Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2018

Jerry Nurmi

YRITYKSEN TIETOTURVAN TESTAUS JA KEHITYS

– kohteena theFIRMA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

Syksy 2018 | 52 sivua, 41 liitesivua

Jerry Nurmi

YRITYKSEN TIETOTURVAN TESTAUS JA KEHITYS

- kohteena theFIRMA

Opinnäytetyön aiheena oli laatia Turun ammattikorkeakoulun ICT-projektioppimisympäristölle theFIRMAlle tietoturvatestaus ja -kartoitus. Työn tavoitteena oli auttaa toimeksiantajaa tunnistamaan mahdolliset puutteet ja ongelmat ja antaa suosituksia, kuinka nämä voitaisiin korjata.

Työssä selvitettiin theFIRMAn tärkeimmät suojattavat kohteet ja toimitilojen sekä henkilöstön tietoturvallisuuden ja tietoturvatietoisuuden taso. Kartoitukseen kuului avainhenkilöiden haastattelu, theFIRMAssa oleville harjoittelijoille laadittu kysely ja omatoiminen katselmointi. Toimitilojen ja harjoittelijoiden tietoturvaa ja tietoisuutta testattiin erilaisilla käyttäjän manipulointitekniikoilla, kuten tietojenkalastelulla. Tietoturvatestauksessa testattiin myös theFIRMAn kotisivut.

Havaittujen riskien perusteella tehtiin riskienarviointi ja luotiin theFIRMAlle tietoturvankehityssuunnitelma sekä henkilöstön tietoturvaohjeet. Suunnitelmaa on mahdollista jatkossa käyttää tietoturvan kehittämiseen.

ASIASANAT:

tietoturva, uhka, riski, käyttäjän manipulointi

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information- and communications technology

Autumn 2018 | 52 pages, 41 pages in appendices

Jerry Nurmi

TESTING AND DEVELOPING THE COMPANY'S INFORMATION SECURITY

- case study: theFIRMA

The subject of the thesis was to conduct a security testing and assessment for the ICT project learning environment theFIRMA of Turku University of Applied Sciences. The purpose of the thesis was to help the client to identify possible weaknesses and problems in their information security and to give recommendations on how to fix and improve their processes.

TheFIRMA's most important assets to protect were identified, and the level of information security and security awareness of the premises and personnel were tested. The security was tested by various social engineering techniques, such as with phishing. The security assessment included an interview with the key persons, a survey for theFIRMA interns and an independent inspection. TheFIRMA home pages were also part of the security testing.

Based on the identified risks, risk assessment was conducted, and a security development plan and information security guidelines for personnel were developed for theFIRMA. In the future the development plan can be used to further improve information security.

KEYWORDS:

information security, threat, risk, social engineering

SISÄLTÖ

LIITTEET

KUVAT

TAULUKOT

KÄYTETYT LYHENTEET TAI SANASTO

BIOS	Basic Input-Outout System
CIA	Luottamuksellisuus, eheys, saatavuus (confidentiality, integrity, availability)
GDPR	Euroopan Unionin yleinen tietosuoja-asetus (General Data Protection Regulation)
HID	(Human interface device)
IPS	Tunkeilijanestojärjestelmä (Intrusion Prevention System)
SQLi	SQL-injektio (SQL injection)
XSS	Cross-site scripting

1 JOHDANTO

Kyberrikollisuus on vakava ja maailmanlaajuisesti erittäin kallis uhka yrityksille. Hyökkäysten määrä lisääntyy vuosi vuodelta, ja jopa 60 % pienistä yrityksistä, joihin kohdistuu tietomurto, lopettaa liiketoimintansa puolen vuoden sisällä (Miller 2016). Tietomurtojen vaikutus ei usein rajoitu pelkästään ensimmäiseen murtautumiskohteeseen, sillä varastettuja käyttäjätietoja ja salasanoja voidaan edelleen käyttää hyväksi hyökkääjien murtautuessa uusiin palveluihin (Perlroth 2017).

Media uutisoi näyttävästi uusista tietomurroista kertomalla viruksista ja hakkereista ja luo mielikuvaa tietoturvan teknisestä puolesta, mutta ei siihen liittyvistä muista osa-alueista, joilla voi olla jopa teknisiä suojauskeinoja suurempi merkitys. Lehtiartikkelit eivät yleensä mainitse sitä, että tietomurron aiheuttaja on hyvin suurella todennäköisyydellä inhimillinen virhe. Hyvä esimerkki tästä on huhtikuussa 2018 liiketoimintasuunnitelma.com-palveluun tehty tietomurto, jossa paljastui 130 000 käyttäjän tunnukset ja salasanat, koska salasanat oli tallennettu tietokantaan selväkielisinä (Viestintävirasto 2018).

Ensimmäinen Euroopan unionin (EU) tietosuojadirektiivi luotiin 1995. Tästä eteenpäin eri maat alkoivat luoda omia versioitaan tästä direktiivistä. Vuonna 2016 luotiin yhtenäinen tietosuoja-asetus (GDPR), joka tuli voimaan 25.5.2018. Asetus luo uusia velvollisuuksia EU-kansalaisten henkilötietoja käsitteleville organisaatioille ja muun muassa määrittelee organisaatioille asianmukaiset tekniset ja organisatoriset toimenpiteet turvallisuustason varmistamiseksi.

1.1 Tavoitteet ja rajaukset

Opinnäytetyöni tavoitteena on suorittaa theFIRMAlle tietoturvakartoitus ja -testaus ja näiden avulla arvioida tietoturvan nykytilaa. Työn tavoitteena on kehittää theFIRMAn tietoturva GDPR- artikla 32:n mukaiselle vaatimustasolle sekä tulevaisuudessa täyttämään ISO 27001 -standardin vaatimukset.

Toisessa luvussa käyn läpi yleisiä asioita tietoturvasta, sen peruskäsitteet sekä siihen kuuluvat eri osa-alueet, koulutussektorille kuuluvat suurimmat uhat sekä kerron tarkemmin käyttäjän manipuloinnista ja siihen kuuluvista erilaisista tekniikoista.

Kolmannessa luvussa käyn läpi riskienhallintaa, johon kuuluvat erilaiset prosessit ja tavoitteet sekä se, kuinka riskienhallinta toteutetaan. Tämän luvun tarkoituksena on ohjata opinnäytetyön toimeksiantajaa toteuttamaan riskienhallintaa löytämiini riskeihin.

Neljännessä luvussa kerron toteuttamastani tietoturvakartoituksesta, mihin kuuluu avainhenkilöiden haastattelu ja harjoittelijoille laadittu kysely. Käyn läpi, mikä on tietoturvakartoituksen tarkoitus, kuinka sen toteutin ja mitä haastatteluun ja kyselyyn kuuluu.

Viidennessä luvussa käyn läpi tekemiäni tietoturvatestauksia, joihin kuuluu yrityksen kotisivujen testaaminen, toimitilojen testaaminen ja henkilöstön testaaminen erilaisilla testeillä. Testaaminen on rajattu käyttäjän manipulointiin ja fyysiseen tietoturvatestaukseen sekä verkkosivujen testaamiseen, koska theFIRMAlla ei ole muita ulkoverkossa olevia palveluita. Verkkosivujen testaus on rajattu yleisten automaattisten ohjelmien käyttöön. Ne etsivät mahdollisia haavoittuvuuksia sovelluksista.

Kuudennessa luvussa käyn läpi kartoituksessa ja testauksessa havaitut puutteet ja ongelmat. Löydetyistä puutteista teen riskienarvioinnin ja esitän parannusehdotuksia tekemäni tietoturvan kehittämissuunnitelman avulla, jonka avulla theFIRMA voi kehittää tietoturvan nykytilaa. Tietoturvakartoitukseen liittyvän haastattelun olin suorittanut ennen opinnäytetyön aloittamista ja korjannut joitakin löydettyjä ongelmia, joten haastatteluosiossa käyn läpi vain ne ongelmat, joita ei ollut vielä korjattu harjoitteluni aikana.

Viimeisessä luvussa pohdin, kuinka opinnäytetyön tekeminen onnistui, sainko asettamani tavoitteet tehtyä ja miten työtä voisi jatkaa tulevaisuudessa. Käyn myös läpi lyhyesti puutteet ja ongelmat, joita huomasin opinnäytetyötä tehdessäni.

Varsinaisen työn lisäksi toteutin henkilökunnalle tietoturvaohjeet (Liite 1). Käytin ohjeiden pohjana VAHDIN tekemää henkilöstön tietoturvaohjetta sekä olemassa olevia hyviä käytäntöjä ja suosituksia (SANS ja NIST).

1.2 Kohteen perustiedot

TheFIRMA on vuonna 2015 perustettu oppimisympäristö, joka on yhdistelmä jo 2000-luvun alussa toimintansa aloittaneita ympäristöjä. TheFIRMA toimii kuten oikea yritys ja opiskelijat työskentelevät siellä oikeiden asiakasprojektien kanssa. Ympäristö työllistää yli 100 opiskelijaa projekteihin, joiden sisältö vaihtelee verkkosivujen luomisesta erilaisiin laatumäärityksiin ja testaamisesta graafiseen suunnitteluun. Opiskelijat ansaitsevat työstään opintopisteitä. Projektien toteuttamista valvovat palkalliset opiskelijaprojektipäälliköt (opiskelija-assistentit), opiskelijatoimitusjohtaja sekä ammattikorkeakoulun henkilökunta. (theFIRMAn kotisivut 2018.)

2 YRITYKSEN TIETOTURVA

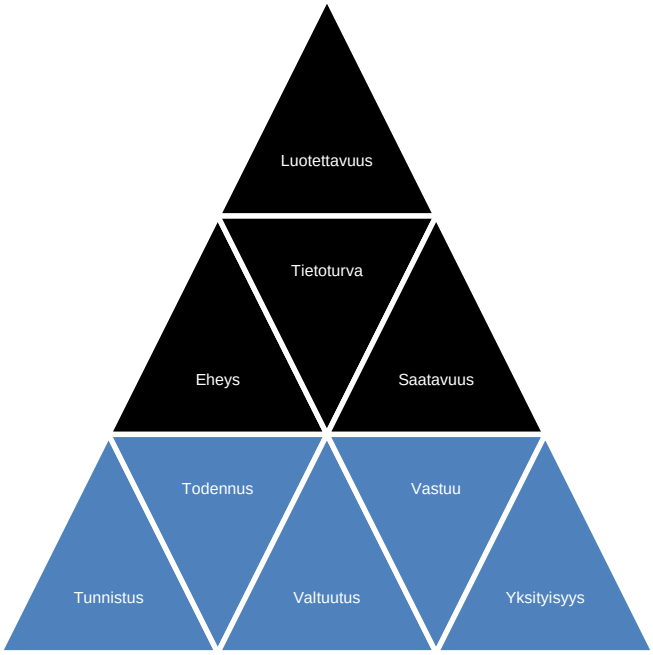
Tietoturvalla tarkoitetaan tiedon ja tietojärjestelmien suojaamista luvattomalta pääsyltä ja käytöltä, tarkoituksena estää tiedon paljastuminen, häirintä, muuttaminen, lukeminen, tarkastaminen, tallentaminen tai hävittäminen (Soriano 2013, 7).

Tietoturvaan kuuluu erilaisia hallinnollisia ja teknisiä toimenpiteitä, jotka tulee suunnitella lainsäädännön vaatimukset huomioon ottaen (Laaksonen, Nevasalo & Tomula 2006, 17–18). Tietoturva vaatii jatkuvaa monitorointia ja hallintaa tiedon luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi ja sen varmistamiseksi, että uudet haavoittuvuudet ja kehittyvät uhat ovat nopeasti tunnistettu ja huomioitu (Nieles, Dempsey & Pillitteri 2017, 10).

On tärkeää, että yrityksen henkilökunta ymmärtää ja omaksuu tietoturvan tärkeyden jokapäiväisessä työssään ja työympäristössään ja tekee parhaansa sen turvallisten käytäntöjen ylläpitämiseksi (Laaksonen ym. 2006, 17–18). Tietoturva on luonnostaan epäkäytännöllistä, sillä monimutkaiset tietoturvamekanismit kuten salasanat ja monivaiheiset tunnistautumismetodit vaikuttavat työntekoa hidastavasti. Tietoturvaa suunniteltaessa tulisi ottaa huomioon sekä turvan tavoitetaso, että käytön helppous. (Mallery 2013, 3.)

2.1 Tietoturvan peruskäsitteet

Tietoturvan peruskäsitteistö luokitellaan normaalisti kolmeen osa-alueeseen, jotka ovat luottamuksellisuus, eheys ja saatavuus. Näitä kutsutaan yleensä CIA-malliksi/kolmioksi. Tietoturvan yhtenä tehtävä on pitää nämä kolme osa-aluetta tasapainossa. Cherdantsevan ja Hiltonin (2013) mukaan CIA-malli ei ole enää nykypäivänä riittävä tietoturvamalli, sillä se ei ota huomioon uusia nykypäivän uhkia. Alsmadi ym. (2018) onkin ehdottanut uutta CIA-mallia, josta käytetään myös nimitystä CIA-kolmio (Kuva 1). Seuraavissa luvuissa käyn läpi tähän malliin kuuluvien periaatteiden sisällön.



Kuva 1. Tietoturvan peruskäsitteitä kuvaava uusi CIA-malli (Alsmadi ym. 2018, 5–6).

2.1.1 Luottamuksellisuus

Luottamuksellisuudella varmistetaan, että tieto on vain ja ainoastaan oikeudenhaltijoiden käsiteltävissä. Tiedon luottamuksellisuuden suojaaminen edellyttää sopivien käyttöoikeustasojen määrittämistä ja valvomista. Tämä yleensä sisältää tiedon jakamista pienempiin kokoelmiin, jotka on järjestelty sen perusteella kenellä pitäisi olla pääsy tietoon ja kuinka tärkeää tieto on. Yleisimpiä tiedon suojaustapoja ovat käyttöoikeuksien valvonta, kulunvalvontalistat sekä tiedon salaaminen. (Perrin 2008.) Tiedostojen ja kansioiden käyttöoikeudet, todennusvektorit ja käyttöoikeuslistat voivat myös suojata luottamuksellisuutta. Luottamuksellisuus koskee myös tietoa, joka ei ole digitaalista. (Crawley 2017.)

Crawleyn (2017) mukaan yleisiä luottamuksellisuutta vastaan kohdistettuja hyökkäystyyppejä ovat esimerkiksi arkaluonteisten, yksityisten ja salattujen tietojen vuotaminen, purkaminen ja siirtäminen luvattomille osapuolille sekä erilaiset salakuuntelu hyökkäykset, kuten mies välissä-hyökkäykset (engl. man-in-the-middle) ja Spyware-haittaohjelmat.

2.1.2 Eheys

Tiedon eheydellä tarkoitetaan sitä, että tieto ei missään vaiheessa saa muuttua tahattomasti tai tahallisesti. Esimerkiksi pieni muutos käyttäjätilin hallinnassa voi johtaa vakaviin palveluiden keskeytymisiin ja luottamuksellisuuden murtumiseen. Muunkaltaisen tiedon, kuten käyttäjien tiedostojen, täytyy puolestaan olla paljon helpommin muokattavissa. Versiokontrollijärjestelmä ja varmuuskopiot ovat yleisimpiä tapoja eheyden varmistamiseen. (Perrin 2008.)

2.1.3 Saatavuus

Saatavuudella tarkoitetaan sitä, että tieto on saatavilla käyttöoikeuden haltijoille silloin kun he sitä tarvitsevat. Hyökkäyksiä saatavuutta vastaan ovat esimerkiksi erilaiset palvelunestohyökkäykset, joilla pyritään häiritsemään palvelinkeskuksen toimintaa sekä ransomware-hyökkäykset. Keinoja saatavuuden varmistamiseen ovat esimerkiksi tiedon varmuuskopiointi, IPS-järjestelmät ja palomuurit. (Crawley 2017.)

2.1.4 Kiistämättömyys

Kiistämättömyys on menetelmä sen varmistamiseksi, että jotakin pätevää ei voida hylätä tai kieltää. Tietoturvan näkökulmasta kiistämättömyys koskee yleensä muodollista sopimusta, tiedonsiirtoa tai tietojen siirtämistä. Sen tavoitteena on varmistaa, että sopimusehtojen tai tietyn viestinnän tai asiakirjojen siirron osapuolet eivät pysty kieltämään allekirjoitusten aitoutta sopimukseen liittyvissä asiakirjoissa tai että ne ovat toimittaneet tietyn viestin tai siirron. (Finjan Team 2017.)

2.1.5 Pääsynvalvonta

Pääsynvalvonta on menetelmä erottaa, kenellä on tai ei ole pääsyä tai oikeutta tehdä jotain. Pääsynvalvonta perustuu useimmiten kolmeen osa-alueeseen:

1) Tunnistus, jolla tunnistetaan käyttäjä.

2) Todennus, jolla varmistetaan, että olet se, joka väität olevasi. Kolme ensisijaista menetelmää käyttäjien todentamiseksi on:
    - jotain mitä tiedät (esim. salasana),
    - jotain mitä sinulla on (esim. kulkukortti),
    - jotain mitä olet (esim. sormenjälki).
3) Valtuutus, jolla tarkistetaan, mihin tietojärjestelmiin sinulla on oikeudet.

2.2 Tietoturvan eri osa-alueet

Tietoturva määritellään kotimaisissa valtion organisaatioissa yleensä valtionhallinnon tietoturvallisuuspäätöksissä (VM 1992, VM 1993) esitetyn mallin mukaan. Mallia hyödynnetään myös yksityisellä sektorilla (Kerttula 2000, 83). Malliin kuuluvat osa-alueet on esitetty luvuissa 2.2.1 – 2.2.8.

2.2.1 Hallinnollinen tietoturva

Organisaation tietoturvan perustaan kuuluu tietoturvallisuuden hallinta, joka sisältää muun muassa tietoturvaan liittyvät prosessit ja toimintatavat (KPMG n.d.). Tietoturvallisuuden hallinta voidaan jakaa seuraaviin osiin: järjestelmien tietoturvan hallinta, riskianalyysi, tietoturvasuunnitelmat ja –politiikat ja vahingoista toipuminen (Kerttula 2000, 105). Organisaation tulisi luoda tietoturvaohjelma, jonka tehtävänä on kehittää ohjeita ja toimintamalleja sekä teknisiä suojauskeinoja tietojenkäsittelyn turvaamiseksi (Laaksonen ym. 2006, 117).

Liiketoimintavaikutusten arviointiprosessi on tärkeää kokonaisvaltaisessa liiketoiminnan jatkuvuudessa. Näillä arvioinneilla tunnistetaan ja arvioidaan organisaatiolle kriittisiä funktioita, sisältäen toiminnalliset, taloudelliset ja fyysiset jatkuvuusvaatimukset. Liiketoiminnan jatkuvuussuunnitelmien kehityksellä ja toteutuksella varmistetaan, että kriittinen liiketoiminta saadaan uudelleen käynnistettyä mahdollisimman nopeasti. (Khan 2010, 6.)

2.2.2 Fyysinen tietoturva

Fyysisen tietoturvan tarkoitus on estää luvattomat fyysiset pääsyt, vahingot ja häiriöt organisaation tiloihin ja tietoihin. Fyysisellä turvallisuudella pyritään luomaan organisaatiolle turvallinen toimintaympäristö ja perusta kaikille muille suojaustoimille. (Laaksonen ym. 2006, 125–126.) Fyysisen tietoturvan osa-alueeseen kuuluu mm. kameravalvonta, kulunvalvonta, muu tekninen valvonta ja vartiointi sekä sähkö-, palo-, vesi-, ilmastointi- ja murtovahinkojen ehkäisy (VAHTI 2009a). Kulunvalvonnalla yritetään pääasiassa estää luvattomien osapuolien pääsy yrityksen tärkeisiin tiloihin ja sallia oman henkilökunnan kulku sinne, minne heillä on työtehtäviensä puolesta tarkoitus päästä (Laaksonen ym. 2006, 51).

Fyysiset hyökkäykset voivat mahdollisesti tehdä enemmän vahinkoa yrityksille kuin verkkohyökkäykset. Fyysisen tietoturvan toteutuksessa tulisi kiinnittää huomiota tietojärjestelmiin kohdistuvista käyttökatkoista jotka saattavat haitata tietojen saatavuutta tai menetystä, kun niihin kohdistuu fyysinen hyökkäys. (Giannoulis & Northcutt 2015.)

2.2.3 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan laitteistojen turvaamista niiden koko elinkaaren ajan. Siihen kuuluu asennus, takuu, ylläpito sekä erilaiset tukipalvelut ja sopimukset ja elinkaaren lopussa laitteiston turvallinen poistaminen. Varmuuskopioilla varmistetaan, että laitteissa olevat tiedot voidaan palauttaa, kun toivutaan poikkeamista. Laitteita tulisi valvoa jatkuvasti ja niiden käyttöasteita seurata säännöllisesti. Kaikkia järjestelmän laitteita on kyettävä jatkuvasti valvomaan ohjelmien avulla ja niiden käyttöasteiden kehittymistä seuraamaan säännöllisesti. Järjestelmien tietoturvapäivityksiä varten tarvitaan selkeät ohjeet ja ne testataan ennen tuotantojärjestelmän asennusta. Päivitysten perumisen tulee olla mahdollista, mikäli päivityksessä havaitaan ongelmia. (VAHTI 2009b.)

Laitteet tulee dokumentoida mahdollisimman tarkasti, esimerkiksi laitteen omistajat, toiminta ja siihen liittyvät sopimukset kuten ylläpito ja huolto sekä takuutiedot. Laitteistopolitiikalla voidaan määrätä miten ja mitä laitteita saa käyttää. Henkilöstö tulee kouluttaa laitteiden turvalliseen käyttöön. Kun laite poistetaan käytöstä, tulee huomioida mitä se

saattaa sisältää. Laite tulee poistaa käytöstä turvallisesti ja esimerkiksi kovalevyt tuhota oikeilla tavoilla. (Xifof n.d.)

