TAMPEREEN
AMMATTIKORKEAKOULU

EDUIX OY:N TIETOTURVARISKIANALYYSI

Taru Pyylampi

Opinnäytetyö
Huhtikuu 2018
Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

PYYLAMPI TARU:
Eduix Oy:n tietoturvariskianalyysi

Opinnäytetyö 60 sivua, joista liitteitä 7 sivua
Huhtikuu 2018

Opinnäytetyönä toteutettiin tietoturvariskianalyysi tietojärjestelmiä ja asiantuntijapalveluita tarjoavalle Eduix Oy:lle. Taustatietoina käytettiin muun muassa ISO/IEC 27001:2013 -standardia, jossa on määritelty vaatimukset informaatioteknologian turvallisuustekniikoille ja tietoturvallisuuden hallintajärjestelmälle. Työn tavoitteena oli kerätä organisaatiossa havaittuja sekä olemassa olevia tietoturvauhkia mahdollisimman laaja-alaisesti sekä täyttää ISO/IEC 27001:2013 -standardin vaatimukset tietoturvariskien arvioinnin osalta. Työssä käytettiin pääasiassa kvalitatiivista riskianalyysimenetelmää ja organisaatiossa havaittujen tietoturvauhkien keräämiseen hyödynnettiin henkilöstölle osoitettua tietoturvauhkakyselyä. Kyselyn avulla kartoitettiin myös Eduix Oy:n tämänhetkistä tietoturvatilannetta. Tietoturvauhkakyselyn aikana henkilöstölle esitettiin tietoturvatietoiskuja, minkä tarkoituksena oli parantaa yrityksen työntekijöiden tietoturvatietoisuutta ja näin havaita laajemmin olemassa olevia tietoturvahaavoittuvuuksia.

Tietoturvauhkakyselyn tuloksista ilmeni henkilöstön havaitsemat tietoturvauhat, jotka liittyivät tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen. Kyselyyn vastasi noin puolet Eduix Oy:n henkilöstöstä ja kyselyn tulokset osoittivat tietoturvallisuuden kehityskohteet. Tulokset olivat myös osiltaan yhteneväisiä ISO/IEC 27001:2013 -standardin tietoturvavaatimusten kanssa. Tietoturvatilanteen kartoitus osoitti Eduix Oy:n huolehtivan tietoturvallisuudesta enimmäkseen hyvin, vaikkakin ISO/IEC 27001:2013 -standardin vaatimusten täyttämiseksi on myös lisättävä joitakin tietoturvallisuuden hallintamenetelmiä. Tietoturvatietoiskujen osalta havaittiin Eduix Oy:n henkilöstön kiinnostus tietoturvallisuutta kohtaan ja halu osallistua tietoturvallisuuden hallintajärjestelmän kehittämiseen.

Tietoturvauhkakyselyssä esille tulleet ja yleisesti olemassa olevat tietoturvauhat koottiin tietoturvariskien arviointitaulukkoon ja jokaisen taulukkoon kerätyn tietoturvauhan haavoittuvuudet, todennäköisyys ja vaikutukset Eduix Oy:lle analysoitiin tarkemmin tietoturvariskianalyysissä. Tietoturvariskianalyysissä pohdittiin myös riskiä alentavia hallintatoimenpiteitä ja nämä hallintatoimenpiteet käytännön esimerkkeineen koostettiin erilliseen dokumenttiin. Eduix Oy:n ylimmälle johdolle luovutettiin kooste tietoturvauhkakyselyn tuloksista, tietoturvariskien arviointitaulukko, tietoturvariskianalyysi sekä ehdotelma tietoturvallisuuden hallintatoimenpiteistä ja nämä dokumentit ovat opinnäytetyön salassa pidettäviä liitteitä. Tietoturvariskianalyysin jälkeen tarkoituksena on toteuttaa ehdotetuista hallintatoimenpiteistä soveltuvimmat ja kehittää tietoturvallisuuden hallintajärjestelmää yhdessä eri liiketoimintayksikköjen edustajien kanssa, jotta lopulta Eduix Oy voisi sertifioitua ISO/IEC 27001:2013 -standardia vasten.

Asiasanat: tietoturvariskianalyysi, tietoturva, organisaatio, riskianalyysi, ISO 27001

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Information and Communication Technology
Telecommunication Technology and Information Networks

PYYLAMPI TARU:
Eduix Ltd's Information Security Risk Analysis

Bachelor's thesis 60 pages, appendices 7 pages
April 2018

The purpose of this study was to identify and analyze the most common information security risks and vulnerabilities in Eduix Ltd. The object of the Eduix Ltd's Information Security Risk Analysis was to formulate documented information of risk assessment and to propose risk management methodologies. This bachelor's thesis is based on ISO/IEC 27001:2013 -standard and the final aim is to fulfill the requirements of the information security management system. The risk assessment was completed by gathering information from the Eduix Ltd's employees about their discoveries of information security risks and vulnerabilities as well as compiling the requirements of the ISO/IEC 27001:2013. The method used in the information security risk analysis was mainly qualitative because of the scenario based risk assessment. In addition, during this risk analysis the awareness of the current information security risks were educated to the employees of the Eduix Ltd.

The results of the discoveries about information security risks reported by the employees consisted of the problems about information's confidentiality, integrity and availability. The most of the observed threats were similar to the requirements in ISO/IEC 27001:2013. When gathering the information security risks inside the organization, the employees were also asked about the current state of information security in Eduix Ltd. The questionnaire indicated that the state of Eduix Ltd's information security is already quite good, but to fulfill the requirements of the ISO/IEC 27001:2013 some management procedures are still needed.

The information security risk analysis consisted of four separate documents which were handed out to the top management of the Eduix Ltd and which are confidential attachments of this bachelor's thesis. The first document was the summary of the results of the employee questionnaire. Another document was the risk assessment table which included all the risks and vulnerabilities gathered from the ISO/IEC 27001:2013 and from the employees. In the information security risk analysis each of these risks and the precautions caused by the risk were covered and the impact and the likelihood of the risk were defined. In the information security risk analysis there were also suggestions of risk treatment methodologies. These methodologies were compiled to the proposal of the risk treatment document, which included the decisions needed by the top management as well as the suggestion of the employees' information security instructions. Further actions after the information security risk assessment would be the risk treatment, which would lead to the statement of applicability and to the certification against the ISO/IEC 27001:2013.

Key words: information security, organization, risk, analysis, ISO 27001

SISÄLLYS

LYHENTEET JA TERMIT

CIA-malli	Tietoturvan analysointimalli, jossa tiedon turvaaminen jaetaan kolmeen osa-alueeseen; luottamuksellisuuteen (*Confidentiality*), eheyteen (*Integrity*) ja saatavuuteen (*Availability*)
DoS	Denial of Service, palvelunestohyökkäys
DDoS	Distributed Denial of Service, hajautettu palvelunestohyökkäys
HTTPS	Hypertext Transfer Protocol Secure on protokolla, jota käytetään tiedon suojattuun siirtoon selaimen ja palvelimen välillä
ICMP	Internet Control Message Protocol, verkkokerroksen informaation välittämiseen käytetty protokolla
ISMS	Information Security Management System, tietoturvallisuuden hallintajärjestelmä
ISO/IEC 27001:2013	Standardi, joka määrittelee vaatimukset organisaation tietoturvallisuuden hallintajärjestelmälle ja informaatioteknologian turvallisuustekniikoille
LAN	Local Area Network, lähiverkko
PDCA	Plan-Do-Check-Act eli Suunnittele-Toteuta-Arvioi-Toimi on prosessin toteuttamiseen ja kehittämiseen käytettävä malli
Phishing	Tietojen kalastelu
Ransomware	Kiristyshaittaohjelmat
RSA	Julkisen avaimen salausalgoritmi
SoA	Statement of Applicability, sovellettavuuden selvitys
Social engineering	Sosiaalinen manipulointi
SSL	Secure Sockets Layer, verkkoliikenteen salausprotokolla
Tietoturvariski	Hyväksyttävän riskitason ylittävä tietoturvauhka
Tietoturvauhka	Yhtä tai useampaa tietoturvan osa-aluetta vaarantava uhka
UDP	User Datagram Protocol, yhteydetön kuljetusprotokolla
VPN	Virtual Private Network, virtuaalinen erillisverkko
WLAN	Wireless Local Area Network, langaton lähiverkko

1 JOHDANTO

Nykypäivänä jokaisen organisaation on panostettava tietoturvallisuuteen ja sen asianmukaiseen hallintaan. Tietoturvauhat kehittyvät ja lisääntyvät joka päivä, minkä vuoksi myös organisaatioiden tulee parantaa ja ylläpitää tietoturvaansa jatkuvasti. Tietoturvalliset toimintatavat ja yhtenäiset toimintalinjaukset ovat toisaalta myös merkittävässä osassa yrityksen liiketoiminnan näkökulmasta. Tietoturvauhkia kohdataan päivittäin, mutta harvassa organisaatiossa osataan tunnistaa niitä tai niiden toteutumisen vaikutuksia.

Tietoturva jaetaan yleisimmin CIA-mallin mukaisesti kolmeen osa-alueeseen; tiedon luottamuksellisuuteen (*Confidentiality*), tiedon eheyteen (*Integrity*) ja tiedon saatavuuteen (*Availability*). Tiedon luottamuksellisuus tarkoittaa käytännössä sitä, että tieto on vain luvallisten henkilöiden saatavissa, eivätkä ulkopuoliset pääse näkemään tai kuulemaan luottamuksellista tietoa. Tiedon eheydellä pyritään puolestaan varmistamaan se, että tietoa ei ole luvattomasti muutettu tai väärennetty ja tarpeen vaatiessa tietoon tehdyt muutokset ovat jäljitettävissä sekä palautettavissa. Tiedon saatavuus merkitsee sitä, että olennainen tieto on esimerkiksi organisaation työntekijöiden saatavilla tarvittaessa.

Jokaiseen tietoturvan osa-alueeseen kohdistuu erilaisia uhkia ja riskejä, joiden toteuttaminen on mahdollista niin organisaation ulkopuoliselle hyökkääjälle, kuin myös organisaatiossa työskenteleville henkilöille. Käytännössä tiedon luottamuksellisuus olisi uhattuna esimerkiksi silloin, jos työntekijä puhuu työasioita ulkopuolisten kuullen tai mikäli ulkopuolinen henkilö pystyy julkisella paikalla tarkkailemaan työntekijän työtietokoneen näyttöä. Tiedon eheys olisi puolestaan vaarassa silloin, jos työtietokoneelle tai organisaation tietojärjestelmiin päästäisi ulkopuolisen henkilön, jolla on mahdollisuus tehdä luvattomia muutoksia tietoihin tietokoneen omistajan tai pääsyoikeuksien haltijan nimissä. Tiedon saatavuuden takaamiseksi tärkeässä roolissa on tiedon asianmukainen dokumentointi ja varmuuskopiointi niin, että se on myös muiden työntekijöiden tai tarvittaessa asiakkaiden saatavilla, mikäli avainhenkilö ei ole paikalla.

Tietoturvaa voidaan jaotella myös monella muulla tapaa. Organisaation tietoturvan voidaan ajatella koostuvan eri henkilöiden, laitteiden, ohjelmistojen ja verkkojen muodostamasta kokonaisuudesta, joiden hallinnoimisessa yhtenäiset toimintalinjaukset ja -ohjeistukset ovat avainasemassa. Ei ole olemassa vain yhtä oikeaa tapaa jaotella, arvioida ja

käsitellä tietoturvallisuutta, vaan parhaat käytänteet voivat vaihdella esimerkiksi organisaation koosta ja toimialasta riippuen.

Organisaation tietoturva alkaa laadukkaasta ja asianmukaisesta johtamisesta sekä hyvästä tietoturvallisuuden hallintajärjestelmästä. Tähän kuuluu muun muassa se, että yrityksessä on pohdittu tietoturva-asioita ja laadittu niitä koskevat selkeät toimintalinjaukset ja -ohjeistukset. Ylimmän johdon osoittama tuki ja esimerkillinen toiminta tietoturvan hallintajärjestelmää kohtaan on ensiarvoisen tärkeää, sillä se kannustaa myös muuta henkilöstöä noudattamaan tietoturvallisia toimintatapoja. Ylimmän johdon käsissä on myös tarvittavien fyysisten suojausmekanismien toteuttaminen ja hallinnoiminen, vaikkakin aloitteet niihin voivat tulla myös muulta henkilöstöltä. Kun hallinnolliset ja fyysiset mekanismit on määritelty ja toimintavalmiudessa, on tärkeimmässä roolissa tietoturvallisuuden hallintajärjestelmässä yrityksen henkilöstö. Täytyy kuitenkin muistaa, että henkilöstö tulee ensin saattaa tietoiseksi heidän panoksensa merkittävyydestä tietoturvallisuuden hallintajärjestelmässä.

Tässä opinnäytetyössä toteutettiin tietoturvariskianalyysi tietojärjestelmiä ja asiantuntijapalveluita tarjoavalle Eduix Oy:lle. Opinnäytetyö etenee tietoturvallisuuden hallintajärjestelmän ja tietoturvariskianalyysissä käytettävien menetelmien esittelystä tietoturvauhkien keräämiseen ja analysointiin. Tietoturvauhkien keräämisessä hyödynnettiin tietoa Eduix Oy:n henkilöstön havaitsemista tietoturvauhista, yleisimmistä suomalaisten organisaatioiden kohtaamista tietoturvauhista sekä ISO/IEC 27001:2013 -standardissa määritellyistä organisaation tietoturvallisuuden hallintajärjestelmän vaatimuksista sekä sen velvoittavasta Hallintatavoitteiden ja -keinojen viiteluettelosta. Tietoturvauhat koostettiin tietoturvariskien arviointitaulukkoon ja jokaisen tietoturvauhan toteutumisen vaikutuksia sekä toteutumiseen johtavia haavoittuvuuksia analysoitiin eri näkökulmista varsinaisessa tietoturvariskianalyysissä. Kaikille kerätyille tietoturvariskeille pohdittiin hallintatoimenpiteitä, joilla pystyttäisiin ennaltaehkäisemään riskin toteutumista tai pienentämään sen toteutumisesta aiheutuvia vaikutuksia. Opinnäytetyön lopussa on esitelty joitakin kehitysehdotuksia tietoturvariskianalyysin toteuttamiseen sekä pohdittu prosessin onnistumista ja havaittujen tietoturvauhkien vastaavuutta olemassa oleviin tietoturvauhkiin. Tietoturvariskianalyysin jälkeisiä toimenpiteitä kartoitettiin koko työn ajan ja työ tähtääkin mahdollisimman mutkattomaan tietoturvariskien käsittelyvaiheeseen.

2 TIETOTURVARISKIANALYYSI OSANA TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄÄ

Tietoturvariskianalyysi on osa yrityksen tietoturvallisuuden hallintajärjestelmää. Tietoturvallisuuden hallintajärjestelmän yhtenä suurimpana tarkoituksena on muodostaa toimintalinjaukset ja menettelytavat muun muassa tietoturvan johtamiseen, hallinnoimiseen ja ylläpitämiseen. Tietoturvariskianalyysin lisäksi muita tärkeimpiä tietoturvallisuuden hallintajärjestelmän osia ovat tietoturvapolitiikka sekä tietoturva-, jatkuvuus- ja toipumissuunnitelmat. (Laakso.)

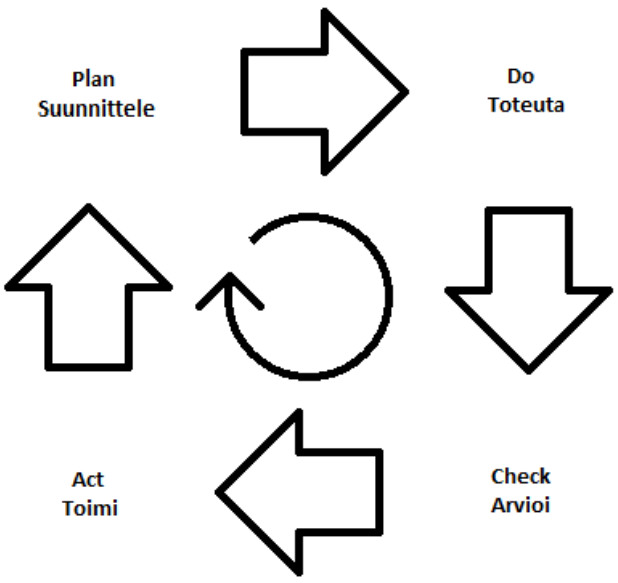
Yrityksen tietoturvallisuuden hallintajärjestelmä eli ISMS (*Information Security Management System*) osoittaa yrityksen huolehtivan omalta osaltaan riittävästi tietoturvallisuudesta sen eri prosesseissa. Tietoturvallisuuden hallintajärjestelmään vaadittavat toimenpiteet on määritetty kansainvälisessä ja ympäri maailmaa tunnustetussa ISO/IEC 27001 -standardissa. Uusimmassa ISO/IEC 27001:2013 -standardissa vaatimuksina on muun muassa tuottaa kirjallista dokumentaatiota organisaation tietoturvariskien arviointimenetelmistä, tietoturvariskien käsittelymenetelmistä sekä sovellettavuuden selvityksestä. Riskien arvioinnin prosessin tulee ISO/IEC 27001 -standardin vaatimusten mukaan sisältää tietoturvariskien määrittelemisen, analysoinnin ja arvioimisen vaiheet (ISO/IEC 27001:2013, 3–4).

Eduix Oy:n tietoturvariskianalyysissä kartoitettiin yrityksessä kohdatut sekä yleisesti olemassa olevat tietoturvauhat. Koostettujen tietoturvauhkien todennäköisyys ja toteutumisen vaikutukset arvioitiin Valtiovarainministeriön (2003, 41–46) laatimien VAHTI-ohjeiden mukaisesti. Tietoturvauhat analysoitiin tietoturvariskeiksi, mikäli niiden todennäköisyyden ja vaikutusten yhteenlaskettu lukema ylitti määritellyn hyväksyttävän tietoturvariskitason. Kaikille havaituille tietoturvauhille ja tietoturvariskeille esitettiin toteutettavaksi hallintatoimenpiteitä, joilla pyrittiin vaikuttamaan uhan todennäköisyyteen tai mahdollisen toteutumisen vaikutuksiin. Vaikkakin tietoturvariskianalyysi on oma prosessinsa, on suuremman kokonaisuuden, tietoturvallisuuden hallintajärjestelmän, mielessä pitäminen järkevää työn tavoitteiden kannalta.

Tietoturvallisuuden hallintajärjestelmän ja ISO/IEC 27001:2013 -standardin määrittelemien vaatimusten osalta tietoturvariskianalyysin jälkeen päästäisiin edelleen tietoturvariskien käsittelyvaiheeseen ja sen myötä sovellettavuuden selvitykseen. Sovellettavuuden selvityksessä eli SoA:ssa (*Statement of Applicability*) on lueteltuna yrityksen tietoturvariskit sekä niille päätetyt ja toteutetut hallintatoimenpiteet. Sovellettavuuden selvitys on myös osa ISO/IEC 27001:2013 -standardin vaatimuksia ja pohja sertifiointiauditoinnille.

