättä ole mitään suojausta, joten tiedot liikkuvat suojaamattomina ja siksi näiden käyttö vaatii huolellisuutta ja tarkkaavaisuutta käyttäjän näkökulmasta. Tämä asettaa myös paineita Laurealle ja sen tiedottamisesta vastaaville henkilöille, sillä uusia riskejä esimerkiksi haittaohjelmia tulee jatkuvasti lisää eivätkä Laurean torjuntaohjelmistot voi estää kaikkia näitä. Tämän takia on hyvin tärkeää, että tietoturvariskeistä tiedotetaan oikeaoppisesti niin Laurean henkilöstölle kuin opiskelijoillekin (Valtiovarainministeriö 2013a, 32; Laurea 2016f).

7.1 Sisäinen tiedottaminen

Hyvä sisäinen viestintä toteutuu esimerkiksi oikeaoppisesti rakennetun intranetin avulla. Intranet tarkoittaa yrityksen sisäistä verkkopalvelua, jonka perustarkoituksena on viestinnän tehostaminen. Hyvä intranet voi sisältää työkaluja muun muassa seuraavien asioiden tehostamiseen tai hoitamiseen; uutiset, vierailijat, poissaolot, keskusteluryhmät, kommentoinnit, pikalinkit, uusimmat asiat ynnä muita sellaisia. Kun kaikki nämä löytyvät yhden palvelun alta, työn tekeminen tehostuu eikä monimutkaisia koulutuksia tarvitse järjestää useisiin eri ohjelmiin (Alfame 2016).

Mitä sisäiseen tiedottamiseen tulee, me osallistumme kaikki siihen koko ajan enemmän ja enemmän. Niin kuin Kirsi Pihan kirjassa Rytmihäiriö sanottiin, että ”meistä kaikista on tullut sisällöntuottajia ja sitä kautta vaikuttajia ja vallankäyttäjiä”. Tämä siis tarkoittaa sitä, että yleisesti ottaen viestintää kuuluu hoitaa nykypäivänä siten, että siihen otetaan mukaan koko henkilöstö ja annetaan mahdollisuus osallistua keskusteluun, antaa mahdollisuus vaikuttaa ja tehdä päätöksiä. (Piha 2015, 80)

Kyselyn ja omien kokemuksien mukaan Laurean sisäistä tiedottamista toteutetaan useiden eri kanavien kautta, mikä mahdollistaa jokaisen käyttäjän tavoittamisen tarpeen vaatiessa. Näitä kanavia ovat intranet, sähköposti, Laurean verkkolevyasema, Skype for business ja puhelimeen lähetetyt tekstiviestit. Useiden kanavien käyttö myös nostaa useampien henkilöiden mahdollisuutta osallistua ja antaa palautetta tiedotettaviin asioihin liittyen.

Monipuoliset yhteydenottomahdollisuudet kasvattavat myös tietoturvallisuutta, sillä jossain tilanteissa ei voida ottaa yhteyttä esimerkiksi sähköpostitse, mikäli on tapahtunut vakava riskitekijä esimerkiksi koulun tiloissa. Vakavien riskien kohdalla nykypäivänä nopein ja varmin tapa on tavoittaa ihmiset puhelimitse, tämän takia Laurean tekstiviestitse tapahtuva yhteydenotto on tehokas ja nopea tapa tiedottaa riskeistä.

7.2 Kaikille käyttäjille tiedottaminen

Laureassa käytetään kaikkien käyttäjien tavoittamiseksi tiedottamisessa muutamia eri kanavia. Sähköpostitse tapahtuva tiedottaminen on hyvä vaihtoehto sellaisessa tapauksessa, missä kiirettä ei ole, sillä kaikki eivät välttämättä lue sähköpostiaan päivittäin tai edes joka toinen päivä. Toinen Laurean tiedotuskanava on heidän omat kotisivunsa, jossa on tiedotettu muun muassa erilaisista tapahtumista sekä tiedotteista, nämä ovat näkyvissä jopa Laurean ulkopuolisille henkilöille. Sähköpostin ja kotisivujensa lisäksi Laurea on verkostoitunut hyvin sosiaalisen median maailmaan ja täten käytössä ovat Facebook, Instagram, Pinterest sekä Twitter.

Heillä on käytössään kotisivujensa lisäksi myös opiskelijoille ja henkilökunnalle suunnattu intrasivusto, joka on nimeltään Link. Tällä sivustolla tiedottamista hoidetaan aktiivisemmin, sillä näkyvissä ovat muun muassa uutiset, tulevat tapahtumat, uutissyöte sekä päivän sitaatti. Näistä tehokkain tiedottamiskanava on uutissyöte, sillä siinä opiskelijat, henkilökunta ja muut Laurean asiantuntijat voivat keskustella aiheesta kuin aiheesta ja auttaa muita esimerkiksi tietynlaisten tietojen etsimisessä koskien Laurean internetsivustoa. Link sivustolta voidaan myös tarkkailla muun muassa luokkatilojen varauksia ja tehdä niitä sekä tämän lisäksi ilmoittautua tentteihin sekä hakea muuta hyödyllistä tietoa tai materiaalia liittyen Laureaan.