2.2.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmiin ja muihin ohjelmistoihin tarkoitettuja toimintoja, kuten esimerkiksi ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi (VAHTI 2009c).

2.2.5 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan kaikkien tietojen suojausta kaikissa eri talletusmuodoissa kuten paperiset asiakirjat, optiset ja magneettiset muistivälineet, mikrofilmit, äänitteet sekä muut vastaavat laitteet. Tietoaineistoturvallisuus kattaa tietoaineiston käsittelyn koko elinkaaren (Kuva 2). Erilaisia keinoja tietoaineiston luottamuksen, eheyden ja käytettävyyden takaamiseksi on esimerkiksi luettelointi ja luokitus sekä ohjeistettu hallinta, käsittely, säilytys ja hävittäminen. (VAHTI 2009d.)

Kuva 2. Tietoaineiston elinkaari.

Tietojen luokittelu on hyvä lähtökohta tietoriskien hallinnalle. Sen avulla organisaatiot voivat asettaa tiedolle arvon ja tehdä asianmukaisen arvioinnin sijoituksesta, jonka he haluavat tehdä suojatakseen tätä tietoa. Tämä prosessi mahdollistaa tärkeiden tietojen helposti tunnistamisen ja kun tiedetään missä tieto sijaitsee, voidaan samaa luokittelua käyttää tietojärjestelmille ja muille prosesseille, jotka näitä tietoja käyttävät. (Totton 2018, 12–13.)

Usein tietoja joudutaan jakamaan ja lähettämään sähköpostilla, salassa pidettävää materiaalia ei saisi koskaan lähettää salaamattomana sähköpostilla, vaan tiedon lähettämiseen pitää esimerkiksi käyttää erillistä turvasähköpostia (Järvinen & Rousku 2017, 50). Salassa pidettävää tietoa sisältävät tulosteet tulisi laittaa erilliseen lukittuun tietoturvapaperisäiliöön, ja jossa näiden tietojen hävittäminen tapahtuu turvallisesti ja hallitusti. Myös paperisilppureita voidaan käyttää salassa pidettävän tiedon hävittämiseen. Tietovälineiden kuten USB-muistitikkujen hävittämiseen tulisi myös olla oma keräyssäiliö, näitä tietovälineitä ei saa koskaan laittaa roskakoriin tai jättää johonkin lojumaan. (Järvinen & Rousku 2017, 52–53.)

2.2.6 Tietoliikenneturvallisuus

Erilaisia keinoja tietoverkoissa liikkuvan tiedon turvallisuuden varmistamiseen ovat muun muassa laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen (VAHTI 2009e).

Tietoliikenteen turvaamiseen tulisi käyttää palomuureja. Palomuurin tehtävä on eristää tietoverkkoja toisistaan ja kontrolloida tietoliikennettä näiden verkkojen välillä asetettujen sääntöjen perusteella. (VAHTI 2009e).

2.2.7 Henkilöstöturvallisuus

Henkilöstöturvallisuuteen kuuluu henkilöstöön kohdistuvien uhkien sekä henkilöstön toimista kuten heidän aiheuttamien väärinkäytöksien ja tahattomien virheiden hallinta. Työntekijän luotettavuus, nuhteettomuus ja soveltuvuus tehtävään ovat oleellisia asioita, jotta organisaatio voi varmistaa tietojenkäsittelyn turvallisuuden. Tehtävien eriyttäminen siten, että vaarallisia työyhdistelmiä ei pääse syntymään on oleellinen asia. Vaarallisia työyhdistelmiä ovat muun muassa tilausten tekeminen, vastaanottaminen ja hyväksyminen tai muutoksen suunnittelu, testaaminen ja tuotantoon siirto. Henkilöstöturvallisuuteen kuuluu henkilöstöhallinnon prosessi, joka sisältää työntekijän palkkaamisen, työnkuvan muutokset ja työsuhteen päättymisen. (Laaksonen ym. 2006, 138.)

2.2.8 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan tietotekniikan turvallista käyttöä luomalla ja ylläpitämällä sopivat toimintaolosuhteet. Tämä voidaan toteuttaa esimerkiksi toimivuuden valvonnasta, käyttöoikeuksien hallinnasta, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuuskopioinnista sekä häiriöraportoinnista. Myös tietojärjestelmien suojaaminen haittaohjelmilta on osa käyttöturvallisuutta. (VAHTI 2009f.)

2.3 Tietoturvauhka

Uhka on mikä tahansa seikka tai tapahtuma, jolla voi olla haitallisia vaikutuksia organisaation toimintaan ja omaisuuteen, yksilöihin, muihin järjestöihin tai valtion tietojärjestelmiin. Uhka lähde yrittää hyödyntää haavoittuvuutta tarkoituksella tai menetelmällä. Eri tyyppisiä uhka lähteitä ovat muun muassa vihamieliset verkko- tai fyysiset hyökkäykset, inhimilliset virheet laiminlyönnistä tai provisioista johtuen, organisaation valvonnan alaisten resurssien (esimerkiksi laitteiston, ohjelmiston, ympäristön kontrollit) rakenteelliset puutteet ja luonnolliset ja ihmisen aiheuttamat katastrofit, onnettomuudet ja epäonnistumiset. (NIST 2012, 8.) Nykypäivän tietoturvauhilla voi olla vakavia seurauksia kuten tietoturvamurrot ja haittaohjelmien leviäminen (Nieles ym. 2017, 7).

Haavoittuvuus on heikkous järjestelmässä, järjestelmän suojausmenettelyssä, sisäisissä kontrolleissa tai toteutuksessa, jota uhka saattaa käyttää hyväksi. Haavoittuvuudet jättävät järjestelmiä alttiiksi monille toiminnoille, jotka voivat aiheuttaa merkittäviä ja joskus peruuttamattomia menetyksiä yksilölle, ryhmälle tai organisaatiolle. Oikeilla työkaluilla ja tietämyksellä hyökkääjä voi hyödyntää järjestelmän heikkouksia ja saada näille tallennettuja tietoja. (Nieles ym. 2017, 20.)

Haittaohjelma on suunniteltu luomaan järjestelmiin haavoittuvuuksia mitkä aiheuttavat järjestelmiin takaoven, tietoturva rikkomuksia, tietojen varastamista sekä muita mahdollisia vahinkoja (Kaspersky n.d.). Suosituimpia tapoja haittaohjelman levittämiseen on käyttäjän manipulointi.

Koska theFIRMA kuuluu koulutussektorille, käyn läpi tälle sektorille kohdistuvat suurimmat tietoturvauhat. Web-ohjelmistohyökkäykset ja erilaiset käyttäjävirheet edustavat globaalisti 40 %:a kaikista tietomurroista. Näiden aiheuttajista jopa 19 % on sisäisiä uhkia, mikä korreloi suoraan erilaisten virheiden kanssa. 41 % tietomurroista on aiheutunut käyttäjän manipuloinnin takia. Tästä 25 % tapahtui tietojen kalastelun kautta ja 16% virheistä. Tämä luultavasti johtuu koulutuslaitosten avoimuudesta ja opiskelijoista. 6 % tietomurroista aiheutuu päivittämättömistä tietojärjestelmistä. (Verizon 2018 Data Breach Investigations Report.)

2.4 Käyttäjän manipulointi

Käyttäjän manipulointi tai sosiaalinen hakkerointi on tekniikka, joka luottaa voimakkaasti ihmisen vuorovaikutukseen toisten ihmisten kanssa ja kannustaa yksilöä luovuttamaan luottamuksellisia tietoja. Tällaisia hyökkäyksiä tehdään yleisesti puhelimitse tai verkossa. Puhelimeen kohdistuneet hyökkäykset ovat kaikkein yksinkertaisempia käyttäjänmanipulointihyökkäyksiä. Hyökkääjä voi esimerkiksi johtaa yritystä uskomaan, että hyökkääjä on heidän asiakkaansa ja yrittää saada yritystä antamaan tietoa kyseisestä asiakkaasta. Verkossa tätä tekniikkaa kutsutaan tietojenkalasteluksi (engl. phishing). (Nieles ym. 2017, 21.)

Tietojenkalastelulla tarkoitetaan henkilökohtaisten- tai luottamuksellisten tietojen saamista esimerkiksi erilaisilla huijaussähköposteilla. Tietojenkalastelu on suurin uhka yritysten tietoturvalle, koska heikoin lenkki ovat käyttäjät itse. Yleensä näiden viestien tarkoitus on saada henkilö painamaan sähköpostissa olevaa linkkiä, joka ohjautuu hyökkääjän tekemälle omalle sivustolle, joka näyttää täysin samalta kuin kyseinen sivusto normaalisti näyttäisi. Sivustot ovat yleensä kopioituja sähköpostitarjoajan tai pankin sivustoja. Huijaussivustolla käyttäjä kirjautuu sisälle ja lähettää hyökkääjälle käyttäjätunnuksen ja salasanansa. Hyökkäyksiä tapahtuu myös haittaohjelmamakrojen muodossa, missä hyökkääjä lähettää sähköpostin liitteenä olevan tiedoston (usein Word- tai Exceltiedosto), johon on asennettu haittaohjelma. Kun käyttäjä avaa tiedoston ja sallii makrojen suorittamisen, haittaohjelma suoritetaan.

Kesällä tapahtui suuria tietojenkalasteluhyökkäyksiä, jotka kohdistuivat kouluihin. Helsingin yliopistossa on 70 000 käyttäjää ja heistä yli 300 antoi käyttäjätunnuksen ja salasanansa. (Hakkarainen 2018.) Kyseiset kalastusviestit olivat hyvin alkeellisia ja silti ne onnistuivat huijaamaan ihmisiä. Tämän perusteella voidaan päätellä, että ihmiset ovat organisaatioiden tietoturvan heikoin lenkki.

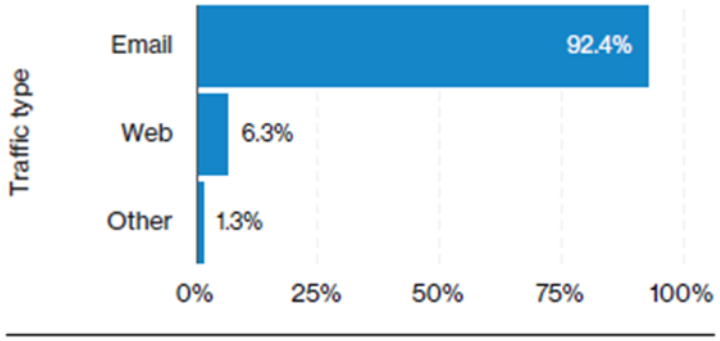
Tekstiviestihuijaus (engl. smishing) tarkoittaa samaa asiaa, mutta siinä käytetään sähköpostin sijaan teksti- tai pikaviestejä. Kohdistetulla tietojenkalastelulla (engl. spear phishing) tarkoitetaan kohdennettua tietojenkalastelua esimerkiksi jollekin tietylle organisaatiolle tai henkilölle. Hyökkääjät käyttävät paljon aikaa tutkiakseen ja etsiäkseen tietoa organisaatiosta ja sen työntekijöistä ja luovat näiden tietojen avulla mahdollisimman luotettavan näköisen huijausviestin. BEC-hyökkäys (Business email compromise) tunnetaan myös nimellä CEO fraud tai whaling. Tämän huijauksen tarkoitus on yleensä esittää toimitusjohtajaa, jotta kohdetta saataisiin huijattua tekemään suuria tilisiirtoja omalle pankkitilille tai maksamaan keksittyjä laskuja.

Sosiaalisen median kasvu on antanut verkkorikollisille mahdollisuuden hyödyntää alustaa kohdennettujen hyökkäysten suorittamiseksi. Käyttämällä väärennettyjä ja varmentamattomia sosiaalisen median tilejä tietoverkkorikolliset voivat imitoida työtovereita, palveluntarjoajia tai muita luotettuja henkilöitä linkkien lähettämiseksi vahingolliselle koodille, joka varastaa henkilökohtaisia tai arkaluonteisia organisaatiotietoja. Sosiaalisen median tilit tarjoavat keinon tavoittaa kohdennetun henkilön tietoon perustuvia tietoja, etuja ja henkilökohtaisia yhteyksiä, joita puolestaan voidaan käyttää käyttäjänmanipulointihyökkäyksen suorittamiseen. (Nieles ym. 2017, 21.)

Mobiililaitteisiin kohdistuvat tietomurrot ovat vielä harvinaisia, mutta näillä laitteilla on usein pääsy organisaation ympäristöön ja niitä käytetään kaksivaiheiseen tunnistautumiseen. Yleinen tapa on käyttää tietojenkalastelua ja muita käyttäjän manipulointi hyökkäyksiä saadakseen mobiilikäyttäjän ladattua haitallisen ohjelmiston. (Verizon Data Breach Investigations Report 2018.)

Jopa 90 % kyberhyökkäyksistä kohdistuu ihmiseen, ei koneisiin (Kuva 3). Sähköpostiuhkia vastaan rakennetut suojausmekanismit ovat helppoja käyttää ja halpoja toteuttaa, mutta silti organisaatiot eivät käytä uusimpia työkaluja ja tekniikoita suojatakseen sähköpostijärjestelmiään. Verizonin (2018) tutkimuksen mukaan suurin osa haittaohjelmista

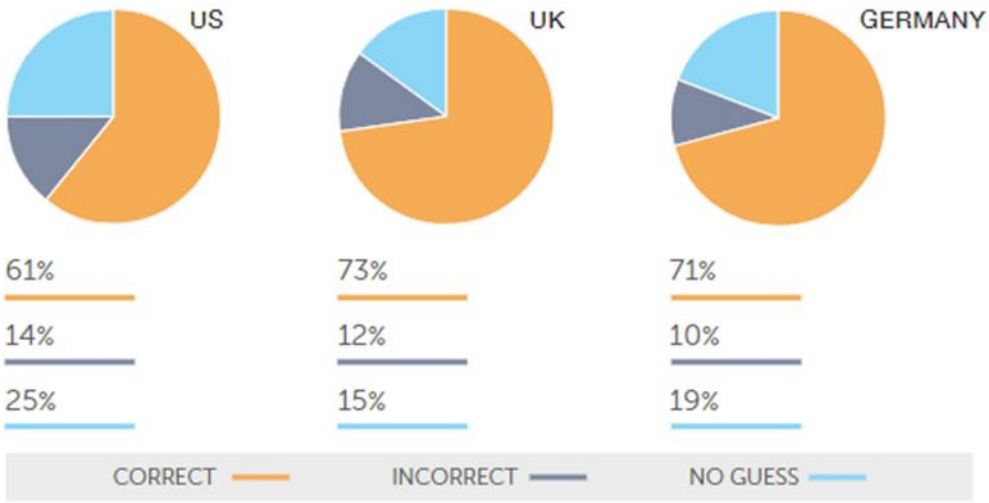
tulee sähköpostin kautta ja vain 8 % tietoturvabudjetista käytetään sähköpostin suojaamiseen. Samaan aikaan yli 50 % budjetista käytetään perinteiseen verkkosuojaukseen kuten palomuurit, IPS, hiekkalaatikot, jne. (Rosvold & Moe 2018).



Kuva 3. Mistä haittaohjelmat tulevat (Verizon 2018).

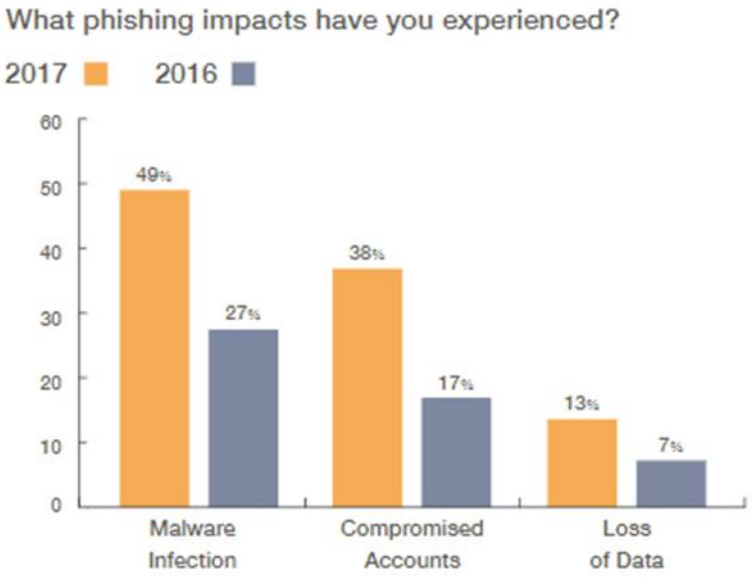
Parhaiten tietojenkalastelua vastaan voidaan suojautua kouluttamalla henkilökunta tunnistamaan nämä huijausyritykset, vaikka Aitel (2012) väittääkin, että käyttäjien kouluttaminen on turhaa ja tämän sijaan yritysten pitäisi keskittyä parantamaan järjestelmiään sillä oletuksella, että kun käyttäjät joka tapauksessa tulevat painamaan sähköpostissa olevaa linkkiä tai avaamaan liitetiedoston, siitä ei tapahtuisi yritykselle minkäänlaista haittaa.

Arviolta 95 % organisaatioista kouluttaa työntekijöitä huomaamaan kalasteluyritykset. Vuoden kestäneen testin aikana lähes kaksi miljoonaa käyttäjää raportoi kaikki sähköpostinsa tietoturvatiimille ja 60 % näistä sähköposteista oli luokiteltu potentiaalisiksi kalastusviesteiksi. Yhteensä 3 000 käyttäjältä kysyttiin, mitä tietojenkalastelu tarkoittaa. (Wombat 2018.) Kuvassa 4. on esitetty tämän testin tulokset. Ne vaikuttavat tukevan jonkin verran Aitelin väitettä, sillä kolmasosa testiin osallistuneista henkilöistä vastasi kysymykseen väärin tai ei osannut edes arvata. Paremman selvyyden tähän saisi, jos nämä kysymykset olisi esitetty myös ennen testin aloittamista.

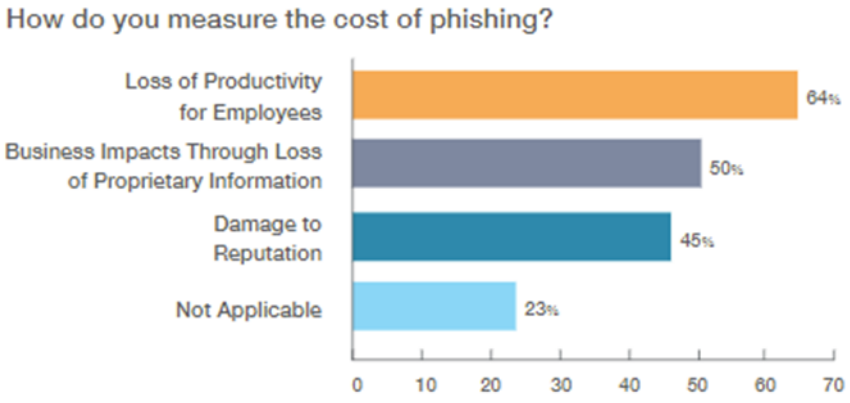


Kuva 4. Tietojenkalastelukysymyksen tulokset (Wombat 2018).

Wombatin (2018) raportin mukaan 76 % tietoturva-ammattilaisista kohtaa tietojenkalasteluyrityksiä ja 53 % kohdistettua tietojenkalastelua. Klikkausten määrä on vähentynyt verrattuna vuoteen 2016, mutta silti keskimäärin 9 % klikkaa sähköpostin linkkiä. Smishing-testissä saatiin sama tulos, mutta tulevaisuudessa kun yhä useammat käyttävät älypuhelintaan ja pikaviestiohjelmia töissä, määrä voi nousta. Testin mukaan onnistuneimpia kalastusviestejä lähes 100 %:n onnistumisella oli ensinnäkin viesti, joka oli naamioitu tietokannan salasanan nollaukseksi, ja toinen viesti, joka väitti sisällökseen rakennuksen päivitetyn evakuointisuunnitelman. Kuvassa 5. on esitetty suurimmat tietojenkalastuksen vaikutukset ja Kuvassa 6. esitetty näiden suurimmat kustannukset. (Wombat 2018, 3–5.)



Kuva 5. Tietojenkalastelun erilaisia vaikutuksia (Wombat 2018).



