Waltteri Kaivola

YRITYKSEN TIETOTURVAN PÄIVITTÄMINEN

Tietojenkäsittelyn koulutusohjelma

2019

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

YRITYKSEN TIETOTURVAN PÄIVITTÄMINEN

Kaivola, Waltteri
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Toukokuu 2019
Sivumäärä: 34
Liitteitä: -

Asiasanat: Tietoturva, päivitys, tietomurto, yritysturvallisuus

---

Opinnäytetyön tavoitteena oli syventyä yritysten tietoturvaan ja sen kehittämiseen. Opinnäytetyössä tarkasteltiin erilaisia digitaalisia ja fyysisiä uhkia, joita yritys voi toiminnassaan kohdata. Uhkien esittelyn ohella tutkittiin esimerkkiratkaisuja, miten voidaan suojautua ja välttyä hyökkäyksiltä.

Tutkittiin, miten yrityksen tietoturvan nykytilannetta kannattaa tarkastella. Mitä tulee ottaa huomioon, kun tarkastusta tehdään ja mitä metodeja voidaan hyödyntää.

Opinnäytetyössä käytiin läpi tietoturvan päivittämistä ja kyseisen projektin kulkua. Projektiin liittyen esiteltiin siinä hyödynnettäviä työkaluja. Samalla tutkittiin tietosuoja-asetuksen osuutta aiheeseen.

Työssä hyödynnettiin IT-yrityksen kahden työntekijän haastattelua. Haastattelusta saatiin hyvin kosketuspintaa todelliseen käytännöstä ammennettuun kokemukseen aiheesta.

Tietoturvan päivittämisen käsittelyn jälkeen tutkittiin vielä vaihtoehtoisia tietoturvaratkaisuja. Verrattiin hyötyjä ja haittoja sekä ulkoistamisen kannattavuutta suhteessa yrityksen toimintaan ja sen kokoon nähden.

Aihe oli erittäin laaja ja opinnäytetyön olikin tarkoitus tuoda aihetta lähemmäs yrityksiä, joilta ei vielä löydy tarkempaa käsitystä tai ovat täysin tietämättömiä tietoturvasta. Työssä keskeisimmäksi teemaksi nousi yritysten käyttäjien osuus tietoturvassa ja tietoturva kulttuurin rakentamisen merkitys.

UPDATING COMPANY INFORMATION SECURITY

Kaivola, Waltteri
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Business Information Technology
May 2019
Number of pages: 34
Appendices: -

Keywords: Information security, update, security breach, industrial security

---

The purpose of this thesis was to go deep into company information security and how to develop it. In the thesis we examined different digital and physical threats that companies may face in their operation. Alongside with the introduction of threats we studied example solutions on how to protect and avoid such attacks.

It was studied how to evaluate the current state of information security. What to consider when evaluating and which methods can be utilized.

The thesis went through of updating information security and how that project is carried out. Tools that can be utilized with the project were examined. Also, the involvement of general data protection regulation was studied.

Thesis makes use of an interview with two employees of an IT-company. The interview gave a good insight to true knowledge from practical experience with the topic.

After covering the updating of information security, the thesis examined alternative solutions to information security. Pros an cons of outsourcings profitability were compared in relation to companies operations and size.

The topic was very broad, and the purpose of the thesis was to bring information security closer to companies that don’t yet have a good understanding on it or are completely clueless of it. The company’s employees significance in information security and the importance of establishing an information security culture became central themes in the thesis.

SISÄLLYS

1 JOHDANTO

Maailman digitalisoituessa on suurin osa yrityksille elintärkeästä informaatiosta siirtynyt myös digitaaliseen muotoon. Näin tietoa on helpompi käsitellä ja hyödyntää liiketoiminnassa. Kaikilla yrityksillä on jotain digitaalista omaisuutta, jota halutaan suojella. Toisilla koko toiminta voi perustua verkkokauppojen ja logistiikan järjestelmien toimintaan. Näin ollen yrityksen toiminnalle on elintärkeää varmistua tietojen turvallisuudesta.

Tietoturvalla ei kuitenkaan tarkoiteta vain digitaalista näkökulmaa vaan myös työpaikalla ja sen ulkopuolella tapahtuvia käytäntöjä ja toimintamalleja. Nämä turvaavat sekä yrityksen että sen asiakkaiden tietojen säilymisen tahoilla, joille ne kuuluvat. EU:n tietosuoja-asetuksen, eli General Data Protection Regulation, myöhemmin GDPR, myötä asiakkaiden henkilötietojen käsittelystä on tullut entistä tarkempaa ja tärkeämpää. Tietosuoja-asetus on voimaan astuessaan tuonut hyvin esille kuluttajien oikeuksia ja vastuita koskien heidän tietojensa käsittelyä yrityksien kanssa toimiessa.

Pahimmillaan tietomurto tai muu tietoturvaa loukkaava tapaus voi keskeyttää koko yrityksen toiminnan. Tietomurroista koituvat taloudelliset tappiot voivat tulla erityisesti pienille ja keskisuurille yrityksille todella kalliiksi suhteutettuna toiminnan laajuuteen. Sanotaankin, että tietoturvaan panostaminen on aina halvempaa kuin onnistuneen tietomurron aiheuttamat kustannukset.

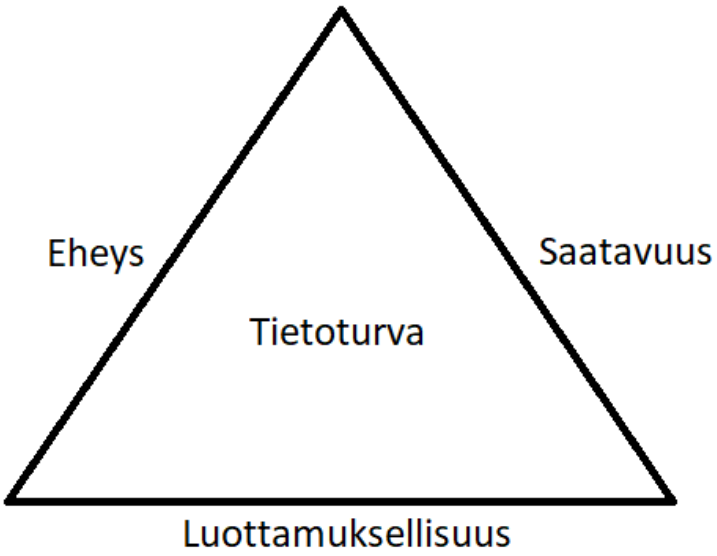
Teknologia kuitenkin kehittyy nopeasti ja lainsäädäntö muuttuu. Yrittäjällä sekä yrityksillä voi olla vaikeuksia pysyä kehityksen mukana. Opinnäyteyöni onkin tarkoitus luoda selventävä katsaus tietoturvan maailmaan sekä tuoda esille menetelmiä ja työkaluja, joiden avulla yritykset voivat päivittää toimintansa tietoturvan tilanteen nykypäivän tasolle.

2 TIETOTURVA

Tietoturvan ylläpitäminen on yrityksille toiminnan turvaamisen kannalta ehdottoman elintärkeää. Sen avulla taataan yrityksen toiminnan jatkuvuus sekä luotettavuus. Tiedon luottamuksellisuus onkin yksi tietoturvan tukipilareista. Luottamuksellisuudella varmistetaan, että tietoihin pääsevät käsiksi vain he, joiden on tarkoitettukin. Luottamuksellisuuden tasoa voidaan korottaa käyttämällä yrityksen toiminnassa toimintoja kuten tiedostojen kryptaus, salatut sähköpostit, riittävän kompleksiset salasanat sekä työtiloissa vaadittavat kulkukortit.

Toinen tietoturvan tukipilareista on saatavuus. Saatavuudella tarkoitetaan toimintamalleja, jotka pitävät tiedon saatavilla ja valmiina käytettäväksi. Tällaisia toimintamalleja ovat esimerkiksi tiedon kahdentaminen useammalle levylle tai muulle medialle. Tieto voidaan myös viedä pilvipalveluun säilytettäväksi, jolloin siihen käsiksi pääsyyn ei tarvita muuta kuin verkkoyhteys. Pilvipalveluiden käyttö tuo mukanaan kuitenkin omat riskinsä. Kun dataa siirretään toisen tahon säilytettäväksi, asetetaan tahtomattakin tiedot alttiiksi hyökkäyksille, jotka eivät muuten olisi koskettaneet yrityksen dataa.

Viimeinen tieturvan kolmesta tukipilarista on tiedon eheyden varmentaminen. Eheys tietoturvassa tarkoittaa tiedon muuttumattomuuden varmistamista sekä hyökkäys tilanteissa että sisäisissä toiminnoissa. Jos tiedon eheyttä ei voida varmentaa tulisi muutos vähintäänkin huomata. Eheyden varmentamisessa tulee myös hyödyntää kryptausta sekä hajautusalgoritmeja.



Kuva.1 Suomennettu versio tietoturvan CIA-kolmiosta. (Study.com www-sivut n.d.)

Nämä kolme tukipilaria muodostavat niin sanotun tietoturvan CIA-kolmion. Kirjainyhdistelmä CIA tulee englannin kielen sanoista confidentiality (luottamuksellisuus), integrity (eheys) sekä availability (saatavuus). Tätä tietoturvan CIA-kolmiota voidaan hyödyntää yrityksen tietoturvaa arvioitaessa sekä tutkittaessa. (Techopedia www-sivut n.d.)

3 TIETOTURVAN UHAT

Tietoturvaan kohdistuvia onnistuneita hyökkäyksiä kutsutaan tietomurroiksi. Tietomurrot voivat olla seurauksia niin digitaalisista kuin fyysisitä tietoturvaan kohdistuvista hyökkäyksistä. Onnistuneen hyökkäyksen seuraamukset ovat lähes poikkeuksetta vakavat yritykselle sekä sen asiakkaille. Hyökkääjä voi tietomurrossa viedä esimerkiksi yrityksen toiminnalle kriittistä tietoa. Kriittisenä tietona voidaan pitää valmistettavien tuotteiden piirustuksia tai salaisia yhteistyökumppaneiden kanssa laadittuja asiakirjoja. Asiakkaalle uhka realisoituu usein vasta kun hyökkäyksen yhteydessä on viety henkilötunnukset tai maksukorttien tiedot. Tällöin on jo liian myöhäistä

toimia ja siksi ennakointi onkin ehdottoman tärkeää tietoturvaan kohdistuvien hyökkäysten minimoimisessa.