Tietoturvallisuuteen sekä häiriötilanteisiin liittyvät tiedottamisilmoitukset julkaistaan vähintään Linkin etusivulla, riippuen koskeeko asia koko Laureaa vai vain henkilöstöä tai opiskelijoita. Joistain asioista tiedotetaan vain sähköpostitse ja näitä ovat esimerkiksi salasanan vaihdokset tai niihin liittyvät ”salasanojen kalastelu viestit”, joita huijarit lähettävät. Joissakin tapauksissa kaikkia käyttäjiä voidaan lähestyä myös tekstiviestitse, mutta tämä on harvinaista. (Laurea 2015a, 17)

8 Yhteenveto ja parannusehdotukset

Opinnäytetyöprosessin aikana havaittiin ongelmia Service desk -tilojen epäkäytännöllisyyden kanssa koskien lähitukitilanteita. Tietoturvallisuussyistä harjoittelijoiden näyttöjen uudelleen suuntaaminen olisi välttämätöntä, sillä tällä hetkellä ne on suunnattu siten, että ne näkyvät Service desk’in sisäänkäynnille päin. Tietoturva huomioon ottaen toimistotila kannattaisi suunnitella uudelleen, mutta välttämättömänä parannusehdotuksena esimerkiksi henkilötietojen salassa pitämiseksi esitettiin tietoturva- ja näytönsuojakalvoja. Näytönsuojakalvot estävät näytön katsomisen sivusuunnasta.

Käyttäjätunnusten hallinnointi sekä käyttö on hyvin järjestetty Laurean Service desk'issä. Kaikki harjoittelijat ovat kyselyn mukaan hahmottaneet eri tunnusten oikean käytön. Järjestelmävalvojan osalta salasankäytäntöä voidaan tehostaa vaihtamalla salasanaa säännöllisin väliajoin. Nykyään myös käyttäjä voi käyttää kahta eri salasanaa vuorotellen. Tätä käytäntöä voi muuttaa esimerkiksi niin että käyttäjä joutuisi käyttämään kolmea tai useampaa eri salasanaa

Kyselyiden tuloksena ilmeni mielipiteitä myös puhelinvaihteen uudelleen sijoittamisesta erillisiin tiloihin, jotta puhelimessa tapahtuva asiakaspalvelu saataisiin kokonaan erilleen nykyisistä Service desk'in tiloista. Tämä ratkaisu olisi paras mahdollinen työrauhan sekä tietoturvallisuuden kannalta. Tietoturvariski on kahdensuuntainen. Tilassa olevat henkilöt voivat seurata puhelinkeskustelua ja puhelimen toisessa päässä oleva henkilö voi kuunnella tai kuulla, mitä Service desk'in tiloissa puhutaan. Varsinkin, jos Service desk'in palvelijalla on puheessaan tauko, kun etsii tai hakee vastausta ongelmaan.

Perehdytyksessä käytettävään materiaaliin tulisi lisätä tietoturva-aineistoa. Aineisto voi olla kerättynä valittuun sijaintiin erilaisissa tiedostomuodoissa ja uusi harjoittelija käy aineiston läpi ensimmäisten työviikkojen aikana. Näin saataisiin kaikille vähintään perustason tietämys tietoturvasta ja siihen liittyvistä asioista, kuten yksilönsuoja ja salassapitovelvollisuus.

Kyselyssä ilmeni, että tällä hetkellä Laurean tietoturva-asiantuntijan rooli on hajautettu eri henkilöille. Lisäksi vastaajilla ei ollut selkeää kuvaa kuka on päävastuussa tietoturvaan liittyvissä asioissa. Vastuuhenkilön tarkempi nimeäminen parantaa tietoisuutta tietoturvallisuudesta, tietoturvariskeistä sekä kehityskohteista (Kysely 2016).

Lähteet

Lehtonen, J. Pesonen, H. Toskala, A. 2002. Asiakaspalvelu vuorovaikutuksena. Jyväskylä: Gummerus.

Piha K. 2015. Rytmihäiriö, tartu mahdollisuuksiin tai kuole. Helsinki: Talentum.

Puolustusministeriö. 2015. Katakri - Tietoturvallisuuden auditointityökalu viranomaisille. Helsinki: Puolustusministeriö.