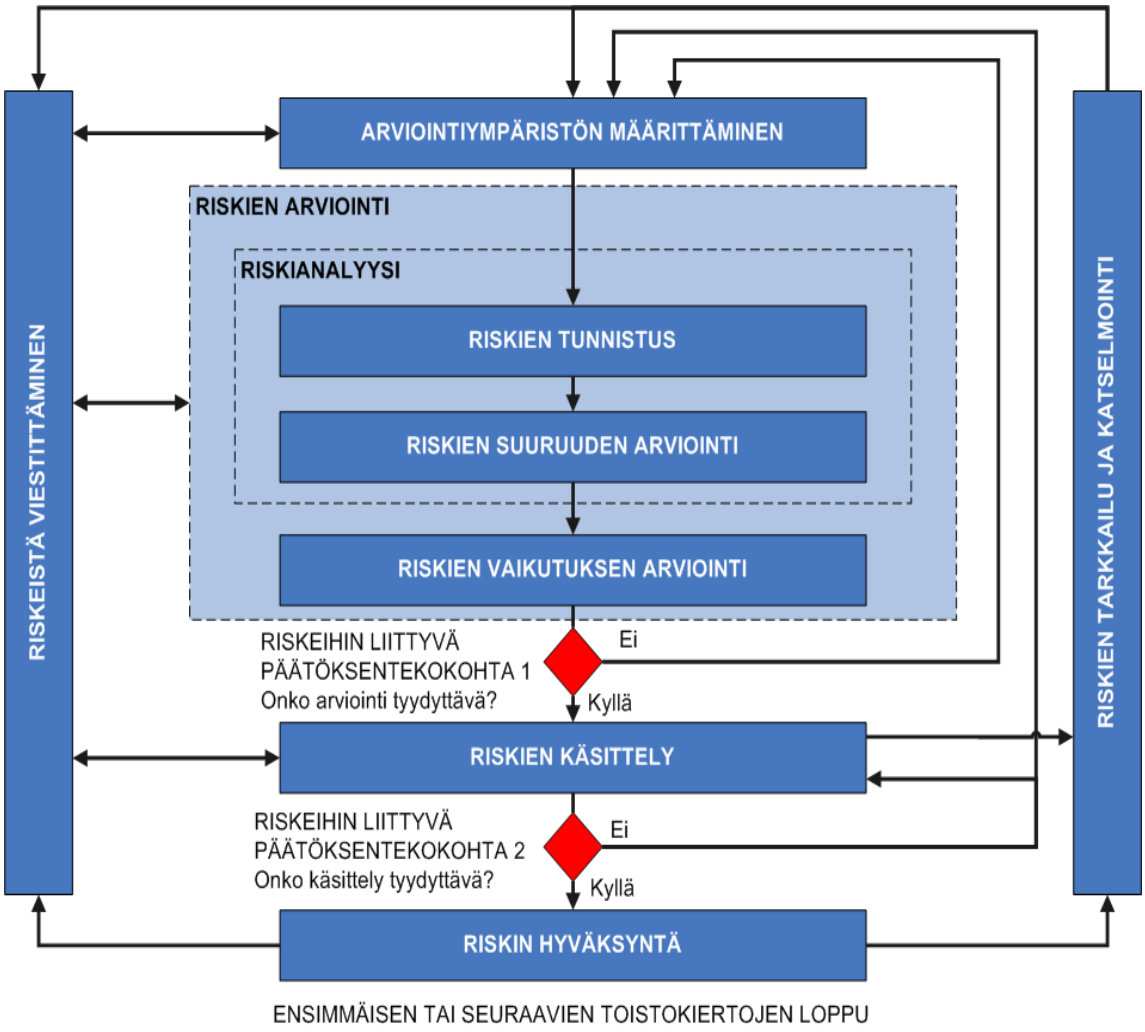
Kuva 6. Tietojenkalastelun suurimmat kustannukset (Wombat 2018).

3 RISKIENHALLINTA

Yrityksen johto on päävastuussa tietojärjestelmiä koskevien, hyväksyttävien riskitasojen määrittämisestä, ottaen huomioon tietoturvakontrollien kustannukset. Tietoturvariskejä ei voida kokonaan poistaa, ja sen vuoksi tavoitteena on löytää optimaalinen tasapaino tiedon ja järjestelmien suojaamisessa. (Nieles ym. 2017, 8.)

Riski kuvaa sitä, missä määrin kokonaisuutta uhkaa mahdollinen tilanne tai tapahtuma. Riski muodostuu haitallisista vaikutuksista ja niiden esiintymisen todennäköisyydestä. Tietoturvariskit johtuvat tietojen tai tietojärjestelmien luottamuksellisuuden, eheyden tai saatavuuden menetyksestä ja aiheuttavat mahdollisia negatiivisiä vaikutuksia organisaation toimintaan. (NIST 2012, 6.)

Riskienhallinnan ensisijaisena tavoitteena on toteuttaa tietoturvasuojauksia, jotka ovat suhteessa riskien vakavuuteen. Tarpeettomien suojausten soveltaminen saattaa tuhlata resursseja ja vaikeuttaa järjestelmän käyttöä ja ylläpitämistä. Sitä vastoin, tietojärjestelmän suojaamatta jättämäinen voi jättää sen ja sen sisältämän tiedon alttiiksi tietomurroille. (Nieles 2017, 8.) Kuvassa 7 on esitetty riskinhallinnan eri vaiheet.



Kuva 7. Riskinhallinnan vaiheet ISO 27005 -riskienhallintastandardin mukaan (SFS).

Seuraavissa luvuissa käydään läpi ISO 27005 -standardin pääkohtia.

3.1 Arviointiympäristön määrittäminen

Ulkopuolisen ja sisäisen arviointiympäristön määrittäminen luo riskinhallintaprosessin taustat, toiminnan luonteen ja potentiaalisten vaikutusten laajuuden. Tämä johtaa keskeisien sidosryhmien tunnistamiseen, riskienhallinnan tavoitteiden ja rakenteen luomiseen, ja riskin arviointiperusteisiin. Lopuksi määritellään riskinhallintaprosessin laajuus. Ensimmäinen vaihe on ymmärtää kohde, jota analysoidaan ja kuvata sen tärkeys liiketoiminnalle, josta arvioinnin tavoitetta voidaan kehittää. (Turner 2016.)

3.2 Riskien arviointi

Riskinarviointiprosessin tarkoituksena on tunnistaa, arvioida ja priorisoida riskejä. Prosessi vaatii uhka- ja haavoittuvuustietojen tarkkaa analysointia sen määrittämiseksi, missä määrin olosuhteet tai tapahtumat voivat vaikuttaa haitallisesti organisaatioon. Lisäksi arvioidaan todennäköisyyttä riskien toteutumiselle. (NIST 2012, 6.)

Riskianalyysissä tunnistetaan organisaation omaisuus ja näihin kohdistuvat uhkat ja todennäköisyys näiden uhkien toteutumiselle sekä minkälaista vahinkoa nämä uhkat saattavat aiheuttaa (Kerttula 2000, 106).

Riskin tunnistaminen on prosessi, jossa määritetään riskit, jotka saattavat estää ohjelman, yrityksen tai investointien saavuttamasta tavoitteita. Se sisältää ongelmien dokumentoinnin ja viestinnän. Tavoitteena on tapahtumien aikainen ja jatkuva tunnistaminen, jos ne tapahtuvat, niillä on negatiivinen vaikutus projektin kykyyn tai lopputulokseen. (Mitre n.d.)

Todennäköisyydenarviointi voidaan tehdä joko kvalitatiivisella tai kvantitatiivisilla menetelmillä. Todennäköisyyslaskennan jälkeen riskinarvioijan tulisi antaa arvio riskin todennäköisyydestä ja seurauksista. Seuraukset voidaan ilmaista esimerkiksi rahallisten, teknisten tai inhimillisten vaikutusten perusteella. Arvioitu riski on yhdistelmä riskin todennäköisyydestä ja sen vaikutuksesta. (Warren 2014.)

Riskinarvioinnit eivät ole pelkästään kertaluonteisia toimintoja, vaan ne tarjoavat pysyviä ja määriteltäviä ohjeita tietoturvariskeihin. Organisaatiot käyttävät jatkuvasti riskinarviointeja järjestelmän kehityksen elinkaaren ja kaikkien riskienhallintajärjestelmien eri tasojen kautta. (NIST 2012, 5.) Riskinarvioinnin tarkoitus on tuottaa lista havaituista tietoturvariskeistä, jotka voidaan priorisoida niiden riskintasoon perustuen ja kerrotaan, kuinka nämä riskit voitaisiin käsitellä (NIST 2012, 29).

Riskin vaikutuksen arviointi vaiheessa riskin tasoa verrataan riskinarviointikriteereihin ja riskien hyväksymiskriteereihin, jotka on määritelty arviointiympäristön määrittämisvaiheessa. Riskinarvioinnissa verrataan jokaista riskitasoa riskien hyväksymiskriteereihin ja tehdään luettelo riskeistä ja niiden korjaustoimenpiteistä. Riskinarvioijan on yleensä tehtävä päätös siitä, miten jokin riski korjataan. (Warren 2014.)

3.3 Riskien käsittely

Riskien käsittely on prosessi, jossa valitaan ja toteutetaan toimenpiteet riskien muokkaamiseksi. Tämän vaiheen tarkoitus on, että organisaation päättäjillä on tarpeeksi riskiin liittyvää tietoa, jotta he voivat tehdä riskiin liittyviä päätöksiä. (NIST 2012, 37). Riskien käsittelyn toimenpiteet voivat olla esimerkiksi: 1) Riskin muuttaminen — lisäämällä, poistamalla tai muuttamalla kontrolleja niin, että jäännösriski voidaan arvioida hyväksyttäväksi. 2) Riskin välttäminen — välttää, sivuttaa tai lopettaa toiminnat, jotka aiheuttavat riskin. 3) Riskin jakaminen — jakaa riskin kolmannen osapuolen kanssa kuten vakuutus tai ulkoistaminen. 4) Riskin hyväksyminen — yrityksen johto hyväksyy jäljelle jääneet riskit. Tämä on yleensä valinnainen riskienhallinnan vaihe, koska se voidaan sisällyttää myös riskien käsittelyyn. (ENISA).

4 TIETOTURVAKARTOITUS

Toteuttamani tietoturvakartoituksen tarkoituksena oli selvittää theFIRMAn tietoturvan nykytilanne ja tehdä sen pohjalta kehityssuunnitelma (Liite 2). Kehityssuunnitelma on tehty tietoturvatestauksessa ja –kartoituksessa havaitsemieni tietoturvaongelmien perusteella. Suunnitelmassa määrittelen tietoturvan toimenpiteet, vastuut, yhteiset tietoturvaperiaatteet ja menettelytavat. Käytän kehittämissuunnitelman teossa hyväksi luvussa 2.2 läpikäytyjä tieturvan eri osa-alueita. Jotta tietoturvaa voidaan kehittää, täytyy tunnistaa yritykselle tärkeä omaisuus kuten laitteisto ja tietoaineisto, niiden toiminta ja arvo.

Tietoturvakartoitus toteutettiin avainhenkilöiden haastattelututkimuksena, harjoittelijoille annetulla kyselyllä sekä omatoimisella katselmoinnilla, johon sisältyi dokumentaation, tietojärjestelmien, toimitilojen ja toimintatapojen tarkistaminen. Kartoitus perustuu ISO/IEC 27005:2011 -standardiin, joka antaa ohjeita tietoturvariskien hallintaan ja tukee ISO 27001 -standardissa määriteltyjä yleisiä käsitteitä.

4.1 Haastattelu

Haastattelun kysymykset ovat peräisin VTT:n pk-yrityksen riskienhallintasivustolta (Kyrölä, Vuori, & Halmevuo. 2004.; Liite 3). Haastattelussa oli mukana neljä theFIRMAn avainhenkilöä (vastuuopettaja, järjestelmävalvojat, pääkoodari), joilla oli tietoa kysymyksiin liittyvistä asioista. Sivulta löytyvät viisiosaisen kyselyn kysymykset olivat minulle aikaisemmasta koulussa tehdystä tietoturvakartoitus projektista tuttuja, joten päätin käyttää niitä.

4.2 Kysely

Kyselyn tarkoituksena on selvittää theFIRMAssa olevien harjoittelijoiden yleistä tietoturvaosaamisen tasoa sekä heidän käsitystään turvallisista toimintatavoista. Tämän selvitän peruskysymyksillä, joissa esimerkiksi kysytään harjoittelijoiden salasanan vahvuus ja se, ovatko he lukeneet theFIRMAn tietoturvapolitiikan sekä kuinka he turvaavat oman tietokoneensa. Kyselyn kysymykset tukevat ja vahvistavat omatoimisessa katselmoinnissa ja toimitilojen testaamisessa läpi käytyjä asioita.

Toteutin kyselyn Webporol-ohjelmalla ja lähetin sen 23:lle theFIRMAssa olevalle harjoittelijalle. Kysely toteutettiin englanniksi, koska osa harjoittelijoista on vaihto-opiskelijoita. Kyselyn kysymykset sekä opiskelijoiden antamat vastaukset on esitetty liitteessä 4. Kyselyyn vastanneiden nimiä ei näytetä anonymiteetin suojaamiseksi.

5 TIETOTURVATESTAUS

Tätä opinnäytetyötä tehdessä theFIRMAn ainoa ulkoverkossa oleva palvelu oli kotisivut, joten tämä on ainoa palvelu, mitä testasin.

5.1 TheFIRMAn kotisivujen testaaminen

Kotisivuilla ei ollut yhtään kenttää, johon käyttäjä syöttää tietoa. URL oli ainoa paikka sivuilla mihin XSS- tai SQLi- hyökkäyksiä oli mahdollista yrittää. Laittamalla esimerkiksi heittomerkin sivun loppuun huomataan, että sivustolla on tehty jonkinlainen suodatus, joten SQLi ei tässä tapauksessa onnistunut. Testaamalla XSS laittamalla seuraavan komennon URL-kenttään <script>alert(document.cookie);</script>, tuli ilmoitus, että Wordfence on estänyt haitallisen operaation.

WordPress-sivustoissa on oletuksena admin-sisäänkirjautumissivu, jota ei ollut piilotettu (https://thefirma.fi/wp-login.php). Kokeilin kirjautua satunnaisella tunnuksella, mutta käytössä oli Wordfence, joka esti sivun käytön heti ensimmäisen väärinkirjautumisen jälkeen. Yrittämällä saada salasanan resetointi sähköposti, Wordfence lähettää sähköpostin vain ennalta määritetyssä listassa oleviin osoitteisiin. Dirbuster löysi myös muita WordPressin oletussivuja, mutta näistä ei ollut hyötyä.

WPScania käyttämällä yritin saada listan käyttäjätunnuksista, mutta tämä ei onnistunut, joten kokeilin brute forcea admin-käyttäjällä, mutta taas Wordfence blokkasi muutaman yrityksen jälkeen. Sivustolta löytyi mahdollinen xml-rpc-haavoittuvuus mikä mahdollistaa huomaamattoman brute force -yrityksen, mutta en lähtenyt tätä menetelmää kokeilemaan, sillä ilman oikeaa käyttäjätunnusta sisäänpääsy on epätodennäköistä. WordPress luo automaattisesti satunnaisen admin-tunnuksen, ja ellei tätä jostain syystä ole vaihdettu esimerkiksi admin tai root nimeksi, ei ole järkevää lähteä yrittämään brute forcea. Kaikki käytössä olevat lisäosat oli päivitetty, eikä niistä löytynyt tunnettuja haavoittuvuuksia.

Nmappia käyttämällä löytyi auki olevat portit 22 (ssh), 80 (http) ja 443 (https). Nämä ovatkin yleensä nettisivuilla avoinna olevat portit. Koska ssh-portti 22 oli auki, yritin päästä sitä kautta brute forcella sisälle seuraavalla komennolla:

hydra –l root –P /usr/share/wordlists/rockyou.txt ip-osoite –t 4 ssh

mutta nämäkin yrityskerrat oli rajoitettu.

5.2 Toimitilojen fyysinen testaaminen

Kun harjoittelijat olivat vaihtuneet ja theFIRMAssa aloitti uusia henkilöitä, joita en ollut ennen tavannut, testasin, kuinka helposti he päästäisivät minut sisätiloihin. Testasin tätä muutaman kerran eri päivinä, eri harjoittelijoille. Yksikään ei kysynyt minulta, kuka olen tai mitä olen täällä tekemässä, vaan he avasivat oven ja menivät takaisin töihin. Pääsin myös pari kertaa sisään samalla oven avauksella, kun tulin heidän perässään, tätä taktiikkaa kutsutaan peesaukseksi (engl. tailgating/piggybacking). Se on yleinen ongelma fyysisessä tietoturvassa (Peiponen 2018). TheFIRMAn tiloissa ei myöskään ollut valvontakameroita.

Päästyäni sisätiloihin huomasin, että taululle on kirjoitettu yleinen käyttäjätunnus ja salasana. Kokeilin tunnuksia ja havaitsin, että niillä ei pystynyt asentamaan mitään ohjelmia, eikä ollut käyttöoikeuksia verkkolevyille. Pääsin verkossa oleviin tietokoneisiin, mutta tunnuksella oli vain lukuoikeudet joihinkin kansioihin, missä ei ollut mitään tärkeää tietoa. Myöskään powershell-skriptejä ei pystynyt tietokoneessa suorittamaan. Ainoa asia mitä pystyi tekemään, oli pääsy nettiin. Selaimeen tallennetut salasanat pystyi näkemään, jos joku käyttäjä on ne sattunut tallentamaan, mutta tässä tapauksessa niin ei oltu tehty.

Avecto (2017) mukaan noin 88 % kriittisistä haavoittuvuuksista voidaan estää poistamalla käyttäjiltä järjestelmävalvojan oikeudet, mutta silti jää 12 %, mitä voi käyttää hyväksi. Esimerkiksi käyttämällä nollapäivähaavoittuvuuksia, joka tarkoittaa, että siihen ei ole vielä olemassa päivitystä. Hiljaittain löydetyllä uudella haavoittuvuudella olisin voinut tällä yleisellä tunnuksella saada järjestelmätason (SYSTEM) oikeudet (SandboxEscaper 2018).

TheFIRMAn uusien koneiden BIOS:ia ei oltu salasanasuojattu eikä Secure Boot -asetusta oltu laitettu päälle. Nämä mahdollistavat esimerkiksi rootkitin asentamisen.

5.3 Henkilöstön testaaminen

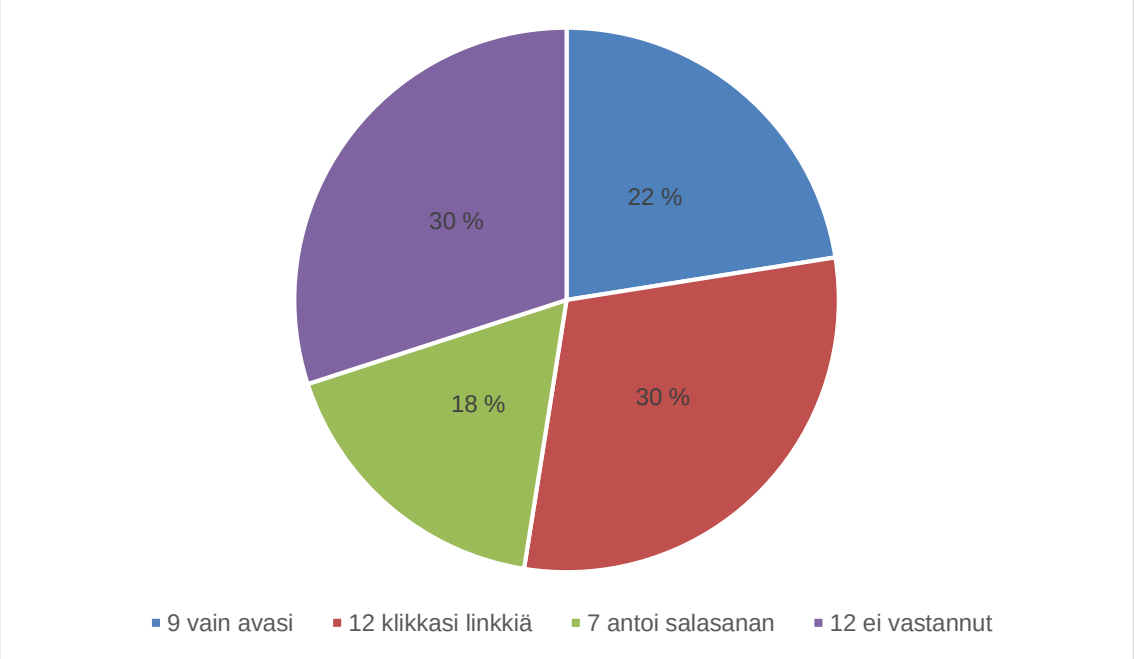
Henkilöstön testaus toteutettiin erilaisilla USB-muistitesteillä sekä tietojenkalastelusähköpostilla.

Ensimmäisessä testissä jätin tavallisen USB-muistitikkuja erilaisiin paikkoihin muun muassa lattialle ja pöydälle, ja katsoin, mitä tikun löytäjä tekee. Tikkuihin oli asennettu ohjelma, joka ilmoittaisi minulle, mikäli laite kytketään tietokoneeseen kiinni. Ohjelman avulla saisin selvitettyä käytetyn tietokoneen IP-osoitteen, jonka avulla saisin edelleen tietooni, mikä tietokone on kyseessä ja kuka tikun on koneeseen laittanut.

Toisessa testissä minun oli tarkoitus laittaa theFIRMAn logo muutamaan muistitikkuun ja jättää ne pöydälle, jossa olisi ollut kortti, missä lukee "saa ottaa", tai jakaa niitä kuten yleensä erilaisissa seminaareissa tai yritysvierailuissa on tapana. Tikku olisi voinut esimerkiksi sisältää Word- tai Excel-tiedoston, jotka olisi nimetty houkuttelevalla nimellä, kuten ”harjoittelunarvioinnit”. Tiedosto olisi sisältänyt haittaohjelman, joka olisi käynnistynyt, kun käyttäjä sallii makrojen suorituksen. Myös PDF-tiedostoja voisi käyttää. Tässä tiedostomuodossa pelkästään tiedoston avaaminen riittää siihen, että haitallinen ohjelma suoritetaan. Tämä testi jäi kuitenkin toteuttamatta rahoituksen ja USB-muistitikkujen puutteen takia.

Suunnittelemassani ja Väisäsen (2018) toteuttamassa kolmannessa testissä entuudestaan tuntematon henkilö antoi kahdelle koehenkilölle USB-tikun, jossa oli Excel-tiedosto. Molemmat koehenkilöt avasivat kyseisen tiedoston ja sallivat makrot ajamisen, jolloin he saivat ilmoituksen epäonnistuneesta tehtävästä.

Tietojenkalastelutestin toteutin knowbe4-yrityksen tekemällä tietojenkalastelu-testiohjelmalla. Koska theFIRMAssa käytetään Turun AMK:n Office365 -sähköpostia, en voinut suoraan sallia lähettämiäni testisähköposteja. Sen sijaan testasin, minkälaisen viestin saan roskapostisuodattimen läpi. Liitteessä 5 on esimerkki epäonnistuneesta sähköpostista ja onnistunut sähköposti on esitetty liitteessä 6. Kyseinen sähköposti lähetettiin 40:lle theFIRMAssa olevalle harjoittelijalle. Kuvassa 8. on esitetty testin tulokset



Kuva 8. Sähköpostitse theFIRMAaan lähetetyn tietojenkalastelutestin tulokset.