Digitaalinen tietoturva on huomattavasti laajempi osa-alue kuin fyysinen tietoturva. Digitaaliset uhat ovat yleisimmin ulkopuolisen tahon suunnittelemia ja toteuttamia esimerkiksi phishing tai DDoS hyökkäyksiä.

Kuitenkin suurin yrityksen digitaaliseen tietoturvaan kohdistuva uhka on yrityksen työntekijät. Omalla toiminnalla voidaan usein välttyä suurimmalta osalta tietomurroista. Tiedon jakaminen ja asiasta tiedottaminen sekä keskusteleminen ovat ehdottoman tärkeitä ja tehokkaita tapoja suojata yrityksen tietoja.

Fyysinen tietoturvaan kuuluvat tietoturvaan kohdistuvat uhat, jotka ovat nimensä mukaisesti fyysisiä. Tähän luokkaan kuuluvat uhat kuten tulipalot, vesivahingot, sään aiheuttamat muutokset, virran syötön varmistaminen sekä itse ihmisen toiminnallaan aiheuttamat uhat. Näistä esimerkeistä ehdottomasti suurimman uhan muodostaa ihminen. Ihminen voi vahingossa tai tahallaan aiheuttaa hyvinkin suurta vahinkoa laitteistoille sekä ohjelmistoille.

Fyysiseen tietoturvaan kuuluu myös tilojen tietoturvallisuuden varmistaminen. Tästä huolehditaan esimerkiksi järjestämällä toimitiloihin kulkukortteja ja lukollisia keräysastioita tietoturvajätettä varten.

4 YLEISET DIGITAALISEN TIETOTURVAN UHAT

Käsitteenä digitaalinen tietoturva on todella laaja. Sitä on vaikea rajata mihinkään tiettyihin kohteisiin, mutta voitaisiin sanoa, että se käsittää kaiken käyttäjän ja palvelimen väliltä sekä näiden ympäriltä. Maailman digitalisoituessa riskitekijöidenkin määrä on lisääntynyt. Seuraavissa luvuissa käsitellään yleisimpiä digitaalisen tietoturvan riskejä yrityksille.

4.1 Tietomurto

Tietomurto on tekona rangaistava jo sen yrittämisenkin tasolla. Tietomurrossa hyökkääjä hyödyntää jotain heikkoutta järjestelmässä, kuten suojaamatonta tai huonosti suojattua langatonta verkkoa, päästäkseen sisälle järjestelmiin. Murto voi tapahtua myös hyödyntämällä hyökkääjälle kuulumatonta käyttäjätunnusta ja salasanaa.

Hyökkääjä voi viedä arkaluontoista tietoa kuten henkilötunnuksia tai maksukorttitietoja. Luonnollisesti arkaluontoisten tietojen vuotaessa yrityksen mainekin kärsii. Hyökkääjän tavoitteena voikin olla vain kohteena olevan yrityksen imagon tahriminen.

Onnistunutta hyökkäystä on todella vaikea huomata ja pahimmillaan voi mennä vuosiakin. Toisinaan hyökkäys voi jäädä kokonaan huomaamattakin. Hyviä esimerkkejä pitkään huomaamatta olleista tietomurroista ovat Yahoon! tietomurrot, jotka tapahtuivat vuosina 2013 ja 2014. Kyseisissä murroissa vietiin yli miljardin käyttäjän tiedot ja asiasta tiedotettiin vasta joulukuussa 2016. (Trend Micro n.d; Viestintäviraston www-sivut 2016.)

4.2 Pilvipalveluiden riskit

Pilvipalveluita käytettäessä vastaan tulee useampikin riskitekijä. Pk-yritykset helposti kuvittelevat työntävänsä tietoturvaongelmansa suuremman yrityksen hoidettavaksi, kuitenkaan ottamatta huomioon kohteena olemisen riskin kasvua. Isommat yritykset, jotka pilvipalveluita tarjoavat ovat hyökkääjille haukuttelevampia kohteita kuin pienemmät yritykset. Näin siirtämällä tietonsa pilvipalveluun säilytettäväksi asettaa yritys tietonsa helposti huomaamattaan suuremmalla todennäköisyydellä hyökkäyksen kohteeksi.

Pilvipalvelun tarjoajaa valittaessa tulisi tutustua palvelun sopimuksiin, palvelinten sijaintiin ja kyseessä olevan maan lakeihin. Joissain aiemmissa tapauksissa valtioiden lakien ja asettamien säädösten takia on vuotanut yritysten salaista tietoa esimerkiksi,

kun rikoksen tutkinnan aikana palvelun tarjoaja on joutunut luovuttamaan hallussaan olevia tietoja.

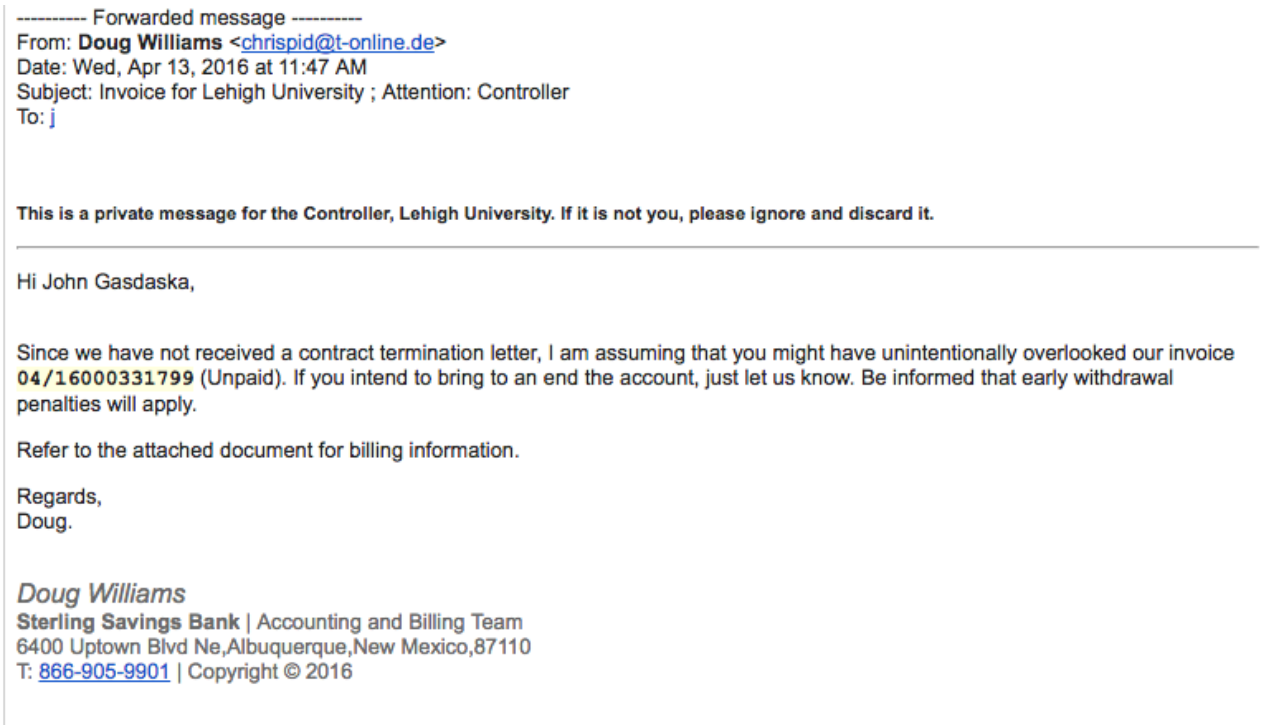
Pilvipalveluita käytettäessä on oltavana tarkkana sen suhteen, mitä pilvessä kannattaa säilyttää. Palveluissa voi tapahtua katkoksia, jolloin siellä olevat tiedot jäävät yrityksen saavuttamattomiin hetkellisesti. Tällainen katkos voi pitkittyessä tulla todella kalliiksi, jos pilvipalvelussa säilytettään toiminnalle kriittistä tietoa. Yrityksen tietoturvaa arvioitaessa tässäkin kohtaa voitaisiin hyödyntää jo aiemmin mainittua CIA-kolmiota. (Calyptix 2016; Bhattacharya 2017.)

4.3 Phishing

Yksi yleisimmistä tavoista, joilla kyberrikolliset yrittävät päästä sisään yrityksen järjestelmiin on phishing. Phishingillä tarkoitetaan esimerkiksi sähköposteja, kuten kuvan 2 esimerkki, jotka näyttävät luotettavilta mutta klikkaamalla liittettä saakin tartunnan. Haitallinen tiedosto on voitu naamioida näyttämään PDF-dokumentilta tai muulta tavanomaiselta tiedostolta. Phishing viestissä voi sisältää linkin verkkosivulle, jotka näyttävät alkuperäisen kaltaisilta, mutta käyttäjän syöttäessä tunnuksiaan ne lähetetäänkin kyberrikollisen laitteelle.

Useimmin phishing-yritykset on helppo tunnistaa huonosta englannin kielestä tai heikosta käännöksestä suomen kielelle. Lauseenrakenteet ovat erikoisia ja saattavat sisältää kohteesta jo kerättyä tietoa, kuten kaupungin tai nimen.

Phishingistä on olemassa myös henkilökohtaisempi versio spear phishing. Spear phishingissä hyökkääjä räätälöi huijausviestinsä kohteen mukaan. Hyökkääjä kerää tietoa kohteesta esimerkiksi sosiaalisten medioiden avulla ja kykenee luomaan hyvinkin vakuuttavan näköisiä viestejä, tiedostoja ja linkkejä. Näitä viestejä onkin jo huomattavasti vaikeampi erottaa. (Microsoft n.d; Trend Micro 2015.)



---------- Forwarded message ----------
From: **Doug Williams** <chrispid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: j

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

Hi John Gasdaska,

Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice **04/16000331799** (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

Refer to the attached document for billing information.

Regards,
Doug.

Doug Williams
Sterling Savings Bank | Accounting and Billing Team
6400 Uptown Blvd Ne,Albuquerque,New Mexico,87110
T: 866-905-9901 | Copyright © 2016

Kuva 2. Esimerkki phishing-viestistä. (Lehigh yliopiston www-sivut 2016.)