2.1 Tietoturvallisuuden hallintajärjestelmään johtava prosessi

Tietoturvallisuuden hallintajärjestelmän toteuttamisessa on muistettava, että kyseessä on moniosainen prosessi, jota tulee ylläpitää ja kehittää yrityksen koko elinkaaren ajan. Siksi siinä voidaan hyvin hyödyntää monissa prosesseissa ja standardeissa käytettyä PDCA-sykliä (kuvio 1). PDCA-sykli eli Plan-Do-Check-Act tarkoittaa suomennettuna Suunnittele–Toteuta–Arvioi–Toimi. Nämä ovat avainkohdat esimerkiksi juuri tietoturvallisuuden hallintajärjestelmän muodostamiseen ja jatkuvaan parantamiseen. PDCA-menetelmää käytettäessä päätarkoituksena onkin ymmärtää tietoturvallisuuden hallintajärjestelmän olevan jatkuvasti kehitettävä ja ylläpidettävä kokonaisuus.



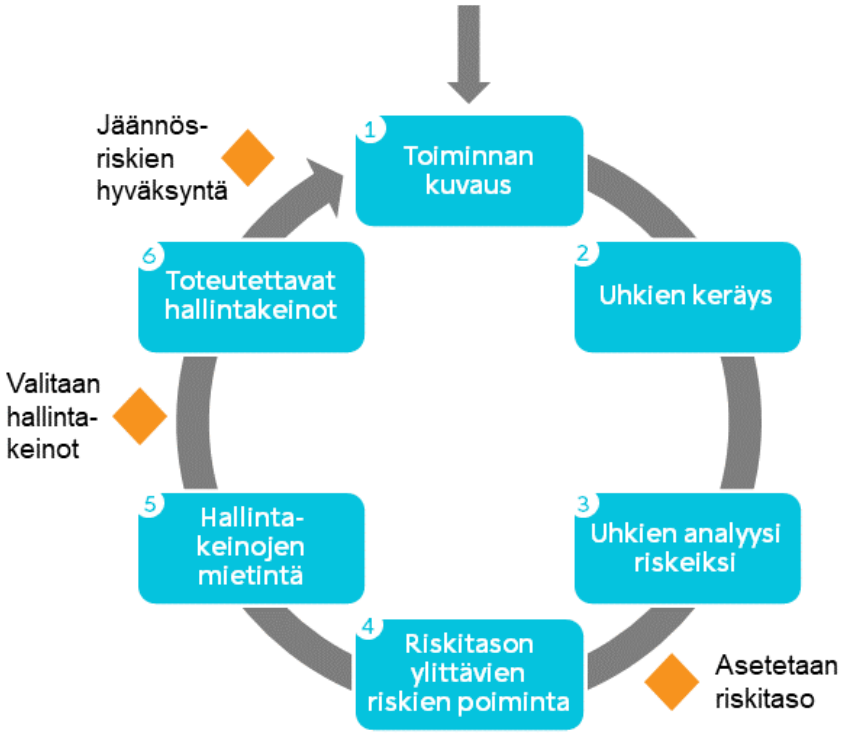
KUVIO 1. PDCA-sykli (Laakso, muokattu)

PDCA-syklin työjärjestyksen mukaisesti yrityksessä tulisi ensin suunnitella tietoturvallisuuden hallintajärjestelmään johtava prosessi esimerkiksi projektisuunnitelman muo-

dossa, määritellä suojattavat kohteet sekä miettiä yritykselle sopiva tietoturvan taso. Tämän jälkeen tietoturvallisuuden hallintajärjestelmä toteutetaan esimerkiksi hankkimalla tarvittavat fyysiset suojausmekanismit sekä laatimalla yhtenäiset toimintaohjeistukset ja kouluttamalla ne organisaation henkilöstölle. Toteuttamisvaiheen jälkeen tietoturvan hallintajärjestelmää, sen puutteita sekä vaikutuksia arvioidaan ja saadut tulokset analysoidaan tietoturvan hallintajärjestelmän tavoitteisiin peilaten. Tulosten arvioinnin perusteella toimintaa kehitetään edelleen toivottuun suuntaan. Muuttuvissa olosuhteissa ja uusien tavoitteiden puitteissa PDCA-sykli aloitetaan alusta, mikä mahdollistaa järjestelmän jatkuvan kehittämisen.

2.2 Tietoturvariskianalyysiin johtava prosessi

Tietoturvariskianalyysi on osa edellä mainittua tietoturvallisuuden hallintajärjestelmän suunnitteluvaihetta. Tietoturvariskianalyysiin johtavaa prosessia voidaan puolestaan kuvata esimerkiksi seuraavan prosessikaavion avulla (kuvio 2).



KUVIO 2. Tietoturvariskianalyysin prosessisuunnitelma (Digitaalinen Helsinki, 2017)

Tässä tietoturvariskianalyysissä käytettiin pohjana kuvion (2) mukaista prosessisuunnitelmaa, sillä näin jokainen työvaihe tulisi käsiteltyä järjestelmällisesti ja suunnitellusti. Alla on esitelty kuvion jokainen työvaihe ja tietoturvariskianalyysissä käytetyt menetelmät tarkemmin.

2.2.1 Alkutilanteen ja tavoitteiden kartoitus

Kuvion (2) mukaisesti ensimmäisenä työvaiheena on toiminnan kuvaus, mikä tarkoittaa käytännössä organisaation tietoturvallisuuden alkutilanteen sekä tavoitteiden kartoittamista. Tavoitteena tässä tietoturvariskianalyysissä oli koostaa havaittuja ja muita olemassa olevia tietoturvauhkia mahdollisimman laaja-alaisesti. Tämän jälkeen tarkoituksena oli löytää tietoturvauhille parhaiten soveltuvia ja taloudellisesti järkeviä hallintatoimenpiteitä, joiden toteuttamisen myötä ISO/IEC 27001:2013 -standardia vasten olisi mahdollista sertifioitua.

Eduix Oy:n tietoturvatilannetta päätettiin kartoittaa tietoturvauhkakyselyn muodossa. Eduix Oy on ohjelmistoalan yritys, jossa tietoturva on varmasti otettu huomioon ainakin tekniseltä osin eri toiminnoissa. Tietoturvaan kuuluu kuitenkin teknisten tietoturvavaatimusten lisäksi myös paljon inhimillisiä tietoturvauhkia. Henkilöstölle osoitetun tietoturvauhkakyselyn vastausten toivottiin osoittavan muun muassa sen, kuinka kiinnostuneita työntekijät ovat tietoturvallisuudesta, millaisia uhkia he ovat työssään kohdanneet ja millaisena he kokevat Eduix Oy:n tämänhetkisen tietoturvatilanteen tason.

2.2.2 Tietoturvauhkien kerääminen

Tietoturvariskianalyysin prosessisuunnitelmassa (kuvio 2) seuraavana työvaiheena on tietoturvauhkien kerääminen. Tietoturvauhkien keräämisessä on tärkeää kartoittaa organisaation kohtaamat tietoturvauhat sekä yleisesti olemassa olevat tietoturvauhat. Yrityksessä huomattujen tietoturvauhkien kartoittamisessa parhaimmat asiantuntijat ovat yrityksen omat työntekijät. Näin uhkat ovat sellaisia, joita juuri kyseisen yrityksen eri toiminnoissa on havaittu. Tämän vuoksi tietoturvauhkien keräämiseen ja yrityksen tietoturvatilanteen kartoittamiseen käytettiin henkilöstölle suunnattua tietoturvauhkakyselyä.

Tietoturvauhkien keräämisellä pyrittiin osallistamaan henkilöstöä miettimään yrityksen tietoturvatilannetta ja käsittelemiensä tietojen suojausmenetelmiä. Kyselyn myötä työntekijöille haluttiin myös antaa matala kynnys ilmoittaa eri toiminnoissa havaitut tietoturvauhat ja heidän olisi tarvittaessa mahdollista pyytää juuri heidän työnkuvaansa liittyviä yhtenäisiä tietoturvaan liittyviä toimintaohjeistuksia.

Organisaation tietoturvallisuudessa avainasemassa ovat yrityksen omat työntekijät. Koko yrityksen tietoturvan taso on tismalleen yhtä vahva, kuin sen heikoin lenkki ja sen vuoksi työntekijöiden tietoturvatietoisuuden lisääminen on ensiarvoisen tärkeää. Tietoturvauhkakyselyn kanssa samanaikaisesti organisaation henkilöstölle esitettiin tietoturvatietoiskuja. Tällä pyrittiin aktivoimaan henkilöstöä miettimään tietoturvauhkia eri näkökulmista ja vastaamaan tietoturvauhkakyselyyn olemassa olevat tietoturvauhat tiedostaen.

Tietoturvauhkia koostettiin myös ISO/IEC 27001:2013 -standardin pohjalta ja standardin velvoittava hallintakeinojen ja -tavoitteiden viiteluettelo käytiin läpi, jotta jokainen standardissa määritelty tietoturvauhka käsiteltäisiin ja samalla standardin vaatimukset täytettäisiin. Tietoturvauhkia kartoittaessa etsittiin lisäksi tietoa muista yleisimmistä organisaation kohtaamista tietoturvauhista ja nämä uhat otettiin myös huomioon tietoturvariskianalyysissä.

2.2.3 Tietoturvauhkien analysointi

Kuvion (2) kolmannessa vaiheessa uhat kootaan ja analysoidaan riskeiksi, jolloin myös lasketaan jokaisen tietoturvauhan riskiluku ja asetetaan hyväksyttävä riskitaso. Yrityksen henkilöstön kohtaamat ja yleisesti olemassa olevat tietoturvauhat koostettiin tietoturvauhkakyselyn jälkeen tietoturvariskien arviointitaulukkoon. Riskienarviointitaulukossa määriteltiin yrityksen omaisuutta koskevat uhat, niiden omistajat ja haavoittuvuudet sekä jokaisen tietoturvauhan todennäköisyys ja toteutumisen aiheuttamat vaikutukset. Todennäköisyys voi olla esimerkiksi odotusarvo siitä, kuinka monta kertaa vuodessa juuri tietty tietoturvauhka voisi toteutua. Uhkan vakavuuden määrittelyssä taas voidaan pohtia esimerkiksi tapahtuman seurausten aiheuttamia kustannuksia, kuten jälleenhankinnan ja hukatun ajan kustannuksia sekä esimerkiksi yrityksen maineen heikkenemisen vaikutuksia liiketoiminnalle. Näiden odotusarvojen avulla laskettiin jokaisen tietoturvauhan riskiluku

ja määriteltiin ehdotus hyväksyttävästä riskitasosta, joka kuitenkin on aina viime kädessä ylimmän johdon päätettävissä.

Tietoturvauhkia analysoitiin lisäksi tarkemmin erillisessä tietoturvariskianalyysissä, jossa viitattiin tietoturvariskien arviointitaulukossa lueteltuihin riskeihin. Tämän analyysin tarkoituksena oli arvioida riskien mahdollisen toteutumisen aiheuttamia ongelmia yrityksen eri toiminnoissa ja esittää perustelut määritetyille tietoturvariskien todennäköisyyksille ja toteutumisen vaikutuksille.

Eduix Oy:n tietoturvariskianalyysissä käytettiin pääasiassa kvalitatiivista eli laadullista riskianalyysimenetelmää, jossa kuvattiin mahdollisimman laaja-alaisesti sekä olemassa olevat tietoturvauhat, että yrityksessä kohdatut tietoturvauhat. Tietoturvauhat ja niiden suuruus määriteltiin uhkakuvapohjaisesti arvioinnin, oivallusten ja kokemusten perusteella. Ero kvantitatiiviseen eli määrälliseen tietoturvariskianalyysiin on siinä, että kvantitatiivisessa tietoturvariskianalyysissä olisi arvioitu tarkasti yrityksen omaisuuden ja niihin kohdistuvien tietoturvauhkien toteutumisen taloudellisia kustannuksia sekä tarkasteltu tietoturvariskejä esimerkiksi tilastotietojen ja erilaisten laskentamenetelmien avulla. (Stewart, Tittel & Chapple 2005, 190-193.)

2.2.4 Tietoturvariskien hallintatoimenpiteet

Tietoturvariskianalyysin prosessisuunnitelman (kuvio 2) mukaisesti seuraavina työvaiheina ovat riskitason ylittävien tietoturvariskien poiminta ja hallintakeinojen mietintä. Tietoturvauhan riskiluku voi kuitenkin vaihdella muuttuvissa olosuhteissa ja tämän vuoksi kaikille kerätyille tietoturvauhille sekä tietenkin riskitason ylittäville tietoturvariskeille ehdotettiin hallintatoimenpiteitä. Kaikille tietoturvauhille mietittiin hallintatoimenpiteitä myös sen vuoksi, että ISO/IEC 27001:2013 -standardin vaatimukset täytettäisiin.

Pohdituista hallintatoimenpiteistä muodostettiin ehdotelma yrityksen ylimmän johdon käsiteltäväksi. Ehdotelmassa tietoturvariskien hallintatoimenpiteistä esiteltiin ylimmän johdon päätöstä vaativat asiat sekä alustavat tietoturvalliset toimintaohjeistukset henkilöstölle. Opinnäytetyön rajallisesta aikaikkunasta johtuen tässä tietoturvariskianalyysissä ei kuitenkaan voitu jäädä odottamaan ylimmän johdon päätöstä toteutettavista hallintatoimenpiteistä ja tietoturvariskien käsittelystä.

2.2.5 Hallintakeinojen toteuttaminen ja jäännösriskien hyväksyminen

Tietoturvariskianalyysin jälkeen tarkoituksena olisi edetä tietoturvariskien käsittelyvaiheeseen ja tämän myötä sovellettavuuden selvitykseen. Ehdotelmaan tietoturvallisuuden hallintatoimenpiteistä kerättiin käytännön esimerkkejä sekä ylimmän johdon päätettävissä olevista asioista että henkilöstölle suunnatuista tietoturvaohjeistuksista, jotta päätösten tekeminen toteutettavista hallintakeinoista olisi mahdollisimman sujuvaa ja käytännönläheistä.

Kun toteutettavista tietoturvallisuuden hallintatoimenpiteistä tehdään päätös, on jokaisen riskin hallintakeinolle määritettävä vastuuhenkilö, joka vastaa hallintatoimenpiteen toteuttamisesta ja ylläpitämisestä sekä viestii sen tehokkuudesta ylimmälle johdolle. Toteutettavia hallintatoimenpiteitä päätettäessä on kuitenkin syytä punnita esimerkiksi riskin välttämisestä ja sen hallintakeinoista aiheutuvat kulut ja verrata niitä riskin mahdollisesti toteutuessa aiheutuviin kuluihin ja vaikutuksiin. Mikäli jonkin riskin olemassaoloa ei ole mahdollista tai taloudellisesti järkevää poistaa kokonaan, voidaan tietoturvariskille valita sellaisia hallintatoimenpiteitä, jotka alentavat riskin kokonaistason hyväksyttävälle tasolle. Mikäli joidenkin riskien hallintatoimenpiteistä koituvat kustannukset ovat kuitenkin merkittävästi suuremmat, kuin uhkan mahdollisesta toteutumisesta aiheutuvat kustannukset tai tietoturvariskin suuruutta ei saada niistä huolimatta hyväksyttävälle tasolle, ei tietoturvauhkan hallintatoimenpiteitä ole välttämättä järkevää toteuttaa. Tällöin organisaation ylimmän johdon tulee hyväksyä jäljelle jäävien riskien olemassaolo ja esittää perustelut jäännösriskeille sovellettavuuden selvitykseen. (Digitaalinen Helsinki 2017.)

3 ORGANISAATIOSSA KOHDATUT TIETOTURVAUHAT

Jokaisessa organisaatiossa kohdataan erilaisia tietoturvauhkia organisaation koosta, toimialasta ja luonteesta riippuen. Näiden tietoturvauhkien kartoittaminen ja analysoiminen on vähintäänkin yhtä tärkeää, kuin yleisesti kaikkia organisaatioita koskevien tietoturvauhkien määrittäminen. Eduix Oy:n tietoturvariskianalyysissä pyrittiin kartoittamaan sekä organisaation sisällä havaittuja että yleisesti olemassa olevia tietoturvauhkia ja analysoimaan niiden vaikutuksia Eduix Oy:n liiketoimintaan.

Yliopettaja Esko Vainikka (Harjun 2010 mukaan) mainitsee yrityksen onnistuvan tietoturvan kehittämisessä, mikäli suojattavat kohteet osataan määritellä. Yritykselle tärkeiden suojattavien kohteiden määrittelemisestä ja mahdollisista tietoturvahaavoittuvuuksista tietävät yleensä parhaiten yrityksen eri toiminnoissa työskentelevät henkilöt, jotka näkevät saman kohteen eri näkökulmista. Koska tietoturvallisuuden hallintajärjestelmä ja siihen liittyvät toimenpiteet tulisivat myös koskettamaan koko henkilöstöä, haluttiin heille antaa mahdollisuus olla mukana tietoturvallisuuden hallintajärjestelmän muodostamisessa alusta alkaen. Tällä haluttiin myös osaltaan minimoida tietoturvallisuuden hallintajärjestelmän aiheuttamaa muutosvastarintaa ja saattaa koko henkilöstö tietoiseksi kehitteillä olevasta tietoturvallisuuden hallintajärjestelmästä.

3.1 Tietoturvariskianalyysin perehdytys henkilöstölle

Tietoturva on yrityksen ja kaikkien sen työntekijöiden yhteinen asia. Vaikka organisaatiossa laadittaisiin kaikki tietoturvan hallintajärjestelmään vaadittavat dokumentit ja toimintalinjaukset, ei niistä olisi juurikaan hyötyä, jos henkilöstö ei tietäisi oman panoksensa merkitystä tietoturvallisuuden hallintajärjestelmässä. Ihminen on tietoturvan heikoin lenkki ja erityisesti sen vuoksi henkilöstön tietoturvatietoisuuden lisääminen sekä tietoturvallisten toimintalinjausten noudattaminen on ensiarvoisen tärkeää (Vainikka, Harjun 2010 mukaan).

Jotta yrityksen olisi mahdollista muodostaa tietoturvallisuuteen liittyvät toimintalinjaukset ja hallintatoimenpiteet, on tiedettävä juuri omaan yritykseen ja sen eri toimintoihin

liittyvät tietoturvariskit. Kuten sanottu, parhaat asiantuntijat yritykseen kohdistuvien tietoturvariskien kartoittamisessa ovat yrityksen omat työntekijät. Organisaation tietoturvariskianalyysin voisi toteuttaa myös valitsemalla tietoturvariskejä käsittelevään projektiryhmään yksittäisiä eri osastojen edustajia, jotka raportoisivat eri toiminnoissa havaituista tietoturvariskeistä (Digitaalinen Helsinki 2017). Keskisuuressa yrityksessä oli kuitenkin järkevämpää kerätä havaittuja tietoturvauhkia koko henkilöstöltä ja antaa samalla kaikille mahdollisuus vaikuttaa yrityksen tietoturvan tasoon.

Tietoturvariskianalyysi perehdytettiin henkilöstölle samaan aikaan, kun tietoturvauhkakysely ja tietoturvatietoiskut julkaistiin. Varsinainen perehdytys toteutettiin Eduix Oy:n sisäisen keskustelukanavan välityksellä. Henkilöstö saatettiin tietoiseksi kehitteillä olevasta tietoturvallisuuden hallintajärjestelmästä sekä siihen kuuluvan tietoturvariskianalyysin toteuttamistavasta ja työn tavoitteista.