6 THEFIRMAN TIETOTURVAN NYKYTILAN ARVIOINTI

Tässä luvussa käyn läpi tietoturvakartoituksessa ja tietoturvatestauksessa havaitut puutteet ja ongelmat ja laatinut riskiarvioinnin löydettyjen puutteiden ja ongelmien perusteella. Arviossa on listattu havaitut riskit, syyt ja erilaiset tekijät riskin taustalla, mahdolliset seuraukset riskin toteutumisesta ja ehdotetut toimenpiteet riskin käsittelylle. Arvioinnin pohjana on käytetty VAHTI-riskinarviointidokumenttia (VAHTI 2017). Liite 7 sisältää yhteenvetoraportti tekemästäni riskinarvioinnista.

6.1 Kotisivut

IBM:n (2018) tekemän analyysin mukaan vuonna 2017 ylivoimaisesti suurin hyökkäysvektori oli komentoinjektio, joka tarkoittaa haitallisen tiedon syöttämistä tärkeän tiedon saamiseksi tai kohdejärjestelmän häiritsemiseksi.

TheFIRMAn kotisivujen testaamisessa ei löytynyt vakavia haavoittuvuuksia. Tämä oli oikeastaan selvää ennen testin aloittamista, koska sivujen toteutus on niin pelkistetty. Sivuilla ei ole yhtään syöttökenttää, joita voisi yrittää hyödyntää, eikä myöskään rekisteröitymistä. Tiesin myös jo entuudestaan, että sivu käyttää SQL-tietokantaa, mutta vain sivulla olevien henkilöiden nimen ja tittelin esittämiseen, joten tietokannasta ei ole mahdollista saada tärkeitä tietoja kuten käyttäjätunnuksia tai salasanoja. Sitä en tiennyt, että sivulla on käytössä Wordfence, joka esti myös bruteforce-hyökkäykset ja XSS-hyökkäyksen.

WordPressin admin-sivu oli saatavilla. Tämä kannattaisi piilottaa, sillä vaikka bruteforce-hyökkäys on tätä kautta hankalaa, voi onnistuneella tietojenkalastelulla saatua admin-tunnusta kuitenkin käyttää. Sivun ottaminen pois käytöstä estäisi tämän mahdollisuuden. Hyökkääjän pitäisi saada WordPress-kehitysalustaan fyysinen yhteys, koska se on paikallisesti hostattu theFIRMAn palvelimella.

Wordfence esti minut heti ensimmäisen väärin menneen sisäänkirjautumisyrityksen jälkeen. En tiedä millä perusteella Wordfence yrityksiä estää, mutta tämä voi ehkä mahdollistaa palvelunestohyökkäyksen, sillä jos jotenkin saisi tietää admin-tunnuksen, mutta ei salasanaa, voitaisiin admin-tunnuksen käyttö estää kirjauttamalla salasana väärin. Tämä

on kyllä WordPressissä helppo resetoida, joten hirveästi hyötyä tästä ei hyökkääjälle olisi.

6.2 Toimitilat

6.2.1 Toimintaympäristön, työ- ja palvelutilojen turvallisuudessa havaittuja puutteita

TheFIRMAn tiloihin pääsee käytännössä kuka tahansa. Vaikka sisäänpääsy vaatii kulkukortin, ei sillä ole merkitystä sen vuoksi, että harjoittelijat eivät yleensä kysy henkilöltä, onko hänellä oikeutta tulla tiloihin tai mitä hän on täällä tekemässä. Olen havainnut asian monta kertaa. Edes uudet, entuudestaan minulle tuntemattomat harjoittelijat eivät kysyneet minulta mitään. Käyttämällä peesausta on myös mahdollista päästä toimitiloihin sisälle. Pääsyn helppous voi johtua harjoittelijoiden suuresta vaihtuvuudesta ja siitä, että tästä asiasta ei kunnolla kerrota, eikä pääsyä valvota.

Avainkortit tuovat pääsynhallintaa yksittäisiin oviin ja jättävät tarkastusreitin, mutta ne eivät itse asiassa ole niin hyviä, koska korteista on helppo kaapata pääsytietoja ja tehdä kopioita (Covington 2015). Tätä asiaa en kuitenkaan pystynyt testaamaan, koska minulla ei ollut käytössäni korttien kopioimiseen tehtyä laitetta.

Edelleen Covingtonin mukaan (2015) suurimpia fyysisiä tietoturvauhkia yrityksille ovat puutteellinen valvonta- ja hälytinlaitteisto. Kamerat voivat suorittaa kahta asiaa, huomata mahdollisen uhan ja mahdollistaa rikoksien tarkastelun. Lisäksi ne vaikuttavat myös psykologisesti. Varkaus on theFIRMAlle suuri uhka, koska sisälle on helppo päästä, tiloissa ei ole valvontakameroita tai hälytinlaitteistoa eikä vierailijoiden taustoja tarkisteta. Mahdollinen ulkopuolinen henkilö voi tulla sisälle esittämällä toista henkilöä ja odottaa, että kaikki muut lähtevät ja sitten varastaa theFIRMAn omaisuutta, kuten tietokoneet, koska niitä ei ole fyysisesti suojattu esimerkiksi turvaketjuilla. Näistä varkauksista ei myöskään jää valvontakameroiden puutteessa mitään jälkiä tai todisteita.

Yleiset taululle kirjoitetut tai luotetuille henkilöille pyydettävät käyttäjätunnukset voivat luoda riskin nollapäivähaavoittuvuuksien hyväksikäytölle.

Käytännön työsuojeluun liittyen theFIRMAn toimitiloista puuttuu myös palonsammutuslaitteisto, eikä tulipalon varalle ole tehty ohjeita tai harjoituksia. Vaikka tiloissa onkin palohälytin, ilman sammutuslaitteita mahdollista tulipaloa ei saada nopeasti sammutettua ja se voi tuhota tärkeää omaisuutta, ja pahimmassa tapauksessa aiheuttaa myös henkilövahinkoja.

Arkaluontoisten jätepaperien hallinta ei ole hallittua. Papereita löytyi lojumasta työpöydiltä, kun ketään ei ollut paikalla. Tuhottavia arkaluontoisia papereita heitetään tavalliseen roskakoriin tai niitä säilytetään jossain siihen saakka, kunnes joku vie ne tietosuojasäiliöön. Asiakastiloja ei ole sijoitettu niin, että asiakkaiden liikkumista voitaisiin valvoa. Neuvottelutiloja ei ole ääni- ja näköeristetty. Asiakaspalvelutilojen puutteet luovat erilaisia uhkia, kuten salakuuntelun.

Yhden ulkopuolisen palvelun salasanaa pidettiin liimapaperilla laatikossa, tämä ei kuitenkaan ollut tärkeä palvelu. En testannut tai kysynyt, onko sama salasana mahdollisesti käytössä muissa palveluissa.

6.2.2 Tiedon ja tietojärjestelmien turvallisuus

Koska tietokoneiden USB-portteja ei ole otettu pois käytöstä, koneisiin on mahdollista asentaa esimerkiksi fyysinen näppäilyntallentaja tai USB-Ethernet-adapteri, ja näitä käyttämällä varastaa käyttäjien salasanat, salakuunnella verkkoa tai esimerkiksi suorittaa mies välissä-hyökkäyksiä. Näiden käyttö ei vaadi sovelluksien asentamista, joten ei ole väliä, vaikka oikeudet asentamiseen puuttuisivat. USB-porttien pois ottaminenkaan ei aina auta tällaisia hyökkäyksiä vastaan, koska osa laitteista on tehty niin, että tietokone ei tunnista niitä USB-laitteina, vaan esimerkiksi HID-laitteina. Näillä laitteilla voidaan myös kiertää se, että Windowsin käyttöjärjestelmiin rakennettu USB-tikulta tehtävä automaattinen käynnistys on nykyään oletuksena pois päältä.

Koska BIOS-salasanaa ei ole asetettu uusiin koneisiin, voidaan Secure Boot -toiminto ottaa koneista haluttaessa helposti pois päältä (toiminto ei ollut tätä kirjoittaessa ollenkaan käytössä). Tämä mahdollistaa esimerkiksi ulkopuolisen käyttöjärjestelmän tai ohjelman käynnistämisen USB-tikulta ja rootkitin asentamisen tietokoneeseen. Tällä tavalla toimimalla hyökkääjä voi saada itselleen järjestelmänvalvojan oikeudet ja pysyvän pääsyn verkkoon, mitä on myös erittäin vaikea havaita. Ongelman luo myös tietokoneiden

sijainti; tietokoneet ovat kahdessa rivissä vastakkain, joten olisi helppo laittaa haitallinen laite edessä olevan tietokoneen taakse ilman, että toinen henkilö huomaa mitään.

Tietojen siirto tietovälineillä ei ole hallittua ja suojattua, eikä turvallisia etätyötapoja ole ohjeistettu. Tietojen siirto esimerkiksi käyttämällä USB-tikkuja luo riskin, että laite jätetään joko pöydälle tai tietokoneeseen kiinni, jolloin joku voi sen varastaa ja saa käsiinsä kaikki tikussa olevat tiedot, jos niitä ei ole salakirjoitettu.

Työasemilla ja palvelimilla olevaa tietoa ja sähköpostiliikennettä ei ole salakirjoitettu. Kaikki luottamukselliset tiedot kannattaa salakirjoittaa, jotta jos ulkopuolinen taho saa tietoja käsiinsä, eivät he voi lukea niitä. Testauksessa huomattiin kuinka helposti esimerkiksi Pod Slurpingia käyttämällä voi varastaa tietoja. Tsb-authorin (2017) mukaan Pod Slurping tarkoittaa tekniikkaa jolla tärkeää tietoa voidaan varastaa tietojärjestelmistä käyttämällä laitteita kuten USB-tikkuja. Hyökkääjä voi laittaa laitteen koneeseen kiinni ja tieto siirtyy nopeasti tähän laitteeseen. (Tsb-author 2017.) Salakirjoitus toisi yhden suojauskerroksen lisää. Myös GDPR:ssa suositellaan salakirjoittamaan kaikki henkilötiedot.

Työntekijöiden salasanojen muotoa ja turvallisuutta ei tarkisteta. Windows group policyssa on määritelty kompleksisuusvaatimus, mutta tämä esimerkiksi sallii käytettävän salasanaa kuten Käyttäjännimi1! ja sen, että salasanan vaihtamiseen riittää vain yhden merkin vaihtaminen, mikä ei ole turvallista. Tämä luo hyökkäysriskin, mikäli sama salasana on käytössä muissa palveluissa ja jokin niistä murretaan ja vuodetaan julkisesti. Hyökkääjän on helppo kokeilla saman salasanan muunnelmia.

Teknisten järjestelmien rikkoutumiseen ei ole varauduttu eikä teknistä ympäristöä ja sen muutoksia ole dokumentoitu. Jos jokin järjestelmä kuten tärkeä palvelin hajoaa, ei varapalvelinta ole olemassa. Tämä voi aiheuttaa pitkän tauon työntekoon. Muutosten dokumentointi on tärkeää, koska harjoittelijat vaihtuvat usein, eivätkä he tällä hetkellä tiedä, mitä heidän edeltäjänsä ovat tehneet. Kuluu paljon työaikaa selvittää, mitä on jo tehty ja mitä tulisi tehdä.

Tietojen hävittämiselle ei ole olemassa hävitysmenettelyä. Tämä luo ensinnäkin riskin sille, että paperisten asiakirjojen sisältämät luottamukselliset tiedot heitetään roskakoriin, eikä luottamuksellisille papereille tarkoitettuun jätesäiliöön taikka paperisilppuriin. Myös kovalevyillä oleva tieto on helposti palautettavissa, jos kovalevyjä ei tyhjennetä tai tuhota

oikein. Hyökkääjä voi ottaa roskakorista nämä paperit tai laitteet, ja saada niiden sisältämät tärkeät tiedot.

Varmuuskopioiden ottamiseen ja palauttamiseen ei ole olemassa toimintaohjeita, eikä varmuuskopioinnin palauttamista testata säännöllisesti. Varmuuskopioita säilytetään vain yhdessä paikassa, joka ei ole paloturvakaappi. Jos tietoturvapoikkeaman, esimerkiksi ransomware-hyökkäyksen, takia menetetään kaikki tiedot eikä varmuuskopioita ole testattu, ei voida olla varmoja siitä, että kaikki tieto saadaan palautettua takaisin. Myöskään automaattisiin varmuuskopioihin ei kannata luottaa, vaan niiden toiminta olisi hyvä tarkistaa välillä manuaalisesti. Varmuuskopioita olisi myös hyvä säilyttää kahdessa eri paikassa siltä varalta, että toinen paikoista tuhoutuu.

6.3 Henkilöstö

Harjoittelijoiden mielestä tietoturva on tärkeää ja theFIRMAn tietoturvan taso on heidän mielestänsä sopivalla tasolla, eikä vaikuta negatiivisesti heidän työntekoonsa. Tietoturvan tasosta olen kuitenkin heidän kanssaan eri mieltä. Harjoittelijoiden mielestä he itse ovat theFIRMAn suurin uhka, josta olen myös tämän tutkimuksen tehtyäni samaa mieltä.

6.3.1 Tietojenkalastelu

Huijausviestien tunnistaminen näyttäisi olevan suuri ongelma. Harjoittelijat eivät tienneet, että tunnetultakaan henkilöltä tulleita sähköpostin liitteitä tai linkkejä ei kannata automaattisesti mennä avaamaan. Tästä aihepiiristä tulisi järjestää erillinen koulutus, vaikka se saattaakin viedä paljon aikaa muilta tehtäviltä. Koulutuksen helpottamiseksi voidaan käyttää netistä löytyviä valmiita opetusvideoita ja pelejä, joissa testataan kuinka hyvin käyttäjä tunnistaa erityyppisiä huijausviestejä.

Yhteensä 17,5 % tietojenkalastelutestiin osallistuneista henkilöistä antoi käyttäjätunnuksensa ja salasanansa. Tämä on lähes kaksi kertaa suurempi mitä keskimääräinen tulos, mutta kuitenkin 7,5 % pienempi kuin keskimäärä koulutussektorilla (Verizon 2018). En pysty sanomaan annettujen ”ei-vastausten” perusteella, olivatko kalasteluviestit menneet suoraan roskapostiin, ei oltu avattu, vaiko käyttäjä ei ollut testiviikolla paikalla. Käyt-

täjät todennäköisesti luottivat liikaa lähettäjään ja osoitteeseen mistä sähköposti oli lähetetty, joka tässä testissä oli väärennetty. Vaikka käytinkin sähköpostissa omaa nimeäni, voisi mahdollinen ulkopuolinen huijausviestin lähettäjä selvittää nimeni ja tittelini theFIRMAn kotisivuilta. Viestissä oli pari kohtaa, joista tämän huijauksen olisi voinut tunnistaa. Käytin allekirjoituksessa tiimiä, jota ei ole olemassa, lisäksi siitä puuttui theFIRMAn logo, jota yleensä sähköpostien allekirjoituksissa käytetään. Myöskin theFIRMAn kotisivujen linkki ei ollut oikea linkki, vaan teksti, joka oli maalattu siniseksi, että se näyttäisi linkiltä. Viimeistään siinä vaiheessa, kun käyttäjä meni linkissä olevaan osoitteeseen, olisi pitänyt huomata kuinka oudolta kyseisen linkin osoite ja sivun ulkonäkö näyttää. Tämän testin suuren onnistumisen myötä en nähnyt tarpeelliseksi suorittaa kohdistettua tietojenkalastelua. Vaikka en testannut haitallisten liitetiedostojen lähettämistä sähköpostilla, niin uskon silti, että tulokset voisivat olla samankaltaisia kuin tietojenkalastelutestissä. Samaan aikaan suoritettavat testit olisivat todennäköisesti laskeneet onnistumisprosenttia.

6.3.2 Henkilöstön tietoisuus ja toimintatavat

Käyttäjät ymmärtävät, että löydettyjä tuntemattomia USB-tikkuja ei kannata laittaa tietokoneeseen kiinni, mutta he ovat liian luottavaisia ja ystävällisiä, jos tuntematon henkilö pyytää heiltä apua ja antaa heille USB-tikun. Eri paikkoihin jätetyssä testissä kukaan ei koskenut kyseisiin tikkuihin. Tämä voi johtua enemmänkin siitä, että USB-tikkua ei kehdata ottaa tai kysyä kenelle se saattaisi mahdollisesti kuulua, vaan se mieluummin jätetään siihen mistä se on löydetty.

Testien perusteella kuitenkin ulkopuolinen henkilö voi helposti tulla toimitiloihin sisälle ja antaa jollekin tiloissa olevalle henkilölle USB-tikun, joka sisältää haitallisen ohjelman, ja saada käyttäjä ajamaan kyseinen ohjelma. Tällä tavalla mahdollinen ulkopuolinen hyökkääjä pystyy esimerkiksi laittamaan tikulle Macro-haittaohjelman, joka suoriutuu, kun käyttäjä hyväksyy macrot ajettavan Microsoft Officen tuotteissa. Näin hyökkääjä voi esittää tarvitsevansa apua ja antaa USB-tikun käyttäjälle ja tiedoston (Word, Excel, PowerPoint) sisältö voi olla normaalia tekstiä, kaavoja tai esitys, mutta se sisältää esimerkiksi takaoven, mikä asentuu, kun käyttäjä hyväksyy makrot. Käyttäjä ei ole tietoinen siitä, että haittaohjelma asentuu hänen koneelleen. Tämä voitaisiin estää käyttämällä Group Policy-asetusta “block macros from running in Office files from the Internet”.

Tietokoneen lukitseminen, kun poistutaan paikalta, on yleisesti hyvällä tasolla, vaikka tässäkin olisi vielä parannettavaa. Lukitsematta jättäminen mahdollistaa takaoven asentamisen esimerkiksi käyttämällä Rubber Duckya, joka luo sen muutamassa sekunnissa.

Harjoittelijat tietävät, että virustentorjuntaohjelma ei suojaa kaikilta mahdollisilta haittaohjelmilta. Suurin osa tietää, että kun tiedosto poistetaan ja roskakori tyhjennetään, niin tämä tiedosto ei täysin häviä järjestelmästä sekä sen, että vaikka tunnetulta lähettäjältä tulee Feedback.doc.exe-niminen tiedosto, tälläistä tiedostoa ei saa avata. Kuitenkin muutama henkilö ei näistä asioista tiennyt, joten nämä aiheet voitaisiin lisätä tietoturvakoulutukseen.

Henkilöstölle ei ole selvää, millaisia tietoja tulisi suojata, eikä ole olemassa tietojen luokitteluohjeita tai käytäntöjä. Tämä luo tietojenkäsittelyyn erilaisia riskejä; esimerkiksi luottamuksellisten asiakirjojen käsittely ei välttämättä ole hallittua, ja tietoja voi päätyä väärälle henkilölle.

Harjoittelijat eivät kirjoita käyttäjätunnuksia tai salasanoja ylös työaseman lähettyville, mutta he käyttävät samaa salasanaa useissa eri palveluissa, joka on selvä tietoturvauhka. Arvioiden mukaan keskivertohenkilöllä on käytössään 30 eri käyttötunnusta, mutta vain kuusi eri salasanaa näille kaikille tunnuksille, lähes 75 % kaikista tileistä on suojattu samoilla salasanoilla (Røgeberg 2018, 6). OpenVPN (2018) tekemän tutkimuksen mukaan 25 % työntekijöistä käyttää samaa salasanaa kaikkiin palveluihin (Madsen 2018). Tekemäni kyselyn mukaan 67 % theFIRMAn harjoittelijoista käyttää samaa salasanaa useissa eri palveluissa. Tämä aiheuttaa suuren tietoturvariskin, koska jos tietomurron seurauksena palvelun salasanat varastetaan, niin hyökkääjät käyttävät näitä samoja salasanoja hyökätäkseen muihinkin palveluihin. Hyökkääjät yleensä valitsevat huonosti suojatun palvelun ja tätä kautta saavat salasanan. Joten ei ole mitään väliä, vaikka palvelu olisikin hyvin suojattu ja salasana erittäin monimutkainen, jos sattuu käyttämään samaa salasanaa muissakin palveluissa.

LastPass (2018) tekemän tutkimuksen mukaan 53 % käyttäjistä ei ole vaihtanut salasanaansa vuoden aikana, kun tietomurrosta on uutisoitu. 42 % säilyttää salasanoja tiedostoissa kuten esimerkiksi Word-dokumentissa tai Excelissä. Käyttäjistä 39 % ei ikinä vaihtaisi salasanaansa, jos se ei olisi pakollista. (Petrillo 2018.) Näitä tuloksia katsoessani ymmärsin, että minun olisi myös kannattanut lisätä omaan kyselyyni nämä kysymykset.

Kyselystä huomaa, että harjoittelijoille on opetettu yleisesti tunnetut salasanakäytännöt (vähintään 8 merkkiä, isoja kirjaimia, erikoismerkkejä ja numeroita), jotka sinänsä eivät nykypäivänä ole enää niin hyviä kuin voisi luulla. SecurityIntelligencen (2017) mukaan heikkojen salasanojen käyttö on aina ollut ongelma organisaatioissa. Tietokoneiden laskentatehon kasvamisen ja laitteiston halpenemisen vuoksi salasanat, jotka ennen oli ajateltu vahvoiksi, voidaan nykyään helposti purkaa. Vuonna 2017 IBM X-Force Red esitti salasanan purkutietokoneen, jolla demonstroi tätä ongelmaa. Hyökkääjät joilla on vain muutama tuhat dollaria rahaa, pystyvät rakentamaan järjestelmän, joka purkaa suurimman osan Windows-salasanoista muutamassa päivässä. (SecurityIntelligence 2017.)