Useimmiten phishingiä yritetään sähköpostin välityksellä, joten työntekijöiden kouluttaminen ja phishingistä kertominen on erityisen tärkeää. Kehotus tarkastaa aina linkkien ja lähettäjien osoitteet ovat hyvä perusta hyökkäyksiä vastaan. Monissa palveluissa kuten Office365 ja Lotus Notes on olemassa suojaus phishing-hyökkäyksiä vastaan, joka voidaan ottaa käyttöön. Tällaisessa niin kutsutussa Anti-phishing suojauksessa administraattori luo säännöt, joiden pohjalta algoritmi tarkistaa saapuvat viestit ja suorittaa sääntöjen mukaiset määritellyt toimenpiteet. Anti-phishingissä hyödynnetään myös koneoppimista, joten järjestelmä kehittyy koko ajan sen käytössä ollessa. (TechTarget n.d.; Microsoftin officen www-sivut n.d.)

4.4 DDoS

DDoS eli distributed denial of service on hyökkäys, joka tapahtuu massiivisella määrällä kyselyitä palvelimelle. Tavoitteena hyökkääjällä on kaataa kohteen järjestelmä ja näin häiritä yrityksen toimintaa. DDoS-hyökkäyksillä useimmiten tavoitellaan kilpai-

luetua, poliittista tai rahallista hyötyä. DDoS-hyökkäyksen suorittamiseen ei aina tarvita edes tietoa tai taitoa sen toteuttamisesta. On olemassa verkkosivuja, joilla myydään todella laajoja ja tehokkaita DDoS-hyökkäyksiä.

Hyvin toteutetuilta hyökkäyksiltä voi olla hyvinkin vaikeaa suojautua, sillä normaalit protokollat näkevät liikenteen tavanomaisena. Näin ollen yrityksen tietohallinto ei voi vain yksinkertaisesti estää DDoS-hyökkäyksissä käytettäviä väyliä. DDoS-hyökkäyksiltä suojautumisen tekee hankalaksi myös niiden tapa mukautua hyökkäyksen tapahtuessa. Tavallisista kotikäyttöön tarkoitetuista reitittimistäkin löytyy lähes kaikista suojaus yksinkertaisia DDoS-hyökkäyksiä varten. (Cisco n.d; Cisco www-sivut n.d.)

4.5 Bring your own device mallin riskit

Bring your own device, eli BYOD, tuo mukanaan useamman vaikeasti hallittan riskin. Suurin osa näistä riskeistä johtuu käyttäjän tietämättömyydestä sekä varomattomuudesta. Esimerkiksi kotiverkossaan työntekijä voi käydä tietoturvalle vaarallisilla sivuilla tai ladata tiedostoja, jotka sisältävät haittaohjelmia. Kun työntekijä tuo koneensa takaisin työpaikalle ja liittää sen verkkoon saattaa koneella oleva haittaohjelma hyökätä työpaikan verkon välityksellä muihin verkossa oleviin tietokoneisiin. Esimerkin kaltaisissa tilanteissa tietoturvasta huolehtiminen jää pitkälti työtekijän murheeksi, sillä tietohallinnon työkalut voivat loppuvat kesken yrityksen verkosta poistuttaessa ja käytettäessä työtekijän omaa tietokonetta. Puhelimien päivityskin on työntekijän vastuulla. Päivittämättömänä laitteen suojaus voi sisältää heikkouksia uusia haittaohjelmia vastaan.

Suurin haaste yrityksille on tietysti laitteilla olevan yrityksen omistaman tiedon hallinta. Työntekijän laitteista on vaikea yrityksen puolelta huolehtia, kun ei aina päästä asentamaan laitteelle yrityksen käyttämiä hallinta ohjelmistoja tai virusturvaa. Työpaikan ulkopuolella kulkevat laitteet aiheuttavat myös tietoturvariskin. Kannettava tietokone tai puhelin voidaan helposti varastaa tai laitteen auki ollessa voidaan luvattomasti koneella tai näytöllä olevia tietoja selata. Varomaton käyttäjä voi liittyä avoimeen WLAN-verkkoon, joka altistaa laitteen hyökkäyksille. Kotonakin koneeseen saattaa

epähuomiossa lapsi päästä käsiksi, joka toiminnallaan aiheuttaa laitteelle tietoturvariskin. Toisinaan riskit voivat johtua vahingoista kuten yrityksen tietojen poistaminen tai laitteen tuhoaminen kaatamalla päälle nesteitä tai tiputtamalla laitteen. (Hoelscher 2017.)

BYOD-laitteella oleva yrityksen data on arvokasta ja siksi olisi tärkeä järjestää varotoimia esimerkiksi laitteen katoamisen varalle. MDM eli Mobile Device Management-ohjelmilla voidaan hallita yrityksen työntekijöiden laitteita ja niillä olevaa dataa. Kadonneet laitteet voidaan paikantaa tai lukita niiden kadotessa. Jos kannettavalla tietokoneella tai puhelimella on yritykselle arvokasta tai salaista dataa, päästään laitteella olevat tiedot tuhoamaan etänä. Näiden toiminnallisuuksien heikkoutena on niiden verkon tarve. Jotta etähallinnan toimintoja voidaan hyödyntää, täytyy laitteeseen saada yhteys muodostettua. Yrityksellä olisi hyvä olla voimassa jonkin asteen NAC, eli Network Access Control, ratkaisu. NAC ohjelmilla taas voidaan hallita laitteiden ja käyttäjien oikeuksia dataan. Tiukimmillaan sääntöjen avulla NAC:lla voidaan täysin estää käyttäjien pääsy tietoihin, jotka heille eivät kuulu. NAC:lla voidaan myös rajata oikeudet kellonajan tai laitteen sijainnin mukaan. (Hoelscher 2017.)

4.6 Sosiaalisen median riskit

Nyky-yhteiskunnassa lähes jokaisella henkilöllä tai yrityksellä on jokin sosiaalinen media käytössään. Se voi olla todella tehokas työkalu yrityksen toiminnan kehittämiselle, mutta on samalla tuonut mukanaan riskejä. Julkisilla henkilökohtaisilla tileillään yrityksen työntekijät saattavat huomaamattaan jakaa tietoa, joka ei ulkopuolisille kuuluisi. Julkiset tilit ovat myös täydellisiä paikkoja ulkopuolisille hyökkääjille kerätä tietoja, joita he voivat myöhemmin hyödyntää aiemmin mainituissa phishing ja spear phishing-hyökkäyksissä. Hyökkääjä voi hyödyntää clickjacking-nimistä tekniikkaa, jossa esimerkiksi Facebookissa tehdyssä päivityksessä käyttäjä houkutellaan avaamaan häntä kiinnostavan videon linkki. Linkin auettua play-näppäintä painettaessa käyttäjä painaakin vahingossa näkymätöntä latausnäppäintä ja saa laiteelleen tartunnan. Sosiaalisessa mediassa hyökkäyksillä voidaan myös pyrkiä vaikuttamaan yrityksen imagoon väärennettyjen huonojen arvostelujen ja palautteiden avulla. (Shakeel 2012; Cooper 2017.)

Sosiaalisen median aiheuttamilta uhkilta on yrityksen vaikea suojautua, sillä ne ovat lähes kokonaan riippuvaisia käyttäjien toiminnasta. Yritys voisi luoda tiukat säännöt sosiaalisten medioiden käyttöön ja estää niiden toiminta täysin työpaikalla. Pahimmillaan tämä johtaisi vain työntekijöiden tyytymättömyyteen ja he käyttäisivät aikansa estojen kiertämiseen. Jatkuva työtekijöiden sosiaalisten medioiden tilien tarkkailulla saataisiin myös huonoa tulosta aikaiseksi. Tehokkain tapa välttyä uhalta on kouluttaminen ja tiedottaminen. Työntekijöille tulee tehdä selväksi mahdolliset riskit sekä uhat ja miten niiltä suojaudutaan. Yrityksen linjaus siihen liittyvistä asioista, joita saa julkaista sosiaalisessa mediassa, tulee myös tehdä selväksi. (Shakeel 2012; Cooper 2017.)

Nykyisin on hyviä esimerkkejä todistetuista ryhmistä, jotka toiminnallaan vaikuttavat yrityksen tai valtion toimintaan/ imagoon. Joskus ”Trolli farmiksikin” kutsutuilla tahoilla tarkoitetaan ryhmiä, jotka hallinnoivat automatisoimalla jopa tuhansia sosiaalisen median tilejä ja ajavat omaa agendaansa. Ehkä merkittävimpänä tapauksena mainittakoon Venäjän IRA, eli Internet Research Agency, joka pyrki Venäjän presidentin Vladimir Putinin käskystä vaikuttamaan Amerikan presidentin vaaleihin vuonna 2016. Twitterin ylläpito on onnistunutkin löytämään ainakin 3843 eri Twitter-tiliä, jotka kaikki oletettavasti kuuluivat IRA:lle. (Twitterin tutkimus 2019.)

4.7 Käyttäjän toiminnan riskit

Kuten aiemmissa kohdissa huomattiin, käyttäjällä on suuri vaikutus yrityksen tietoturvaan. Käyttäjää usein pidetäänkin suurimpana uhkana juurikin inhimillisyyden takia. Työntekijä saattaa esimerkiksi turhautua yritykseen muiden työntekijöiden menestyksen takia, jolloin hänestä voi tulla huolimattomampi tai pahimmassa tapauksessa hän voi tahallaan vahingoittaa yritystä. IBM:n tekemän vuoden 2016 Cyber Security Intelligence Indexin mukaan 60 prosenttia kaikista hyökkäyksistä yrityksiä kohtaan oli sisäisiä. Näistä neljäsosa oli tahattomia ja kolme neljäsosaa tahallisia. Tahattomien osuutta suuresti edustavat tietohallinnon henkilöt, jotka hyväntahtoisesti tekevät poikkeuksia ja näin asettavat yrityksen tietoturvan vaaraan. (Chowdhury 2008; Van Zadelhoff 2016.)