Alfame. 2016. Intranet. Viitattu 3.4.2016
http://www.alfame.com/intranet?gclid=Cj0KEQiA3t-2BRCKivi-suDY24gBEiQAX1wiXPgDJBA-vzhSBrpu2lfCmLm2qTV8ilriHtq-YPTYOCE8aAjmJ8P8HAQ

Bundesamt für Sicherheit in der Informationstechnik. 2013. IT- Grundschutz – Catalogues. Luettu 7.3.2016 https://gsb.download.bva.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf

Call Waves. 2015. Hyvän asiakaspalvelun tunnusmerkit. Viitattu 26.2.2016.
http://www.callwaves.fi/blogi/hyvan-asiakaspalvelun-tunnusmerkit/

Keepass. 2016. What is KeePass? Viitattu 21.3.2016.
http://keepass.info/

Kotus. 2013. Puhelinkäyttäytymisen perussäännöt. Viitattu 25.2.2016
http://www.kotus.fi/nyt/kotus-blogi/vesa_heikkinen/puhelinkayttaytymisen_perussaannot.9934.blog

Laurea-ammattikorkeakoulu. 2016. IT-Tuki. Viitattu 17.4.2016. https://laureauas.sharepoint.com/sites/linkfi/opiskeluntueksi/ittuki/Sivut/default.aspx

Laurea-ammattikorkeakoulu. 2015. Tietojärjestelmätunnuksen hallinta. Tulostettu 28.1.2016.
https://my.laurea.fi/?pwchange

Laurea-ammattikorkeakoulu. 2016. Laurean käyttäjätunnukset ja salasanat. Viitattu 26.2.2016. https://www.laurea.fi/palvelut/kayttajatuki/tunnukset-ja-salasanat/

Laurea-ammattikorkeakoulu. 2015. Medialle. Viitattu 12.3.2016.
https://www.laurea.fi/laurea/medialle

Laurea-ammattikorkeakoulu. 2016. Tietoturva ja säännöt. Tulostettu 25.2.2016. https://laureauas.sharepoint.com/sites/linkfi/opiskeluntueksi/ittuki/tietoturvajasaannot/Sivut/default.aspx

Laurea-ammattikorkeakoulu. 2011. Tietoturvapolitiikka. Tulostettu 28.1.2016.
https://intra.laurea.fi/fi/laurea/turvallisuus/tietoturva/politiikka/Sivut/default.aspx

Laurea-ammattikorkeakoulu. 2013. Laurea-ammattikorkeakoulun tietotekniikkapalveluiden käyttäjäsäännöt. Viitattu 27.2.2016.
(https://www.laurea.fi/palvelut/kayttajatuki/kayttosaannot

Microsoft. 2016. Vihjeitä vahvojen salasanojen ja tunnuslauseiden luomiseen. Viitattu 1.3.2016. http://windows.microsoft.com/fi-fi/windows7/tips-for-creating-strong-passwords-and-passphrases

Microsoft. 2016. Etätyöpöytä-sovelluksen ohje. Viitattu 10.3.2016.
http://windows.microsoft.com/fi-fi/windows/remote-desktop-app-faq#1TC=windows-8

Microsoft. 2016. Yhteyden muodostaminen toiseen tietokoneeseen etätyöpöytäyhteyden avulla. Viitattu 10.3.2016.
http://windows.microsoft.com/fi-fi/windows/connect-using-remote-desktop-connection#connect-using-remote-desktop-connection=windows-7

National Security Agency. 2011. About NSA. Viitattu 13.4.2016.
https://www.nsa.gov/about/index.shtml

TeamViewer. 2016. Ruudunkaappaukset. Viitattu 8.3.2016.
http://www.teamviewer.com/fi/products/screenshots.aspx

TeamViewer. 2016. Tietoa TeamViewerista. Viitattu 8.3.2016.
http://www.teamviewer.com/fi/company/company.aspx

TeamViewer. 2016. Turvallisuus ja tietosuoja. Viitattu 8.3.2016.
http://www.teamviewer.com/fi/products/security.aspx

Valtionvarainministeriö. 2013. Henkilöstön tietoturvaohje. Viitattu 18.3.2016.
https://www.vahtiohje.fi/c/document_library/get_file?uuid=4e21a518-82ff-4dfe-b725-efcb6f97126d&groupId=10128&groupId=10229

Valtionvarainministeriö. 2013. Toimitilojen tietoturvaohje. Viitattu 19.3.2016.
https://www.vahtiohje.fi/c/document_library/get_file?uuid=78751ee8-c2c8-4ac4-945c-72cb9ec4a01b&groupId=10128&groupId=10229