3.1.1 Tietoturvauhkakyselyn perehdyttäminen

Henkilöstöä kannustettiin vastaamaan tietoturvauhkakyselyyn (liite 1), jotta he pääsisivät vaikuttamaan tietoturvallisuuden hallintajärjestelmän kehittämiseen. Anonyymin tietoturvauhkakyselyn avulla haluttiin antaa henkilöstölle myös matalampi kynnys ilmoittaa huomaamistaan epäkohdista yrityksen tietoturvallisuudessa ja pyytää tarvittaessa tarkempia tai yhtenäisempiä toimintalinjauksia eri toimintoihin.

Tietoturvauhkakyselyssä (liite 1) tarkennettiin tietoturvaan liittyviä käsitteitä, jotta tietoturvauhkia osattaisiin ilmoittaa mahdollisimman monipuolisesti. Tietoturvauhkakyselyssä kysymykset oli jaoteltu tiedon luottamuksellisuuteen, eheyteen, saatavuuteen ja muihin tietoturvan osa-alueisiin. Toisaalta henkilöstöä muistutettiin siitä, että tietoturvauhkien kategorisoiminen ei ole vastaamisessa olennaisinta, vaan tärkeämpää on ylipäätään tuoda mielipiteensä ilmi tietoturvauhkakyselyssä ja sen monivalintakysymyksissä, jotta Eduix Oy:n tietoturvatilanne voitaisiin laadukkaasti kartoittaa.

3.1.2 Tietoturvatietoiskut

Tietoturvatietoiskujen (liite 2) tavoitteena oli lisätä henkilöstön tietoturvatietoisuutta ja aktivoida huomaamaan erilaisia tietoturvallisuutta vaarantavia asioita. Tietoturvatietoiskuilla haluttiin tuoda henkilöstön tietoisuuteen erilaisia olemassa olevia tietoturvariskejä, jotta tietoturvauhkakyselyyn vastatessa henkilöstö tietäisi, mitä kaikkea tietoturvaan kuuluu. Henkilöstön tietoturvatietoisuuden lisääminen on lisäksi tärkeä osa organisaation tietoturvallisuuden hallintajärjestelmää. Yliopettaja Vainikan (Harjun 2010 mukaan) mukaan yrityksen tietoturvasta vain noin 20 % on tekniikkaa ja jopa 80 % on kaikkea muuta, mitä tietoturvaan liittyy. Tekniikkaan liittyvät esimerkiksi palomuurit, pääsynvalvonta ja haittaohjelmien torjunta. Yrityksessä loput 80 % koostuu toimintatavoista, säännöistä ja ohjeista, joten pääroolissa yrityksen tietoturvassa on ihminen. Henkilöstölle suunnattujen tietoturvatietoiskujen tarkoituksena oli saada yrityksen työntekijät huomaamaan, kuinka paljon heidän omat toimintatapansa vaikuttavat koko yrityksen tietoturvan tasoon.

Ensimmäisessä tietoturvatietoiskussa (liite 2) esiteltiin tietoturvallisuuden CIA-malli eli tietoturvan jakaminen tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen. Tietoiskussa muistutettiin myös siitä, että jokaisen työntekijän tulisi tunnistaa käsittelemiensä tietojen suojaustaso ja toimia sen mukaisesti. Muut tietoturvatietoiskut liittyivät aina johonkin tiettyyn tietoturvauhkaan, kuten erityyppisiin tietomurtoihin ja siihen, millainen on työntekijän rooli niiden tunnistamisessa ja välttämisessä. Tietoturvatietoiskuja julkaistiin kaksi kertaa viikossa, jotta henkilöstö ehti perehtyä rauhassa yhteen aiheeseen kerrallaan. Tietoturvatietoiskuja kiinnitettiin muun muassa Eduix Oy:n toimitilojen seinille, jotta työntekijät pääsivät tutustumaan rauhassa tietoturva-aiheeseen esimerkiksi virvoketauoillaan. Tietoturvatietoiskut herättivät paljon keskustelua ja uusien tietoturvatietoiskujen ilmestymisajankohtaa tiedusteltiin lähes päivittäin.

3.1.3 Johdon tuki tietoturvallisuuden hallintajärjestelmää kohtaan

Johdon asenne tietoturvallisuuden hallintajärjestelmää kohtaan on ensiarvoisen tärkeää, sillä organisaation tietoturvan on lähdettävä johdon sitoutumisesta (Heljaste 2008, 72). Organisaation tietoturvallisuuden hallintajärjestelmän kehittäminen vaatii aina ylimmän johdon tuen ja hyväksynnän. Ylimmän johdon tehtävänä on muun muassa osoittaa tietoturvallisuuden hallintajärjestelmän muodostamiseen ja ylläpitämiseen tarvittavat resurssit

sekä kannustaa omalla toiminnallaan henkilöstöä noudattamaan tietoturvallisia toimintatapoja. ISO/IEC 27001:2013 -standardissa (2013, 2) määritellään ylimmän johdon tehtäviksi esimerkiksi tietoturvallisuuden hallintajärjestelmän tärkeydestä viestimisen sekä ihmisten ohjeistamisen ja tukemisen osallistumaan tietoturvallisuuden hallintajärjestelmän tehokkuuteen.

Eduix Oy:n ylin johto osoitti tukeaan tietoturvallisuuden hallintajärjestelmää kohtaan muun muassa aloittamalla niin kutsutun tietoturvallisuuden aktiivimallin. Työntekijöitä kannustettiin tietoturvalliseen työskentelyyn ja puhtaan näytön toimintamenetelmiin aktiivimallilla, jossa jokainen työntekijä, joka poistuu työpisteeltään lukitsematta tietokonettaan, sai kuvitteellisen poikkeusmerkinnän eli niin kutsutun antipapukaijamerkin. Myös tämä aktiivimalli otettiin hyvin vastaan ja asia herätti työntekijöissä paljon positiivista keskustelua.

3.2 Tietoturvauhkien kerääminen henkilöstöltä

Tietoturvauhkakysely (liite 1) toteutettiin e-lomakkeella, jossa oli ensin pohjustettu tietoturvauhkakyselyn tarkoitus. Lomakkeen esipuheessa painotettiin jokaisen työntekijän vastausten merkitystä tietoturvariskianalyysin muodostamisessa ja sillä pyrittiin myös antamaan väylä huomattujen tietoturvauhkien sekä puutteellisten toimintaohjeistusten ilmoittamiseen. Esipuheessa myös kerrattiin mitä tieto on ja missä eri muodoissa sitä voi esiintyä. Tämän tarkoituksena oli tuoda ilmi, että tietoturva ei liity ainoastaan tietokoneella käsiteltyyn ja tietoverkkojen välityksellä välitettyyn tietoon, vaan tieto voi olla muun muassa vuosien varrella kertynyttä kokemusta ja osaamista, jota välitetään myös suullisesti. Lisäksi esipuheessa esiteltiin tietoturvan jakaminen tiedon luottamuksellisuuden, eheyden ja saatavuuden mukaan. Tätä jaottelua hyödynnettiin myös itse kyselyssä, jotta kohdattuja tietoturvauhkia saataisiin kerättyä mahdollisimman laaja-alaisesti. Varsinainen kysely koostui muutamasta avoimesta kysymyksestä sekä monivalintakysymyksistä.

Kyselyssä kysyttiin aluksi työntekijän työnkuvaa ja pääsääntöistä toimipistettä. Tietoturvallisuuden hallintajärjestelmää muodostaessa ja ISO/IEC 27001 -standardia vasten sertifioituessa vaaditaan tietoturvallisuuden hallintajärjestelmälle määritelty laajuus, joka

voi olla esimerkiksi toimipiste- tai liiketoimintaosastokohtainen. Kun vastaajasta tiedetään nämä asiat, on yrityksen eri toiminnoissa ja toimipisteissä havaittujen tietoturvariskien hallintatoimenpiteet myös helpompi määrittää.

Seuraavaksi kyselyssä oli vuorossa avoimet kysymykset, joilla pyrittiin keräämään erilaisia kohdattuja tietoturvauhkia yrityksen henkilöstöltä mahdollisimman kattavasti. Vastaajan oli mahdollista jaotella havaitsemansa tietoturvauhat tiedon luottamuksellisuutta, eheyttä ja saatavuutta uhkaavien asioiden mukaan. Ennen jokaista avointa tekstikenttää vielä määriteltiin hieman tarkemmin, millaisia olisivat näihin eri osa-alueisiin liittyvät tietoturvauhat. Henkilöstöä muistutettiin myös siitä, että mikäli ei tiedä mihin osa-alueeseen jokin uhka kuuluu, sen voi laittaa sellaiseen kohtaan, joka itsestä tuntuu sopivimmalta. Lisäksi kyselyssä oli avoin tekstikenttä sellaisille tietoturvauhille ja toimintaohjeistuspyynnöille, jotka eivät välttämättä kuulu juuri näihin tietoturvan osa-alueisiin.

Kyselyn lopussa oli muutamia monivalintakysymyksiä, joiden tarkoituksena oli kartoittaa Eduix Oy:n tämänhetkistä tietoturvatilannetta henkilöstön näkökulmasta. Monivalintakysymyksissä tiedusteltiin muun muassa sitä, millaisena työntekijät kokevat Eduix Oy:n tämänhetkisen tietoturvan tason. Lisäksi monivalintakysymysten avulla kartoitettiin sitä, kuinka hyvin työntekijät omalta osaltaan huolehtivat Eduix Oy:n tietoturvasta tiedon luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta.

3.3 Tietoturvauhkakyselyn tulokset

Tietoturvauhkakyselyyn vastasi lähes puolet koko Eduix Oy:n henkilöstöstä. Ensimmäiset tallennukset tehtiin vain hetken kuluttua tietoturvauhkakyselyn julkistamisesta, mikä kertoo osaltaan siitä, että matalan kynnyksen ilmoittamisväylää oli odotettu. Tietoturvauhkakysely oli auki kaksi viikkoa ja henkilöstöä muistutettiin kyselyyn vastaamisesta viikoittain. Muistutusviestien jälkeen tallennuksia tehtiin enemmän, kuin muina aikoina.

Vastaukset tulivat kattavasti jokaisesta Eduix Oy:n eri liiketoimintayksiköstä. Osa havaituista riskeistä liittyi juuri tiettyyn toimenkuvaan ja omassa työssä havaittuihin tietoturvaa vaarantaviin tilanteisiin. Suurin osa vastauksista oli kuitenkin koko henkilöstöä koskettavia tietoturvauhkia ja useat vastaajat ilmoittivat samankaltaisista asioista. Eräs tällaisista

asioista oli esimerkiksi toimitilojen äänieristettyjen neuvottelutilojen vähäisyys, joka vaaransi tiedon luottamuksellisuutta, sillä myös muut työntekijät tai toimitiloissa vierailevat henkilöt saattoivat kuulla yksityisiä keskusteluja. Kun kooste tietoturvauhkakyselyn tuloksista (liite 3) esiteltiin Eduix Oy:n ylimmälle johdolle, muun muassa tähän asiaan puututtiin heti ja toimitiloihin suunniteltiin hankittavaksi lisää äänieristettyjä neuvottelutiloja.

Monivalintakysymysten tulokset osoittivat hyvin Eduix Oy:n tämänhetkisen tietoturvan tason ja sen, missä asioissa olisi vielä parannettavaa. Monivalintakysymysten vastauksista ei havaittu suurta hajontaa minkään aihealueen osalta, vaan vastaukset olivat pääosin samankaltaiset kaikilla vastaajilla. Työntekijöille esiteltiin tietoturvauhkakyselystä vain monivalintakysymysten tulokset, sillä niiden osalta vastauksia ei voinut yhdistää tiettyyn työntekijään.

Henkilöstön ilmoittamat tietoturvauhat, puuttuvat toimintaohjeistukset ja monivalintakysymysten tulokset koostettiin erilliseen dokumenttiin (liite 3). Koosteen tarkoituksena oli viestiä tietoturvauhkakyselyn tuloksista ylimmälle johdolle huolehtien samalla siitä, että työntekijöiden anonymiteetti säilyy. Koosteen avulla myös tietoturvariskien arviointitaulukon täydentäminen yrityksessä havaittujen tietoturvauhkien osalta oli järjestelmällisempää.

4 OLEMASSA OLEVAT TIETOTURVAUHAT

Tietoturvauhkakyselyn tarkoituksena oli kartoittaa juuri kyseisessä yrityksessä havaitut tietoturvauhat, mutta yleisesti olemassa olevia ja eri standardien määrittelemiä tietoturvauhkia on olemassa vielä paljon enemmän. Esimerkiksi ISO/IEC 27001:2013 -standardissa määritellyt tietoturvariskit ja tietoturvallisuuden hallintajärjestelmälle asetetut vaatimukset on pyritty laatimaan niin, että jokaisella organisaatiolla on mahdollisuus soveltaa suurinta osaa esitetyistä hallintatavoitteista ja -keinoista organisaation koosta, toimialasta tai luonteesta riippumatta. Yksittäisten tietoturvariskien suuruus ja toteutettavat hallintatoimenpiteet riippuvat kuitenkin aina organisaation infrastruktuurista ja tietoturvauhkien kriittisyydestä organisaation liiketoiminnan näkökulmasta.

Tässä luvussa esitellään joitakin yleisimpiä olemassa tietoturvauhkia niin Suomessa havaittujen, kuin myös ISO/IEC 27001:2013 -standardissa määriteltyjen tietoturvauhkien osalta. Uhkiin on pyritty keräämään myös tarvittavia organisaatiokohtaisia hallintatoimenpiteitä, joilla tietoturvauhan todennäköisyyttä tai sen toteutumisen vaikutuksia olisi mahdollista minimoida.

4.1 Yleisimpiä organisaation kohtaamia tietoturvauhkia

Organisaatioiden kohtaamat tietoturvauhat lisääntyvät vuosi vuodelta ja myös tietoturvahyökkäykset päivittyvät sekä kehittyvät. Alla olevassa kuvassa (kuva 1) on esitelty Viestintäviraston Kyberturvallisuuskeskuksen koostamat yleisimmät organisaatioiden kohtaamat tietoturvauhat vuodelta 2017. Kuvan oikealla puolella on esitelty myös toimivat suojautumiskeinot näitä uhkia vastaan.

KUVA 1. Tyypillisimmät organisaatioita koskevat tietoturvauhat ja ratkaisut vuonna 2017 (Viestintävirasto Kyberturvallisuuskeskus 2018)

Kuvassa 1 esiteltyjä organisaatioiden kohtaamia tietoturvauhkia analysoitiin myös Eduix Oy:n tietoturvariskianalyysissä. Suurin osa mainituista tietoturvauhista on sellaisia, joita pystyisi ehkäisemään lisäämällä henkilöstön tietoturvatietoisuutta ja ohjeistamalla toimimaan eri tilanteissa oikeaoppisesti. Henkilöstön tietoturvatietoisuuden lisäämisellä ja uusista tietoturvauhista tiedottamisella voitaisiin ehkäistä esimerkiksi tietojen kalasteluun lankeamista tai kiristyshaittaohjelmien aiheuttamien vahinkojen suuruutta. Sisäisen viestinnän ja tietoturvatietoisuuden lisäämisen merkitys korostuu myös siinä, että henkilöstö osaisi ilmoittaa havaitsemansa tietoturvahaavoittuvuudet. Suurin osa tietoturvauhkien hallintatoimenpiteistä koostuu organisaation ylimmän johdon asettamista toimintaperiaatteista ja -ohjeistuksista, joita noudattamalla voidaan ennaltaehkäistä tietoturvauhkia ja toimia oikeaoppisesti poikkeustilanteissa.

Alla on esitelty ja analysoitu yleisimpiä organisaatioiden kohtaamia tietoturvauhkia tarkemmin. Henkilöstölle esitetyt tietoturvatietoiskut koskivat juuri kyseisiä tietoturvauhkia. Tällä pyrittiin antamaan henkilöstölle ajantasaista tietoa organisaatioiden kohtaamista tietoturvauhkista, jotta he osaisivat myös tunnistaa erilaisia tietoturvauhkia ja -hyökkäyksiä.

4.1.1 Palvelunestohyökkäykset

DoS (*Denial of Service*) eli palvelunestohyökkäys tarkoittaa sitä, että yhtä tietokonetta ja yhtä verkkoyhteyttä käytetään ylikuormittamaan palvelunestohyökkäyksen kohteen kaistaa ja muita resursseja lähettämällä suuri määrä esimerkiksi UDP- tai ICMP-paketteja. Palvelunestohyökkäyksiä on myös muunlaisia, kuten ohjaustietojen häiritsemistä tai vääränlaisen lähetteen lähettämistä (Viestintävirasto Kyberturvallisuuskeskus 2016, 1). Kaikilla eri tavoilla pyrkimyksenä on kuitenkin pystyä estämään palvelua tai heikentämään sitä valitussa kohteessa, esimerkiksi kohteen verkkosivuilla (Munson 2014).

DDoS (*Distributed Denial of Service*) eli hajautettu palvelunestohyökkäys on taas kehittyneempi versio tavallisesta palvelunestohyökkäyksestä. Siihen käytetään yleensä ympäri maailmaa kaapatuista tietokoneista ja niiden yhteyksistä muodostuvaa botnettiä. Botnetin avulla suoritetun hajautetun palvelunestohyökkäyksen päätekijää on vaikeampi jäljittää. Hajautetun palvelunestohyökkäyksen vaikutukset ovat lisäksi yleensä paljon suuremmat, kuin tavallisen palvelunestohyökkäyksen, sillä yhden tietokoneen sijasta palvelua pyrkii kuormittamaan mahdollisesti jopa sadat tai tuhannet tietokoneet ympäri maailmaa. (Munson 2014.)

Ohjelmistoyrityksen näkökulmasta onnistunut palvelunestohyökkäys henkilöstön käyttämiin tehtävänhallintajärjestelmiin aiheuttaisi sen, että tiedon saatavuus kärsisi ja toisaalta myös työaikaa kuluisi hukkaan. Asiakkaan käyttämiin, yrityksen hallinnoimiin järjestelmiin tehty palvelunestohyökkäys taas aiheuttaisi asiakkaalle tiedon saatavuuden sekä todennäköisesti yrityksen maineen heikkenemistä.

Eräitä tärkeimpiä suojauskeinoja palvelunestohyökkäyksiä vastaan on pitää organisaation omat verkkosivut erillään organisaation muusta toiminnasta. Hyökkääjät hyökkäävät yleensä julkisina näkyviin verkkosivustoihin, eivätkä he välttämättä tiedä organisaation muiden palveluiden rakennetta. Yrityksen verkkosivut kannattaa myös pitää internetin näkökulmasta liikkuvana. Tämä onnistuu käyttämällä esimerkiksi suuria pilvipalveluiden tarjoajia, joilla on monia datakeskuksia ympäri maailmaa. Näin yrityksen palveluiden sujuva pyörittäminen sekä siirtely on mahdollista. Ulkoisia palveluntarjoajia käytettäessä

puolestaan tulee varmistaa palveluntarjoajalta, että heillä on käytössään DDoS-hyökkäysten torjuntapalvelu ja että se sisältyy myös yrityksen kanssa tehtyihin sopimuksiin. (Paajanen 2016.)