Käyttäjien aiheuttamien riskien minimoiminen voi olla hankalaa, sillä muuttujia on todella paljon. Joissakin yrityksissä on kokeiltu ns. Zero Trust -toteutusta, jossa oletetaan kaiken liikenteen olevan vaarallista ja niiden vaativan verifiointia. Ongelmaksi nousivat kustannukset, heikko suorituskyky sekä käyttäjien turhautuminen. Tärkeää käyttäjien aiheuttamilta riskeiltä suojautuessa on tiedottaminen heihin kohdistuvista vaaroista ja kouluttaminen, jotta suojautumiseen tarvittavat taidot ovat ajan tasalla. Yrityksistä usein löytyy todella laaja kirjo eritasoista tietoturvatietämystä. Opettamalla käyttäjille oikeat toimintamallit ja terävöittämällä mahdollisten virheellisten toimien vaikutuksen yrityksen toiminnalle tehostavat käyttäjien aktiivista oman toimintansa tarkastelua. Yrityksissä tietoturvaan voidaan myös parantaa kartoittamalla potentiaalisesti riskialttiimmat henkilöt ja tarkkailemalla tarkemmin heidän oikeuksiaan ja toimiaan. (Tuulinen 2017.)

5 FYYSISEN TIETOTURVAN UHISTA TARKEMMIN

Puhuttaessa fyysisestä tietoturvasta tarkoitetaan kaikkia mahdollisia fyysisiä uhkia, jotka saattaisivat vaikuttaa tai uhata yrityksen tietojärjestelmien toimintaa. Se kattaa niin tietojen säilytyksen kuin laitetilojen ja laitteiden suojaamisen. Tärkeintä fyysisessä tietoturvassa, niin kuin digitaalisessakin, on jatkuvasti tarkkailla ja parannella järjestelmää.

5.1 Datan säilytys

Kun tietoa viedään ulkoiselle medialle säilytettäväksi, on olennaista miettiä mitä on järkevä säilyttää. Mitkä tiedot voidaan myöhemmin hyödyntää tai ovat yritykselle rahanarvoisia tietoa. Säilytettäväksi valikoituu usein asiakkaiden ja kumppaneiden tiedot sopimuksineen.

Kaikki toiminnalle kriittinen data tulisi kryptata, kopioida ja säilyttää useammassa kuin yhdessä paikassa. Jos tärkeä tieto halutaan pois digitaaliselta medialta suojaan

hyökkäyksiltä, voidaan tiedot säilöä esimerkiksi nauha-asemien avulla kaseteille, polttaa cd:lle tai kirjoittaa usb-kovalevylle. Kun data on tallella sopivassa tallennusmediassa, ne säilötään turvallisesti esimerkiksi kassakaappiin. Tallennusmedioiden selkeä merkintä päivänmäärien sekä sisällön mukaan on myös erittäin tärkeää myöhemmän käytettävyyden kannalta. Viemällä data ulkoiselle tallennusmedialle mahdollistetaan myös sen hyödyntämistä tilanteissa, joissa ei ole pääsyä työpaikalla sijaitseviin verkkolevyihin. (Lonoff Schiff 2013.)

5.2 Laitteiden suojaus

Varkaus on suurin uhka laitteiden fyysiselle tietoturvalle. Laitteistoa ei ole myöskään helppo turvata hankaloittamatta käyttäjän toimintaa. Älypuhelimet löytyvät nykypäivänä lähes jokaiselta työntekijältä ja monet käyttävätkin puhelintaan työasioiden hoitamiseen. Puhelimiin ei ole vielä kovinkaan paljoa apua turvallisuuden puolella. Paras suoja on käyttäjän tarkkaavaisuus ja varovaisuus. On tietysti työntekijän vastuu huolehtia hänelle tarjotuista laitteista. Tarvittaessa puhelimiin voidaan asentaa GPS-jäljittimiä, joiden avulla voidaan jäljitettävää laitetta seurata toiselta laitteelta, vaikka seurattava laite olisikin pois päältä.

Laitteet tulee suojata fyysisien vahinkojen varalta. Kunnollinen suojakuori auttaa suojaamaan puhelinta iskuilta sekä tippumisilta. Näyttöihin voidaan asentaa tietosuoja kalvoja, joiden avulla estetään niin kutsutut shoulder surfaajat. Shoulder surfaajilla tarkoitetaan henkilöitä, jotka pyrkivät selän takaa seuraamaan käyttäjän toimintaa ja selvittämään pin-koodeja, salasanoja tai lukemaan näytöllä olevia tietoja. Kannettaviin tietokoneisiin on mahdollista kiinnittää myös lukkoja, joilla laitteet voidaan kiinnittää esimerkiksi messuilla pöytään.

5.3 Toimitiloihin kohdistuvat uhat

Toimitiloihin kohdistuu monenlaisia uhkia, kuten luonnonvoimat, varkaus ja tahallinen vahingonteko. Konesalien kanssa täytyy olla tarkkana suunniteltaessa paloturvallisuutta ja vesipisteitä. Sammutuslaitteiston tulisi olla soveltuva konesalien kanssa käytettäväksi. Hiilidioksidi sammuttimet eivät tuhoa laitteistoa kuten vettä käyttävät

versiot. Jauhesammuttimet voivat puolestaan aiheuttaa korroosiota jauheen reagoidessa kosteuden kanssa. Taas kerran on erittäin tärkeää tiedottaa henkilökuntaa tarvittavista toimenpiteistä.

Vesi ja laitteisto ovat selvästikin huono yhdistelmä, joten vesiliitäntöjä konesaliin tulisi välttää. Ilmastointilaitteet saattavat rikkoutua ja mahdolliseen kondenssiveden valumiseen täytyy varautua. Luonnonvoimista johtuvien sähkökatkosten varalle asennetaan varavirtageneraattoreita tai UPS-järjestelmiä. UPS eli uninterruptible power supply, on akkujärjestelmä, joka mahdollistaa katkeamattoman toiminnan niin kauan, kun varausta riittää. (Virgillito 2014; Laakso, M. n.d.)

Varkautta ja tahallista vahingontekoa vastaan suojaudutaan ensi kädessä kulunhallinnalla. Perinteisten lukkojen lisäksi voidaan asentaa sähköinen kulunvalvontajärjestelmä, jolla voidaan hallita yksittäisten henkilöiden kulkuoikeuksia. Tärkeimmät tilat voidaan suojata näppäinpaneeleilla tai biometrisillä lukoilla kuten sormenjälki- tai iirisskannerit. Toimitiloihin ja alueelle on hyvä asentaa videovalvontajärjestelemä, jotta mahdollisia rikoksia on helpompi estää ja selvittää. (Virgillito 2014; Laakso, M. n.d.)

5.4 Käyttäjän manipulointi

Yksinkertaisimmillaan käyttäjän manipulointi voi olla vain yksittäinen puhelu tai käynti toimipisteellä, jossa hyökkääjä esittää luotettavaa tahoa ja pelkästään kysymällä saa selville haluamansa tiedon hyväksikäyttäen kohteen ystävällisyyttä. Hyökkääjä voi myös käyttää hyväkseen työntekijöiden uteliaisuutta jättäen esimerkiksi houkuttelevalla tekstillä merkityn USB-tikun yrityksen tiloihin. Kun joku yrityksen henkilöstöstä päättää tutkia tikun sisältöä, tikulla oleva haittaohjelma aktivoituu ja hyökkääjällä on yhteys yrityksen järjestelmään. (Infosecinstitute 2013; Norton n.d.)

6 YRITYKSEN NYKYTILANTEEN TARKISTAMINEN

Olennaista yrityksen tietoturvan päivittämisessä on nykytilanteen kartoittaminen. On tärkeää luoda kattava kuvaus yrityksen ympäristön rakenteesta, sovelluksista sekä laitteista, jotta tietoturvan päivittämiselle voidaan laatia toimiva suunnitelma ja toteutus.

Tietoturva tarkistusta voidaankin kuvata auditoimiseksi. Auditointia tehdessä on mietittävä sen toteuttavaa tahoa. Hankkeeseen voidaan valita tekijät yrityksen sisältä tai hyödyntää ulkopuolista konsulttia. Pieniltä sekä keskisuurilta yrityksiltä harvoin kuitenkaan löytyy tehtävään sopivaa henkilöä tai ryhmää sisältä, joilta löytyisi riittävät tiedot ja taidot auditoinnin toteutukselle. Monesti objektiivisimman ja tarkimman toteutuksen saakin aikaan ulkopuolinen konsultti. Ulkopuolisella konsulteilla on valmiit paketit, joista löytyvät mukautettavat suunnitelmat sekä työkalut auditoinnin toteutukselle. Konsultin mukanaan tuoma kokemus aiemmista projekteista mahdollistaa nopean ja tehokkaan toteutuksen.

6.1 Auditoinnin toteutus

Kun auditoinnin tekevä taho on päätetty, on aika suorittaa itse auditointi. Auditoinnille on olemassa oma ISO/IEC 27006:2015 standardi, joka määrittää vaatimukset valtuutetuille virallisille tietotekniikan auditointeja suorittaville tahoille. Tätä standardia voi kuitenkin hyödyntää myös sisäisesti suoritettavissa auditoinneissa, sillä se sisältää ohjeistuksia ja kuvaajia auditoinnin suorittamiselle. Tosin sisäisesti toteutettuna auditoinnista ei ole mahdollista saada virallista ISO merkintää, vaikka se olisikin suoritettu standardin mukaisesti. (ISO:n www-sivut 2015.)

Sisäisesti suoritettavassa auditoinnissa kannattaa hyödyntää jotain verkostakin löytyvää tarkistuslistaa. Listat ovat laajoja ja usein sisältävät kohtia, jotka eivät toteutusta suunnitellessa tule välttämättä mieleen. Alla olevassa kuvassa esitetty esimerkki sivu auditoinnissa hyödynnettävästä tarkistuslistasta on osa neljäkymmentäkolme sivua pitkää dokumenttia. Dokumentti käsittelee laajasti niin digitaalista kuin fyysistä tietoturvaa. (Thiagarajan V. 2015.)

Information Security Management BS ISO IEC 17799:2005 SANS Audit Check List					
Reference		**Audit area, objective and question**		**Results**	
Checklist	**Standard**	**Section**	**Audit Question**	**Findings**	**Compliance**
2.1.3	6.1.3	**Allocation of information security responsibilities**	Whether responsibilities for the protection of individual assets, and for carrying out specific security processes, were clearly identified and defined.		
2.1.4	6.1.4	**Authorization process for information processing facilities**	Whether management authorization process is defined and implemented for any new information processing facility within the organization.		
2.1.5	6.1.5	**Confidentiality agreements**	Whether the organization's need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed. Does this address the requirement to protect the confidential information using legal enforceable terms		
2.1.6	6.1.6	**Contact with authorities**	Whether there exists a procedure that describes when, and by whom: relevant authorities such as Law enforcement, fire department etc., should be contacted, and how the incident should be reported.		
2.1.7	6.1.7	**Contact with special interest**	Whether appropriate contacts with special interest groups or other specialist security forums, and professional associations are maintained.		