Kuvat

Liitteet

Liite 1: Kysely tietohallinnon henkilöstölle

1. Kuinka paljon Service desk'illä on asiakkaita keskimäärin? Keitä asiakkaat ovat?
2. Kuinka monta henkilöä työskentelee Laurean tietohallinnossa?
3. Kuka on tietoturva-asiantuntijan roolissa tällä hetkellä?
4. Kuinka aikaisemman tietoturva-asiantuntijan poistuminen on vaikuttanut tietoturvan kehittämiseen?
5. Kuinka usein tietoturvapolitiikkaa päivitetään ja miten hyvin sitä yleisesti noudatetaan?
6. Mikä on tärkein ongelma tietoturvallisuuteen liittyen Laureassa?
7. Miten ongelmaa pyritän ratkaisemaan?
8. Millainen on optimaalinen tila tietoturvallisuuteen liittyen Laureassa?
9. Millaisia tunnuksia Service desk'issä käytetään ja miten on päädytty käyttämään useampaa tunnusta?
10. Kuka pyytää käyttäjälle tunnukset ja mitä tietoa tunnuksen luomiseksi tarvitaan?
11. Mitkä ovat Assari tunnuksen salasanan vaatimukset?
12. Onko koskaan Service desk'istä työntekijä lähtenyt riitaisissa merkeissä?
13. Kuinka pian tällaisessa tapauksessa on käyttäjän tunnukset suljettu? Onko ehtinyt tapahtua vahinkoa järjestelmissä?
14. Onko koskaan käyttäjän tunnusta jouduttu vaihtamaan? Millaisessa tilanteessa näin joudutaan toimimaan?
15. Mikä on paikallinen järjestelmänvalvojantunnus ja miksi se on käytössä?
16. Kuinka usein paikallisen järjestelmänvalvojantunnuksen salasanaa vaihdetaan?
17. Millaiset salasana vaatimukset järjestelmänvalvojantunnuksella on ja miten usein salasana vanhenee?
18. Miten harjoittelijat perehdytetään? Miten suuri osa perehdytyksestä liittyy tietoturvaan?
19. Millaisia etäyhteystyövälineitä Service desk'issä käytetään?
20. Mitä eroa TeamViewer'illä ja Remote Desktopilla on? Miten niitä hyödynnetään Service desk'issä?
21. Millaisia tietoturvariskejä näet etäyhteystyökalun käytössä?
22. Mitä kanavia sisäiseen tiedottamiseen käytetään?
23. Mitä kanavia kaikille käyttäjille suunnattuun tiedottamiseen käytetään?
24. Kuinka arkaluontoista tietoa välitetään harjoittelijalta toiselle?
25. Millaisia tietoja voidaan välittää sähköpostilla? Suojataanko tätä tietoa, miten?
26. Miten asiakastilaa on pyritty rajaamaan Service deskin tiloissa?
27. Onko tilan järjestelyiden muuttaminen muuttanut asiaa?
28. Puhelintyöskentelyn ja asiakaskäynneistä aiheutuvaa meluisuutta on saatu vähennettyä.
29. Onko tilaan suunniteltu muutoksia nykytilan parantamiseksi?

30. Miten on päädytty Front desk ratkaisuun? Miten se toimii?
31. Onnistutaanko asiakkaat pitämään asiakkaille rajatussa tilassa?

Liite 2: Kysely Service Deskin harjoittelijoille

1. Millaisia työvälineitä Service desk’issä käytetään?
2. Millaisia ohjelmia on käytössä? Onko käytettävissä ohjelmaa, joka edistää tietoturvaa?
3. Millaisia etäyhteystyövälineitä Service desk’issä käytetään?
4. Mitä eroa TeamViewer’illä ja Remote Desktopilla on? Miten niitä hyödynnetään Service desk’issä?
5. Millaisia tietoturvariskejä näet etäyhteystyökalun käytössä?
6. Mitä kanavia sisäiseen tiedottamiseen käytetään?
7. Mitä kanavia kaikille käyttäjille suunnattuun tiedottamiseen käytetään?
8. Miksi asiakkaan henkilöllisyyden tunnistaminen on mielestäsi tärkeää esim. Fyysisen tietoturvallisuuden kannalta?
9. Miten lähituki tilanteessa tunnistat asiakkaan? Mitä keinoja tähän on olemassa?
10. Miten tunnistat käyttäjän etätukitilanteessa mm. ohjelmistopäivityksen aikana?
11. Näytöt ovat nähtävissä lähes ovelta asti, koetteko tätä ongelmaksi tietoturvallisuuden kannalta? yksityisyydensuoja yms. huomioiden?
12. Miten työpisteiden sijainti muuten vaikuttaa mielestäsi tietoturvaan? Eritoten miten paikallisen ylläpitäjän työpisteen sijainti vaikuttaa?