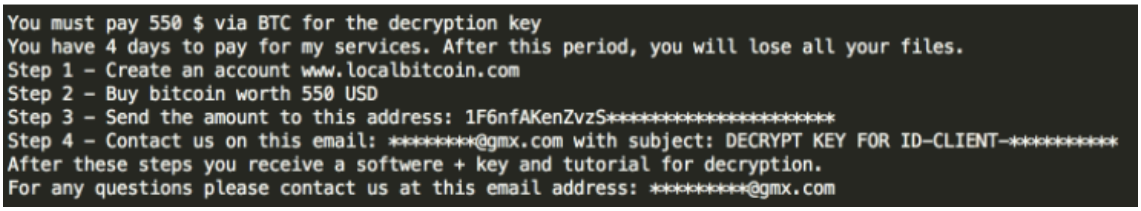
Käyttäjän osalta tärkeintä on muistaa päivittää laitteitaan ja ohjelmistojaan aina, kun niille on saatavilla päivityksiä. Päivittämätön laite on yleensä helpompi kaapata rikolliseen käyttöön ja organisaation työntekijän laitteelle asennetun haittaohjelman kautta hyökkääjän on mahdollista päästä myös käsiksi organisaation järjestelmiin. (Viestintävirasto Kyberturvallisuuskeskus 2018.)

4.1.2 Kiristyshaittaohjelmat

Erinäiset tietoja ja tiedostoja salaavat kiristyshaittaohjelmat ovat viime vuosina olleet yksiä yleisimpiä organisaation kohtaamia tietoturvauhkia (Viestintävirasto Kyberturvallisuuskeskus 2018). Ransomware eli kiristyshaittaohjelmat ovat nykyään eräitä tavallisimpia haittaohjelmia, joihin liittyy yleensä yritys saada käyttäjältä rahaa kiristämällä. Kiristyshaittaohjelma salaa uhriksi joutuneen tärkeät tiedostot ja vaatii lunnaiden maksamista vastineeksi salauksen purkuavaimesta ja tiedostojen palauttamisesta. Toiset kiristysohjelmaperheet käyttävät tiedostojen salaamiseen esimerkiksi RSA-2048-salausalgoritmia, jolloin salauksen purkaminen ei onnistu muuten, kuin käyttämällä alkuperäistä purkuavainta. (Viestintävirasto Kyberturvallisuuskeskus, F-Secure & Poliisi.)

Kyberrikollisuus on nykyään arkipäivää myös yritysmaailmassa. Kilpaileva organisaatio voi esimerkiksi ostaa kyberrikollisuutta harjoittavalta yritykseltä erinäisiä hyökkäyksiä toisen organisaatioon. Kyberrikollisuuden palveluhinnasto vaihtelee palveluntarjoajan ja hyökkäyksen suuruuden mukaan, mutta esimerkiksi Winlocker kiristyshaittaohjelma maksaa halvimmillaan vain noin 10–20 dollaria, kun taas muun muassa organisaation postilaatikon hakkerointi maksaa noin 500 dollaria. Kyberrikollisuuden kasvun myötä yritysten on otettava huomioon myös uudet tietoturvariskit ja suojauduttava niitä vastaan asianmukaisesti. (Lehto 2018.)

Alla olevassa kuvassa (kuva 2) on esimerkki kiristyshaittaohjelmasta. Yleensä vastaavanlainen ilmoitus näytetään käyttäjälle, kun hänen tietokoneellaan ja siihen yhdistetyillä laitteillaan olevat tiedostot on ensin salattu. (Beek 2017.)



KUVA 2. Kiristyshaittaohjelman vaatimus (Beek 2017)

Christiaan Beek tutki vuonna 2017 maailmaa kiristyshaittaohjelmien tekijöiden näkökulmasta ja yritti myös ottaa yhteyttä kiristyshaittaohjelmien tekijöihin. Kolmen kuukauden ajalta kerätyistä kiristyshaittaohjelmien vaatimuksissa (kuva 2) esitetyistä sähköpostiosoitteista noin 30 prosenttia eivät edes olleet toiminnassa. Tämä tarkoittaa sitä, että lunnasrahat maksamalla käyttäjä ei silti olisi saanut tietoonsa tiedostojen salauksenpurkuavainta. Kiristyshaittaohjelmien tekijöiltä saadut vastaukset puolestaan osoittivat sen, että haittaohjelman avulla tekijöiden oli mahdollista tienata paljon rahaa nopeasti, helposti ja turvallisesti ja sen vuoksi kiristyshaittaohjelmat lisääntyvät jatkuvasti. (Beek 2017.)

Vaikkakin kiristyshaittaohjelmalla saastunut tietokone on useimmiten puhdistettavissa, ei salattuja tiedostoja ole yleensä mahdollista saada palautettua ilman oikeaa purkuavainta. Joihinkin tunnettuihin kiristyshaittaohjelmiin on jo onneksi kehitetty salauksenpurkutyökaluja, mutta ei kaikkiin. Ainoa varma suojaus tiedostojen menettämisen varalle on tiedostojen säännöllinen varmuuskopiointi, vaikkakin tärkeässä roolissa on myös maalaisjärki epäilyttävien verkkosivujen ja roskapostin suhteen. Kuten edellä on mainittu, edes lunnaiden maksaminen ei takaa tiedostojen palautumista, vaan se ainoastaan kannustaa verkkorikollisten toimintaa. (Viestintävirasto Kyberturvallisuuskeskus ym.)

4.1.3 Huijausviestit ja tietojen kalastelu

Tietojen kalastelulla tai verkkourkinnalla tarkoitetaan rikollista toimintaa, jossa esimerkiksi luotettavana tahona, kuten palveluntarjoajana, esiintymällä yritetään kalastella verkon välityksellä käyttäjän luottamuksellisia tietoja. Kalasteluyritykset saattavat tulla esimerkiksi sähköpostilla, jossa luotettavana tahona esiintyvä huijari pyytää käyttäjää kirjautumaan tiettyyn palveluun väärennetyn kirjautumissivuston kautta. Kalasteluyritysten kohteena ovat yleensä käyttäjän henkilötiedot, käyttäjätunnukset tai luottokorttitiedot.

Kalasteluyrityksissä käytetään yleensä syöttinä esimerkiksi sitä, että käyttäjä välttäisi jonkinlaisen tiedon tai rahan katoamisen, mikäli hän varmentaisi pikaisesti käyttäjätietonsa väärennetyllä sivustolla. Tällaisia sähköpostiviestejä voi aina pitää epäilyttävinä, eikä viestin ohjeistusten mukaan kuulu toimia. Jos kuitenkin epäilee, voisiko viesti olla aiheellinen, on paras tapa varmistaa se kirjautumalla kyseiselle sivustolle manuaalisesti. (KrebsonSecurity 2017.)

Ennen pystyi luottamaan esimerkiksi siihen, että väärennetyillä netti- tai kirjautumissivuilla oli huonoja käännöksiä ja osoiterivillä ei ollut selaimen ja verkkosivun välisen liikenteen salauksesta kertovaa HTTPS-protokollaa. Nykyään kuitenkin esimerkiksi SSL-varmenteiden saaminen on suhteellisen helppoa ja kalastelusivusto pystyy sen avulla luomaan itselleen https://-alkuisen verkkosivun, joka saattaa näyttää käyttäjälle täysin oikealta. HTTPS-protokollaa käyttämällä tietojen kalastelijat onnistuvat myös luomaan selaimen osoiterivin eteen “turvallisesta” sivusta kertovan vihreän lukko-ikonin (kuva 3). (KrebsonSecurity 2017.)

KUVA 3. HTTPS-protokollaa käyttävä verkkosivu

Suomessa yritysten sähköpostitunnuksia kalastellaan tälläkin hetkellä aktiivisesti. Suomalaisiin yrityksiin kohdistuvissa tietojenkalasteluyrityksissä on esimerkiksi lähetetty yrityksen työntekijälle sähköposti, jonka on väitetty tulevan työntekijän tuntemalta henkilöltä. Sähköpostissa on ilmoitettu, että tämä henkilö haluaisi jakaa tiedoston työntekijän kanssa ja lukeakseen tiedoston, on työntekijän syötettävä sähköpostitunnuksensa sähköpostissa tulleen kirjautumissivuston kautta. Näin hyökkääjä on saanut tietoonsa työntekijän sähköpostitunnukset ja pystynyt esimerkiksi uudelleenohjaamaan saapuvat sähköpostiviestit omaan sähköpostiosoitteeseensa. (Viestintävirasto 2018.)

Tietojen kalastelu ei kuitenkaan aina tapahdu sähköpostin avulla. Toisinaan esimerkiksi salasanoja kalastelevat haittaohjelmat tulevat verkkosivulla olevan videon kautta. Tämä voi tapahtua esimerkiksi siten, että videon tarkastelemista varten pyydetään asentamaan tietty “koodekki”, joka todellisuudessa saattaakin olla haittaohjelma. (KrebsonSecurity 2017.)

Mikäli organisaation työntekijä lankeaa verkkourkintaan, voi hyökkääjä päästä käsiksi yrityksen kriittiseen tietoon tai palveluihin. Avainasemassa verkkourkinnalta suojautumisessa on yrityksen työntekijöiden tietoturvatietoisuuden lisääminen, jotta he osaavat tunnistaa verkon kautta tapahtuvia tietoturvauhkia ja toimia asianmukaisesti sellaisia huomatessaan. Tietojen kalastelun osalta tämä tarkoittaisi esimerkiksi aina selaimen kohdeosoitteen tarkistamista ja sähköpostin uudelleenlähetyksen tarkistamista säännöllisin väliajoin. Tunnusten kalastelulta voidaan suojautua myös kaksivaiheista tunnistautumista käyttäen. Tämä tarkoittaisi käytännössä sitä, että käyttäjätunnus-salasana-parin lisäksi käyttäjältä vaadittaisiin kirjautuessaan esimerkiksi mobiilivarmenne, sormenjälki tai muuttuva avainluku. Tällöin pelkän salasanan joutuminen vääriin käsiin ei välttämättä vielä vaarantaisi yrityksen tietojen luottamuksellisuutta. (Viestintävirasto 2018.)

4.1.4 Sosiaalinen manipulointi

Social engineering eli sosiaalinen manipulointi tarkoittaa toimintaa, jolla yritetään saada käyttäjä, kuten organisaation työntekijä, luottamaan hyökkääjään. Kun käyttäjä luottaa hyökkääjään, hän saattaa vahingossa paljastaa hyökkääjälle salaisia tietoja tai päästää hänet esimerkiksi sisälle yrityksen toimitiloihin. Hyökkääjä voi ottaa uhriinsa yhteyttä esimerkiksi sähköpostilla, puhelimitse, sosiaalisessa mediassa tai tulla jopa henkilökohtaisesti käymään. Yleensä hyökkääjä esiintyy jonain luotettavana tahona, kuten viranomaisena tai palveluntuottajana. Tavoitteena sosiaalisella manipuloinnilla voi olla esimerkiksi yritykselle kriittisen tiedon anastaminen tai taloudellinen hyöty. Sosiaalisen manipuloinnin avulla hakkerointi on yleisesti ottaen helpompaa, kuin yrityksen tietojärjestelmien teknisten suojausten murtaminen. (Susi 2015.)

Vaikkakin ystävällisyys, avuliaisuus ja ihmisiin luottaminen on pohja nyky-yhteiskunnalle, on se turvallisuusnäkökulmasta katsottuna toisinaan haitallista. Avaamalla esimerkiksi ulko-oven toiselle, saattaakin tietämättään päästää sisälle luvattoman, esimerkiksi huoltohenkilöksi pukeutuneen, henkilön. Tämän vuoksi jokaisesta vierailijasta tai sovitusta tapaamisesta tulee ilmoittaa koko henkilöstölle, eikä vierailijoita tule jättää toimitiloihin yksin. Sosiaalinen manipulointi saattaa kohdistua keneen tahansa yrityksen työntekijään, mutta yleensä hyökkääjä pääsee helpommalla ottaessaan suoraan yhteyttä yri-

tyksen johtohenkilöihin tai heidän avustajiin. Hyökkääjä saattaa esimerkiksi pyytää organisaation johtohenkilön nimissä työntekijää maksamaan aiheettoman maksusuoritteen tai paljastamaan yritykselle kriittisiä tietoja. (Susi 2015.)

Sosiaalinen manipulointi ei yleensä vaadi teknistä osaamista, vaan tietomurrot tapahtuvat inhimillisen erehdyksen vuoksi. On kuitenkin mahdollista, että osana sosiaalista manipulointia käytetään teknisiä hyökkäysmenetelmiä. Tämä voi tapahtua esimerkiksi siten, että hyökkääjä pyytää luottamuksen saatuaan käyttäjää liittämään haittaohjelman sisältävän muistivälineen omaan työtietokoneeseensa ja sen myötä tietokoneelle asentuu haittaohjelma tai takaovi, jota hyökkääjä käyttää hyväkseen toteuttaakseen tavoitteensa (F-Secure 2017). Toisinaan sosiaalinen manipulointi on jatkunut erittäin kauan ennen varsinaista hyökkäystä, jotta hyökkääjä on saanut uhrin luottamuksen.

Sosiaaliselta manipuloinnilta suojautumiseen tehokkain tapa on työntekijöiden tietoturvatietoisuuden lisääminen sekä yrityksen turvallisuusprosessien huolellinen suunnittelu, toteutus ja seuranta. Työntekijöiden kouluttaminen sosiaalisen manipuloinnin yritysten huomaamiseen ja poikkeamista ilmoittamiseen ovat tässäkin tapauksessa avainasemassa. Yrityksen olisi myös hyvä miettiä, millaista tietoa yrityksestä, sen työntekijöistä ja rakenteesta jaetaan julkisesti avoimiin tietoverkkoihin, sillä tätä tietoa saatetaan käyttää myös sosiaalisen manipuloinnin avulla toteutettavissa tietomurroissa hyödyksi. (Susi 2015.)

Tyytymättömät työntekijät ovat tutkimusten mukaan alttiimpia sosiaaliselle vaikuttamiselle ja näin myös sosiaaliselle manipuloinnille. Sen vuoksi työtyytyväisyys on myös tietoturvamielessä tärkeä asia, sillä motivoitunut ja tiedostava henkilöstö parantaa yrityksen tietoturvallisuutta merkittävästi. (Susi 2015.)

4.2 ISO/IEC 27001:2013 -standardin pohjalta määritellyt tietoturvariskit

ISO/IEC 27001:2013 -standardin tavoitteena on luoda yritykseen toimiva ja tehokas tietoturvallisuuden hallintajärjestelmä yrityksen tyypistä, koosta ja luonteesta riippumatta. Standardissa esitetään vaatimukset tietoturvallisuuden hallintajärjestelmän luomiselle, toteuttamiselle, ylläpitämiselle ja jatkuvalle parantamiselle. Standardin liitteenä on velvoittava Hallintatavoitteiden ja -keinojen viiteluettelo, jonka kaikki kohdat on käytävä läpi ja soveltuvissa osin toteutettava osana yrityksen tietoturvallisuuden hallintajärjestelmää.

Tämän viiteluettelon kaikki kohdat on määritelty tarkemmin ISO/IEC 27002 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet -standardissa, mutta ISO/IEC 27000 -standardiperheestä vain ISO/IEC 27001 -standardia vasten voi sertifioitua. (SFS Kauppa 2017.)

ISO/IEC 27001:2013 -standardin Hallintatavoitteiden ja -keinojen viiteluettelossa on lueteltu 116 kohtaa, joihin yrityksen tulisi edellä mainitun mukaisesti soveltuvissa osin määritellä tarvittavat hallintatoimenpiteet. Seuraavissa kappaleissa esitellään muutamia standardin määrittelemiä tietoturvauhkia ja niihin liittyviä hallintatoimenpiteitä.

4.2.1 Työntekijät

Työntekijät ovat organisaation tietoturvallisuuden hallintajärjestelmän yksi keskeisimmistä osista. Työntekijät ovat vastuussa muun muassa laitteistojen, ohjelmistojen, tietoaineistojen ja tietoliikenneverkkojen turvallisesta käytöstä, joiden oikeaoppisiin menettelytapoihin heidät täytyy myös kouluttaa. Suurin osa tietoturvallisuuden hallintajärjestelmää on henkilöstölle suunnattuja toimintaohjeistuksia ja menettelytapoja. Tietoturvallisuuden hallintajärjestelmän hallintakeinoja ja -ohjeistuksia laadittaessa tulee ottaa huomioon henkilöstön kohtaamat tietoturvauhat ja heidän tietoturvatietoisuuden taso. Mikäli työntekijät eivät ole tietoisia tietoturvallisuuden hallintajärjestelmään liittyvistä toimintalinjauksista ja oman panoksensa merkityksestä siinä, ei koko yrityksen tietoturvallisuuden hallintajärjestelmä ole riittävällä tasolla.

Työntekijöihin liittyviä tietoturvauhkia on työsuhteen kaikissa eri vaiheissa, sillä eniten tietoturvariskejä aiheuttavat yrityksen omat työntekijät – tahallaan tai vahingossa. Esimerkiksi työntekijän valintaprosessin aikana on varmistettava työnhakijan taustat ja pätevyys työtehtävään muun muassa suosittelijoiden tai riittävän koulutuksen, harjoittelun tai kokemuksen perusteella. Yrityksen ei tule myöskään kertoa työnhakijalle arkaluonteisia tietoja yrityksestä ennen työntekijän valintaa ja salassapitosopimuksen allekirjoittamista sekä yrityksen toimintalinjauksiin sitoutumista. (Kosutic.)

Työsuhteen alkaessa on tärkeää perehdyttää työntekijä tehtäviinsä sekä yrityksen toimintalinjauksiin, jotta työtehtävissä noudatetaan tietoturvallisia toimintatapoja. Työsuhteen alussa ja sen aikana on myös dokumentoitava työntekijälle luovutettavat tietovälineistöt

ja pääsyoikeudet, jotta työsuhteen päättyessä kaikki työntekijälle luovutetut tietovälineet myös palautetaan yritykselle ja pääsyoikeudet poistetaan käytöstä.

Työsuhteen aikana työntekijöiden tietoturvatietoisuuden lisääminen on merkittävä osa tietoturvariskien ennaltaehkäisyä. Ilman ajantasaista tietoturvatietoisuutta työntekijä ei välttämättä osaa huomata erilaisia tietoturvauhkia, kuten tietojen kalasteluyrityksiä tai sosiaalista manipulointia. Tietoturvauhat päivittyvät vuosi vuodelta ja uusista tietoturvauhista tiedottaminen ennaltaehkäisee myös uusiin tietoturvahyökkäyksiin lankeamista.

4.2.2 Tietovälineet

Tietovälineisiin voidaan luetella kaikki yrityksen toiminnan kannalta merkittävät tietovälineistöt, kuten tietokoneet, palvelimet, ulkoiset muistivälineet ja työpuhelimet. Näihin liittyviä tietoturvauhkia on tietovälineen elinkaaren kaikissa eri vaiheissa, kuten hankinnassa, käytössä, ylläpidossa ja käytöstä poistamisessa.

Tietovälinettä hankittaessa on tärkeää analysoida hankittavan tietovälineen soveltuvuus käyttökohteeseensa, mukaan lukien laitteelle asetetut tietoturvavaatimukset. Laitteen valinnassa on suositeltavaa konsultoida alan asiantuntijoita myös ylimääräisten taloudellisten kustannuksen välttämiseksi.