Kuva 3. Esimerkki sivu auditoinnissa hyödynnettävästä tarkistuslistasta. (Thiagarajan V. 2015.)

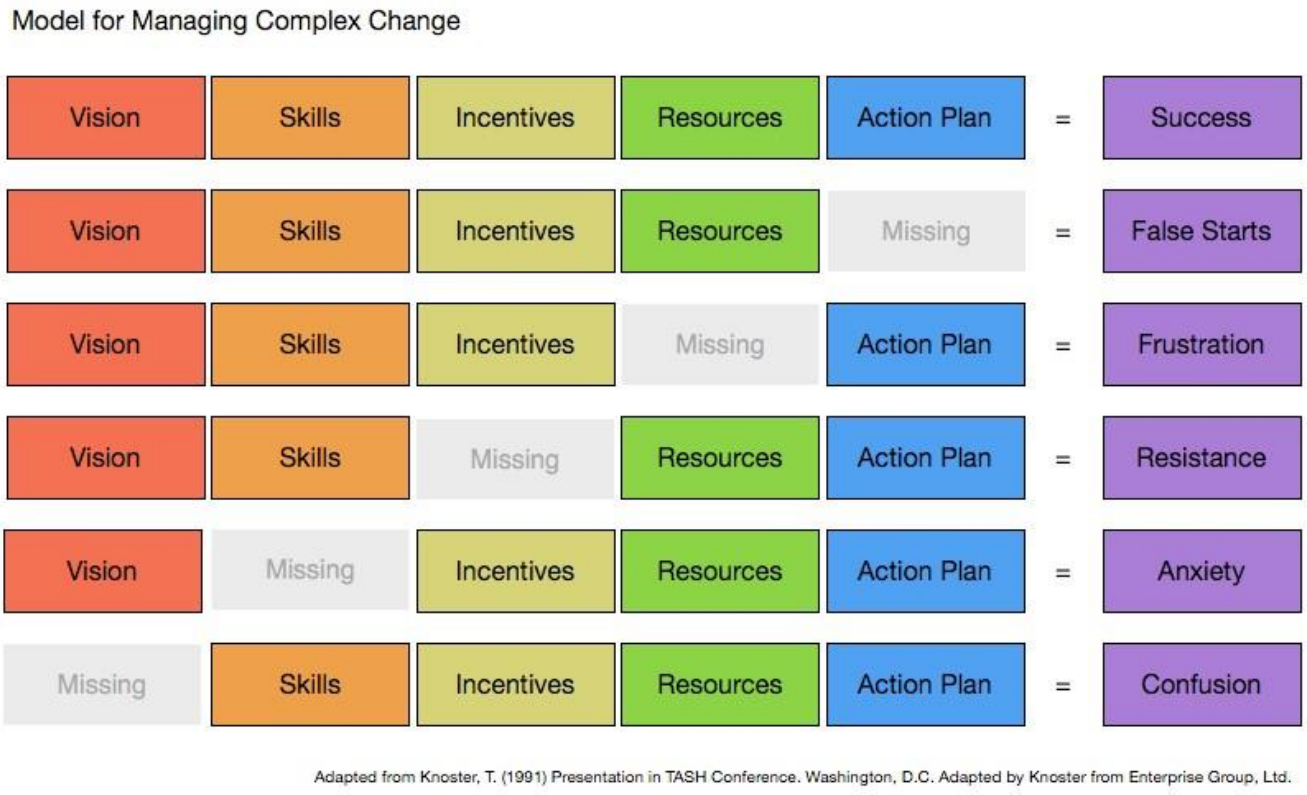
Ulkopuoliselta taholta tilattaessa monesti yritykselle tarjotaan valmista pakettia. Paketti voi sisältää jatko- ja seuranta suunnitelmat, joiden lisäksi keskitytään hallinnan kehittämiseen. Auditoinnissa yritykseen luodaan monitasoinen organisaatioon ja toimialaan pohjautuva tutkimus, joka ottaa huomioon kaikki alakohtaiset vaatimukset. Auditoinnin laajuus on kuitenkin täysin sovittavissa ja halutessaan yritys voi hyödyntää vain tietyissä osissa organisaatiossa ulkopuolisen palveluita. Ulkopuoliselta palvelua ostettaessa ei myöskään tarvitse varoa tilannetta, jossa auditoija tutkisi omaa työtään.

7 YRITYKSEN TIETOTURVAN PÄIVITTÄMINEN

Tärkeintä yrityksen tietoturvan päivittämisen kaltaisessa projektissa on yrityksen johdon oikea tahtotila. Heiltä tulee löytyä valmius hoitaa projekti loppuun asti ja tiedostaa päivityksestä aiheutuvat kulut. Ilman yhteisymmärrystä projektin luonteesta sekä laajuudesta, jää toteutus vajaaksi ja menetetään hyvän pohjatyön tarjoamat mahdollisuudet turvallisuuden edistämiseksi. Päivitys projektista saadaan toimiva kokonaisuus perustamalla projektille oma johtoryhmä. Yrityksen koosta riippuen johtoryhmä koostuu muutamista henkilöistä, jotka valitaan yrityksenjohdosta, henkilöstöhallinnosta, bisnesyksiköistä, it-osastolta ja projektiin olennaisesti kuuluvien prosessien edustajista.

Nykytilanteen selvityksen jälkeen analysoidaan tietoturvan päivityksen hinta sekä siitä saatavat hyödyt. Päivityksen hinta muodostuu projektin laajuudesta ja siihen käytettävästä ajasta. Päivityksen tekemiseen ja sen hallintaan käytetyt työtunnit ovat pois normaaleista toiminnoista ja tätä kautta nostavat kustannuksia. Kun projektia laajennetaan käsittelemään useampia osa-alueita yrityksessä, myös kesto pitenee ja hankkeeseen kuluu enemmän työtunteja. Hintaan vaikuttaa myös mahdollisten ulkopuolisten toimijoiden hyödyntäminen.

Päivityksestä saatavat hyödyt on vaikea konkreettisesti esittää. Hyötyjä voidaan mallintaa toteutuksen johdosta vältettyjen mahdollisten tietomurtojen avulla, tekemällä kustannusarvio tietomurron aiheuttamista kuluista. Kustannusarviota tehtäessä voidaan hyödyntää aiempien murtojen aiheuttamia kuluja tai verrata muiden samankokoisten yritysten murroista aiheutuneisiin kuluihin. Päivityksen tulisi luonnollisesti säästää yrityksen varoja estettyjen hyökkäysten ja tietovuotojen muodossa. (Kauppakamarin www-sivut 2016; Massachusettsin tietoturva www-sivut n.d.)



Kuva 4. Knoster, T. esityksessään käyttämä kuvaaja muutoksen kompleksisuudesta. (LearningAccelerator www-sivut n.d.)

Knoster T. käyttämä kuva on todella hyvä apu jokaiseen projektiin. Tietoturvan päivittämisen kaltaisissa hankkeissa muutokset voivat olla hyvin suuria ja vaikeasti hallittavia. Käymällä kuvan kohdat läpi ja varmistamalla että projektin kokonaisuudesta löytyy jokainen kuvan elementeistä, vältytään yleisimmiltä epäonnistumisilta.

Kun tietoturvaa lähdetään päivittämään, on ehdottoman tärkeää luoda projektille toimintasuunnitelma. Toimintasuunnitelman puuttuessa projekti lähtee helposti heti toteutuksen alussa väärille raiteille. Projektin laajuus sekä aihealueet alkavat rönsyillä ja tekijät ajautuvat keskittymään projektin etenemisen kannalta epäolennaisiin osioihin. Projektia on myös hyvin vaikea kontrolloida, kun ei ole mitään konkreettista suunnitelmaa seurattavana. Lopettaminen muodostuu myös nopeasti ongelmaksi, jos ei ole määritetty mitään lopullista tavoitetta tai aikamäärettä.

Tietoturvan päivittämistä suunnitellessa on hyvä tarkistaa, että toteutukseen löytyy tarvittavat resurssit. Onko henkilöstöllä tarvittavat työkalut ja aika hankkeeseen lähtemiseen? Löytyvätkö tarvittavat tiedot ja taidot yrityksen sisältä jo nyt, vai tarvitseeko työ ulkoistaa? Resurssien puuttuminen aiheuttaa tekijöille turhautumista ja kuormittaa muutakin toimintaa, kun projekti ei etene.

Projektiin lähtemiselle tarvitsee löytyä myös riittävän hyvät perustelut sekä syyt. On vaikea vakuuttaa ja vaatia henkilökunnalta tai asiakkailta suuriakin muutoksia toimintatapoihin, jos niille ei ole järkeviä perusteluja. Tässä avuksi voidaan ottaa lukuisat esimerkit muista tietomurron kohteeksi joutuneista yrityksistä ja niistä aiheutuneista kuluista. Konkreettisesti näyttämällä ja kertomalla mahdollisista omassa yrityksessä piilevistä tietoturva riskeistä, pystytään tuomaan käsitys uhan todellisuudesta lähemmäs henkilöstöä.

Tietoturvan päivittämisen toteuttaminen vaatii tietysti projektin vaatimusten mukaisia taitoja. Näiden puuttuessa aiheutuu projektin tekijöille helposti vältettävää ahdistusta sekä turhautumista. Työt alkavat kasautua ja valmistuneet toteutukset ovat lopputulokseltaan riittämättömiä, kun tekijöiltä ei löydy heille asetettujen tehtävien vaatimaa taito tasoa. Pahimmillaan taitojen puuttuessa ongelmien ratkaisemiseksi suoritetut toimenpiteet aiheuttavat vain lisää riskejä ja puutteita tietoturvassa. Tarvittaessa yrityksen puutteita tällä saralla voidaan paikata ulkoistamalla toteutus.