Uusimpien ohjeistusten mukaan pidemmät salasanalauseet, jotka muodostuvat normaaleista toisistaan liittymättömistä sanoista, ovat itseasiassa vaikeampia purkaa ja helpompi muistaa (IBM X-Force Threat Intelligence Index 2018). Tämän vuoksi NIST ja Microsoft suosittelevatkin nykyään, että monimutkaisia salasanoja, jotka sisältävät erikoismerkkejä ja numeroita ei kannata käyttää. Tämä tosin edellyttää, että yrityksessä otetaan käyttöön esimerkiksi Microsoftin AD-salasanapalvelu, joka tarkistaa, ovatko käyttäjien salasanat olleet käytössä tunnetuissa tietomurtotapauksissa. (Paul ym. 2017.) Harjoittelijat kuitenkin ymmärtävät sen, että salasanoja ei saa antaa kenellekään, ei edes järjestelmävalvojille tai muille luotettaville henkilöille, jotka väittävät niitä tarvitsevansa.

Ne harjoittelijat, jotka käyttävät töidensä tekemiseen omaa konettaan, käyttävät tietokoneensa suojaukseen salasanaa, mutta muissa kyselyssä mainituissa suojauskeinoissa on puutteita. Osalta puuttuu kokonaan jopa virustentorjuntaohjelmisto ja palomuuri. Tämä on vakava uhka, joka voi mahdollisesti aiheuttaa haittaohjelmien leviämisen sisäverkossa. Koska osalta harjoittelijoista puuttui omilta koneiltaan kokonaan virustentorjuntaohjelmisto, on haittaohjelmien leviäminen näiden kautta mahdollista. Testien perusteella käyttäjät myös laittavat tuntemattoman USB-tikun koneeseen kiinni, jos sen joku antaa hänelle ja pyytää apua. Näiden takia BYOD-politiikka, jossa määritellään pakollinen virustentorjuntaohjelmisto, tulisi tehdä mahdollisimman nopeasti, koska kaikki harjoittelijat eivät välttämättä ole suojanneet omia koneitaan tarpeeksi turvallisesti. Tähän ongelmaan auttaisi myös Network Access Control -järjestelmä, johon voidaan määrittää, että omalla koneella ei saa verkkoon yhteyttä, jos siitä puuttuu virustentorjuntaohjelmisto tai uusimmat päivitykset.

Kartoituksen perusteella osaa theFIRMAn harjoittelijoista voitaisiin sanoa tahattomiksi sisäpiiriläisiksi, koska he eivät kunnolla suojaa omia tietokoneitaan. Tällä tarkoitetaan sellaisia henkilöitä, jotka huolimattomuuden tai tietämättömyyden takia aiheuttavat tietoturvapoikkeuksen. Vielä suurempi uhka ovat tarkoituksella pahaa tekevät työntekijät. Tahattomat sisäpiiriläiset olivat vastuussa yli 2/3 kaikista vaarantuneista asiakirjoista vuonna 2017. (IBM X-Force Threat Intelligence Index 2018.) Trustwave (2018) raportin mukaan suurimmat sisäpiiriuhat ovat esitetty Taulukossa 1.

Taulukko 1. Suurimmat sisäpiiriuhat (Trustwave 2018).

Uhkatyyppi	2018 raportti
Luvattomat tiedostonsiirrot esimerkiksi sähköpostin tai pilvipalvelun kautta	24 %
Luvattomien ohjelmistojen ja haittaohjelmien asennus	22 %
Pääsynhallinnan muokkaukset tai eskaloituminen	19 %
Heikot salasanat	14 %
Tietoturvapäivitysten ja ohjelmistopäivitysten asennusten puuttuminen	11 %
Yleinen turvallisuuskoulutuksen puute	10 %

Taulukossa esitetyistä asioista täyttyy theFIRMAan liittyvässä aineistossani ainakin yleinen turvallisuuskoulutuksen puute, heikot salasanat ja haittaohjelmien asennusmahdollisuus.

6.3.3 Tietoturvan hallinta ja organisointi

Olin ennen opinnäytetyön tekemistä theFIRMAssa harjoittelussa, jonka aikana tein erilaisia tietoturvaan liittyviä dokumentteja ja ohjeita. Annoin myös muille tehtäväksi tehdä esimerkiksi tietojärjestelmistä, ohjelmistoista, sisäverkosta ja verkkoon kytketyistä laitteista asianmukaiset dokumentit. Kartoitusta tehdessäni huomasin, että näiden uusien dokumenttien tekoa ei oltu vielä aloitettu, eikä vanhoja oltu tehty valmiiksi. Huomasin myös, että tekemiäni ohjeita ja sääntöjä ei noudatettu. Tämä todennäköisesti johtuu harjoittelijoiden suuresta vaihtuvuudesta, henkilökunnan kesälomista ja yleisestä kommunikaation puutteesta.

Käyttöoikeuksien käsittelyä ja myöntämistä ei ole ohjeistettu. Esimerkiksi tilanteeseen, jossa tuntematon henkilö kertoo olevansa uusi harjoittelija, joka tarvitsee käyttöoikeuksia, ei ole minkäänlaisia ohjeistuksia, kuinka tulee toimia. Myös nykyinen henkilö voi pyytää oikeuksia tiettyyn asiaan ja järjestelmänvalvoja voi vahingossa antaa hänelle liikaa oikeuksia tai ei esimerkiksi muista ottaa väliaikaista oikeutta pois päältä.

Virustentorjuntamenettelyjä ei ole ohjeistettu. Vaikka käytössä oleva virustentorjuntaohjelmistot päivittävät ja tarkistavat tietokoneen säännöllisesti, mahdollisten infektioiden varalle olisi hyvä tehdä ohjeet, jotta tiedetään, kuinka näissä tilanteissa toimitaan. Myös henkilöiden omien koneiden varalle tulisi olla ohjeet virustentorjuntaohjelmistojen käytöstä.

Internetin ja sähköpostin käytölle on olemassa ohjeet, mutta niiden toteutumista ei millään tavalla valvota. Työntekijät voivat mahdollisesti mennä kielletyille sivustoille, ladata vahingossa haittaohjelmia tai joutua tietojenkalastelun uhreiksi. Käyttäjiä ei ole kielletty asentamasta verkkoon tai työasemiin ulkopuolisia ohjelmistoja tai laitteita, mutta heillä on kuitenkin oikeudet asentaa ohjelmistoja. Riskiä lisää myös kartoituksessa havaittu tietokoneiden päälle jättäminen, jolloin hyökkääjä voi asentaa koneille mitä haluaa.

Teknisiä suojauskeinoja ei tarkisteta säännöllisesti. Ongelma tässä on dokumentoinnin puute ja lisäksi vielä järjestelmävalvojien vaihtuvuus. Eihän kukaan voi tietää mitä on tarkistettu ja milloin, koska mitään ei dokumentoida. Tämä luo riskin siihen, että tarkistukset jäävät tekemättä kokonaan.

Uusien työntekijöiden taustat tarkistetaan ennen työsuhteen alkamista, mutta tietoturvaasiat eivät ole mukana uusien työntekijöiden tai harjoittelijoiden perehdyttämisessä. Kuinka työntekijät voivat toimia turvallisesti, jos heitä ei ole riittävästi koulutettu näistä asioista? Heille ei myöskään selvitetä tietoturvapolitiikan ja vaitiolositoumuksen merkitystä. Tietoturvapolitiikka määrittää vastuut, tavoitteet ja keinot tietoturvan toteuttamiseen. Jokaisen uuden työntekijän kanssa pitäisi käydä tietoturvapolitiikka läpi, jotta työntekijät tietävät, kuinka toimitaan. Sisäistä viestintää ja työhön perehdyttämistä tulisi edelleen kehittää, sillä harjoittelijat eivät tiedä, kuka on vastuussa theFIRMAn tietoturvasta, eivätkä ole lukeneet tietoturvaan liittyviä asiakirjoja, kuten tietoturvapolitiikkaa tai hyväksyttävän käytön politiikkaa. Tämä on osittain ymmärrettävää harjoittelijoiden suuren vaihtuvuuden takia, mutta jokaisen uuden harjoittelijan aloittaessa hänelle tulisi pitää tietoturvakoulutus, jossa käydään läpi ohjeistukset sekä muut tietoturvaan liittyvät asiakirjat.

Työntekijöiden ei tarvitse allekirjoittaa erillistä sitoumusta tietojen ja järjestelmien käytöstä tai tietojen palauttamisesta työsuhteen jälkeen, eikä myöskään ole suunniteltu toimenpiteitä, joilla varmistetaan tietoturvallisuus työsuhteen päättyessä. Työsuhteen päättyessä ei huolehdita, että kaikki työntekijän käytössä olleet työ-, tallennusvälineet sekä asiakirjat palautetaan takaisin. Tästä olisi hyvä tehdä jonkinlainen sopimus ja muutenkin varmistaa, että kaikki hallussa olevat tiedot palautetaan, jotta vältytään erilaisilta mahdollisilta tietoturvaloukkauksilta esimerkiksi henkilötietojen päätyessä väärään paikkaan. Myöskään riitaisaan irtisanoutumiseen tai irtisanomiseen ei ole varauduttu. Nieles ym. (2017) mukaan mahdollisten työntekijöiden aiheuttamien vahinkojen lieventämiseksi, irtisanotun työntekijän pääsyoikeudet tulisi välittömästi ottaa pois käytöstä ja henkilö tulisi saattaa ulos yrityksen tiloista (Nieles ym. 2017, 22).

TheFIRMAlla ei ole toiminnan turvaamisen strategiaa eikä ole laadittu tietoturvallisuuden soveltamissuunnitelmaa. Tietojen käsittelytapoja ja turvajärjestelyjä ei arvioida. Ei ole tunnistettu tilanteita, jotka saattavat lamauttaa, häiritä tai haitata liiketoimintaa ja liiketoiminnassa tarvittavien tietojen saantia. Turvaamisen tavoitteita tai turvatyön mittareita ei ole määritelty. Yrityksellä ei ole myöskään toipumissuunnitelmaa tai toimintaohjeita, jotka ohjaisivat vastuuhenkilöitä ja henkilöstöä varajärjestelyjen käyttöönotossa ja toiminnassa häiriötilanteissa. Jos tietomurtojen tai poikkeamien tai muiden tilanteiden varalle ei ole olemassa ohjeita, ei henkilökunta voi tietää kuinka näissä tilanteissa tulisi toimia. IBM X-Forcen (2018) mukaan ne organisaatiot, joilla on varautumissuunnitelmat tieto-

murron varalle ja jotka ovat kouluttaneet henkilöstöä näiden suunnitelmien toteuttamiseen, pystyvät reagoimaan nopeammin ja toipumaan hyökkäyksistä pienemmällä iskulla, lyhyemmillä häiriöajoilla ja pienemmillä taloudellisilla tappioilla.

7 POHDINTA

Opinnäytetyöni lähtökohtana oli toimeksiantajan halu kehittää tietoturvan tasoa. Opinnäytetyön tarkoituksena oli tehdä toimeksiantajalle tietoturvakartoitus sekä -testaus, joilla voitiin tarkistaa tietoturvan nykytila. Kartoituksessa ja testauksessa löydetyistä havainnoista tein riskien arvioinnin, jossa määrittelin löydetyille riskeille syyt ja tekijät niiden taustalla, seuraukset riskien toteutumisesta, riskien todennäköisyyden, vaikutuksen, suuruuden ja toimenpide-ehdotukset. Kartoituksen ja testien perusteella voidaan sanoa, että työssä saadut tulokset vahvistavat ammattilaisten keskuudessa vallitsevan yleisen ajattelumallin, jonka mukaan ihminen on aina organisaation tietoturvan heikoin osa.

Koska tietoturva on erittäin laaja aihealue, päätin keskittyä testauksessa fyysiseen tietoturvaan sekä käyttäjien manipulointiin. Opinnäytetyön teoriaosuuden rajaaminen tuottikin paljon ongelmia aihealueen laajuuden vuoksi, ja jouduin rajaamaan ja karsimaan työtä melko paljon.

Tavoitteeni tätä työtä tehdessä oli, että tietoturvakartoitusta ja testauksesta löytyneitä tuloksia voitaisiin käyttää tietoturvankehityssuunnitelman tekemiseen ja saada theFIRMAn tietoturva GDPR artikla 32:n mukaiselle vaatimustasolle sekä tulevaisuudessa täyttämään ISO 27001 -standardin vaatimukset. Käytännössä tämä oli hankalaa, sillä asianmukaisten toimenpiteiden määrittely vaatii lisätietoa. Toimenpiteissä olisi otettava huomioon esimerkiksi käytössä oleva rajoitettu budjetti sekä oppilaitoksen säännöt ja sen käyttämät sisäiset tietoturvaratkaisut, joihin ei voida itse vaikuttaa.

Työn teoreettisen osuuden oli tarkoitus kertoa tietoturvasta yleisesti ja käydä läpi suurimmat uhat sekä riskienhallintaa, jotta theFIRMA voisi tulevaisuudessa jatkaa tästä työstä eteenpäin tekemällä kehityssuunnitelmassa kerrotut toimenpiteet sekä jatkaa tietoturvan kehittämistä itsenäisesti. Työn laajuuden vuoksi jouduin lopulta karsimaan paljon teoriaa pois ja päätin teoriaosiossa keskittyä pääosin käyttäjän manipulointiin, koska se vaikutti testien perusteella olevan suurin ongelma. Koen onnistuneeni antamaan arvokasta tietoa tietoturvan nykytilasta ja kehitettävistä kohteista. Työni tavoitteet toteutuivat itseäni tyydyttävällä tavalla ja toimeksiantaja oli tyytyväinen tekemääni tietoturvankehityssuunnitelmaan ja siinä mainitsemiini parannusehdotuksiin.

Tietoturvakartoitus toteutettiin harjoittelijoille lähetetyllä kyselyllä ja muutaman avainhenkilön haastatteluilla sekä omatoimisella katsauksella. Kartoituksen haastatteluosuutta varten käytin hyväksi VTTeen tekemää Pk-yrityksen riskienhallinnan -työvälinesarjassa olevia kysymyksiä. Haastattelun aikana huomasin, että osa kysymyksistä oli aiheeni kannalta epäoleellisia. Kysymykset olisi kannattanut käydä läpi tarkemmin ennen haastattelua ja muokata niitä sopivammiksi. Huomasin puutteita myös harjoittelijoille annetussa kyselyssä siinä vaiheessa, kun kirjoitin tietoturvan nykytilan arviointia. Tässä tapauksessa minun olisi kannattanut ensin tehdä tutkimus ja vasta sitten luoda kysely. Tietoturvakartoituksen lopputuloksena sain kuitenkin selkeän käsityksen tietoturvan nykytilasta ja kehitettävistä asioista, joiden pohjalta loin tietoturvakehityssuunnitelman.

Henkilökohtainen tavoitteeni oli oppia enemmän yleisesti tietoturvasta ja sen kehittämisestä ja tietoturvakartoitusten tekemisestä. Olin tätä ennen tutkinut asiaa vain teoreettisesti, enkä ikinä päässyt oikeasti testaamaan näitä asioita, sillä lainsäädäntö asettaa tiettyjä rajoituksia. Työni aihealue oli minulle ennestään tuttua ja olin tehnyt samankaltaista työtä aiemminkin pienemmässä mittakaavassa. Työni aikana sain tutustua laajasti tietoturvan eri osa-alueisiin. Mielestäni sain paljon hyötyä tästä projektista ja opin uusia asioita. Sain muun muassa käytännön kokemusta käyttäjien manipuloinnista.

Käyttäjien manipulointi sujui kuten olin alun perin ajatellutkin, vaikka kalasteluviestin onnistumisprosentti hieman yllätti; oletin, että vastaajat IT-opiskelijoina olisivat osanneet välttää näitä. Koulussa pitäisikin mielestäni lisätä tähän aihepiiriin liittyvää koulutusta. TheFIRMAssa olisi myös hyvä kehittää harjoittelijoiden tietoturvatietoisuutta. Tähän on kyllä tekeillä tietoturvapeli, mikä voi auttaa asiaa. Tietojenkalastusviestin tekemisessä oli omat ongelmansa. Meni monta yritystä, ennen kuin sain tehtyä sopivan viestin, joka pääsi Office 365 -roskapostisuodatuksen läpi. Vaikka en olisi onnistunut tietojenkalastelussa saamaan kenenkään salasanaa, olisi kuitenkin ollut erittäin helppoa päästä sisälle toimitiloihin ja asentaa tietokoneisiin esimerkiksi fyysinen näppäilyn tallentaja. Lisäksi harjoittelijoita voidaan huijata asentamaan haittaohjelma, kuten takaovi heidän tietokoneelleen, antamalle heille USB-tikun ja pyytämällä avaaman siinä olevan tiedoston.

Ongelmana testien toteuttamisessa oli se, että theFIRMAssa olevat henkilöt tuntevat minut, joten en voinut tehdä mitään testejä, missä minun olisi itse pitänyt olla paikalla, (esi-

merkiksi USB-tikkujen antaminen tai esimerkiksi puhelimen välityksellä tapahtuva käyttäjän manipulointi). Toisen USB-testin jouduinkin toteuttamaan kolmannen osapuolen avulla.

Kotisivuja olisi voinut testata laajemmin, mutta tästä aiheesta riittäisi varmasti muutenkin materiaalia toisen opinnäytetyön tekemiseen. Harjoittelijoille tarkoitettuun kyselyyn olisi ollut hyvä saada enemmän harjoittelijoita mukaan. Kyselyssä oli mukana 23 henkilöä, eikä tämä välttämättä ole tarpeeksi suuri määrä tehtäessä oikeita johtopäätöksiä havaituista ongelmista. Lisäksi käyttäjän manipulointia ja tietojenkalastelua olisi voinut viedä vielä pidemmälle tekemällä erilaisia testejä. Tarkoituksena olikin jossain vaiheessa lähettää sähköpostia, jossa olisi liitteenä tiedosto, joka sisältäisi haittaohjelman, mutta tämä jäi lopulta tekemättä. Myös sisäverkkoa olisi voinut testata siltä varalta, jos sieltä löytyisi haavoittuvuuksia. Tämän voisi toteuttaa esimerkiksi skannaamalla kaikki tietokoneet, ja etsimällä puuttuvia kriittisiä päivityksiä tai avoimia palveluja/portteja, joita voisi hyödyntää.

LÄHTEET

Aitel, D. 2012. Why you shouldn't train employees for security awareness. Saatavilla https://www.csoonline.com/article/2131941/security-awareness/why-you-shouldn-t-train-employees-for-security-awareness.html. Viitattu 28.5.2018.

Avecto 2017. Microsoft vulnerabilities report 2017. Saatavilla: https://engage.avecto.com/microsoft-vulnerabilities-report-2017?utm_content=Web-ResourcesMSVR. Viitattu 6.6.2018.

Cherdantseva, Y. & Hilton, J. 2013. A Reference Model of Information Assurance & Security* http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf. Viitattu 21.5.2018.

Covington, R. 2015. Physical security: The overlooked domain. Saatavilla: https://www.csoonline.com/article/2939322/security/physical-security-the-overlooked-domain.html. Viitattu 20.5.2018.

Crawley, K. 2017. All About the CIA Tried. Saatavilla: https://threatvector.cylance.com/en_us/home/all-about-the-cia-triad.html. Viitattu 20.5.2018.

ENISA 2005 - 2018. Risk Treatment. Saatavilla: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment. Viitattu 7.6.2018.

Euroopan parlamentti & Europaan unionin neuvosto 2016. General Data Protection Regulation. Saatavilla: https://gdpr-info.eu/art-32-gdpr. Viitattu 12.6.2018.

Finjan Team 2017. What is Non-Repudiation? A Closer Look at the Principles, Techniques and Best Practices. Saatavilla: https://blog.finjan.com/what-is-non-repudiation/. Viitattu 20.5.2018.

Giannoulis, P. & Northcutt, S. 2015. Physical Security. Saatavilla https://www.sans.edu/cyber-research/security-laboratory/article/281. Viitattu: 20.5.2018.

Grassi, P., Garcia, M. & Fenton, J. 2017. NIST Special Publication 800-63-3. Digital Identity Guidelines. Saatavilla: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf. Viitattu 19.08.2018.

Hakkarainen, J. 2018. Helsingin yliopistoa riivaa poikkeuksellisen suuri kalasteluviestien tulva – satoja ihmisiä on haksahtanut antamaan tietonsa rikollisille. Saatavilla: https://www.hs.fi/kaupunki/art-2000005805242.html. Viitattu 1.9.2018.

IBM 2018. IBM X-Force Threat Intelligence Index. Saatavilla: https://www.ibm.com/security/data-breach/threat-intelligence. Viitattu 3.6.2018.

Izzat Alsmadi, Robert Burdwell, Ahmed Aleroud, Abdallah Wahbeh, Mahmoud Al-Qudah, Ahmad Al-Omari. 2018. Practical Information Security: A Competency-Based Education Course (e-Pubversio). 5-7. p. Sveitsi: Springer. Saatavilla: https://books.google.fi/books?hl=fi&lr=&id=WNBJDwAAQBAJ&oi=fnd&pg=PR5&dq=Whitman,+M.,+%26+Mattord,+H.+(2013).+Management+of+information+security+(4+ed.).+Nelson+Education%5CCengage+Learning.&ots=wHbc56igoR&sig=fscF6KMLZOoAwjAAl6-CHh4gczA&redir_esc=y#v=onepage&q&f=false. Viitattu 21.5.2018

Järvinen, P & Rousku, K. 2017. Työpaikantietoturva opas – tunnista uhat, hallitse riskit. 46. p. Helsinki: Alma Talent.

Kaspersky n.d. What is malicious code? Saatavilla: https://www.kaspersky.com/resource-center/definitions/malicious-code. Viitattu 1.6.2018.

Kerttula, E. 2000. Tietoverkkojen TIETOTURVA. 83, 88, 105-106. p. Helsinki: Edita.

Khan, R. 2010. Practical Approaches to Organizational Information Security Management. p. 3-6. Saatavilla: https://www.sans.org/reading-room/whitepapers/leadership/practical-approaches-organizational-information-security-management-33568. Viitattu 6.6.2018.