Tietovälineiden käyttöikään sekä tiedon saatavuuteen, luottamuksellisuuteen ja eheyteen vaikuttavat esimerkiksi tietovälineiden sijoittelu ja hyväksyttävä käyttö. Tietovälineitä, kuten tietokoneita ja palvelimia ei kannata sijoittaa maan tasalle tai vesiputken alle, jotta mahdollisen vesivahingon sattuessa tietovälineillä olevaa tietoa ei menetettäisi. Ikkunan viereen sijoitettu tietokoneen näyttö puolestaan vaarantaa tiedon luottamuksellisuuden, mikäli tietoväline altistuu salakatselulle. Tietovälineillä olevan tiedon eheyden turvaamiseksi ovat hyvät salasanakäytänteet ja salausmenetelmät avainasemassa. Tietovälineiden hyväksyttävän käytön toimintalinjaukset ovat ylimmän johdon päätettävissä ja hallintamenetelmät riippuvat paljolti tietovälineen käyttötarkoituksesta ja siitä, millaisessa ympäristössä tietovälinettä pääsääntöisesti käytetään. Tietovälineiden ja muiden resurssien vieminen pois toimitiloista tulee aina olla perusteltua ja niissä tapauksissa myös ohjeistettua.

Tietovälineisiin saattaa kohdistua edellä mainitun vesivahingon lisäksi myös monia muita ympäristöllisiä uhkia. Tällaisia ovat esimerkiksi palvelin- tai toimitiloissa tapahtuva tulipalo tai sähkökatkos. Pääosin kyseiset uhat vaikuttavat tiedon saatavuuteen. Tulipalon ennaltaehkäisyssä avainasemassa ovat tarvittavat paloturvallisuustoimenpiteet, kuten automaattiset hälytys- ja sammutusjärjestelmät, mutta uhan vaikutuksia voidaan osiltaan pienentää myös tietojen ja tiedostojen asianmukaisella varmuuskopioinnilla. Sähkökatkosriskiä voi olla vaikeaa järkevillä toimenpiteillä ennaltaehkäistä, mutta sen vaikutuksia voidaan olennaisesti pienentää esimerkiksi akkukäyttöisten tietovälineiden valinnalla ja varavirtajärjestelmällä (Heljaste 2008, 73–74).

Tietovälineiden virheettömän ja luotettavan toiminnan takaamiseksi tietovälineitä täytyy myös säännöllisesti tarkastaa ja asianmukaisesti ylläpitää. Tietovälineiden tarkastamiseen kuuluu esimerkiksi tietovälineen tietoturvavaatimusten katselmointi ja tietovälineen toimivuuden tarkastaminen nimetyn huoltohenkilön toimesta säännöllisin väliajoin sekä muutosten yhteydessä. Jokaisen työntekijän vastuisiin kuuluu havaituista poikkeamista ilmoittaminen sekä omassa käytössä olevien tietovälineiden asianmukainen ylläpitäminen. Tämä tarkoittaa käytännössä esimerkiksi päivitysten asentamista, vain luvallisten ohjelmistojen ja liitännäisten asentamista omalle tietovälineelle sekä tiedon dokumentointia ja varmuuskopiointia niin, ettei tietoaineisto ole vain yhden tietovälineen varassa.

Tietovälineen elinkaaren lopussa on vaarana, että tietoväline hävitetään omatoimisesti ilman riittävää tietovälineen puhdistamista ja alustamista. Jos esimerkiksi alustamattoman työtietokoneen myy kolmannelle osapuolelle, on uuden omistajan mahdollista saada tietoonsa tietokoneelta yritykseen liittyvää informaatiota tai mahdollisesti jopa käyttäjätunnuksia. Tämän vuoksi tietovälineet tulee poistaa käytöstä vain nimetyn vastuuhenkilön kautta, eikä työntekijöiden tule hävittää mitään yrityksen tiedon käsittelyyn käytettyjä tietovälineitä itse.

4.2.3 Dokumentaatio

Tietoa voi olla monissa eri muodoissa. Yksi osa yritykselle tärkeää tietoa on työntekijöille kertynyt kokemus ja osaaminen. Mikäli jonkin toiminnan osaa suorittaa vain yksi henkilö

ja tämä avainhenkilö ei ole paikalla, ei myöskään tietoa ole saatavilla. Tämän tietoturvariskin välttämiseksi tietoa tulee dokumentoida riittävästi ja dokumentaation ajantasaisuus tarkistaa säännöllisesti sekä aina muutosten yhteydessä.

Kuten mainittu, jokaisen työntekijän vastuulla on tiedon dokumentointi ja varmuuskopiointi. Organisaation olisi lisäksi hyvä nimetä tiedon dokumentoinnin ja varmuuskopioinnin ajantasaisuuden varmistamiseen vastuuhenkilöt. Organisaatiossa voidaan tehdä esimerkiksi toimintalinjaus, jossa esimiesten tai projektipäälliköiden vastuulla on varmistaa tiedon riittävä dokumentointi eri toiminnoissa ja varata dokumentoinnille tarpeeksi aikaa. Usein dokumentointia pidetään työläänä ja aikaa vievänä toimintona, vaikka sen avulla saatetaan välttää tulevaisuudessa monta epäselvää tilannetta ja hyvän dokumentoinnin avulla myös muut pystyvät tekemään tiettyjä toimia, mikäli toiminnon aiemmin suorittanut on muissa tehtävissä. Varmuuskopioinnin avulla vältetään tiedon saatavuuden ongelmia muun muassa siinä tilanteessa, jos tietoväline katoaa, varastetaan tai se saastuu esimerkiksi kiristyshaittaohjelmalla. Varmuuskopioinnissa voi käyttää esimerkiksi 3-2-1-taktiikkaa, jossa tiedoista on kolme varmuuskopiota, joista kaksi on eri formaateissa ja yksi on fyysisesti erillään muista (Tamminen 2016). Näin toimiessa tiedot olisivat tallessa esimerkiksi pilvipalvelussa, kiintolevyllä ja ulkoisella kovalevyllä, jolloin tiedot olisivat saatavilla ja palautettavissa myös tietoturvauhan toteutuessa tai vaikka jokin media ei olisi käytettävissä. Tiedon varmuuskopioinnissa tulee huomioida aina se, että kaikki käytettävät tallennusvälineet ja -palvelut ovat myös asianmukaisesti suojattu.

Dokumentaation ajantasaisuuden varmistamisella pyritään takaamaan se, että dokumentaatio on käyttökelpoista silloin, kun sitä tarvitaan. Yritys voi esimerkiksi nimetä vastuuhenkilöt, jotka varmistavat dokumentaation oikeellisuuden ja ajantasaisuuden säännöllisin väliajoin sekä aina muutosten yhteydessä. Joskus samasta asiasta saattaa olla tuotettu monta eri dokumenttia, jolloin myös dokumentaation vastuuhenkilön tehtävänä on tarvittaessa yhdistää eri lähteissä oleva tieto yhdeksi dokumentiksi tai varmistaa, että kaikki niistä on ajan tasalla. Dokumentaatiossa tulisi myös käyttää yhtenäisiä merkintätapoja esimerkiksi dokumentin laatijasta, muokkaajista ja tarvittaessa dokumentin luottamuksellisuudesta. Näin dokumentaatiota on myös vaivattomampaa pitää ajan tasalla ja muokkausten tekijät on helpompi jäljittää. Dokumentaation muokkaamiseen tulisi olla rajatut oikeudet, jotta tiedon oikeellisuus voidaan varmistaa.

4.2.4 Toimitilat

Toimitiloihin liittyy tietoturvauhkia niin tiedon luottamuksellisuuden, eheyden, kuin saatavuudenkin kannalta. Suuri osa toimitiloihin liittyvistä tietoturvauhista on ympäristöön liittyviä, kuten tulipalot, vesivahingot ja sähkökatkokset. Lisäksi toimitiloihin voi kohdistua tarkoituksenmukaista ilkivaltaa tai sosiaalisen manipuloinnin avulla tehtyjä tietomurtoja. Kaikissa näissä tapauksissa toimitiloissa olevat tietovälineet ja niitä tukevat laitteistot sekä mahdolliset paperiset asiakirjat ovat vaarassa tuhoutua sekä altistua salakatselulle ja luvattomalle muokkaamiselle.

Ympäristöllisiä uhkia on vaikeaa poistaa kokonaan, mutta niiden todennäköisyyttä ja vaikutuksia voidaan pienentää harkituilla hallintatoimenpiteillä. Tällaisia olisivat esimerkiksi tulipaloriskin minimoimisen osalta sammutin- ja hälytinjärjestelmät, paloturvallisuussuunnitelman kouluttaminen henkilöstölle sekä tietojen asianmukainen varmuuskopiointi. Vesivahinkoa voidaan puolestaan ennaltaehkäistä vesivuotohälyttimien tai -kytkinten avulla sekä henkilöstöohjeistuksella esimerkiksi astianpesukoneen käytön suhteen. Sähkökatkosten vaikutusten pienentämisessä merkittävässä osassa ovat taas varavirtajärjestelmät sekä akkukäyttöiset laitteistot. Ilkivallan ennaltaehkäisyssä hallintatoimenpiteinä ovat esimerkiksi asianmukaisten valvonta- ja hälytysjärjestelmät.

Toimitiloissa vierailevat henkilöt, kuten asiakkaat ja yhteistyökumppanit tai ulkoistetut palvelut, kuten siivous- ja huoltohenkilöt aiheuttavat myös merkittävän tietoturvariskin. Yrityksen on varmistettava, että toimitiloissa vierailevat henkilöt eivät pääse käsiksi yrityksen kriittisiin tietovälineisiin ja tietoon tai etteivät he kuule toimitiloissa käytyjä arkaluontoisia keskusteluja. Vierailijoihin liittyvien tietoturvariskien ennaltaehkäisyssä suuressa merkityksessä ovat henkilöstölle laadittavat tietoturvaan liittyvät toimintaohjeistukset ja niiden noudattaminen. Ulkoistettujen palveluiden kanssa tehtyihin sopimuksiin täytyy puolestaan aina sisällyttää tietoturvaa koskevat vaatimukset. (ISO/IEC 27001:2013.)

4.2.5 Tietoliikenne

Tietoliikenteen suojaaminen tarkoittaa niin toimitiloissa käytettäviä tietoliikenneverkkoja, kuin myös sen ulkopuolella työasioihin käytettäviä tietoliikenneväyliä. Toimitilojen

sisällä käytettävästä tietoliikenteestä tulee varmistaa sen riittävä suojaustaso ja vain oikeutettujen henkilöiden päästäminen sisälle organisaation tietoverkkoihin. Tämä tarkoittaa esimerkiksi sitä, että yrityksessä määritellään lähiverkon (*LAN*) ja langattoman lähiverkon (*WLAN*) suojausperiaatteet. Organisaation tulee määritellä muun muassa se, kenellä on oikeus päästä käsiksi yrityksen tietoverkkoihin ja millaisia salaustekniikoita verkoissa käytetään. Lähiverkkoon kohdistuva tietoturvauhka on esimerkiksi se, että yrityksen toimitiloissa vieraileva henkilö voisi liittää tietokoneensa vapaisiin verkkopistokkeisiin ja ilman riittävää salaustekniikkaa päästä jopa tarkastelemaan verkon liikennettä. Langattoman lähiverkon salasanan puuttuminen tai sen rajaamaton jakaminen ulkopuolisille voisi puolestaan johtaa minkä tahansa tietovälineen kiinnittämiseen yrityksen verkkoon, ellei toimintalinjauksia ja suojausperiaatteita langattomalle lähiverkolle ole määritelty.

Yrityksen toimitilojen ulkopuolella työskennellessä tietoliikenteen tietoturvan merkitys korostuu entisestään. Ilman ohjeistusta ja tietoturvatietoisuuden lisäämistä työntekijä saattaa yhdistää tietovälineensä esimerkiksi julkiseen, salaamattomaan tietoverkkoon, jossa kaikkia hänen tekemiään toimia voidaan tarkkailla. Lisäksi ISO/IEC 27001:2013 -standardin Hallintatavoitteiden- ja keinojen viiteluettelon kohdassa A.6.2.2 vaaditaan, että etätyöskentelypisteissä käytettävien tietoverkkojen tulee olla hallinnoituja ja turvallisia, jotta tieto on turvallisesti saatavissa, prosessoitavissa ja säilytettävissä. Tämä voi tarkoittaa organisaatiosta ja sen toimialasta riippuen esimerkiksi sitä, että etätyöskentelyssä käytetään salattua virtuaalista erillisverkkoa (*VPN*) ja esimerkiksi datan siirrossa on määritelty toimitusketjun jokaisen vaiheen riittävä tietoturvallisuus.

5 TIETOTURVAUHKIEN ANALYSOINTI

Tietoturvariskien arviointitaulukkoon (liite 4) kerättiin kaikki yrityksen henkilöstön havaitsemat, Suomessa yleisimmät organisaatioiden kohtaamat sekä ISO/IEC 27001:2013 -standardin pohjalta määritellyt tietoturvauhat. Nämä jaoteltiin riskienarviointitaulukkoon sen perusteella, mitä yrityksen hallussa olevaa omaisuutta mikäkin uhka koskee. Yrityksen omaisuutta ovat muun muassa erinäiset tietovälineet, kuten tietokoneet ja palvelimet, mutta omaisuudeksi luokitellaan myös yrityksen toiminnan kannalta tärkeä infrastruktuuri, kuten toimitilat. Riskienarviointitaulukossa käsiteltiin myös tietoturvariskejä, jotka liittyivät esimerkiksi yrityksen työntekijöihin, vierailijoihin ja dokumentaatioon. Tietoturvariskien arviointitaulukossa jokaiselle tietoturvauhalle määriteltiin riskin haltija, eli kenen vastuulla tietoturvauhan hallintatoimenpiteiden käytännön toteuttaminen, kuten laitteistojen ylläpitäminen, on. Tämän lisäksi määriteltiin erilaisia haavoittuvuuksia, jotka voisivat johtaa tietoturvauhan toteutumiseen. Jokaiselle tietoturvauhalle määriteltiin todennäköisyys ja toteutumisen aiheuttamien vaikutusten suuruus ja näiden yhteenlasketusta lukemasta muodostui tietoturvauhkan riskiluku.

Tietoturvariskien arviointitaulukko (liite 4) laadittiin alla oleva esimerkin mukaisesti (taulukko 1). Esimerkissä on esitelty yksi organisaation omaisuus ja siihen liittyvä uhka, referenssinumero ja riskin haltija, sekä kuvitteellinen haavoittuvuus. Erillisessä Tietoturvariskianalyysi-dokumentissa (liite 5) esitettiin perustelut uhkien todennäköisyydeksi ja vaikutukseksi päätetyille lukemille. Tietoturvariskien arviointitaulukossa näiden lukemien yhteenlasketut tulokset eli riskiluvut myös merkittiin yhteneväisillä värikoodeilla, jotta riskit käsiteltäisiin niiden kriittisyysjärjestyksessä.

TAULUKKO 1. Esimerkki tietoturvariskien arviointitaulukosta (Kosutic, muokattu)

Nro.	Omaisuus	Riskin haltija	Uhka	Haavoittuvuus	Todennäköisyys (1-3)	Vaikutus (1-3)	Riskiluku (T+V)
1.	Palvelin	Järjestelmänvalvoja	Sähkökatkos	Ei varavirtajärjestelmää	2	3	5

Riskien suuruuden arvioinnissa käytettiin Valtionvarainministeriön asettaman julkisen hallinnon digitaalisen turvallisuuden johtoryhmän määrittelemiä VAHTI-ohjeita (Valtiovarainministeriö 2003, 41-43). Seuraavissa kappaleissa on esitelty VAHTI-ohjeissa annetut esimerkit uhkan todennäköisyyden ja vaikutusten arviointiasteikoista. Asteikkoa sovellettiin organisaation tilanteen mukaisesti ja jokaisen tietoturvauhan suuruutta harkittiin myös yrityksen liiketoiminnan näkökulmasta. Tietoturvauhkien arvioinnissa päätettiin käyttää juuri VAHTI-ohjeita, jotta jokaisen tietoturvauhan todennäköisyys ja vaikutukset olisivat yhteneväisesti arvioituja. Toisinaan tietoturvauhka täytti kuitenkin arviointikriteerejä monesta eri suuruuskategoriasta, jolloin tietoturvauhan todennäköisyyden ja vaikutusten lukemaksi annettiin sellainen lukema, jonka kriteerit täyttyivät parhaiten.

5.1 Todennäköisyys

Tietoturvauhkien toteutumisen todennäköisyys riippuu monesta eri tekijästä. Yksi tekijä on se, kuinka monella henkilöllä tai käyttäjäryhmällä on mahdollisuus toteuttaa tietoturvauhka. Esimerkiksi lokitapahtumien luvattomaan muokkaamiseen tai poistamiseen on oikeudet vain rajatuilla henkilöillä ja koska tekijä on helpommin jäljitettävissä, on tietoturvauhan todennäköisyys suhteellisen alhainen. Yrityksen luottamuksellisten tietojen julkituomisen voi puolestaan toteuttaa esimerkiksi kuka tahansa yrityksen työntekijä, jolloin myös uhka on todennäköisempi. Työntekijöiden toimia työpaikan ulkopuolella ei voida juuri valvoa, joten tällaisessa tilanteessa tietoturvariskin toteuttaja voidaan jäljittää vain kartoittamalla, kenellä kaikilla on ollut mahdollisuus tuoda julki juuri kyseessä olevaa luottamuksellista tietoa.

Tietoturvauhan ilmenemistaajuus on yksi uhan toteutumisen todennäköisyyteen vaikuttavista tekijöistä. Ilmenemistaajuutta voidaan lähinnä vain ennustaa aiempien tilastotietojen valossa. Mikäli johonkin toimintoon ei ole selkeää ohjeistusta ja toimintoa suoritetaan usein, on siihen liittyvällä tietoturvauhkalla tiheämpi ilmenemistaajuus ja sitä myötä korkeampi todennäköisyys. Alla olevassa taulukossa on esitelty uhkien todennäköisyyden arvioinnissa käytetyt arviointikriteerit (taulukko 2).

TAULUKKO 2. Tietoturvauhkien todennäköisyyden arviointi (Valtiovarainministeriö 2003, 41-42, muokattu)

Lukema	Todennäköisyys	Arviointikriteerit
3	Korkea	• Toiminto tai järjestelmä on heikosti valvottua • Toimintoon tai järjestelmään pääsy on helppoa • Toimintoa tai järjestelmää kohtaan on suurta mielenkiintoa • Toiminnon ohjeistusta ei ole • Tapahtuma ilmenee kerran kuukaudessa • Uhkan toteuttaminen on mahdollista suurelle määrälle käyttäjiä (oma henkilöstö, yhteistyökumppanit, ulkopuoliset)
2	Keskimääräinen	• Toiminto on osittain valvottua • Toiminnon ohjeistus on puutteellista • Tapahtuma ilmenee 1–2 kertaa vuodessa • Uhkan toteuttaminen on mahdollista tietyille käyttäjäryhmille (atk-tuki)
1	Alhainen	• Toiminto on hyvin valvottua ja siihen pääsy on hallittua. • Toiminto on hyvin ohjeistettu • Toimintoa kohtaan ei ole mielenkiintoa • Tapahtuma ilmenee kerran vuodessa • Uhkan toteuttaminen on mahdollista vain yksittäisille työntekijöille (asiantuntijat)
0	Ei merkitystä	• Todennäköisyys on tasan nolla. Tämä uhka ei voi toteutua missään olosuhteissa

Kuten todennäköisyyden arviointikriteereistä (taulukko 1) voidaan havaita, uhan todennäköisyyteen voidaan ainakin osaltaan vaikuttaa muodostamalla riskiä ennaltaehkäiseviä hallintatoimenpiteitä. Erityisesti toimintalinjausten ja -ohjeistusten laatiminen sekä henkilöstön kouluttaminen noudattamaan niitä on ensiarvoisen tärkeää. Merkittävässä roolissa ovat myös muun muassa pääsyoikeuksien rajattu jakaminen ja lokitietojen hallinta, jotta tietoon käsiksi pääsevät henkilöt on mahdollista tarvittaessa jäljittää.