Tietysti onnistuneeseen projektiin tarvitaan näkemystä siitä, mitä hankkeessa oikeasti lähdetään tekemään. Epäselvät tai epärealistiset tavoitteet ja perustelut johtavat helposti sekaannuksiin projektin toteutuksessa. On mahdotonta luoda toimivaa suunnitelmaa toteutukselle tai tehdä hyvää ja perusteellista jälkeä, kun ei tiedä mitä oikeastaan tavoitellaan.

7.1 Suunnitelman luominen tietoturvan päivittämiseksi

Nykytilanteen tarkistamisen jälkeen keskitytään tietoturvan päivittämisen suunnitelman luomiseen. Suunnitelman tekeminen on hyvä aloittaa käymällä läpi tarkistuksessa luotu lista. Listasta poimitaan kaikki tapaukset ja kohdat, joissa on löydetty riskejä tai

heikkouksia. Listaa läpikäydessä täytyy jokaisen löydetyn ongelman kohdalla punnita hyötyjen ja haittojen suhdetta. Saadaanko riskin hallintaan panostetulle työlle riittävästi vastinetta? vai onko kyseessä niin sanottu hyväksyttävä riski? Kustannuksien ja kannattavuuden arvioinnin lisäksi analysoidaan riskien vakavuus. Analysoinnissa apuna voidaan käyttää uhka matriisia. Suurimmat uhat kannattaa käsitellä ensin ja matriisin avulla laajuus on helpompi rajata, kun voidaan verrata eri uhkien vakavuutta. Näille tapauksille selvitetään ratkaisut tai korjaukset. (Konstadinv, D. 2019; Kevin B. 2016.)

Kun kaikki kohdat on käyty läpi ja toimenpiteet selvillä. Laaditaan aikataulu niiden toteuttamiselle. Toimenpiteiden toteuttamiselle ei ole suotavaa asettaa turhan pitkiä aikavälejä. Tällöin pystytään pitämään aihe toteutusten tekijöiden mielessä ja minimoimaan inhimillisten virheiden syntyminen. Samalla päästää minimoimaan turha kustannuksien kasvu. Toimenpiteille määritetään vastuuhenkilöt, jotta ongelmien ratkaisujen implementointi on varmempaa. Asettamalla vastuuhenkilöt voidaan myös seurata toteutuksen valmistumista ja aikataulua paremmin, kun on henkilö jolta asiasta voi tiedustella. (Kevin B. 2016.)

7.2 General Data Protection Regulation

General data protection regulation (GDPR), eli Euroopan unionin tietosuoja-asetus on astunut voimaan toukokuussa 2018. Asetuksella suojataan EU:n kansalaisten oikeuksia tietojensa käsittelyssä sekä suojauksessa. Samalla taataan tietojen reilu ja vastuullinen hyödyntäminen. (ICO:n www-sivut n.d.; Tietosuojamallin www-sivut 2017)

Vastuu tietosuoja-asetuksen toteutumisesta on yrityksillä ja organisaatioilla. Asetuksen toteutumisen tarkistamiselle ei ole olemassa yhtä tiettyä ratkaisua, koska jokainen yritys on erilainen ja käsiteltävästä tiedosta riippuen asetus pätee eri tavoin. Tarkistuksen avuksi on kuitenkin olemassa lukuisia dokumentteja ja testejä, joiden avulla yrityksessä voidaan toteutuminen todentaa ja tarvittaessa korjata. Tarvittaessa yritykset voivat ulkoistaa tarkistamisen. Ulkopuolinen palveluntarjoaja osaa teetetyn tarkistuksen pohjalta valmistella kaikki tarvittavat toimenpiteet, jotta tietosuoja-asetus toteutuu. Jos yrityksessä ei vielä ole tehty mitään tietosuoja-asetuksen toteutumisen eteen, on

nyt viimeistään aloitettava. Tietoturvan päivittämisen yhteydessä on hyvä mahdollisuus tarkastella yrityksen toimintaa ja käytäntöjä myös GDRP:n toteutumisen kannalta. Iso-Britannian Information Commissioner's Officen eli ICO:n sivuilla on valmiit testit, joiden avulla yrityksen tietosuoja-asetuksen toteutumisen tasoa voi testata. Testin lopuksi saa vastauksiin perustuen konkreettisia toimenpiteitä, joilla epäkohtia voi lähteä ratkaisemaan. Suomessakin on valmisteltu julkisen hallinnon tietohallinnon neuvottelukunnan ja julkisen hallinnon digitaalisen turvallisuuden johtoryhmän, eli JUHTA ja VAHTI, yhteishankkeena verkkosivusto arjentietosuoja.fi. Sivulta löytyy koulutusvideoita ja testejä tietosuoja-asetuksen voimaan astumiseen valmistautumista varten. (ICO:n www-sivut n.d.; Tietosuojamallin www-sivut 2017; Arjentietosuojan www-sivut n.d.)

Tilanteessa, jossa yritys ei ole noudattanut tietosuoja-asetuksen mukaista toimintamallia ja on syyllistynyt rikkeeseen, on rangaistuksena taloudelliset sanktiot. Kovimmillaan sanktiot ovat kymmenissä miljoonissa tai kaksi prosenttia kokonaisliikevaihdosta edeltävältä tilikaudelta, riippuen siitä kumpi summa on suurempi. Taloudellisten tappioiden lisäksi yrityksen imago kärsii ja se voi menettää asiakkaidensa luottamuksen. (Tietosuojamallin www-sivut 2017)

7.3 Tietoturvan päivittämisen toteutus

Tietoturvan päivittämisen toteutus voi olla projektin laajuudesta riippuen hyvin pitkä ja monimutkainen prosessi. Koska tarpeet ja suunnitelmat vaihtelevat suurestikin eri yritysten välillä, on mahdotonta luoda koko hankkeen kattavaa yleisesti pätevää ohjeistusta. Tärkeintä onnistuneen toteutuksen aikaansaamisessa on seurata tarkasti aiemmin valmisteltua suunnitelmaa. Vastuu projektin kasassa pysymisestä on projektille määritetyllä johtoryhmällä. Jotta hallinta ei muutu sekavaksi, on projektille valittava projektipäällikkö, jolla on kokonaisuus kasassa. Näin päätöksen teossa ja seurannassa vältytään ylimääräisiltä sekaannuksilta ja harhautumisilta. (Flaherty, K. 2015.)

Muutoksilta suunnitelmaan ei voida kuitenkaan välttyä, kun projektin edetessä vastaan tulee odottamattomia tilanteita. Aiemmin suunnitellut ratkaisut eivät välttämättä kata

koko ongelmaa, kun toteutuksessa aihetta konkreettisemmin tarkastellaan. Kaikki projektin aikana tehdyt ratkaisut ja muutokset tulee dokumentoida. Riittävän kattavasta dokumentaatiosta saadaan myöhemmin tarvittaessa selville, milloin, mitä ja miten on muutoksia tehty. (Flaherty, K. 2015.)

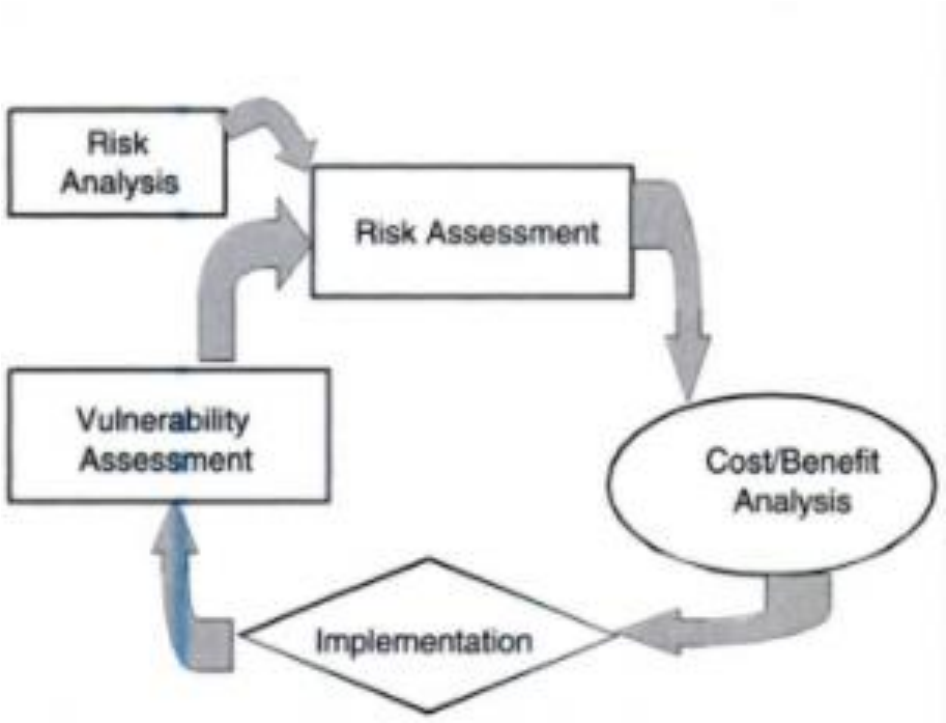
Toteutuksessa voidaan hyödyntää yleisiä projektinhallinta menetelmiä ja työkaluja. Yleisin projektinhallinta menetelmistä on osittaminen. Osittamisessa projekti jaetaan useampiin pienempiin projekteihin ja osiin, jolloin resurssien ja aikataulun asettaminen on huomattavasti helpompaa. Yksinkertaisimmillaan projektipäällikkö onnistuu hallitsemaan koko projekti käyttämällä Microsoftin Excelin taulukoita.

Laajemmat projektit kuitenkin vaativat, tai vähintäänkin helpottuvat, kun avuksi otetaan projektinhallinta ohjelmisto. Käyttämällä ohjelmistoa kuten Microsoft Project saa projektipäällikkö helposti käyttöönsä kaiken tarvittavan tiedon, jonka avulla huolehtia, että projekti sujuu luontevasti. Microsoftin Project tuotteesta löytyy valmiudet projektin kokonaisvaltaiselle hallinnalle ajankäytöstä resursseihin. (Microsoft Project www-sivut n.d.)