KPMG n.d. Hallinnollinen tietoturva. Saatavilla: https://home.kpmg.com/fi/fi/home/palvelut/neuvontapalvelut/liikkeenjohdon-konsultointi/tietoturvapalvelut/hallinnollinen-tietoturva.html. Viitattu 6.6.2018.

Kyrölä, T., Vuori, M. & Halmevuo, J. 2004. Pk-yrityksen riskienhallinnan työvälinesarja. Saatavilla: http://virtual.vtt.fi/virtual/pkrh/riskilajit/tietoriskit/tietoriskit.html. Viitattu 2.7.2018.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja - Ohjeistus, toteutus ja lainsäädäntö. 17.-18. p. Helsinki: Edita.

Madsen, N. 2018. OpenVPN study reveals employee behavior have a direct impact on corporate cybersecurity effectiveness. Saatavilla: https://www.privatetunnel.com/news/cyber-hygiene-openvpn-study. Viitattu 18.6.2018.

Miller, G. 2016. 60 % of small companies that suffer a cyber attack are out of business within six months. Saatavilla: https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/. Viitattu 5.10.2018.

Mitre n.d. Risk Identification. Saatavilla: https://www.mitre.org/publications/systems-engineering-nistguide/acquisition-systems-engineering/risk-management/risk-identification. Viitattu 7.6.2018.

Nieles, M., Dempsey, K. & Pillitteri, V. 2017. Special Publication 800-12 Revision 1. An Introduction to Information Security. Saatavilla: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf. Viitattu 21.5.2018.

NIST 2012. Guide for Conducting Risk Assessments. Special Publication 800-30. Saatavilla: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. Viitattu 22.5.2018.

Peiponen, P. 2018. Katso paljastava piilokameravideo – Ylen toimittaja testasi tärkeiden yritysten ja laitosten tilaturvallisuutta: Lähes kaikilla puutteita kulunvalvonnassa. Saatavilla: https://yle.fi/uutiset/3-10320853. Viitattu 28.7.2018.

Perlroth, N. 2017. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. Saatavilla: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html. Viitattu 10.7.2018.

Perrin, C. 2008. The CIA Triad. Saatavilla: https://www.techrepublic.com/blog/it-security/the-cia-triad/. Viitattu 20.5.2018.

Petrillo, K. 2018. New research: psychology of passwords, neglect is helping hackers win. Saatavilla: https://blog.lastpass.com/2018/05/psychology-of-passwords-neglect-is-helping-hackers-win.html/. Viitattu 18.6.2018.

Røgeberg, J. 2018. Security 2018 report. 5-8. p. Saatavilla: https://www.mnemonic.no/globalassets/noindex/security-report-2018.pdf. Viitattu 4.6.2018.

Rosvold, O. & Moe, J. 2018. Security 2018 report. 42. p. Saatavilla: https://www.mnemonic.no/globalassets/noindex/security-report-2018.pdf. Viitattu 4.6.2018.

SandboxEscaper 2018. Saatavilla: https://www.kb.cert.org/vuls/id/906424. Viitattu 28.8.2018.

SecurityIntelligence 2017. ‘Cracken’ Passwords with EvilMog of IBM X-Force Red. Saatavilla: https://securityintelligence.com/media/cracken-passwords-with-evilmog-of-ibm-x-force-red/. Viitattu: 4.6.2018.

Soriano, M. 2013. Information and Network Security. 7. p. Czech Technical University in Prague. Saatavilla: http://improvet.cvut.cz/project/download/C2EN/Information_and_network_security.pdf. Viitattu 27.5.2018.

The Europen parliament and the council of the europen union 2018. GDPR. Saatavilla: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Viitattu 4.6.2018.

TheFIRMA 2018. Saatavilla: https://thefirma.fi/?page_id=42. Viitattu 1.6.2018.

Trustwave 2018. Security Pressures. Saatavilla: https://www2.trustwave.com/rs/815-RFM-693/images/TW_2018_Pressures_Security_Report_Final.pdf. Viitattu 15.6.2018.

Tsb-author 2017. What is Pod Slurping? Saatavilla https://www.thesecuritybuddy.com/data-breaches-prevention/what-is-pod-slurping/. Viitattu 20.5.2018.

Turner, P. 2016. Risk management Handbook. Establish the context. Saatavilla: https://industry.gov.au/resource/Programs/LPSD/Risk-management/Risk-analysis-and-control/Pages/Establish-the-context.aspx. Viitattu 7.6.2018.

VAHTI 2009a. Fyysinen turvallisuus. Saatavilla: https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus. Viitattu 20.5.2018.

VAHTI 2009b. Laitteistoturvallisuus. Saatavilla: https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus. Viitattu 6.6.2018.

VAHTI 2009c. Ohjelmistoturvallisuus. Saatavilla: https://www.vahtiohje.fi/web/guest/ohjelmistoturvallisuus. Viitattu 6.6.2018.

VAHTI 2009d. Tietoaineistoturvallisuus. Saatavilla: https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus-tietopaaoman-hallinta. Viitattu: 5.6.2018.

VAHTI 2009e. Tietoliikenneturvallisuus. Saatavilla: https://www.vahtiohje.fi/web/guest/tietoliikenneturvallisuus. Viitattu 6.6.2018.

VAHTI 2009f. Käyttöturvallisuus. Saatavilla: https://www.vahtiohje.fi/web/guest/kayttoturvallisuus. Viitattu 6.6.2018. Viitattu 6.6.2018.

VAHTI 2017. Riskienhallintatyökalu. Saatavilla: http://vm.fi/documents/10623/1898625/Riskiarviointi+laaja/3980a4f9-d94b-4014-a259-3c46fe1a05ab. Viitattu 6.6.2018.

Warren, J. 2014. ISO27005 and the Risk Assessment Process. Saatavilla: https://www.vigilantsoftware.co.uk/blog/iso27005-and-the-risk-assessment-process/. Viitattu 7.6.2018.

Verizon 2018. Data Breach Investigations Report. Saatavilla: https://www.verizonenterprise.com/verizon-insights-lab/dbir/. Viitattu 2.6.2018.

Viestintävirasto 2018. Suomalaisten selväkielisiä salasanoja paljastunut. Saatavilla: https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2018/varoitus-2018-01.html. Viitattu 26.8.2018.

Wombat security 2018. State of the Phish. https://www.wombatsecurity.com/state-of-the-phish. Viitattu 22.5.2018.

Väisänen, M. 2018. TheFIRMA:n tietoturvapäällikön henkilökohtainen tiedonanto, keskustelu. 20.5.2018.

Xifof n.d. Laitteistoturvallisuus. Saatavilla: https://www.xifof.com/laitteistoturvallisuus/. Viitattu 6.6.2018.

Information security instructions for personnel

1. USER IDS AND PASSWORDS

The quality of the password affects the security of the service if the system does not include a different authentication method. Quality means that an outsider is not able to guess or clarify a password even if he/she has personal information about the user, a computational password or IT tools such as password-breaking programs. Passwords can be broken more and more rapidly as computers and storage devices get faster and computing capacity increases. A good starting point for the length of the password is 15 characters. Instead of passwords, you should use passphrase if the system accepts it. When multiple characters are used in a password, breaking it is more difficult. Often, it is required that the password be case-sensitive, lower case letters, numbers and special characters. It is not advisable to use obvious substitutions (i = 1, o = 0, € = e, a = 4, s = 5) for numbers or letters because they are easy to guess. If you have trouble remembering many different passwords, a password-management program such as KeePass can be used. When popular services are breached, massive number of passwords are often stolen. For this reason, different passwords should always be used in different services, so that no one else can access other services where the same stolen password is in use.

- Do not tell anyone your personal username, PIN or passwords. Also, a person who is present in an enterprise such as an IT Support Person should not be given a password. IT support will never need your password for doing their job. As a rule of thumb, the user should remember that the password should not be given to anyone.
- Use different passwords for different services - never use the same usernames and passwords for other services you use at work.
- Change your password regularly.
- Make sure your passwords are long enough and complicated. Do not use normal, everyday words. Good password includes big and small letters, numbers and special characters, and it's easy to remember but hard to guess.
- Do not write your passwords or keep them in a place where they can be easily found.
- Do not use the "remember password" function of the software.

2. Premises security

The safety of premises ensures that data, documents and ICT equipment are stored in safe locations. The security of the premises includes eg. access control, technical control, security, fire, water, electric, air conditioning and burglary protection, and messenger services and shipments containing sensitive data. A data breach can happen by traditional methods instead of technical means. Pay attention to strangers who do not have an access right to the company premises.

- Ensure that non-accessible materials are not visible in the conference rooms. When the meeting ends, make sure that any secret or trusted material and notes do not fall on the desk, board or trash.
- Do not leave confidential documents on your desktop when you leave the office.
- Do not leave guests alone in meeting or work areas.
- Make sure the doors are locked when you leave the company premises.
- Do not let outsiders to the company premises.
- Follow the "clean table" principle. Do not store confidential information on the desktop.
- If you print out confidential information, do not leave them in the printer, get them instantly.

3. Internet and communication solutions

Internet and communication solutions (e-mail, calendar, instant messaging, e-conference services) are a good tool for searching and working on information regardless of time and place. However, it should be remembered that e-mail or the Internet does not in itself have any security, but the data is unencrypted on the public network. Using the Internet and communication solutions requires the user to be careful.

- Do not visit websites that are not part of your job.
- When using a browser, make sure that sensitive information is send protected over the network. The connection is encrypted when the address bar of the browser has the letters HTTPS.
- Be careful - If necessary, "Cancel" if the web page does not seem reliable and the site suggests or requires downloading a file on your computer. Ask for help if needed.
- Internet and communication solutions are intended for work use at the workplace. Use private email for private communications.
- Use only the services that you know are safe and which are allowed by theFIRMA.
- It is illegal to pass confidential information on the Internet without proper encryption, such messages and files must be encrypted with products or services approved by theFIRMA.
- It is not worth responding to spam, as you will ensure that you are using this email and spammer will send you more spam.
- If you receive an email from another person, direct the message to the recipient and inform the sender of the recipient's correct email address. If the correct address is not known, report the wrong transmission to the sender. Remember, you have a confidentiality obligation on the message you received.
- Make sure that the email you send is targeted to the right people and the correct addresses, including when you are using distribution lists.
- Downloading and installing programs is forbidden, if you need specific program to hand your work, ask permission for it.

4. Using Terminal devices

Terminal device means a device that uses the organization's data in a terminal device, electronic datasystems or other services. In addition to desktop workstations and laptops, terminal devices include phones and tablets. The data processing of the terminal device can be done on the device itself, and the software or operating environment that is firmly installed or can be started from external exchangeable memory, for example, USB memory. Portable terminals pose a greater risk than conventional desktops, from the point of view of accidental loss or theft. Therefore, make sure that the devices are automatically locked.

- Do not let anyone, even a person you know, use any of your terminal devices.
- Do not install programs or change settings unless this is part of your work.
- Check the memory card, CD / DVD, or other media with an antivirusprogram that is from outside of the organization before using it, unless the antivirus program performs it automatically.
- Always lock your workstation when leaving.
- Prevent unauthorized use of your terminal device by automatically locking it.
- Ensure the physical security of your terminal device (do not leave them in a free time, for example, in a car).

5. Data security

Data security is about protecting data in different forms. It applies to paper documents, optical and magnetic memory media, microfilms, recordings and other similar technical equipment. Data security covers the processing rules of the data from its creation to the destruction.

- Follow the instructions of your organization on how to classify documents.
- Handle (for example, save, move, print, send, copy, transport, store, file, discard) confidential information in accordance with your organization's instructions.
- When creating a confidential document, you are responsible for classifying it.
- When handling confidential information, make sure that third party cannot see information from documents or computer screen.
- If a hard drive or other media, such as a USB-stick or DVD, is corrupted or disabled, do not place them in the trashcan, but in a waste container for data protection media.
- Do not place confidential documents in the garbage bin, but in a waste bin intented for confidential papers.

6. Social engineering

Phishing is a technique that seeks to get private information. Usually, a phisher sends an email that appears to come from a trusted company - a bank or a credit card company - asks to ”certify" the information and warns of any penalties if it does not. An email usually contains a link to a fraudulent webpage that seems to be trustworthy. Be cautious with unusual e-mails, especially if they have attachments, attachments may contain malware. A phisher can also appear as a person responsible for data processing in an organization that asks for a user name and password to access different data systems and services online. Phishing has also been made through text messaging, calls and instant messaging. Calls and text messages have also been used to support e-mail frauds to increase credibility.

The password can also be get with an eavesdropping or illicit viewing. Watching people in a public place can see a lot: what passwords are being typed into and what kind of services are beign logged in. It is therefore essential to enter a password so that third parties cannot see it.

- Be very careful about what you do with email, which contains an attachment or link to an external website, even if the email is from a sender you know well, and even if the message and the name and attachment type appear to be related to your job.
- Service Providers will never ask for your password.
- If possible, ask an information security manager or system administrator to ensure the attachments that cause doubt before opening it.

Tailgating is a technique where an attacker trying to reach a restricted area that has been secured by electronic access control, such as an RFID card, by simply walking past a person with a legitimate access. A person entitled to a general courtesy generally keeps the door open to the attacker or the invaders themselves can ask the employee to keep the door open. A legitimate person may not necessarily ask for an identity document for various reasons, or accepts the claim that the attacker has forgotten or lost the proper identifier. An attacker can also falsify the display of an identity symbol.

7. Social media

Social media does not, in itself, bring new security challenges, but social media uses differ significantly from traditional media usage and traditional Internet services, which is why security threats appear differently. This is because in social media, user actions are more central to the normal use of services. Unintentional negligence can lead to unpleasant consequences, such as leakage of organizational information, presentation of personal opinions as an organization's official statement, spread of malware, etc. Employee must not cause any harm to the employer, so be aware of loyalty and confidentiality.

- Please note that service providers can access all the information that is being processed in the service, including bilateral discussions. It may be impossible to delete the information that came to the Internet at a later date.
- Only handle information in the service tha has been approved by theFIRMA (note what information is public, what is confidential).
- Do not discuss about work assignments in non-work-related services or systems. This also applies to the use of social media.
- Only accept contacts that you identify to your network. Do not accept unknown people and do not open any links that came from th

Tietoturvankehityssuunnitelma

1 HALLINNOLLINEN TIETOTURVA

1.1 Tietoturvaohjelma

TheFIRMA luo tietoturvaohjelman, joka perustuu jatkuvaan uhkien, haavoittuvuuksien ja riskien tunnistamiseen sekä ulkopuolelta tulevien vaatimusten kuten lakiasioiden ja oman toiminnan ja ongelmien seurantaan. Tunnistetut kehittämispuutteet viedään tietoturvaohjelmaan, jossa arvioidaan tasasin väliajoin nykytilan aiheuttamat riskit ja uhat ja näistä mahdollisesti aiheutuvat menetykset. Tästä prosessista vastaa tietoturvaryhmä. Tietoturvaohjelman tavoitteena on luoda vuosittainen kehityssuunnitelma, erillisiä kehittämisprojekteja sekä lista kehittämiskohteista. Toteutettavaksi valitut toimenpiteet vastuutetaan ja niiden toteutus organisoidaan. Osana ohjelmaa on luettelo valituista tietoturvaprosesseista ja –toimenpiteistä sekä niille asetetuista vastuuhenkilöistä.

TheFIRMA perustaa tietoturvaryhmän, joka kokoontuu kerran kuukaudessa ja käy läpi toiminnan kehittämistä, ohjeiden ja koulutuksen läpikäymistä, tietoturvapoikkemat sekä vuosittain tarkastaa olemassa olevan toipumis- ja jatkuvuussuunnitelman sekä toteuttaa näiden harjoituksen. Tietoryhmän kokoonpano: tietoturvapäällikkö, theFIRMAn johto, toimitusjohtaja, pääkoodari ja järjestelmänvalvojat.

1.2 Vastuut

Johdon velvollisuus on sitoutua tieturvaohjelman luomiseen, käyttöönottoon, käyttöön, valvontaan, katselmointiin, ylläpitoon ja parantamiseen mm. seuraavilla tavoilla:

- Huolehtimalla, että käytettävissä on riittävät edellytykset tieturvan kehittämiseen
- Asettamalla tietoturvatavoitteet
- Varmistaa, että tietoturvaan liittyvät roolit ja vastuut on määritelty
- Viestittää henkilökunnalle tavoitteiden ja tietoturvapolitiikan ja muiden siihen liittyvien poliitikkojen, ohjeiden ja suositusten noudattamista ja niihin liittyvistä lakisääteisestä velvoitteiden noudattamisesta

Tietoturvapäällikkö vastaa theFIRMAn tietoturvasta sekä tietoturvaryhmän toiminnasta.

Tietoturvapäällikön vastuulla on mm.

- Tietoturvapolitiikan kehitys
- Tietoturva-asioiden organisointi ja kehitys
- Ohjeistuksen toteuttaminen
- Tietoturvatason seuraaminen
- Tietoturvatietouden ylläpitäminen
- Tietoturvasta raportointi johdolle

Tietosuojaan liittyvissä asioissa, tietoturvapäällikkö raportoi Turun amk:n tietosuoja vastaavalle.

Kaikki theFIRMAn työntekijät ja harjoittelijat ovat omalta osaltaan vastuussa tietoturvan toteutumisesta sekä tietoturvaohjeiden noudattamisesta. Jokainen on velvollinen ilmoittamaan havaitsemistaan tietoturvauhista, -riskeistä, -häiriöistä ja –poikkeamista sekä tietosuojaloukkauksista tietoturvapäällikölle. Jokaisen theFIRMAn esimiehen tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään.

1.3 Omaisuuden hallinta

TheFIRMAn omistamista ja käyttämistä fyysisistä ja virtuaalisista laitteista, tietojärjestelmistä, palveluista sekä ohjelmistoista ja lisensseistä luodaan omaisuusluettelo. Laitteiden, rekistereiden ja tietojärjestelmien omistajuus sekä luetteloiden katselmointi ja päivitys on organisoitu ja vastuutettu. Kaikilla theFIRMAn omaisuudella tulee olla omistaja, joka vastaa sen tietoturvasta. Omistajat vastaavat kohteiden tunnistamisesta ja luokittelusta annettujen ohjeiden mukaisesti. Omistajat luokittelevat omaisuuden tarvittavan tietoturvallisuustason kohteiden kriittisyyden mukaan. Palveluiden ja järjestelmien omistajat myös dokumentoivat kohteiden tietosisällön. Tietosisällön osalta erityisen tärkeää on, sisältääkö palvelu tai tietojärjestelmä henkilötietoja.

1.4 Jatkuvuus- ja toipumissuunnitelma

TheFIRMAlla on olemassa oleva jatkuvuus- ja toipumissuunnitelma. Näissä suunnitelmissa sisältää vastuut ja toimenpiteet erilaisissa yrityksen toimintaan kohdistuneissa häiriötilanteissa. Suunnitelmat sisältää:

- Ohjeet kuinka häiriötilanteissa toimitaan
- Keinot, joilla varaudutaan erilaisiin poikkeustilanteisiin
- Prosessit, tehtävät, henkilöt ja vastuut
- Häiriötilanteessa sovellettavat menettelyohjeet
- Ohjeet palautumisesta normaalitoimintaan

1.5 Järjestelmäkehitys

Tietojärjestelmän kehitysprojektin alussa määritellään kriittisyysluokitus, turvallisuustarpeet ja -taso sekä huomioidaan ja kirjataan tietoturvavaatimukset. Tietojärjestelmän testaus on suunniteltava sekä hallinnolliselta että tekniseltä kannalta. Testaus kohdistuu joko kertaluonteisesti osaan tai koko järjestelmään tai säännöllisesti tuotantoympäristöön, jolloin voidaan testata vähitellen järjestelmässä tapahtuvia pieniäkin muutoksia.

Tietoturva ja huolellinen suunnittelu ovat theFIRMAssa osa kehitystä heti projektin alusta lähtien ja tietoturva huomioidaan jokaisessa projektin tai toimeksiannon toteutusvaiheessa. Kehitysprojektin tietoturvavastuut on määriteltävä projektin käynnistysvaiheessa.

1.6 Riskienhallinta

TheFIRMAssa tehdään vuosittainen suojattavien kohteiden tunnistus, luokittelu ja tietoturvariskien arviointi. Tämän tuloksena laaditaan riskienhallintasuunnitelma, jonka perusteella parannetaan tietoturvaa tietoturvaryhmän päättämillä toimenpiteillä.

Riskienhallinta dokumentti tulee osana tätä opinnäytetyötä, josta voidaan tarvittaessa jatkaa tai ottaa mallia tai kehittää omanlainen systeemi. Riskienhallinta osiossa kerrotaan myös tarkemmin, miten riskienhallinta toteutetaan ja mitä siihen kuuluu.

1.7 Politiikat, dokumentit, ohjeet

TheFIRMA ottaa käyttöön tässä opinnäytetyössä tekemäni henkilökunnan tietoturvaohjeet, jotka löytyvät liitteestä 1.

Tämän lisäksi erilaisia poliitikkoja ja asiakirjoja joita suosittelen theFIRMAn tekemään ja ottamaan käyttöön:

- BYOD policy
- Disaster Recovery/Business Continuity plan
- Muutoksen hallinta dokumentti
- Access control policy
- Backup policy
- Information classification policy
- Network security policy
- Physical security policy
- Wireless network and guest access policy

2 FYYSINEN TURVALLISUUS

2.1 Kulunvalvonta

Tuntemattomia henkilöitä ei saa päästää toimitiloihin. Vierailijoita, asiakkaita tai muita kolmansia osapuolia ei saa jättää toimitiloihin yksin ilman valvontaa. Vierailusta vastaava henkilö varmistaa, että näin tapahtuu.

2.2 Toimitilat

Henkilökunnan tulee huolehtia siitä, että toimitiloihin ja muihin tiloihin ei jätetä luottamuksellista materiaalia.