5.2 Vaikutukset

Vaikkakin yrityksen liiketoiminnan kannalta tärkeää on ennaltaehkäistä tietoturvauhkien toteutuminen, on yrityksen myös suunniteltava tietoturvariskien toteutumisen vaikutuksia pienentäviä hallintatoimenpiteitä. Esimerkiksi sähkökatkoksen toteutumisen todennäköisyyttä on lähes mahdotonta poistaa kokonaan, mutta siinä tilanteessa tiedon saatavuuteen kohdistuvat vaikutukset voidaan kuitenkin minimoida esimerkiksi asianmukaisten varavirtajärjestelmien ja varmuuskopioinnin avulla.

Tietoturvauhkien tapahtumisen vaikutukset voivat vaihdella vähäisistä erittäin vakaviin (taulukko 3). Valtiovarainministeriön (2003, 42-43) laatimien VAHTI-ohjeiden perusteella esimerkiksi yhden työntekijän kohtaamat tiedon saatavuusongelmat eivät aiheuta juurikaan taloudellisia kustannuksia, eikä pitkäkestoista toiminnan keskeytymistä, jolloin tietoturvauhkan toteutumisen vaikutukset jäävät vähäisiksi. Toisaalta taas onnistuneen tietomurron tai tietojen luvattoman julkituomisen vaikutukset saattaisivat yltää erittäin vakaviksi, sillä uhkan toteutuminen aiheuttaisi luottamuksellisuuden menetyksen sekä mahdollisesti erittäin suuret taloudelliset tappiot. Toisinaan taas tietoturvauhkan toteutuminen voi pahimmassa tapauksessa aiheuttaa luottamuksellisuuden menetyksen, mutta mikäli kyseinen tapahtuma ei tule organisaation tietoisuuteen, ei asiasta välttämättä tehdä edes tiedotetta. Tämä voisi käytännössä tapahtua esimerkiksi siten, että ulkopuolinen henkilö kuulee julkisella paikalla organisaation toimintaan liittyvän luottamuksellisen keskustelun, mutta ulkopuolinen henkilö ei kuitenkaan koskaan tuo julki kuulemiaan tietoja.

TAULUKKO 3. Tietoturvauhkien vaikutusten arviointi (Valtiovarainministeriö 2003, 42-43, muokattu)

Lukema	Vaikutukset	Arviointikriteerit
3	Erittäin vakavat	• Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä • Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä • Uhkan toteutuminen aiheuttaa raportoinnin ministeriölle ja tiedotusvälineille • Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin • Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia • Uhkan toteutuminen aiheuttaa vakavan häiriön organisaation toiminnassa (useiden avainhenkilöiden menetys) • Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen • Toiminta on lainsäädännön velvoitteiden vastaista.
2	Vakavat	• Seurauksilla on vaikutuksia organisaation sisällä, esimerkiksi yksittäisten työntekijöiden työmäärät kasvavat (avainhenkilön menetys) • Seuraukset koskevat useita tietojen tai palveluiden käyttäjiä • Seurauksilla on vaikutus organisaation toimintaan (saatava kuntoon tunneissa) • Uhkan toteutuminen aiheuttaa tiedotteen tekemisen • Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia
1	Vähäiset	• Seuraukset koskevat muutamia tietojen tai palveluiden käyttäjiä • Uhkan toteutuminen ei aiheuta välittömästi toimenpiteitä • Uhkan toteutuminen aiheuttaa sisäisen raportoinnin • Uhkan toteutuminen aiheuttaa vähäisiä taloudellisia kustannuksia • Toiminnan keskeytyminen on muutaman minuutin pituinen

Tärkeä osa tietoturvallisuuden hallintajärjestelmää on muodostaa myös toipumis- ja jatkuvuussuunnitelmat niin tietoturvariskin toteutuessa, kuin myös yritykselle tappiollisissa tilanteissa. Toisaalta yrityksen tappiolliset tilanteet voidaan lukea myös tietoturvauhaksi, sillä tällöin kaikkia tietoturvallisuuden hallintatoimenpiteitä ei välttämättä kyetä ylläpitämään tai kehittämään. Tämän tietoturvauhan vaikutuksia pyritään ennakoimaan suunnittelemalla toimintaohjeistukset tietoturvauhan toteutuessa ja määrittelemällä tietoturvallisuuden hallintajärjestelmän vähimmäistoimenpiteet myös yrityksen tappiollisten tilanteiden aikana.

5.3 Riskiluku ja hyväksyttävä riskitaso

Riskiluku on riskin todennäköisyyden ja vaikutusten yhteenlaskettu lukema. Tietoturvauhka analysoidaan tietoturvariskiksi, mikäli sen riskiluku ylittää määritellyn hyväksyttävän riskitason. Tietoturvariskeihin tulee puuttua sitä nopeammin, mitä suurempi riski on kyseessä. Jos todennäköisyyden ja vaikutusten yhteenlaskettu riskiluku määrittelee riskin sietämättömäksi (6), tarvittaviin hallintatoimenpiteisiin on ryhdyttävä välittömästi. Riskiluvun 5 omaavat riskit ovat myös merkittäviä riskejä, joihin tulee muodostaa riskilukua alentavat hallintatoimenpiteet mahdollisimman pian. Alla olevassa taulukossa on esitetty määritelmät erisuuruisille riskiluvuille (taulukko 4).

TAULUKKO 4. Riskiluvun määrittäminen (Valtiovarainministeriö 2003, 45, muokattu)

		Seurausten vakavuus		
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
Uhkan todennäköisyys	Korkea (3)	4. Kohtalainen riski	5. Merkittävä riski	6. Sietämätön riski
	Keski-määräinen (2)	3. Vähäinen riski	4. Kohtalainen riski	5. Merkittävä riski
	Alhainen (1)	2. Merkityksetön riski	3. Vähäinen riski	4. Kohtalainen riski

Käytännössä minkään tietoturvariskianalyysissä käsitellyn tietoturvauhan todennäköisyys tai vaikutukset eivät ole täysin olemattomat. Sen vuoksi taulukossa (3) käytetään

todennäköisyydelle ja seurausten vakavuudelle arvoja 1-3. Pienimmillään riskiluku voi tällöin olla merkityksetön (2).

Hyväksyttävän riskitason päättää aina viime kädessä organisaation ylin johto. Hyväksyttävänä riskitasona käytettiin tässä tietoturvariskianalyysissä riskilukua 3 eli vähäistä riskiä. Riski on vähäinen esimerkiksi silloin, kun uhan todennäköisyys on keskimääräinen, mutta sen toteutumisen vaikutukset jäisivät vähäisiksi. Eduix Oy:n tietoturvariskianalyysissä pohdittiin kuitenkin hallintatoimenpiteitä kaikentasoisille tietoturvauhille, vaikka niitä ei riskilukunsa perusteella luokiteltaisikaan tietoturvariskeiksi. Syynä tähän on se, että tietoturvauhan suuruus saattaa vaihdella muuttuvissa olosuhteissa ja taas toisaalta ISO/IEC 27001:2013 -standardin vaatimusten täyttymiseksi suurimpaan osaan luetelluista tietoturvauhista organisaation on määriteltävä hallintatoimenpiteitä.

5.4 Tietoturvariskianalyysi

Jokainen tietoturvariskien arviointitaulukkoon kerätyistä tietoturvauhista käsiteltiin perusteellisemmin erillisessä Tietoturvariskianalyysi-dokumentissa (liite 5). Jokaisen uhan todennäköisyyden ja vaikutusten lukemien määrittelemisen lisäksi pohdittiin jokaiselle riskille altistavia tietoturvahaavoittuvuuksia. Tietoturvariskianalyysissä käytettiin uhkakuvapohjaista lähestymistapaa ja jokaisen haavoittuvuuden hallintatoimenpiteiden puuttumisen vaikutuksia mietittiin organisaation liiketoiminnan näkökulmasta.

Tietoturvariskianalyysissä jokaisen riskin haavoittuvuuksien, todennäköisyyden ja vaikutusten analysoinnin lisäksi määriteltiin soveltuvimpia hallintatoimenpiteitä, jotka koostettiin vielä lyhennettynä versiona ylimmälle johdolle luovutettuun ehdotelmaan tietoturvallisuuden hallintatoimenpiteistä (liite 6). Tietoturvariskianalyysissä käytiin läpi myös ISO/IEC 27001:2013 -standardin velvoittava Hallintatavoitteiden ja -keinojen viiteluettelo, jotta yhtäkään standardin asettamaa vaatimusta ei laiminlyötäisi. Riskin analysoinnin yhteydessä esitettiin hallintatoimenpiteiden osalta viittaukset kyseiseen viiteluetteloon ja näin jokainen ISO/IEC 27001:2013 -standardin vaatimus myös sisältyy päätettäviin hallintatoimenpiteisiin.

6 TIETOTURVARISKIEN HALLINTATOIMENPITEET

Tietoturvariskianalyysissä pohdittiin jokaiselle tietoturvauhalle erilaisia hallintatoimenpiteitä ja ehdotelma toteutettavista hallintatoimenpiteistä koostettiin erilliseen dokumenttiin (liite 6). Hallintatoimenpide-ehdotelman tarkoitus oli toimia pohjana myös seuraavaa vaihetta eli riskien käsittelyä varten.

Ehdotelmaan tietoturvallisuuden hallintatoimenpiteistä koostettiin ylimmän johdon päätöstä vaativat asiat sekä alustavat henkilöstölle osoitettavat toimintaohjeistukset. Henkilöstön toimintaohjeistukset jaoteltiin yleisiin, jokaista työntekijää koskeviin tietoturvaohjeistuksiin sekä hieman tarkemmin eri liiketoimintayksikköjen työntekijöitä sekä etätyöskentelyä koskeviin toimintaohjeistuksiin.

6.1 Ylimmän johdon päätettävät hallintatoimenpiteet

Ehdotelmaan tietoturvallisuuden hallintatoimenpiteistä koottiin ensin ylimmän johdon päätöstä vaativat asiat. Tällaisia olivat esimerkiksi ylimmän johdon osoittamat resurssit ja tuki tietoturvallisuuden hallintajärjestelmälle. Jokaiseen päätöstä vaativaan asiaan esitettiin joitakin käytännön esimerkkejä, joilla päätettävää asiaa voidaan lähteä purkamaan. Alla olevassa taulukossa on esimerkinomaisesti esitelty tietoturvallisuuden hallintajärjestelmää koskevia hallintatoimenpiteitä, jotka yleensä vaativat ylimmän johdon päätöksen (taulukko 5).

TAULUKKO 5. Ylimmän johdon päätöstä vaativien hallintatoimenpiteiden esimerkki

	Päätös	**Käytännössä**
1.	Tietoturvallisuuden hallintajärjestelmälle osoitettavat resurssit	Tietoturvallisuuden hallintajärjestelmän muodostamiseksi, toteuttamiseksi ja ylläpitämiseksi vaadittavien resurssien osoittaminen.
2.	Vastuuhenkilöiden nimeäminen	Projektipäällikkö, projektitiimi, tietoturvapäällikkö, johtoporras ja eri toimintojen vastuuhenkilöt.
3.	Tietoturvallisuuden hallintajärjestelmän laajuuden ja tavoitteiden asettaminen	Laajuuden määritteleminen fyysisesti ja esimerkiksi liiketoimintakohtaisesti. Tavoitellaanko liiketoiminnan kannalta erottuvuutta, yhteensopivuutta alan säädösten kanssa, yhteneväisempää organisaatiota tai pienempiä kuluja. Millaisia numeerisia tavoitteita tietoturvan kannalta asetetaan.

Kuten ylimmän johdon päätöstä vaativista asioista voidaan huomata, ylimmän johdon päätettävinä ovat enimmäkseen tietoturvallisuuden hallintajärjestelmälle osoitettavat resurssit ja suurpiirteiset toimintalinjaukset. Tarkemmat toimintaohjeistukset ja menettelytavat ovat yleensä tietoturvallisuuden hallintajärjestelmälle nimetyn projektitiimin päätettävissä, vaikkakin myös näistä asioista tulee aina viestiä myös ylimmälle johdolle. Ylimmälle johdolle viestitään myös muun muassa tietoturvallisuuden hallintajärjestelmälle asetettavien tavoitteiden täyttymisestä ja tietoturvallisuuden hallintajärjestelmän tehokkuudesta.

6.2 Henkilöstöohjeistusten laatiminen

Tietoturvallisuuden hallintajärjestelmä on fyysisten suojausmekanismien lisäksi enimmäkseen henkilöstölle osoitettavia toimintalinjauksia ja -ohjeistuksia. Fyysisten suojaus-

mekanismien hankinta, käyttöönotto ja ylläpito ovat yleensä tietoturvallisuuden hallintajärjestelmälle nimetyn projektitiimin vastuulla, mutta myös niistä esiintyvistä poikkeamista ilmoittamisen vastuu on henkilöstöllä.

Henkilöstöohjeistuksissa pyrittiin yhteneväiseen esittämistapaan ylimmän johdon päätöstä vaativien hallintatoimenpiteiden kanssa. Jokainen tietoturvaohjeistus esitettiin ytimekkäästi, mutta sen käytännön toteuttamistavat eriteltiin myös tarkemmin. Alla olevassa taulukossa (6) on esitetty esimerkki henkilöstölle laadituista toimintaohjeistuksista, jotka olivat mukana ylimmälle johdolle laaditussa ehdotelmassa tietoturvallisuuden hallintatoimenpiteistä (liite 6).

TAULUKKO 6. Esimerkki henkilöstölle laadittujen tietoturvaohjeistusten ehdotelmasta

	Tietoturvaohjeistus	**Käytännössä**
1.	Tunnista käsittelemiesi tietojen suojaustaso ja noudata huolellisuutta arkaluonteisten tietojen käsittelemisessä	Älä jätä arkaluonteisia dokumentteja tai tietovälineitä muiden saataville ja käsittele tietoa sen luottamuksellisuuden vaatimalla tavalla. Muistuta tarvittaessa muita tietoturvallisista toimintatavoista.
2.	Ilmoita huomaamasi tietoturvauhat ja poikkeamat esimiehellesi	Raportoi tiedon saatavuuteen, luottamuksellisuuteen ja eheyteen liittyvistä tietoturvapuutteista ja -tapahtumista, kuten toimimattomista tai tietoturvattomista laitteistoista ja ohjelmistoista.
3.	Huomioi salassapitovelvollisuus työpaikalla ja sen ulkopuolella	Älä paljasta yrityksen kriittisiä tietoja, sen infrastruktuuria tai palveluiden rakennetta ulkopuolisille. Noudata julkisilla paikoilla käydyissä keskusteluissa ja vierailijoiden läsnäollessa salassapitovelvollisuutta.

Tietoturvaohjeistukset pyrittiin tekemään selkeiksi, mutta kuitenkin kaikkia eri toimintoja koskeviksi. Ylimmälle johdolle ehdotettiin tietoturvaohjeistusten kouluttamista henkilös-

tölle esimerkiksi tietoturvatietoiskujen muodossa. On tärkeää varmistaa, että työntekijöiden käsitykset tietoturvallisista toimintaohjeistuksista ovat yhteneväisiä ja selkeästi viestittyjä. Tietoturvatietoiskujen muodossa henkilöstö saatettaisiin myös tietoiseksi tietoturvaohjeistusten taustoista ja niiden noudattamatta jättämisen mahdollisista vaikutuksista. Henkilöstölle tulisi myös antaa väylä kysyä tarkennuksia tietoturvaohjeistuksiin tai ilmoittaa uusista tarvittavista ohjeistuksista tarvittaessa.

6.3 Hallintatoimenpiteiden toteuttaminen

Riskien käsittely on tietoturvariskianalyysin jälkeen seuraava vaihe tietoturvallisuuden hallintajärjestelmän toteuttamisessa. Hallintatoimenpiteistä ensimmäisinä on päätettävä sellaiset, joiden puutteen vuoksi jokin tietoturvariski on erittäin merkittävä. Suuri osa päätettävistä hallintatoimenpiteistä tarkoittaa käytännössä yhtenäisten toimintalinjausten muodostamista ja ohjeistusten laatimista ja taas osa hallintatoimenpiteistä merkitsee yrityksen tietoturvaan liittyviä hankintoja. Toteutettavat hallintatoimenpiteet kerätään tietoturvariskien käsittelytaulukkoon ja tässä kohtaa nimetään jokaisen hallintatoimenpiteen toteuttaja, toteutusaikataulu ja siihen osoitettavat resurssit. Tietoturvariskien käsittelytaulukkoon merkitään myös referenssi niihin riskeihin, joihin hallintatoimenpiteen toteuttaminen vaikuttaa ja sen vuoksi riskien arviointitaulukossa oli tärkeää numeroida uhat.

Hyvin suunniteltu ja viestitty tietoturvallisuuden hallintajärjestelmä on helpompi omaksua ja ottaa käyttöön. Alussa saattaa tietysti aina ilmetä asioita, joita ei ole osattu suunnitteluvaiheessa ottaa huomioon, mutta sitä varten hallintajärjestelmää tulee jatkuvasti monitoroida, arvioida ja kehittää. Tietoturvallisuuden hallintajärjestelmän ja toteutettavien hallintatoimenpiteiden käyttöönoton ajaksi on hyvä varata enemmän resursseja tietoturvallisuuden hallintajärjestelmän vastuuhenkilöiltä, jotta mahdolliset epäkohdat ja kysymykset saadaan ratkaistua hallitusti ja nopeasti. Vielä toteutuksen ja käyttöönoton kynnyksellä on syytä tarkistaa koko projektin toimivuus ja ettei yhtäkään tärkeää standardin pykälää tai Hallintatavoitteiden ja -keinojen viiteluettelon kohtaa ole unohdettu tai sivuutettu.

6.4 Jäljelle jäävien riskien hyväksyntä

Joidenkin riskien torjuminen saattaa osoittautua kalliimmaksi, kuin itse tietoturvariskin toteutuminen. Tietoturvallisuuden hallintajärjestelmän tulee kuitenkin olla resursoitu siten, että se on myös yrityksen liiketoiminnan kannalta järkevää. Yleensä esimerkiksi verkon välityksellä tapahtuvilta tietoturvauhilta on mahdotonta puolustautua täydellisesti, mutta sopivilla hallintatoimenpiteillä tietoturvariskiä ja sen vaikutuksia voi kuitenkin minimoida (Sulankivi 2016).

Mikäli joihinkin tietoturvariskeihin ei ole järkevää toteuttaa hallintatoimenpiteitä, on se perusteltava tarkasti ja selvitys jäännösriskeistä on saatettava ylimmän johdon tietoisuuteen. Organisaation ylimmän johdon tulee hyväksyä jäljelle jäävät riskit tai osoittaa riskien pienentämiseksi tarvittavat resurssit. Jäännösriskit perusteluineen tulee myös dokumentoida osaksi sertifiointiauditoijalle luovutettavaa sovellettavuuden selvitystä.