Työntekijöiden kouluttaminen vaatii myös oman aikansa ja suunnitelmansa. Kuten aiemmin on todettu, tietoturvaa tutkiessa usein suurimmaksi riskitekijäksi nousee työntekijöiden aiheuttamat riskit. Tämä näkyy auditoinnissa tehdyssä listassakin ja vaativat toimenpiteitä, jotta ongelmat voidaan ratkaista. Työtekijöitä tarvitsee kouluttaa uusiin toimenpiteisiin ja käytäntöihin. Mahdolliset uudistuneet järjestelmät sekä täysin uudet ohjelmistot tulee opettaa niitä käyttäville henkilöille. Koulutukset vaativat paljon resursseja ja ovat kalliita. Kustannukset muodostuvat mahdollisten kouluttajien palkoista sekä työntekijöiden työnsä parista irrottamisesta aiheutuvista tappioista. Aikaa kuluu myös uusien toimintatapojen opettelusta johtuvaan työteon hidastumiseen, mikä taas nostaa kuluja. Uusien ohjelmistojen asentaminen ja mahdollisten muutostöiden tekeminen työntekijöiden laitteisiin voi viedä yrityksen koosta riippuen paljonkin aikaa.

8 PÄIVITYKSEN JÄLKEINEN SEURANTA JA HALLINTA

Uuden järjestelmän käyttöönoton jälkeen on tärkeää tutkia koko järjestelmä uudelleen ja arvioida toteutuvatko asetetut vaatimukset. Käymällä läpi samat kohdat ja listat kuin aiemmin, voidaan varmistua ratkaisuiden pätevyydestä ja tarvittaessa parannella tehtyjä toimenpiteitä. Yrityksillä helposti sudenkuopaksi muodostuu ajatus siitä, että kerran asennettu tai päivitetty tietoturvajärjestelmä riittää. Todellisuudessa ala kehittyy nopeasti ja uusia uhkia syntyy jatkuvasti. Tämän takia tietoturvan ylläpito onkin loputon prosessi.



Kuva 5. Tietoturvan elinkaari (Peltier, T. 2001, 14.)

Peltierin kuvaamassa tietoturvan elinkaaressa on hyvin kuvattu tietoturvan jatkuvuus. Riski analyysin jälkeen löydetyille riskeille tehdään arviointi. Arvioinnissa tutkitaan vaihtoehtoja riskien käsittelylle sekä muutoksien kannattavuutta. Sopivien toimintamenetelmien löydyttyä arvioidaan mahdolliset työstä saatavat hyödyt ja verrataan niitä kustannuksiin. Kun päätös projektin käynnistämisestä on annettu, on aika toteutukselle. Toteutuksen jälkeen taas arvioidaan heikkouksia ja jatkuvuuden kehä on valmis. (Peltier, T. 2001.)

Järjestelmän toimivuutta voidaan myös testata ns. eettisillä hakkereilla. Hakkerit yrittävät tunkeutua järjestelmään samalla paljastaen heikkouksia ympäristössä ja toteutuksissa. Suorittamalla autentikoituja ja autentikoimattomia skannauksia saadaan luotua kattava kuvaus laitteiden tilasta ja mahdollisista paljastuneista heikkouksista. Eettisten hakkereiden käytössä olevat työkalut ovat täysin riippuvaiset siitä, kuinka yritys haluaa heitä testattavan. (ISACA www-sivut 2017.)

8.1 Yritys X:n työntekijöiden haastattelu

Haastattelin yritys x:n kahta työntekijää, jotka ovat mukana hoitamassa kyseisen yrityksen tietoturvaa ohjelmointitöidensä ohella.

Kysymys 1. Mitkä ovat tärkeimmät rutiinit työssäsi tietoturvan saralla?

Haastattelussa tärkeimmiksi rutiineiksi nousivat kyberturvallisuuskeskuksen tiedotteiden seuranta ja käytössä olevien ohjelmien ja ohjelmakirjastojen versiojulkaisujen ja päivitysten seuranta. Ohjelmointi työssään he pohtivat jatkuvasti mahdollisia tietoturvariskejä liittyen työnalla oleviin toiminnollisuuksiin sekä rajapintoihin. Voisiko tämä kyseinen tapa aiheuttaa riskin? Miten tältä vältytään? Nämä ovat yleisiä kysymyksiä, joihin haetaan ratkaisuja. Tärkeää on myös omien taitojensa ja tietojensa ylläpitäminen.

Kysymys 2. Millä tavoin yrityksessä ylläpidetään tietoturvaa?

Haastateltavat kertoivat yrityksessä teknisen ja fyysisen ympäristön olevan jatkuvan valvonnan piirissä. Tämä mahdollistaa automaattiset hälytykset havaituista poikkeamista, seuraa keskitettyjä päivityksiä ja kerää lokeja. Palomuuri pidetään tarkasti ajan tasalla ja avataan vain ja ainoastaan tarvittaessa pääsyä ulkomaailmasta yrityksen ympäristöön. Turhia avauksia vältellään viimeiseen asti, jotta ylimääräisen tietoturvaa heikentävät tekijät jäävät minimiin. Olennaista on kiinnittää huomiota ohjelmistojen konfiguraatioihin ja niiden osuuteen turvallisuuden ylläpitämisessä. Jatkuvan ylläpidon lisäksi yrityksessä on käytössä vuosineljänneksittäiset huoltokatkokset, jolloin tehdään suurempia järjestelmäpäivityksiä.

Tietoturvan hallinnan ytimessä yrityksessä on käyttäjäoikeuksien hallinta; mihin tietoihin kenelläkin pitää olla pääsy ja mihin ei. Haastateltavien mukaan uuden työntekijän aloittaminen, tehtävämuutokset tai työntekijän lähteminen tuottaa useamman työtiketin, jolla päätetään mm. käyttäjätunnukset, etäyhteydet ja toimitilojen sähköiset avaimet.

Haastateltavat kertoivat yrityksessä tehtävän turvattavan tiedon kartoitus säännöllisesti vakiomuotoisella tietosuojamallilla. Kartoitukseen osallistuu yrityksen ylin johto ja siinä eritellään yrityksen tietopääoma, sen käyttötarkoitus ja suojausmenetelmät. Tavoitteena on, ettei yritykseen synny huomaamatta tietoa, jonka suojaus ei ole tiedon luonteen mukaisella tasolla. Erityinen huomio on EU:n tietosuoja-asetuksen (GDPR) henkilötietojen käsittelyn vaatimuksissa.

Kysymys 3. Mikä/mitkä ovat suurimmat riskit yritysten tietoturvalle?

Haastateltavat kertovat suurimman riskin yrityksen tietoturvalle olevan yrityksen työntekijät. Työntekijöitä on suhteellisen helppo huijata ja johtaa harhaan hyvin kohdistetuilla hyökkäyksillä. Moni käyttäjistä ei ole ottanut käyttöön kaksivaiheista tunnistautumista kirjautuessaan, joten suojauksen taso jää heikoksi. Ihmisiin kohdistuvat hyökkäykset ovat monesti paljon tehokkaampia kuin palvelimeen suoraan kohdistuvat hyökkäykset. Tietoturvasta huolehtiminen ja tietoturvariskien tiedostaminen kuuluvat sekä jokaiselle työntekijälle, että yrityksen kanssa asioivalle asiakkaalle.

Työssään ohjelmoinnin parissa haastateltavat mainitsivat riskiksi vahingossa tulleet tietoturvariskit ohjelmoitaessa. Näitä riskejä on erittäin vaikea havaita etukäteen. Tietoturvariskien päätyminen ohjelmaan tapahtuu helposti, jos testaus tai opastus on jäänyt puutteelliseksi.

Kysymys 4. Onko urasi aikana tullut vastaan selkeää hyökkäystä tietoturvaa kohtaan?

Haastateltavien mukaan yrityksen verkkoon yritetään tunkeutua jatkuvasti. Verkossa pyörivät verkkoskannerit etsivät jatkuvasti palveluista avoimia portteja. Hyökkäämi-

nen on helppoa vähäiselläkin osaamisella, kun verkosta saa valmiita hyökkäysohjelmia, jotka etsivät tunnettuja haavoittuvuuksia tai arvailevat automaattisesti yleisempiä salasanoja.

Haastateltavat mainitsivat myös, että suomen kieli suojaa hyvin sosiaalisilta hyökkäyksiltä. Yksittäiset, esim. pankkien nimissä, lähetetyt sähköpostit tietojen kalastelemiseksi on kirjoitettu käännöskoneen tekemällä huonolla suomenkielellä ja näin ovat helposti tunnistettavissa.

Kysymys 5. Millaisena näet tietoturvan tulevaisuuden? Miten varautua?

Haastateltavien mukaan sekä hyökkäys- että suojaustekniikat kehittyvät jatkuvasti monimutkaisemmiksi. Tämä johtaa siihen, ettei yksittäisellä yrityksellä välttämättä ole riittäviä osaamista huolehtia omasta suojauksestaan. Turvatekniikat tulevat jatkossa olemaan entistä enemmän osana infrastruktuuripalveluja, esim. osana tietoliikenneoperaattorin liittymää tai pilvipalvelun palvelusisältöä. Yritykset ostaisivat tarvitsemansa suojauksen kuukausihintaisella palvelulla. Palvelun sisällön ja palvelutason hahmottaminen tulee olemaan haasteellista. Palvelutarjoajat hakevat erilaisilla sertifioinneilla vakuutusta, että heidän palvelunsa täyttää tietyn vaatimustason.

Myös ohjelmapuolella hyökkäykset kehittyvät jatkuvasti. Haastateltavien mielestä parasta onkin jatkuvasti ylläpitää yrityksen tietoturvaa, jotta riskit minimoidaan ja tietomurroilta vältytään. Haastateltavat suosittelivat kaksivaiheista kirjautumista standardiksi ja kehottivat ehdottomasti välttämään käyttämästä samaa salasanaa useammassa paikassa.

9 VAIHTOEHDOT OMAN TIETOTURVAN YLLÄPITÄMISELLE

Yritysten kannattaa myös perehtyä vaihtoehtoisiin ratkaisuihin tietoturvan ylläpitämiseksi. Ympäristöstä riippuen tietoturvan kehittäminen, päivittäminen ja ylläpitämi-

nen voi olla kallista ja vaivalloista. Erityisesti, jos yrityksestä ei löydy tarvittavia tietoja ja taitoja tämän hoitamiseen. Suojattavan tiedon ollessa erittäin arkaluontoista on kannattavampaa ja varmempaa pitää se yrityksen omassa verkossa sekä tiloissa. Tiedon ollessa taas vähemmän kriittistä voidaan harkita työn ulkoistamista ja ulkoisten tietoturvapalveluiden hyödyntämistä. On kuitenkin mahdotonta vetää selkeää rajaa, josta tietäisi kannattaako ulkoistaa vai ei. (Inmicsnebula 2019.)