Toimitiloihin asennetaan kameravalvonta sekä ostetaan palonsammutuslaitteisto.

Asennetaan sandbox-ympäristö tai käytetään ylimääräistä tietokonetta, joka ei ole verkossa, tuntemattomien USB-tikkujen ja muiden laitteiden testaamiseksi.

3 LAITTEISTOTURVALLISUUS

Palvelimien ja sovellusten ylläpito on estetty normaaleilta työasemilta. Kaikki tähän liittyvät työt pitäisi tehdä erillisiltä ylläpitoasemilta tai palvelimilta, jotka toimivat korkeammalla tietoturvatasolla kuin normaalit työasemat. Internetyhdeydet on rajoitettu näiltä ylläpitoasemilta. Jokaiselle henkilölle, jotka tarvitsevat suurempia oikeuksia, tulisi tehdä erillinen admin-tunnus, johon on määritelty oikeudet jotka henkilö tarvitsee työtehtäviensä tekemiseen. Tätä tunnusta tulisi käyttää vain kun tarvitaan, muulloin käytetään normaalia käyttäjätunnusta, millä ei ole hallinnollisia oikeuksia.

Kaikkia laitteita tulee hallita aktiivisesti verkossa niin, että vain valtuutetuille laitteille annetaan pääsy ja luvattomat ja valvomattomat laitteet löytyy ja niiden pääsy verkkoon estetään. Työasemat tulee olla yksilöityjä ja tietoverkon tunnistettavissa niin, että yksittäinen laite voidaan merkitä lähiverkkoon kuuluvaksi tai kuulumattomaksi.

Kaikista verkossa olevista tietojärjestelmistä ja verkkolaitteista ylläpidetään omaisuusinventaariota jossa on vähintään verkon osoite, laitteen nimi, niiden tarkoitus ja omistaja. Otetaan käyttöön 802.1x -autentikointijärjestelmä. Tätä verrataan omaisuusinventaariossa oleviin laitteisiin kun päätetään ketä saa pääsyn verkkoon ja ketä ei. Kaikille laitteille tulee tehdä turvaluokitus.

Ennen kuin uusi laite kytketään verkkoon, oletussalasanat ja käyttötunnukset vaihdetaan kaikille ohjelmistoille ja laitteille. Kauan poissa käytöstä olleiden koneiden ohjelmat tarkistetaan ennen niiden kytkemistä sisäverkkoon.

TheFIRMAn käytössä olevat laitteet on dokumentoitu. Dokumentti sisältää tarkat kuvaukset käytössä olevista laitteista ja niiden käyttöohjeista. Dokumentaation ylläpidosta vastaa järjestelmänvalvojat.

Käytöstä poistuvien laitteiden magneettisten tallenteiden sisältö täytyy tuhoa luotettavalla menetelmällä. Tietojen poistoon käytetään niihin tarkoitettuja erikoisohjelmistoja. Niiden poistosta vastaa järjestelmänvalvojat.

Kaikkiin tietokoneisiin asetetaan BIOS-salasana sekä Secure Boot -ominaisuus.

4 OHJELMISTOTURVALLISUUS

Kaikki järjestelmät konfiguroidaan tekemään lokitiedon ja varoituksen, kun tunnus lisätään tai poistetaan Domain Administrator -ryhmästä tai kun uusi Local Administrator -käyttäjä on lisätty järjestelmään. Myös väärin menneistä sisäänkirjautumisyrityksistä tulee olla lokitieto.

Koska theFIRMAssa tehdään paljon ohjelmistoja asiakkaille, suosittelen ottamaan käyttöön Application threat modeling- ja System development lifecycle -prosessit. Lisäksi ohjelmistokehittäjiä tulee kouluttaa turvalliseen ohjelmointiin.

TheFIRMAn kotisivujen julkinen admin-sivu otetaan pois käytöstä.

4.1 Virustorjunta

Virustorjuntaohjelmistot konfiguroidaan niin, ettei käyttäjillä ole mahdollista tehdä muutoksia ohjelmien asetuksiin eikä sammuttaa tai poistaa tätä ohjelmistoa. Järjestelmävalvojien tulisi seurata torjuntaohjelmiston käyttöön liittyviä tapahtumia. Torjuntaohjelmiston tulee riittävän usein tarkistaa virustunnisteiden ajantasaisuus ja suorittaa haittaohjelmien skannaus.

TheFIRMA ottaa käyttöön Network access control (NAC), joka asetetaan niin, että se estää tietokoneiden pääsyn verkkoon, jos niissä ei ole asennettu virustorjuntaohjelmistoa eikä uusimpia käyttöjärjestelmäpäivityksiä.

4.2 Dokumentaatio

Kaikista theFIRMAn käytössä olevista ohjelmistoista on olemassa dokumentaatio, josta selviää vähintään ohjelmiston nimi, mihin se on asennettu, ohjelmistoversio ja lisenssitiedot.

5 TIETOAINEISTON TURVALLISUUS

Tiedon tuottaja on sen omistaja. Omistaja on vastuussa tiedon turvaluokituksesta turvaluokituskäytännön mukaisesti. Tiedon haltija on se ketä käyttää tietoa mutta ei ole sitä tuottanut. Tiedon haltija käsittelee tietoa sen luokituksen määräämällä tavalla. Kaikki mahdolliset asiakirjat, tietojärjestelmät ja muut aineistot luokitellaan theFIRMAn tietoturvaluokituspolitiikan mukaisesti kolmeen eri luokkaan: julkinen, sisäinen tai salainen.

5.1 Tietoaineistojen käsittely, suojaaminen, säilytys ja tuhoaminen

Salassa pidettäviä tietoja tulee käsitellä huolellisesti niin, että vain siihen oikeutetut henkilöt pääsevät käsiksi salassa pidettävään tietoon. Tietoja tullaan käsittelemään niiden luokittelun perusteella asetettujen ohjeiden mukaan. Tärkeiden ja sensitiivisten tietojen suojaamiseksi otetaan käyttöön esimerkiksi Bitlocker-ohjelma, jolla salakirjoitetaan salassa pidettävät tiedot. Sensitiivisten paperisten tietojen säilyttämiseen hankitaan lukollinen arkistointikaappi ja poistettaville papereille hankitaan pieni tietosuojasäiliö. Tarpeettoman salaisen paperisen tiedon tuhoamiseen hankitaan paperisilppuri.

6 TIETOLIIKENNETURVALLISUUS

Verkkoliitännät suojataan niin, että sisäverkkoon on pääsy ainoastaan sallituilla osapuolilla. Tarpeettomat palvelut, ohjelmat ja protokollat poistetaan verkon aktiivilaitteista. Laitteiden portit tulee estää oletuksena uusien laitteiden vapaan liittämisen sisäverkkoon. Sisä- ja ulkoverkon liikennettä tulisi rajoittaa niin, että vain tarpeellinen liikenne pääsee läpi. Sallitut yhteydet ulkoverkosta pitää dokumentoida. Etäyhteyksien tekemiseen käytetään VPN-tunnelointia.

Verkko jaetaan käyttötarkoituksen mukaan loogisesti erilliseen aliverkkoihin kuten sisäinen, ylläpito, testi, kehitys tai asiakasverkko. Ulkoverkkoon tarjottavien palveluiden tulee sijaita sisäverkosta erotetulla DMZ-alueella.

Tietoliikennettä tulisi seurata ja suodattaa, jotta saadaan haitallinen kuormittaminen rajoitettua ja haittaohjelmat ja roskaposti havaittua, estettyä ja poistettua.

Verkon tietoturva tulisi auditoida säännöllisesti kerran vuodessa ja aina kun tehdään merkittäviä muutoksia.

Otetaan käyttöön automaattinen haavoittuvuusskanneri kuten openvas, joka automaattisesti skannaa verkon läpi kerran kuukaudessa ja etsii mahdollisia haavoittuvuuksia.

6.1 Tiedonsiirto

Luottamuksellisten tietojen siirtoon käytetään hyväksi havaittuja salauskäytäntöjä. Uusia tietoliikenneyhteyksiä avatessa on tiedonsiirtoon liittyvät riskit ja uhat otettava huomioon. Luottamuksellisten tietojen tallentaminen internettiin ei ole sallittua.

6.2 Ohjelmistojen käyttö

TheFIRMAn tietoverkkoa saa käyttää vain ja ainoastaan työtehtäviensä hoitamiseen. Ohjelmien lataaminen ja asentaminen tulee olla estetty normaaleilta käyttäjiltä. Vain järjestelmävalvojilla on oikeus asentaa ohjelmistoja. Käyttötunnusten oikeuksiin

käytetään Least Privilege -periaatetta, joka määrittää, että kaikilla käyttäjillä, ohjelmilla tai prosesseilla on vain minimioikeudet, jotka ovat välttämättömiä sen toiminnan kannalta.

Turun ammattikorkeakoulusta saatua sähköpostiosoitetta ei saa käyttää muihin kuin theFIRMAn ja kouluun liittyvissä asioissa. Vapaa-ajan sähköpostia saa käyttää vain vapaa-ajan toimintoihin. Arkaluontoisten ja luottamuksellisten tietojen lähettämiseen ei saa käyttää tavallista sähköpostia vaan se lähetetään salattuna.

6.3 Auditointi

Verkon tietoturvallisuus auditoidaan säännöllisesti vähintään vuoden välein ja aina merkittävien muutosten yhteydessä joko omin resurssein tai ulkopuolisen tahon toimesta.

6.4 Dokumentaatio

Sisäverkosta sekä verkkoon kytketyistä laitteista ja komponenteista tehdään ajantasainen dokumentaatio.

7 HENKILÖSTÖTURVALLISUUS

7.1 Henkilöstö ja harjoittelijat

Työ-/harjoittelusuhteen alussa jokainen henkilö tullaan perehdyttämään theFIRMAn työtapoihin ja tehtäviin. Osana jokaisen uuden henkilön perehdyttämistä ovat tietoturva-asiat. Työ-/harjoittelusuhteen päätyttyä tulee henkilön tunnukset ottaa pois käytöstä sekä kaikki theFIRMAlle kuuluva omaisuus otetaan takaisin.

7.2 Tietoturvakoulutus ja ohjeistus

TheFIRMAn työntekijöiltä ja harjoittelijoilta ei voida edellyttää oikeanlaisia työtapoja ja menetelmien osaamista jos ei ole saatavilla olemassa olevia tietoturvaohjeita sekä niiden noudattamiseen kehitettyä koulutusta ja perehdyttämistä. Ohjeiden pitää olla kaikkien saatavilla ja jokainen jäsen tullaan perehdyttämään näiden ohjeiden sisältämään tietoon. TheFIRMAn tulisi järjestää aina uusi tietoturvakoulutus kun uusi erä harjoittelijoita saapuu ja varmistaa, että he ymmärtävät koulutuksen sisällön ja heillä on riittävä osaaminen suoriutua työtehtävistään tietoturvallisilla toimintatavoilla. Henkilökunnan ja harjoittelijoiden tulee sisäistää theFIRMAn tietoturvapolitiikka ja tähän liittyvät muut dokumentit ja ohjeet.

Suosittelen otettavaksi käyttöön jatkuvan tietoturvatietoisuusohjelman, jossa toteutetaan erilaisia testejä, kyselyitä, tietoiskuja ja opetusta. Jotta tietoturvan opettelusta saataisiin mielenkiintoisempaa ja hauskempaa, voidaan tietoturvakoulutukset pelillistää tietovisan tyylisiksi. Osana ohjelmaa voi olla kuukausittainen tietoturva hints, tips and tricks -ohjelma, jossa käydään läpi ajankohtaisia asioita ja annetaan ohjeita kyseisistä asioista. Ohjelmassa voidaan käyttää apuna esimerkiksi https://www.wombatsecurity.com/demo-security-awareness-training-modules-2017 olevia opetusohjelmia sekä https://www.sans.org/security-awareness-training/ouch-newsletter löytyviä kuukausittaisia uutiskirjeitä.

8 KÄYTTÖTURVALLISUUS

8.1 Työpisteet ja työasemat

TheFIRMAn laitteet on tarkoitettu vain työtehtävien hoitoon. Jokainen käyttäjä vastaa oman työasemansa turvallisesta käytöstä saamiensa ohjeiden mukaan. TheFIRMAssa käytetään puhtaan pöydän periaatetta, kaikki luottamuksellinen materiaali tulee poistaa työpöydältä ja säilyttää asianmukaisesti esim. lukitussa kaapissa sekä tietokone täytyy olla lukittuna aina kun poistutaan työpisteeltä. Harjoittelijat jotka käyttävät töissä omaa tietokonettaan, huolehtivat oman tietokoneensa tietoturvasta myös vapaa-aikana.

8.2 Varmuuskopiot

Palvelinten tiedostojen varmuuskopiointi on automatisoitu tapahtumaan riittävän usein. Varmuuskopioinnin onnistumista valvotaan systemaattisesti. Palvelinten ja muiden verkkokomponenttien varusohjelmistoympäristöstä asetuksineen otetaan varmuuskopiot ennen olennaisia muutoksia, asennuksia tai vastaavia toimenpiteitä sekä edellä mainittujen toimenpiteiden jälkeen.

Varmuuskopiotallenteita säilytetään riittävän monta varmuuskopiosukupolvea palo- ja murtoturvallisessa paikassa. Tallennusvälineitä, joissa varmuuskopioita säilytetään, voidaan kierrättää ja käyttää uudelleen.

Tärkeimmistä järjestelmistä otetaan suojakopioita katastrofi- ja kriisitilanteiden varalta ja niitä säilytetään palvelimista niin etäällä, etteivät sekä palvelimet että suojakopiot voi tuhoutua samassa onnettomuudessa.

8.3 Lokienhallinta

Kaikkien järjestelmien ja sovellusten, jotka käsittelevät tai sisältävät luottamuksellista tietoa, hyväksyvät yhteyksien muodostamista tai tekevät pääsynhallintapäätöksiä (autentikointi tai valtuutus) on tuotettava lokitietoja, joiden avulla pystytään vastaamaan vähintään seuraaviin kysymyksiin:

- Mikä toiminto suoritettiin?

- Kuka tai mikä suoritti kyseisen toiminnon ja missä tai millä järjestelmällä toiminto suoritettiin?
- Mihin toiminto kohdistui?
- Koska toiminto suoritettiin?
- Mikä oli toiminnon tila (onnistui/ epäonnistui) tai lopputulos?

Lokientuottamista määritettäessä on huomioitava tarkasti kerättävien lokien tarpeellisuus ja tarkoitus. Lokien säilyttämistä varten lokeille on määritettävä säilytysajat. Lokien säilyttämiselle voi olla ulkoisia vaatimuksia lainsäädännöstä, mikä tulee huomioida lokien säilytysaikoja määritettäessä. Lokit tulee poistaa, kun tarve niiden säilyttämiselle on päättynyt. Ylläpitäjillä ei tule olla mahdollisuutta poistaa ylläpitolokeja, jotka muodostuvat heidän omista toimistaan. Lokeja tulee seurata tietoturvapoikkeamien havaitsemiseksi.

Haastattelu kysymykset

Henkilöstön tietoisuus tietoriskeistä

Onko henkilöstölle koulutettu nykyaikaisen liiketoiminnan ja tuotekehityksen luottamuksellisuuteen ja tietosuojaan liittyviä yleispiirteitä?

Tunteeko henkilöstö yrityksen vastuut tietojen luottamuksellisuuden ja muun tietoturvallisuuden suhteen?

Onko kaikille selvää, millaisten tietojen suojaaminen on tärkeää?

Onko kaikille selvää, mitä yrityksen toiminnasta saa kertoa ulkopuolisille?

Onko yritykselle määritelty tietoturvaperiaatteet ja laadittu niiden toteuttamiseksi ohjeet?

Kattavatko ohjeet sähköisten tietojärjestelmien lisäksi suullisen viestinnän ja paperidokumenttien käsittelyn ja jakelun?

Onko henkilöstö koulutettu tunnistamaan tietoriskejä ja noudattamaan yrityksen turvakäytäntöjä?

Onko olemassa menettely tietoturva-asioiden käsittelyä varten?

Onko jokainen työntekijä allekirjoittanut tietojen käyttösäännöt?

Ovatko tietojen luokitteluohjeet ja käytännöt osa arkipäivän toimintaa?

Tietääkö henkilöstö, minne ilmoittaa havaitsemistaan tietoturvarikkeistä tai käytäntöjen puutteista?

Uudet työntekijät

Tarkistetaanko uusien työntekijöiden taustat ennen työsuhteen alkamista?

Ovatko tietoturvaasiat mukana uusien työntekijöiden perehdyttämisessä?

Selvitetäänkö myös uusille ja väliaikaisille työntekijöille yrityksen tietoturvapolitiikan ja vaitiolositoumuksen merkitys?

Allekirjoittavatko työntekijät erillisen sitoumuksen tietojen ja järjestelmien käytöstä sekä tietojen palauttamisesta työsuhteen jälkeen?

Työsuhteen päättyminen

Onko suunniteltu toimenpiteet, joilla varmistetaan tietoturvallisuus työsuhteiden päättyessä?

Onko henkilön irtisanoutumistilanteessa esimiehellä tieto kaikista henkilön käyttäjätunnuksista ja käyttöoikeuksista, joiden voimassaolo tulee poistaa?

Huolehditaanko, että kaikki työntekijän käytössä olleet työ-, tallennusvälineet sekä yritystä koskevat asiakirjat palautetaan yritykselle?

Onko varauduttu työntekijöiden riitaisaan irtisanoutumiseen tai irtisanomiseen?

Onko irtisanomistilanteissa varmistettu, että irtisanomisperuste on lainmukainen ja dokumentein perusteltavissa?

Henkilöstön toimintatavat

Käsittelevätkö työntekijät työhönsä liittyviä, luottamuksellisia tietoja tarkoituksenmukaisesti?

Ovatko yrityksen keskeiset tiedot suojattu mm. rajaamalla niiden saatavuus ja määrittelemällä niiden käyttöoikeudet?

Onko minimoitu mahdollisuus myydä tai luovuttaa yritykselle keskeisiä tietoja ja dokumentteja?

Ovatko yrityksen sisäiset valvontajärjestelmät asianmukaiset (työnvalvonta, tilojen valvonta, tietojen käytön ja tietojärjestelmien valvonta)?

Onko työntekijöiden omien töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)?

Onko luottamuksellisten tietojen säilyttämiseen riittävästi lukittuja tiloja?

Hoidetaanko jätepaperin keräys ja käsittely hallitusti?

Ovatko puhelinkäyttäytymisohjeet olemassa?

Onko toiminta tulipalon varalle ohjeistettu ja harjoiteltu?

Onko varahenkilöjärjestelyistä huolehdittu?

Tietojärjestelmien ja tietokoneiden käyttö

Onko henkilöstöllä riittävä perusosaaminen järjestelmien käyttöön?

Saavatko työntekijät häiriö- ja virhetilenteissa apua ja neuvontaa?

Käyttääkö jokainen työntekijä työssään vain omaa käyttäjätunnustaan?

Onko varmistettu turvallisen salasanan muodostaminen?

Onko estetty mahdollisuus muilta työntekijöiltä lukea tai muuttaa käyttäjän tietoja käyttäjän huomaamatta?

Onko varmuuskopioiden ottamiseen ja palauttamiseen olemassa toimintaohjeet?

Valvotaanko varmuuskopioiden ottamista?

Onko Internetin käyttö ohjeistettu?

Onko sähköpostin käyttö ohjeistettu?

Onko virustentorjuntamenettelyt ohjeistettu työ- sekä kotikoneiden osalta?

Ovatko virusohjelmien ja muiden vastaavien päivitykset automatisoitu?

Salakirjoitetaanko kannettavilla laitteilla (tietokoneet, kämmentietokoneet yms.) olevat luottamukselliset tiedot?

Onko käyttäjiä kielletty asentamasta yrityksen verkkoon tai työasemiin ulkopuolisia ohjelmistoja tai laitteita?

Tietojen ja järjestelmien käyttöperiaatteet

Onko järjestelmien käyttöoikeuksien hallintaan nimetty vastuuhenkilö?

Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?

Ovatko pelisäännöt ja käytännöt työnantajalle kuuluvan sähköpostin lukemisesta poikkeustilanteissa sovittu yhdessä henkilöstön kanssa?

Onko jokaisella käyttäjällä oma käyttäjätunnus ja henkilökohtainen salasana?

Onko työntekijöille rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?

Onko luottamuksellisille asiakirjoille ja muille tietovälineille lukitut kaapit?

Onko luottamuksellisten tietojen hävittämiselle silppurit tai lukitut paperisäiliöt?

Onko tietojen siirto levykkeillä, CD:llä ja muilla tietovälineillä hallittua ja suojattua?

Ovatko laitteet, ohjelmistot ja tiedot kirjattu omaisuusrekisteriin mahdollisen varkausvakuutuksen korvausta varten?

Onko turvalliset etätyötavat ohjeistettu?

Teknisen ympäristön hallinta ja valvonta

Ovatko tietotekniset turvatehtävät vastuutettu?

Ovatko teknisen ympäristön ylläpidosta vastaavat henkilöt päteviä?

Onko järjestelmien ylläpidosta vastaavat koulutettu tietoriskien hallintaan ja järjestelmien suojaamiseen?

Ovatko varahenkilöt tietoisia nykykäytännöistä?

Onko tietojärjestelmäsuunnittelijoilla valmius sekä riittävät taidot ennakoida järjestelmää uhkaavat tilanteet ja suunnitella ja arvioida tarpeellisia suojaustapoja?

Ovatko tuotantoympäristön ja kehitys- sekä testausympäristön järjestelmät erillisiä toisistaan?

Seurataanko järjestelmän virheitä ja levytilojen täyttymistä?

Seurataanko järjestelmän käyttöä ja puututaanko siihen tarvittaessa?

Teknisen järjestelmän hankinta, huolto, muutokset ja poisto käytöstä

Huomioidaanko tietoturvallisuusasiat laitehankinnoissa?