7 JOHTOPÄÄTÖKSET JA POHDINTA

Eduix Oy:n tietoturvariskianalyysi koostui organisaatiossa havaittujen ja yleisesti olemassa olevien tietoturvauhkien kartoittamisesta, koostamisesta, arvioinnista ja analysoinnista sekä ehdotettavien hallintatoimenpiteiden laatimisesta. Eduix Oy:n tietoturvauhat ja tämänhetkinen tietoturvatilanne kartoitettiin henkilöstölle osoitetun tietoturvauhkakyselyn avulla, johon vastasi noin puolet yrityksen työntekijöistä. Kartoituksen avulla saatiin selville yleisimmät yrityksen työntekijöiden kohtaamat tietoturvauhat ja heidän käsityksensä Eduix Oy:n tämänhetkisen tietoturvallisuuden tilasta. Tietoturvatilanteen kartoitus osoitti Eduix Oy:n huolehtivan jo tällä hetkellä enimmäkseen riittävän hyvin tietoturvasta, mutta ISO/IEC 27001:2013 -standardin vaatimusten täyttymiseksi myös joitakin uusia hallintatoimenpiteitä vaaditaan.

Tietoturvauhkien todennäköisyys ja seurausten vakavuus arvioitiin Valtiovarainministeriön laatimien VAHTI-ohjeiden avulla. Arvioinnissa käytettiin kvalitatiivista eli uhkakuvapohjaista tietoturvariskien arviointimenetelmää, joka perustui harkintaan, aavistuksiin ja kokemuksiin eikä niinkään laskentateknisiin tai euromääräisiin analyyseihin. Tietysti tietoturvariskin arvioimiseksi voitaisiin myös käyttää kvantitatiivista tutkimusmenetelmää, mutta se olisi vaatinut tarkkaa tietoa kunkin tietoturvauhan torjumiseksi ja toteutumiseksi koituvista kustannuksista sekä mittavien tilastotietojen keräämistä ja hyödyntämistä. Osana hallintatoimenpiteiden arviointia ja toteuttamista olisi silti järkevää kartoittaa eri vaihtoehtojen vaatimat resurssit ja verrata niitä tietoturvariskin tapahtumisesta aiheutuviin tappioihin. Toteutettavista hallintatoimenpiteistä koituvat taloudelliset kustannukset tulee kuitenkin aina olla järkevästi suhteutettuna, jotta tietoturvallisuuden hallintajärjestelmän toteuttaminen on myös organisaation liiketoiminnan kannalta perusteltua.

Tietoturvariskianalyysissä pohdittiin tietoturvariskeille erilaisia mahdollisia hallintatoimenpiteitä ja nämä hallintatoimenpiteet koostettiin ylimmälle johdolle luovutettuun ehdotelmaan tietoturvallisuuden hallintatoimenpiteistä. Ehdotetut hallintatoimenpiteet koostuivat ylimmän johdon tai tietoturvallisuuden hallintajärjestelmän projektitiimin päätöstä vaativista toimenpiteistä sekä henkilöstölle ja eri toimintoihin liittyvistä tietoturvaohjeistuksista. Niin päätöstä vaativat asiat, kuin myös tietoturvaohjeistukset pyrittiin laatimaan mahdollisimman ytimekkäästi, mutta myös käytännön esimerkkien avulla.

7.1 Havaittujen ja olemassa olevien tietoturvauhkien yhteneväisyys

Tietoturvariskianalyysissä yksi mielenkiintoisimmista vaiheista oli vertailla henkilöstön kohtaamia tietoturvauhkia yleisesti olemassa oleviin tietoturvauhkiin ja ISO/IEC 27001:2013 -standardin määrittelemiin tietoturvallisuuden hallintakeinoihin. Vastaukset viestivät myös henkilöstön tämänhetkisen tietoturvatietoisuuden tasosta.

Tietoturvauhkakyselyn vastaukset osoittivat, että Eduix Oy:n henkilöstö on tiedostanut tietoturvallisuuden eri osa-alueet ja kiinnittänyt omassa toiminnassaan tietoturvaan liittyviin uhkiin huomiota. Tietoturvauhkakyselyn vastaukset koostettiin ensin ylimmälle johdolle erilliseen dokumenttiin (liite 3), jossa tietoturvauhat jaoteltiin tiedon luottamuksellisuutta, eheyttä ja saatavuutta koskeviin tietoturvauhkiin sekä toimintaohjeistuspyyntöihin. Koosteessa myös esiteltiin vastaajien lukumäärä ja sijoittuminen eri liiketoimintayksikköihin ja toimipisteisiin. Lisäksi koosteessa esiteltiin henkilöstön vastaukset tietoturvatilannetta kartoittaviin monivalintakysymyksiin. Tietoturvariskien arviointitaulukon täyttäminen aloitettiin henkilöstön havaitsemista tietoturvariskeistä ja sitä täydennettiin olemassa olevilla ja ISO/IEC 27001:2013 -standardin perusteella määritellyillä tietoturvauhilla. Henkilöstön ilmoittamat tietoturvauhat olivat suurilta osin samankaltaisia kuin edellä mainitut yleisesti olemassa olevat tietoturvauhat. Tämä puolestaan osoittaa sen, että työntekijät ovat omaksuneet tietoturvan eri osa-alueet, tietoturvallisuuden hallintajärjestelmän merkityksen sekä oman panoksensa tärkeyden tietoturvallisuuden hallintajärjestelmän muodostamisessa, ylläpitämisessä ja jatkuvassa kehittämisessä.

Tietoturvauhkakyselyn vastaukset osoittautuvat liittyvän suurimmalta osin fyysisiin tietoturvaa parantaviin toimenpiteisiin sekä ihmisisten tietoturvattomista toimintatavoista aiheutuviin tietoturvahaavoittuvuuksiin. Vain murto-osa vastauksista liittyi teknisiin tietoturvahaavoittuvuuksiin, mikä osoittaa myös yliopettaja Vainikan (Harjun 2010 mukaan) väittämän ihmisten merkityksestä organisaation tietoturvassa toteen. Käytännössä hyvän tietoturvallisuuden lähtökohtana organisaatiossa on työntekijöiden kouluttaminen, ohjeistaminen ja yhtenäisten toimintalinjausten muodostaminen. Tietoturvasta tulisi tehdä koko henkilöstölle mielenkiintoista ja mielekästä, jotta myös säädeltyjä toimintaohjeistuksia noudatettaisiin ja niiden noudattamatta jättämisen vaikutukset ymmärrettäisiin.

7.2 Jatkotoimenpiteet

Tietoturvariskianalyysin osalta seuraava vaihe olisi soveltuvimpien hallintatoimenpiteiden valinta. Tämä päätös on viime kädessä ylimmän johdon tehtävissä ja juuri siksi ylimmälle johdolle laadittiin ehdotelma hallintatoimenpiteistä, jossa myös esiteltiin käytännön esimerkkejä jokaisen hallintatoimenpiteen toteuttamisesta. Tämän opinnäytetyön aikataulun puitteissa ei kuitenkaan vielä olisi ehditty tekemään lopullisia päätöksiä ja sen vuoksi hallintatoimenpidedokumentista käytetään nimitystä ”ehdotelma”.

Päätettävien hallintatoimenpiteiden yhteydessä tehdään myös päätös siitä, mitä hallintatoimenpiteitä ei ole esimerkiksi taloudellisesti järkevää toteuttaa. Jos jollekin tietoturvariskille ei päätetä toteuttaa hallintatoimenpiteitä tai hallintatoimenpiteiden toteuttaminen ei alenna tietoturvariskiä hyväksyttävälle riskitasolle, on tällaisten riskien olemassaolo hyväksyttävä. Jäännösriskien hyväksymisessä täytyy kuitenkin käyttää harkintaa ja lopullisen päätöksen jäännösriskien hyväksymisestä tekee ylin johto.

Tietoturvallisuuden hallintajärjestelmän osalta seuraava vaihe tietoturvariskianalyysin jälkeen olisi riskien käsittely. Käytännössä tämä tarkoittaisi päätöstä hallintatoimenpiteiden toteuttamisesta ja niihin käytettävien resurssien osoittamista. Jokaisen päätetyn hallintatoimenpiteen toteuttaminen tulee myös aikatauluttaa ja niiden toteuttamiseen on nimettävä vastuuhenkilö. Hallintatoimenpiteiden toteuttamisen jälkeen tulee myös katselmoida hallintatoimenpiteiden tehokkuutta ja tarvittaessa kehittää tietoturvallisuuden hallintajärjestelmää saatujen tulosten perusteella. Tietoturvariskien käsittelyyn liittyvät toimenpiteet ja tulokset on tarkoitus dokumentoida tietoturvariskien käsittelytaulukkoon. Kyseisessä taulukossa puolestaan viitataan tietoturvariskien arviointitaulukossa esiteltyihin tietoturvariskeihin ja sen vuoksi tietoturvariskien arviointitaulukossa jokaiselle riskille määritettiin referenssinumero.

ISO/IEC 27001:2013 -standardin asettamien vaatimusten mukaisesti kaikki aiemmat työvaiheet ovat tähdänneet tietoturvallisuuden hallintajärjestelmän muodostamiseen ja lopulta sen sertifiointiin. Tietoturvariskianalyysin ja riskien käsittelyn jälkeen voidaan muodostaa dokumentti sovellettavuuden selvityksestä (*Statement of Applicability*). Tähän dokumenttiin tulee dokumentoida muun muassa toteutettavat hallintatoimenpiteet ja niiden tavoitteet sekä jäljelle jäävät riskit perusteluineen. ISO/IEC 27001:2013 -standardin

vaatimusten täyttämistä varten tulee olla dokumentoituna myös muita koko projektiin liittyviä asioita, kuten tietoturvallisuuden hallintajärjestelmän laajuus, tietoturvapolitiikka sekä suunnitelma sisäisistä auditoinneista.

7.3 Tietoturvariskianalyysin arviointi ja kehityskohteet

Tietoturvariskianalyysi onnistui kaiken kaikkiaan melko hyvin. Parasta antia työssä oli huomata työntekijöiden kiinnostus tietoturvaa kohtaan ja erityisesti halu oppia uutta. Sen vuoksi jatkossa myös toimintaohjeistukset olisi parasta viestiä henkilöstölle kiinnostavalla tavalla, esimerkiksi juuri tietoturvatietoiskujen muodossa. Tällöin jokaisen toimintaohjeistuksen laiminlyömisen uhat osattaisiin tunnistaa ja sen vuoksi työntekijät myös haluaisivat noudattaa tietoturvallisia toimintatapoja.

Tietoturvariskianalyysiä olisi voinut kehittää esimerkiksi valitsemalla jokaisesta liiketoimintayksiköstä yhden henkilön mukaan riskianalyysin tekemiseen. Tällöin jokaista suojattavaa kohdetta olisi analysoitu ja arvioitu vielä tarkemmin eri näkökulmista ja myös ehdotetut hallintatoimenpiteet ja toimintaohjeistukset olisivat näin saattaneet olla vielä tarkemmin eri toimintoihin kohdistettuja. Tärkeintä on kuitenkin ottaa ainakin soveltuvimpia hallintatoimenpiteitä valittaessa mukaan eri liiketoimintayksikköjen edustajia, jotka näkisivät jo suunnitteluvaiheessa eri hallintatoimenpiteiden puutteet ja toisaalta potentiaaliset kehitysmahdollisuudet.

LÄHTEET

Beek, C. 2017. Looking Into the World of Ransomware Actors Reveals Some Surprises. McAfee. Luettu 5.3.2018. https://securingtomorrow.mcafee.com/mcafee-labs/looking-into-the-world-of-ransomware-actors-reveals-some-surprises/

Digitaalinen Helsinki. 2017. Tietoturvan ja tietosuojan riskianalyysi. Luettu 10.2.2018. https://digi.hel.fi/kehmet/menetelmalaari/riskianalyysi/

F-Secure. 2017. 10 Tips for business OpSec. Luettu 11.3.2018. https://business.f-secure.com/10-tips-for-business-opsec?_ga=2.105524800.2123919598.1515567157-1879034739.1501060430

Harju, E. 2010. Tietoturvasta huolehtiminen on elinehto. Varsinais-Suomen Yrittäjä -lehti 03/2010. Luettu 25.2.2018. https://www.y-lehti.fi/arkisto/artikkeli/3192/Tietoturvasta+huolehtiminen+on+elinehto+

Heljaste, J-M. 2008. Yrityksen turvallisuusopas. 1. painos. Helsinki: Helsingin Kamari Oy 2008 ja tekijät, 69–83.

ISO/IEC 27001:2013. 2013. Information technology – Security techniques – Information security management systems – Requirements. International standard. Second edition. Tulostettu 7.6.2017.

Kosutic, D. ISO 27001:2013 Foundations Course. Advisera eTraining -verkkokurssi. https://training.advisera.com/course/iso-27001-foundations-course/

KrebsonSecurity. 2017. Phishers Are Upping Their Game. So Should You. Luettu 11.3.2018. https://krebsonsecurity.com/2017/12/phishers-are-upping-their-game-so-should-you/

Laakso, M. Tietoturvan hallintajärjestelmä. Tietojesisuojaksi.fi. Luettu 10.2.2018. https://tietojesiturvaksi.fi/tietoturvasuunnitelma/tietoturvan-hallintajarjestelma

Lehto, M. professori. 2018. Kyberturvallisuus tänä päivänä. Luento. 26.1.2018. Tampereen ammattikorkeakoulu. Tampere.

Munson, L. 2014. DoS vs DDoS – What is the difference?. Security-FAQs. Luettu 4.3.2018. http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html

Paajanen, E. 2016. Miten suojautua palvelunesto-hyökkäyksiltä (DDoS) ja kalasteluyrityksiltä. F-Secure. Luettu 4.3.2018. https://fi.business.f-secure.com/miten-suojautua-laajoilta-palvelunestohyokkayksilta-ddos-ja-kalasteluyrityksilta

Stewart, J., Tittel, E. & Chapple, M. 2005. CISSP : Certified Information Systems Security Professional. John Wiley & Sons, Incorporated, 190–193.

Sulankivi, T. 2016. Dos-hyökkäys kaataa nettipalvelun – miten voi suojautua?. Tivi-lehti. Luettu 4.3.2018. https://www.tivi.fi/Kaikki_uutiset/dos-hyokkays-kaataa-nettipalvelun-miten-voi-suojatua-6535679

Susi, M. johtava asiantuntija. 2015. Onko yrityksesi joutunut inhimmillisen hakkeroinnin kohteeksi? Elinkeinoelämän keskusliitto. Luettu 11.3.2018. https://ek.fi/ajankohtaista/uutiset/2015/09/21/onko-yrityksesi-joutunut-inhimillisen-hakkeroinnin-kohteeksi/

Tamminen, T. 2016. Muistitko varmuuskopioida? Tänään se kannattaa tehdä. Mikrobitti. Luettu 17.3.2018. https://www.mikrobitti.fi/2016/03/muistitko-varmuuskopioida-tanaan-se-kannattaa-tehda/

Valtiovarainministeriö. 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. 7/2003, 41-46.

Viestintävirasto. 2018. Suomalaisten yritysten sähköpostitunnuksia kalastellaan aktiivisesti. Luettu 11.3.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801171021.html

Viestintävirasto Kyberturvallisuuskeskus. 2016. Palvelunestohyökkäysten tekniikkaa puolustajille. Ohje. Luettu 4.3.2018. https://www.viestintavirasto.fi/attachments/tietoturva/Ohje_3_2016_liite_1_Palvelunestohyokkaysten_tekniikkaa_puolustajille.pdf

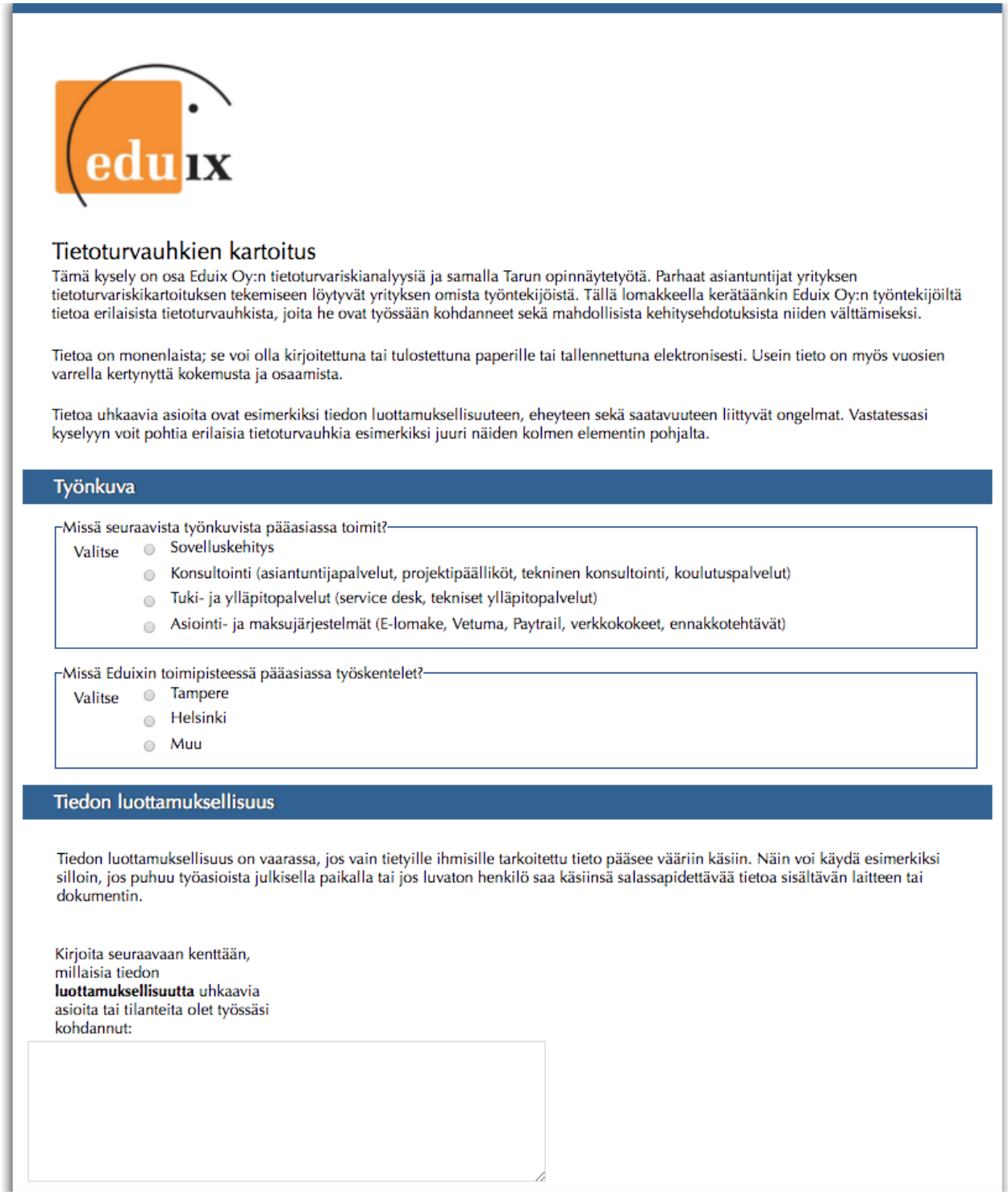
Viestintävirasto Kyberturvallisuuskeskus. 2018. Organisaatioiden 5 yleisintä tietoturvauhkaa ja ratkaisua vuonna 2017. Luettu 3.3.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801161310.html

Viestintävirasto Kyberturvallisuuskeskus, F-Secure, Poliisi. Look out for ransomware. Luettu 5.3.2018. http://www.ransomware.fi/

LIITTEET

Liite 1. Tietoturvauhkakysely

1 (3)



Tietoturvauhkien kartoitus

Tämä kysely on osa Eduix Oy:n tietoturvariskianalyysiä ja samalla Tarun opinnäytetyötä. Parhaat asiantuntijat yrityksen tietoturvariskikartoituksen tekemiseen löytyvät yrityksen omista työntekijöistä. Tällä lomakkeella kerätäänkin Eduix Oy:n työntekijöiltä tietoa erilaisista tietoturvauhkista, joita he ovat työssään kohdanneet sekä mahdollisista kehitysehdotuksista niiden välttämiseksi.