Onko varauduttu teknisten järjestelmien rikkoutumiseen (varaosien saatavuus, kahdennus, varajärjestelmät, korvaavat toimintatavat)?

Käytetäänkö vain luotettavia huoltoyrityksiä, joiden kautta tiedot eivät ole vaarassa joutua kolmansille osapuolille?

Onko tekninen ympäristö ja sen muutokset dokumentoitu?

Onko tietojen hävitysmenettely olemassa, jos laitteita myydään työntekijöille tai ulkopuolisille?

Ohjelmistot

Hankitaanko ohjelmistot, laitteet ja muu tuki osaavilta ja luotettavilta toimittajilta?

Käytetäänkö vain lisenssoituja laillisia ohjelmistoversioita?

Selvitetäänkö uusien ja käytössä olevien ohjelmistojen yhteensopivuus ennalta?

Huomioidaanko hankintojen yhteydessä ohjelmistojen turvallisuus ja luotettavuus? (Puolueettomat tutkimuslaitokset, oma testaus)

Ovatko tietojen varmistuskäytännöt vastuutettu ja suunniteltu?

Onko testattu ja harjoiteltu varmistusten palauttamista onnistuneesti?

Säilytetäänkö varmistuksia paloturvakaapissa?

Onko virustentorjuntaohjelmiston ajantasaisuudesta huolehtiminen vastuutettu?

Tapahtuuko työasemien virustentorjuntaohjelmistojen ja vastaavien päivitys automaattisesti?

Tekniset suojaamiskeinot

Tarkistetaanko / auditoidaanko suojaamiskeinojen kattavuus säännöllisesti?

Onko järjestelmien käyttö ilman käyttäjän luotettavaa yksilöintiä estetty?

Varmistetaanko tiedot automaattisesti ja aukottomasti?

Käytetäänkö UPS-laitteita varasähkön ja järjestelmien hallitun alasajon varmistamiseksi?

Salakirjoitetaanko työasemilla ja palvelimilla olevat tiedot ja sähköpostiliikenne?

Vaatiiko käyttöä valvova ohjelmisto salasanalle tietyn määrämuotoisuuden ja

salasanan ennalta ajoitetun vaihtamisen, estääkö se vanhan salasanan käytön?

Tarkistetaanko työntekijöiden salasanojen muoto ja turvallisuus ajoittain?

Jääkö järjestelmän lokitiedostoihin merkintä järjestelmän käyttäjistä?

Rajataanko ulkopuolisilta pääsy yrityksen verkkoon?

Todennetaanko käyttäjä ja tämän oikeudet otettaessa yhteys yrityksen paikallisverkkoon ulkopuolelta?

Käytetäänkö etäyhteyksissä VPN tunnelointia?

Onko asiaton pääsy ja muu asiaton verkkoliikenne yrityksen verkkoon estetty?

Onko paikallisverkko, extranet ja WWW-palvelin eristetty toisistaan riittävästi?

Tarkistetaanko sähköpostiliitteiden asianmukaisuus ja virukset ennen pääsyä

yritysverkkoon?

Tarkistetaanko lähtevät sähköpostiliitteet?

Salakirjoitetaanko kannettavien laitteiden tiedot? (Tietokoneet, kämmentietokoneet, muut kannettavat laitteet, jotka sisältävät yrityksen tietoja.)

Johdon tietoisuus tietoriskeistä

Onko toimitusjohtaja ja johtoryhmä tietoinen tietoriskien vaikutuksista liiketoimintaan?

Onko tunnistettu yrityksen liiketoiminnalle elintärkeät tiedot?

Onko johto sitoutunut tietoturvallisuuden hallintaan?

Tietoriskien hallinnan johtaminen

Onko toiminnan turvallisuudesta huolehtiminen vastuutettu nimetylle henkilölle yrityksen johdossa?

Onko yrityksen omaisuuden ja tietojen suojaamistahto konkretisoitu tietoturvapolitiikaksi ja -käytännöiksi?

Onko yrityksellä toiminnan turvaamisen strategia osana liiketoimintastrategiaa?

Onko laadittu tietoturvallisuuden soveltamissuunnitelma? (Edellytetään esim. BS7799 standardissa)

Arvioidaanko tietojen käsittelytapoja ja turvajärjestelyjä laatujärjestelmän auditointien yhteydessä?

Kykeneekö johto vakuuttamaan omistajat ja sijoittajat tietojen ja tietämyksen säilymisestä yrityksessä?

Ovatko työntekijät motivoituneita työssään ja sitoituneita yritykseen, eivätkä ole esim. siirtymässä kilpailijalle?

Tietoriskien hallinta Tietoriskien tunteminen

Onko tunnistettu tilanteet, jotka saattavat lamauttaa liiketoiminnan?

Onko tunnistettu tilanteet, jotka häiritsevät ja haittaavat liiketoiminnassa tarvittavien tietojen saantia?

Onko tunnistettu tilanteet, jotka voivat aiheuttaa tietojen häviämisen tai muuttumisen? Onko arvioitu em. tilanteiden menetyksiä tai vahinkoja?

Onko turvakäytäntöjen kehittämiskustannukset suhteutettu toiminnan keskeytymisestä aiheutuviin menetyksiin?

Tietoriskien hallintamenettelyt

Onko turvaamisen tavoitteet määritelty?

Onko turvatyön mittarit määritelty?

Onko yrityksellä käytettävissä laaja-alaista turva-asioiden osaamista?

Onko olemassa toimintamalli tietokonevirusten ja muiden haittaohjelmien hallitsemiseksi?

Onko olemassa toipumissuunnitelma ja toimintaohjeet, jotka ohjaavat vastuuhenkilöitä ja muuta henkilöstöä varajärjestelyjen käyttöönotossa ja toiminnassa häiriötilanteissa? Onko käyttäjille laadittu ja koulutettu tietoturvaohjeet?

Seurataanko järjestelmien käyttöä esimerkiksi etäkäyttöä epämääräisinä kellonaikoina, tärkeiden tietojen kopiointia tai lähettämistä?

Tiedotetaanko yrityksessä tapahtuneesta häiriötilanteesta kaikille asianosaisille?

Onko yrityksessä nimetty vastuuhenkilö tietoturvakäytäntöjen kehittämiseen?

Liike- ja sidosryhmäsuhteiden suunnittelu

Onko liikekumppanit luokiteltu toiminnan jatkuvuuden kannalta elintärkeisiin, tärkeisiin ja tarpeellisiin?

Onko eri osapuolten valinnassa huomioitu myös tietoriskit? (Tahojen luotettavuus, kyky hallita heille luovutettuja tietoja jne.)

Onko kaikilla osapuolilla sama käsitys liike- ja sidosryhmäsuhteiden luonteesta?

Liiketoiminnan tietoriskien tunnistaminen

Onko selvitetty ja arvioitu liikekumppaneilla tapahtuvat tilanteet, jotka aiheuttavat haittaa yrityksen liiketoiminnalle?

Onko liikekumppaneilla kirjallinen tietoturvapolitiikka ja toimintamallit tietojen käsittelyyn?

Onko omassa yrityksessä tietoturvapolitiikka dokumentoitu siten, että dokumentti voidaan luovuttaa liikekumppaneille ja kumppanit saavat sen perusteella kuvan toiminnan luotettavuudesta?

Onko kaikkien liikekumppanien tietoturvallisuustoiminta katselmoitu yhteistyössä?

Tietoriskien hallinta. Verkosto- ja alihankintayhteistyön käynnistys

Onko yhteistyöhön luotu yhteiset tietoturvaperiaatteet?

Onko liikekumppanien välisiin yhteistyösopimuksiin liitteestty yrityksen tietoturvavaatimukset sekä tietojen siirron ja käsittelyn menettelyohjeet?

Sovitaanko erilliskäytäntöjä luottamuksellisten tietojen käytöstä, siirto- ja suojaustavoista? (Esim. tuotekehitystiedot)

Onko kaikki osapuolet koulutettu yhteisiin tietojärjestelmiin?

Onko yhteistyössä edellytettävät tietoturvaperiaatteet, menettelytavat ja järjestelmät koulutettu alihankkijoille?

Onko suunniteltu, miten hallitaan yhteistyösuhteen päättyminen?

Onko olemassa käytäntö, jolla käsitellään liikekumppanin henkilöstön tarve päästä yrityksen tietoliikenneverkkoon ja järjestelmiin?

Onko sovittu osapuolten toimenpiteet eri häiriötilanteiden hoitamiseksi?

Arvioidaanko liikekumppanien turvakäytäntöjä?

Asiakkaiden ja yhteistyökumppanien käynnit yrityksessä

Syntyykö asiakaskäynneillä kuva oman yrityksen luotettavuudesta ja luottamuksellisuudesta?

Suojataanko omat ja yhteistyötahojen luottamukselliset tiedot? (Ei neuvotteluhuoneissa, ei asiakaspalvelutiloissa)

Selvitetäänkö uusien vierailijoiden taustat riittävän huolellisesti? (Koskee sekä koti- että ulkomaisia vierailijoita.)

Kiinteistön turvallisuus

Onko kiinteistö altis onnettomuuksille?

Sijaitseeko se lähellä rautatietä tai isoa valtatietä?

Onko sähkön- ja muun energiansaannin häiriöihin varauduttu?

Onko kiinteistössä turvallisuuspäällikkö ja turvallisuussuunnitelma?

Onko kiinteistössä yrityksiä, joissa käy paljon vieraita?

Onko kiinteistössä kulunvalvontaa?

Onko kiinteistössä vartiointia?

Onko kiinteistön yleisiin tiloihin, kuten puhelinkeskukseen, piha-alueelle, kellariin, katolle, asiaton pääsy estetty ja valvottu?

Onko toimitiloissa rikosilmoitinjärjestelmää?

Pidetäänkö toimitilojen ja kiinteistön ulkoovet ja ikkunat aina lukittuina, kun sisällä ei ole ihmisiä?

Onko yrityksen avaintenhallinta asianmukainen?

Toimintatilojen turvajärjestelyt

Onko kulkuoikeuksien myöntäminen nimetty vastuuhenkilölle?

Onko liikkuminen tiloissa rajattua ja valvottua?

Onko muilla kuin työntekijöillä avaimia toimitiloihin, onko näiden avainten hallinta erityisen huolellista?

Onko työntekijöiden omien töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)?

Ovatko vierailusäännöt ja –käytännöt asianmukaisia ja voimassa?

Ovatko tärkeät laitteet, kuten työasemat ja palvelimet, sijoiteltu valvottuihin tiloihin? Onko tärkeät tilat sijoitettu pois viemärien ja putkistojen läheisyydestä?

Onko laitetiloissa nostettu kaikki laitteet pois lattiatasosta?

Onko laitetiloissa ilmastointia? (Lämpötilanvaihtelut sekä savun ja pölyn vaikutukset) Onko laitetiloissa paloilmoitinjärjestelmä?

Onko alkusammutuskaluston käyttöä harjoiteltu?

Onko tulipalon ja muiden hätätilanteiden varalle harjoiteltu tiloista poistumista?

Asiakaspalvelutilat

Pidetäänkö luottamukselliset tiedot poissa asiakaspalvelutiloista?

Pidetäänkö tietokonepäätteet, kirjoittimet, faksit yms. poissa kulkuväyliltä?

Onko asiakastilat sijoitettu siten, että asiakkaiden liikkumista voidaan valvoa?

Ovatko neuvottelutilat ääni- ja näköeristetty?

Huolehditaanko neuvottelutilojen siivouksesta siten, että neuvotteluiden asiakirjat, fläpit, piirtoheitinkalvot sekä muut tietovälineet eivät jää tilaan?

Onko asiakkaiden ja vieraiden käytössä olevat laitteet sellaisessa paikassa, ettei niiden käyttö aiheuta riskiä? (Ei esimerkiksi työhuoneessa)

Kyselyn kysymykset ja tulokset

1. Do you keep your usernames or passwords on paper near your workstation?

100% vastasi ei

2. Do you reuse same password on multiple services?

Yes	11	64,71%
No	6	35,29%

3. What kind of password is good enough in your opinion?

salasna
a few words stringed together
As I've studied the best password is the one that contains a combination of everything, letters, numbers and characters.
characters (uppercase and lowercase) and numbers
complex and long
8-15 kirjainti, isoja kirjaimia sekaisin, numeroita ja erikoismerkkejä myös.
Pitkä salasana joka sisältää isoja ja pieniä kirjaimia, sekä mahdollisesti numeroita/muita merkkejä.
One that has multiple different capital/normal letters and numbers and isn't a clear word.
qwerty
One that has uppercases, lowercases, numbers and preferably one that isn't even a normal word but just randeom letters.
One that you can remember and is like 8 or so chars long so it would take atleast a few tries to bruteforce
long (10 characters minimum), atleast couple of digits and some upper case letters
Capital letters, numbers and minimum length of 8 characters.
password with capital letter, small letter, number, sign and atleast 10 letter long.

6tTjja%dn%df>faDA
Capital letters Lower-case letters At least 8 characters In-cludes numbers and symbols Is not a real word
Long (minimum 12 characters), contains numbers and special symbols in addition to letters.

4. In your opinion, what level theFIRMA's security is?

Poor	0	0%
Nor-mal	15	88,24%
High	2	11,76%

5. Do you know who is responsible for theFIRMA's security?

Yes	6	35,29%
No	11	64,71%

6. What a word "information security" brings to your mind?

lol
protection of personal data stored online, from hackers and leaks.
Security and safety of personal data
security that secures all sorts of informations documents, infor-mation flows, no
privacy
Se tuo mieleen palomuurit ja viruksentorjunnat.
Ihmiset pitää huolta omista tunnuksistaan ja ei tee tyhmiä asi-oita.
Securing information through encryption, virus protection, fire-walls etc.
dirty cow

Strong password
Boring classes
uneasiness of getting personal insensitive information by other unknown individual
Prevention of unauthorized access to information that's supposed to be kept secure.
protection against unauthorized uses
Information: Accessible by the owner solely. strict verification of consent before information exchange Transparency in stored location and process or Not much hidden layers in process
Keeps documents safe from viruses etc and prevents unauthorized access
Guidelines to help users to keep their information safe from malicious intent.

7. Have you read theFIRMA's information security policy?

Yes	8	47,06%
No	9	52,94%

8. When leaving your workstation, how do you secure your computer?

I turn my monitor off	0	0%
I log off	5	29,41%
I lock the computer	9	52,94%
I turn the computer off	1	5,89%
I have a password protected screensaver	1	5,88%
None of the above	1	5,88%

9. Do you leave sensitive documents on your desktop?

Yes	2	11,76%
No	15	88,24%

10. Do you think USB-stick is good place to store sensitive information?

Yes	4	23,53%
No	13	76,47%

11. Should you open any attachments or links in emails from sender you do know?

Yes	7	41,18%
No	10	58,82%

12. If you find a USB-stick lying on the floor/table, what would you do?

rofl
leave it, if it's on the floor put it on a desk or give it to a project leader.
Give it to the responsible in Firma
search for its owner or put it in somekindof foundedbox
give it to the boss
Tarkistan tikun sisällön.
Jätän sen siihen.
Leave it there, it's not mine.
nothing
Probably would give/show it to one of the regulars.
Plug it in and see what it contains

either leave it there or ask around whose USB stick is lying there on the table. If that doesn't work i will ask firmas employees whether or not they can store it somewhere until USB stick owner is identified.
Give it to the information security manager.
handover to responsible person within the room who can further take care of it.
Probably ask if it belongs to someone If not will leave it so or responsibly place it in Lost and Found.
Leave it there (table) or take it to info etc
Hand it over to someone who might know who it belongs to.

13. Person tells you that he/she is responsible for theFIRMA's information systems and needs you username and password. Should you give them to him/her?

Yes	1	5,88%
No	16	94,12%

14. A good and up-to-date antivirus program protects against all viruses?

Yes	1	5,88%
No	16	94,12%

15. When you delete a file and empty recycle bin, does the file gets complete removed from the system?

Yes	4	23,53%
No	13	76,47%

16. Feedback.doc.exe attachment from trusted sender is safe to open?

Yes	4	23,53%
No	13	76,47%

17. Do you know what your own security responsibilities are?

Yes	12	70,59%
No	5	29,41%

18. Do you use your own computer at theFIRMA?

Yes	4	23,53%
No	13	76,47%

19. Have you ever opened theFIRMA's door for someone you don't know?

Yes	0	0%
No	17	100%

20. If you use your own computer, do you have/use?

Antivirus software	4	80%
Firewall	4	80%
Password	5	100%

Encryption	1	20%
UAC	1	20%

21. How do you feel about information security?

Information security enables high-quality activities and gives me my organization a reliable image.	12	70,59%
Information security is needed so that I can handle the information I need at work.	3	17,65%
I understand why data security is needed but it causes extra work.	2	11,76%
Information security is a constant disaster, I do not understand why it is needed.	0	0%

22. How do you feel that information security has been implemented in theFIRMA?

If you answered poorly or very badly, what exactly affects your work?

Very well - work and the use of services are smooth and easy.	13	76,47%
Well, but it may occasionally hamper my work.	4	23,53%
Poorly because it often hampers and complicates my work.	0	0%
Very badly, because it is hindering and hindering my work constantly.	0	0%

23. In your opinion, what is the biggest security threat to theFIRMA?

me, myself and I
password leaks
I don't know what it could be.
Not people from the firma(workers and trainees)
information leaking
Oman laitteen käyttö theFirman verkossa.
(nimi sensuroitu)
The biggest threat is the people who don't know/believe the risks of not following security practices. Lack of information.
lack of pentest
If someone gains access to theFIRMA's network, they could gain access to some of the projects.
NSA
-
Maybe trainee's opening carelessly links and files from email's on theFIRMA's computer. There has also recently been a lot of new trainees and with fairly high turnover rate I could see people getting inside theFIRMA's working place without X person not knowing Y shouldn't be here.
Learners/interns may unknowingly do something wrong.
Since its a learning environment, self-learning is required a lot. So downloads of various programs for work completion knowingly or unknowingly might cause continuous expose to new programs in computer and can be vulnerable.
Leaving sensitive information open when leaving the work-station
Users carelessness with personal computers, accounts or other things related to security.

24. Do you know what constitutes acceptable use of your work computer?

Yes	12	70,59%
No	5	29,41%

Esimerkki roskapostisuodattimeen jääneestä sähköpostista

Dear user,

Your IT administrator has recently enacted a security policy within our system, which changes security requirements for passwords. **All users are required to change their Office 365 password immediately**.

Please click here to log into Office 365 to change your password.

You must complete the password change within 24 hours.

Sincerely,

The Office 365 Team

This message was sent from an unmonitored email address. Please do not reply to this message.

Privacy | Legal

Microsoft

Tietojenkalasteluviesti

PLEASE READ

Due to a recent rise in attacks on computer networks, new regulations and policies have now mandated stricter information security standards. As passwords remain the primary method for defending against unauthorized access, your passwords must be checked for sufficient complexity. You will receive recommendations for making changes if they fall short of the new requirements.

Please help in completing this review as soon as possible by visiting here to test the strength of your passwords. Continuing to use an insecure password may result in your account being locked out.

Thanks for your support.

IT Security Team

Jerry Nurmi

Turku University of Applied Sciences

Joukahaisenkatu 3, 20520 Turku

thefirma.fi

Riskien arvioinnin yhteenveto

#id	ja riskin nimi	Riskin merkittävyys		Toimenpiteet riskille
1	Tulipalo	4	Huomioitava riski	Palosammuttimen tai peitteen osta
2	Luvattomien ohjelmien	4	Huomioitava riski	Estetään ohjelmien asentaminen
3	Luvattoman henkilön p	6	Merkittävä riski	Koulutetaan harjoittelijoita tarkista
4	Tietokoneen lukitsema	8	Merkittävä riski	Käyttäjien koulutus/muistutus tieto
5	Sensitiivinen tieto häv	4	Huomioitava riski	Käyttäjä koulutus, tietojen luokitte
6	Virustorjunnan laiminly	6	Merkittävä riski	Tarkistetaan, että käyttäjät asenta
7	Työntekijän/harjoittelija	1	Ei riskiä	Kerrotaan käyttäjille, että tärkeitä
8	Sisäinen käyttäjäuhka	3	Huomioitava riski	Vanhoilta käyttäjiltä pääsy tiloihin
9	Käyttäjän manipulointi	9	Sietämätön riski	Koulutetaan käyttäjiä havaitsema
10	Laitteisto vika	1	Ei riskiä	Vara palvelin
11	Ohjelmisto vika	1	Ei riskiä	Vara palvelin
12	Haittaohjelmat	8	Merkittävä riski	Henkilökunnan koulutus sähköpos
13	Tietovuoto	1	Ei riskiä	Muistutus sähköpostin huolellises
14	Tietojen muuttaminen	2	Ei riskiä	Muistutetaan huolellisuudesta
15	Tietojen tuhoaminen v	2	Ei riskiä	Muistutetaan huolellisuudesta
16	DoS/DDoS hyökkäys	1	Ei riskiä	Hyväksytään riski
17	Käyttöoikeuksien väär	2	Ei riskiä	Käyttöoikeuksien huolellinen anta
18	Liikenteen analyysi (m	2	Ei riskiä	Koulutetaan käyttäjiä, että ei pääs
19	Varkaus	8	Merkittävä riski	Koulutetaan käyttäjiä, että ei pääs
20	Verkossa haavoittuvu	6	Merkittävä riski	Suoritetaan verkkoskannaus
21	Tietoja ei ole luokiteltu	2	Ei riskiä	Luodaan tietojenluokittelupolitiikka
22	Tietoturvapoikkeusten	6	Merkittävä riski	Järjestelmävalvojien on seurattav
23	Ohjeiden puute	4	Huomioitava riski	Ohjeiden luominen ja kouluttamine
24	Kulunvalvonta	4	Huomioitava riski	Ostetaan kamera
25	Jatkuvuuden hallinta	4	Huomioitava riski	Luodaan jatkuvuudenhallintapolitii