Tietoa on monenlaista; se voi olla kirjoitettuna tai tulostettuna paperille tai tallennettuna elektronisesti. Usein tieto on myös vuosien varrella kertynyttä kokemusta ja osaamista.

Tietoa uhkaavia asioita ovat esimerkiksi tiedon luottamuksellisuuteen, eheyteen sekä saatavuuteen liittyvät ongelmat. Vastatessasi kyselyyn voit pohtia erilaisia tietoturvauhkia esimerkiksi juuri näiden kolmen elementin pohjalta.

Työnkuva

Missä seuraavista työnkuvista pääasiassa toimit?

Valitse
- Sovelluskehitys
- Konsultointi (asiantuntijapalvelut, projektipäälliköt, tekninen konsultointi, koulutuspalvelut)
- Tuki- ja ylläpitopalvelut (service desk, tekniset ylläpitopalvelut)
- Asiointi- ja maksujärjestelmät (E-lomake, Vetuma, Paytrail, verkkokokeet, ennakkotehtävät)

Missä Eduixin toimipisteessä pääasiassa työskentelet?

Valitse
- Tampere
- Helsinki
- Muu

Tiedon luottamuksellisuus

Tiedon luottamuksellisuus on vaarassa, jos vain tietyille ihmisille tarkoitettu tieto pääsee vääriin käsiin. Näin voi käydä esimerkiksi silloin, jos puhuu työasioista julkisella paikalla tai jos luvaton henkilö saa käsiinsä salassapidettävää tietoa sisältävän laitteen tai dokumentin.

Kirjoita seuraavaan kenttään,
millaisia tiedon
luottamuksellisuutta uhkaavia
asioita tai tilanteita olet työssäsi
kohdannut:

Tiedon eheys

Tiedon eheys on vaarassa, jos luvaton henkilö pääsee muokkaamaan tietoa tai jos tieto muuttuu käsittelyn, siirron tai tallennuksen aikana. Luvatonta muokkaamista pyritään estämään muun muassa siten, että vain tarpeellisilla henkilöillä on oikeus päästä eri järjestelmiin ja kaikki muokkaukset niin asiakkaiden järjestelmissä, kuin myös käyttämissämme tehtävänhallintajärjestelmissä (esimerkiksi Teamissa) ovat jäljitettävissä ja palautettavissa.

Kirjoita seuraavaan kenttään,
millaisia tiedon **eheyttä** uhkaavia
asioita tai tilanteita olet työssäsi
kohdannut:

Tiedon saatavuus

Tiedon saatavuus tarkoittaa sitä, että tieto on kaikilla auktorisoiduilla henkilöillä saatavissa silloin, kun sitä tarvitaan. Tämä tarkoittaa esimerkiksi hyvää dokumentaatiota, jotta kaikki tieto ei ole vain yhden henkilön varassa. Tiedon saatavuutta uhkaavia asioita olisivat esimerkiksi avainhenkilön sairastuminen tai tietoa sisältävän laitteen katoaminen.

Kirjoita seuraavaan kenttään,
millaisia tiedon **saatavuutta**
uhkaavia asioita tai tilanteita olet
työssäsi kohdannut:

Muut tietoturvan osa-alueet

Tietoturvaa voidaan jakaa eri osa-alueisiin monella tapaa ja yllä oleva jaottelu on vain yksi niistä. Muita tarkasteltavia osa-alueita ovat myös muun muassa tietoturvan hallinnoiminen, fyysinen tietoturva (toimistojen ja laitteiden suojaaminen), ohjelmistojen ja tietoaineistojen tietoturva sekä henkilöstön rooleihin ja vastuihin liittyvät tietoturvaohjeistukset ja -asiat.

Mikäli mieleesi tulee esimerkiksi näihin asioihin liittyviä tietoturvauhkia tai puuttuvia ohjeistuksia, kirjoitathan ne seuraavaan kenttään. ?

Tietoturvasta huolehtiminen Eduix Oy:ssä

	Usein	Toisinaan	Silloin tällöin	Harvoin	En koskaan
Oletko joskus puhunut työasioista ulkopuolisille tai ulkopuolisten kuullen?	○	○	○	○	○

	Usein	Toisinaan	Silloin tällöin	Harvoin	En koskaan
Oletko joskus antanut toisen työntekijän tai ulkopuolisen henkilön käyttää työtietokonettasi tai muita järjestelmiä omilla tunnuksillasi?	○	○	○	○	○

	Aina	Useimmiten	Silloin tällöin	Harvoin	Ei koskaan
Onko tietoa mielestäsi tarpeeksi saatavilla silloin, kun sitä tarvitaan?	○	○	○	○	○

	Aina	Useimmiten	Silloin tällöin	Harvoin	En koskaan
Huolehditko mielestäsi itse tarpeeksi tiedon dokumentoinnista?	○	○	○	○	○

?

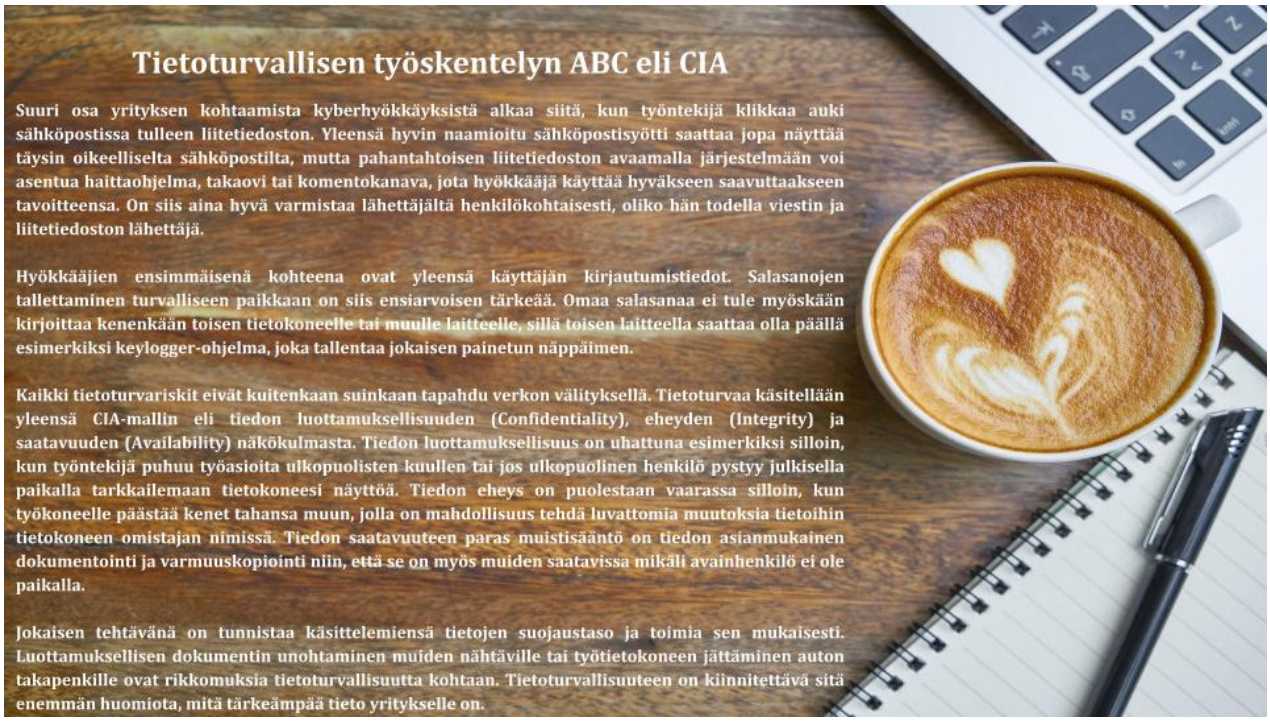
	Usein	Toisinaan	Silloin tällöin	Harvoin	En koskaan
Oletko joskus jättänyt työasioihin käytettävän tietovälineesi vartioimatta?	○	○	○	○	○

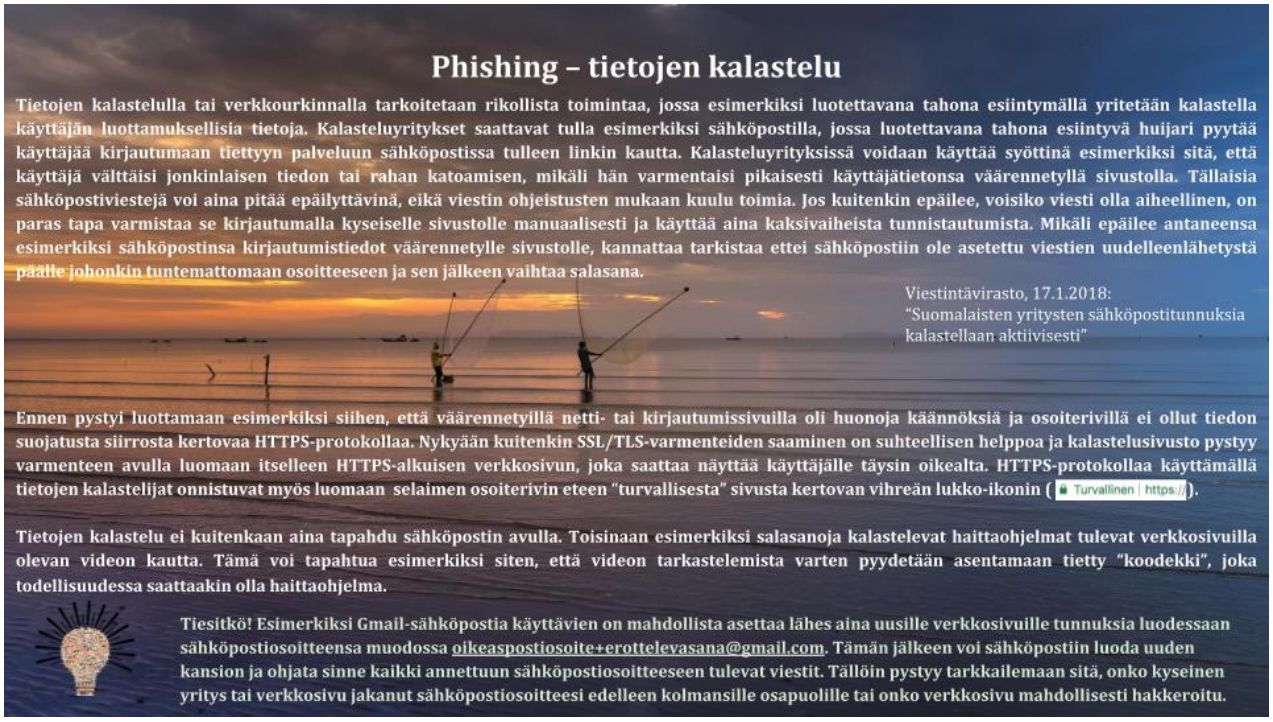
	Kyllä	Enimmäkseen	Jonkin verran	Ei	En osaa sanoa
Huolehditaanko Eduix Oy:ssä mielestäsi tällä hetkellä riittävästi tietoturvasta?	○	○	○	○	○

Tietojen lähetys

Tallenna

Liite 2. Tietoturvatietoiskut





Social engineering – käyttäjän manipulointi

Social engineering eli käyttäjän manipulointi tarkoittaa toimintaa, jolla yritetään saada käyttäjä luottamaan hyökkääjään ja paljastamaan siten tälle salaista tietoa. Kun käyttäjä luottaa hyökkääjään, hän saattaa vahingossa kertoa hyökkääjälle salaisia tietoja tai päästää hänet esimerkiksi sisälle yrityksen toimitiloihin. Muun muassa tämän vuoksi on tärkeää ilmoittaa jokaisesta sovitusta vierailijasta ja huoltokäynnistä koko henkilöstölle.

Hyökkääjä voi ottaa uhriinsa yhteyttä esimerkiksi sähköpostilla, puhelimitse, sosiaalisessa mediassa tai tulla jopa henkilökohtaisesti käymään. Yleensä hyökkääjä esiintyy jonain luotettavana tahona, kuten viranomaisena, palveluntuottajana tai vaikkapa asiakkaana. Sosiaalisen manipuloinnin avulla hakkerointi on yleisesti ottaen helpompaa, kuin yrityksen tietojärjestelmien teknisten suojausten murtaminen.

On olemassa myös sellaisia tietomurtoja, joissa puolituttu on pyytänyt apua tietyn yrityksen työntekijältä lähettämällä tälle esimerkiksi haittaohjelman sisältävän liitteen tulostettavaksi tai pyytänyt häntä tulostamaan sen muistitikulta, jonka mukana muistitikun avanneelle koneelle on asennettu haittaohjelma. Toisinaan sosiaalinen manipulointi on jatkunut erittäin kauan ennen varsinaista hyökkäystä, jotta hyökkääjä on saanut uhrin luottamuksen.

Tiesitkö!
Tyytymättömät työntekijät ovat tutkimusten mukaan alttiimpia sosiaaliselle vaikuttamiselle ja näin myös sosiaaliselle manipuloinnille. Sen vuoksi työtyytyväisyys on myös tietoturvamielessä tärkeä asia. Motivoitunut ja tiedostava henkilöstö parantaa yrityksen tietoturvallisuutta merkittävästi.

Kuvan lähde: Viestintävirasto, F-Secure, Poliisi, Look out for ransomware

Kuvan lähde: McAfee, Looking Into the World of Ransomware Actors Reveals Some Surprises, 2017

Ransomware – kiristysohjelmat

Yksi lisäsyy siihen, miksi tietoja ja tiedostoja ei tule pitää ainoastaan yhdellä tietovälineellä, on muiden haittaohjelmien sekä laitteen katoamisen lisäksi tiedostoja salaavat kiristysohjelmat (ransomware). Ne ovat eräitä tavallisimpia haittaohjelmia, joihin liittyy yleensä yritys saada käyttäjältä rahaa kiristämällä. Kiristysohjelma saattaa salata uhriksi joutuneen tärkeät tiedostot ja vaatia lunnaiden maksamista vastineeksi salauksen purkuavaimesta. Toiset kiristysohjelmaperheet käyttävät tiedostojen salaamiseen esimerkiksi RSA-salausalgoritmia, jolloin salauksen purkaminen ei onnistu kuin käyttämällä alkuperäistä purkuavainta.

Suomessa ja muualla maailmalla on jo useamman vuoden ajan ollut liikkeellä kiristysohjelmia, joiden väitetään tulevan paikallisen maan viranomaiselta. Ilmoituksessa saatetaan vaatia käyttäjää maksamaan sakkomaksu, jonka maksamalla koneen lukitus poistetaan. Vaaditut sakkomaksut ovat olleet noin 100–150 euron luokkaa ja viesteissä on jopa käytetty poliisin virallista tunnusta.

Vaikkakin kiristysohjelman saastuttama tietokone on yleensä puhdistettavissa, ei salattuja tiedostoja ole yleensä mahdollista palauttaa ilman oikeaa purkuavainta. Joihinkin tunnettuihin kiristysohjelmiin on jo onneksi kehitetty salauksenpurkutyökaluja, mutta ei kaikkiin. Ainoa varma suojaus tiedostojen menettämisen varalle on tiedostojen säännöllinen varmuuskopiointi, vaikkakin tärkeässä roolissa on myös maalaisjärki epäilyttävien verkkosivujen ja roskapostin suhteen. Edes lunnaiden maksaminen ei takaa tiedostojen palautumista ja se ainoastaan kannustaa verkkorikollisten toimintaa. Mikäli tietokone on saastunut kiristysohjelmalla, irrota laite heti verkosta, puhdista haittaohjelma tietokoneelta, palauta tiedostot varmuuskopioista ja ilmoita asiasta viranomaisille.


DoS ja DDoS
DoS (Denial of Service) eli palvelunestohyökkäys tarkoittaa sitä, että yhtä tietokonetta ja yhtä verkkoyhteyttä käytetään ylikuormittamaan palvelunestohyökkäyksen kohteen kaistaa ja muita resursseja lähettämällä suuri määrä ICMP- tai UDP-paketteja. Palvelunestohyökkäyksiä on myös muunlaisia, kuten ohjaustietojen häiritsemistä tai vääränlaisen lähetteen lähettämistä. Kaikilla eri tavoilla pyrkimyksenä on kuitenkin pystyä estämään palvelua tai heikentämään sitä valitussa kohteessa, esimerkiksi kohteen verkkosivuilla.
DDoS (Distributed Denial of Service) eli hajautettu palvelunestohyökkäys on taas kehittyneempi versio tavallisesta palvelunestohyökkäyksestä. Siihen käytetään yleensä ympäri maailmaa kaapatuista tietokoneista ja niiden yhteyksistä muodostuvaa botnettiä. Botnet muodostuu yleensä siitä, että suureen määrään tietokoneita on saatu tartutettua haittaohjelma tai ne on kaapattu ja näille tietokoneille on asetettu yhteinen tavoite – esimerkiksi juuri hajautetun palvelunestohyökkäyksen suorittaminen. Muita pahantahtoisia tehtäviä voisi olla esimerkiksi spämmiviestien lähettäminen, virusten levittäminen tai henkilökohtaisten tietojen varastaminen identiteettivarkauksia varten. DDoSin vaikutukset ovat tällöin yleensä paljon suuremmat, kuin DoSin, sillä yhden tietokoneen sijasta palvelua pyrkii kuormittamaan mahdollisesti jopa sadat tai tuhannet tietokoneet.
Eräitä tärkeimpiä suojauskeinoja palvelunestohyökkäyksiä vastaan on pitää yrityksen omat verkkosivut erillään yrityksen muusta toiminnasta. Hyökkääjät hyökkäävät yleensä julkisina näkyviin web-sivustoihin, eivätkä he välttämättä tiedä yrityksen muiden palveluiden rakennetta. Ulkoisia palveluja käytettäessä on taas varmistettava palveluntarjoajalta, että heillä on käytössään DDoS-hyökkäysten torjuntapalvelu ja että se sisältyy myös yrityksen kanssa tehtyihin sopimuksiin. Käyttäjän osalta tärkeintä on muistaa päivittää laitteitaan ja ohjelmistojaan aina, kun niille on saatavilla päivityksiä.

Liite 3. Tietoturvauhkakyselyn tulokset

(salassa pidettävä)

Liite 4. Tietoturvariskien arviointitaulukko

(salassa pidettävä)

Liite 5. Tietoturvariskianalyysi

(salassa pidettävä)

Liite 6. Ehdotelma tietoturvallisuuden hallintatoimenpiteistä

(salassa pidettävä)