Yrityksen toiminnan kasvaessa myös hallinnoitavan datan ja laitteiston määrä kasvaa. Useampia ohjelmistoja otetaan käyttöön, kun tarpeita erilaisille toiminnallisuuksille ilmenee. Tätä kautta myös kattavien ja toimivien palveluiden tarjoaminen yrityksen sisällä vaikeutuu sekä kallistuu. Ulkoistamalla tietoturva mahdollistetaan resurssien ja työntekijöiden ajan hyödyntämisen muuhun, kuin jatkuvaan tietoturvan valvomiseen ja päivittämiseen. Samalla osa vastuusta voidaan siirtää tietoturvapalvelun tuottajalle. Tämän toteutuminen tietysti vaatii yritykseltä sitoutumista palveluntarjoajan asettamiin muutoksiin ja toimintamalleihin. Saatavuus myös paranee, sillä ulkoistetussa palvelussa tuki löytyy kellon ympäri. Yrityksen sisällä tuotetuissa tietoturva ratkaisuissa voi ongelmatilanteessa tieto ja taito olla vain yhden ihmisen varassa. (Inmicsnebula 2019.)

10 LOPUKSI

Kuten aiemmin tekstissä on monesti todettu, yrityksen tietoturvan heikoin lenkki on lähes poikkeuksetta sen työntekijät. Tämän takia yritysten tietoturvassa keskeisintä onkin juurruttaa koko henkilöstöön toimivan tietoturvan kulttuuri. Tietoturvatietoutta voidaan ylläpitää pitämällä tietoturvatestejä ja -koulutuksia työtekijöille tasaisin väliajoin. Työntekijöiden pitäisi myös itse ymmärtää tietoturvan aktiivisen ylläpitämisen tärkeyden, jotta suurin riskitekijä päästään minimoimaan. Juuri tämä jatkuvuus mahdollistaa yrityksen tehokkaan suojautumisen alati muuttuvassa ja kehittyvässä ympäristössä.

Vaikka ennaltaehkäisy ja jatkuvuus ovatkin tärkeimpiä osa-alueita tietoturvassa, on olennaista myös miettiä miten toimitaan jos tietomurto tai muu uhka pääsee realisoitumaan. Oikeilla metodeilla minimoidaan tapauksesta aiheutuvat vahingot ja palautetaan yritys toimimaan normaalisti mahdollisimman nopeasti.

Tietoturvan päivitys ja ylläpito on kuitenkin monesti kallista ja vaivalloista. Yritysten tuleekin pohtia kuinka paljon ovat valmiita panostamaan ja verrata sitä tietoturvan pettämisestä aiheutuviin kuluihin. Toimivan tietoturvan toteutuessa kannattavuus kuitenkin nopeasti ylittää kulut. Erityisesti yrityksissä, joissa käsitellään asiakkaiden tai muiden yritysten yksityisiä tietoja.

Tietoturvan merkitys tulee varmasti vain korostumaan jatkossa. Maailmalla datan määrä kasvaa jatkuvasti ja yhä useampia laitteita liitetään verkkoon. Jääkaapeissa on kameroita ja ulko-ovien lukkoja ohjataan puhelimilla. Näiden kaltaiset ominaisuudet avaavat täysin uusia mahdollisuuksia hyökkäyksille ja riskejä tietoturvalle. Opinnäytetyötä tehdessäni opin paljon uutta aiheesta. Ymmärsin myös paremmin sen, miten tietoturva on läsnä kaikissa yritysten toiminnoissa.

LÄHTEET

Arjentietosuojan www-sivut n.d. Arjen tietosuojaa videokoulutukset ja nettitestit Viitattu 11.5.2019. Saatavissa: https://arjentietosuoja.fi/fi/#/front

Bhattacharya, S. 2017. Cloud computing security: Be secure before moving to cloud. Viitattu 1.4.2018 Saatavissa: http://resources.infosecinstitute.com/cloud-computing-security-secure-moving-cloud/#gref

Calyptix 2016. Top 5 Risks of Cloud Computing. Viitattu 1.4.2018 Saatavissa: https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/

Chowdhury J. 2008. Unaware user's highest information security threat. Viitattu 4.4.2018. Saatavissa: https://www.firstpost.com/business/unaware-users-highest-information-security-threat-1865067.html

Cisco n.d. What is a DDoS attack? Viitattu 5.4.2018. Saatavissa: https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

Cisco www-sivut n.d. A Cisco guide to defending against distributed denial of service attacks. Viitattu 5.4.2018. Saatavissa: https://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html#35

Cooper, C. 2017. Social media is a cybersecurity risk for business. Viitattu 4.4.2018 Saatavissa: https://www.csoonline.com/article/3198715/data-breach/social-media-is-a-cybersecurity-risk-for-business.html

Flaherty, K. 2015. Project Management Methodology
Viitattu 12.5.2019 Saatavissa: https://my.bridgew.edu/departments/ITProjectManagementOffice/Shared%20Documents/Project%20Management%20Methodology%20v15.pdf

Hoelscher, P. 2017. BYOD Security: What are the risks and how can they be mitigated? Viitattu 2.4.2018 Saatavissa: https://www.comparitech.com/blog/information-security/byod-security-risks/#What_are_the_risks_of_BYOD

ICO:n www-sivut n.d. Guide to the general data protection regulation (GDPR) Viitattu 11.5.2019. Saatavissa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Infosecinstitute. 2013. Social engineering: a hacking story. Viitattu 6.4.2018. Saatavilla: http://resources.infosecinstitute.com/social-engineering-a-hacking-story/#gref

Inmicsnebula 2019. IT-palveluiden Ulkoistajan opas. Viitattu 9.5.2019 Saatavissa: https://www.inmicsnebula.fi/sites/default/files/2019-01/IT-PALVELUIDEN-ULKOISTAJAN-OPAS_Telia_Inmics_Nebula_2019-V1.pdf

ISACA www-sivut. 2017. Vulnerability assessment. Viitattu 6.4.2018. Saatavilla: https://cybersecurity.isaca.org/info/cyber-aware/images/ISACA_WP_Vulnerability_Assessment_1117.pdf

ISO:n www-sivut 2015. ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems. Viitattu 6.5.2019. Saatavissa: https://www.iso.org/standard/62313.html

Kauppakamarin www-sivut. 2016. Tietoturvaopas yrityksille. Viitattu 6.4.2018. Saatavilla: https://kauppakamari.fi/wp-content/uploads/2016/11/tietoturvaopas-yrityksille.pdf

Kevin B. 2016. Best Practices for an information security assessment. Viitattu 8.5.2019. Saatavissa: https://searchsecurity.techtarget.com/tip/Best-practices-for-an-information-security-assessment

Konstadinv, D. 2019. Cyber Threat Analysis. Viitattu 11.5.2019. Saatavilla: https://resources.infosecinstitute.com/cyber-threat-analysis/#gref

Laakso, M. n.d. Fyysisessä tietoturvassa huomioitavaa. Viitattu 6.4.2018. Saatavilla: https://tietojesiturvaksi.fi/tietoturvasuunnitelma/fyysisessa-tietoturvassa-huomioitavaa

LearningAccelerator www-sivut n.d. Tool: Knoster Model for Managing Complex Change. Viitattu 4.5.2019. Saatavissa: https://practices.learningaccelerator.org/strategies/tool-knoster-model-for-managing-complex-change

Lonoff Schiff, J. 2013. 14 Things you need to know about data storage management. Viitattu 5.4.2018. Saatavilla: https://www.cio.com/article/2382585/virtualization/14-things-you-need-to-know-about-data-storage-management.html

Massachusettsin tietoturva www-sivut. n.d. Information security risk assessment guidelines. Viitattu 6.4.2018. Saatavilla: http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/risk-assessment/risk-assessment-guideline.html

Microsoft n.d. How to recognize phishing email messages, links or phone calls. Viitattu 1.4.2018 Saatavissa: https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx

Microsoft Project www-sivut n.d. Project and portfolio management software. Viitattu 15.5.2019. Saatavissa: https://products.office.com/fi-fi/project/project-and-portfolio-management-software

Microsoftin officen www-sivut n.d. ATP anti-phishing capabilities in Office 365. Viitattu 1.4.2018. Saatavissa: https://support.office.com/en-us/article/atp-anti-phishing-capabilities-in-office-365-5076d0f6-7a59-4d6c-bd07-ba95033f0682?ui=en-US&rs=en-US&ad=US

Norton. n.d. What is social engineering? Viitattu 6.4.2018. Saatavilla: https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

Peltier, T. 2001. Information security risk analysis. Boca Raton: CRC Press. Viitattu 6.4.2018. Saatavilla: https://books.google.fi/books?id=n8Z1RDjEKa0C&printsec=frontcover&hl=fi#v=onepage&q&f=false

Shakeel, I. 2012. Social media & security risk. Viitattu 4.4.2018 Saatavissa: http://resources.infosecinstitute.com/social-media-security-risk/#gref

Study.com www-sivut n.d. Applying the CIA Triad to Security Design for IoT Products. Viitattu 7.5.2019. Saatavissa: https://study.com/academy/lesson/applying-the-cia-triad-to-security-design-for-iot-products.html

Techopedia www-sivut n.d. CIA Triad of Information security Viitattu 21.4.2019. Saatavissa: https://www.techopedia.com/definition/25830/cia-triad-of-information-security

TechTarget n.d. Lotus Notes Domino phishing and email fraud protection. Viitattu 1.4.2018. Saatavissa: https://searchdomino.techtarget.com/resources/Lotus-Notes-Domino-Phishing-and-Email-Fraud-Protection

Thiagarajan V. 2015. BS ISO IEC 17799 SANS Checklist. Viitattu 7.5.2019. Saatavissa: https://www.sans.org/score/checklists/iso-17799-2005

Tietosuojamallin www-sivut 2017. Hallinnollisten sakkojen määräämisen yleiset edellytykse. Viitattu 11.5.2019. Saatavilla: https://fakta.tietosuojamalli.fi/gdpr-asetus/83-hallinnollisten-sakkojen-maaraamisen-yleiset-edellytykset

Trend Micro 2015. Spear Phishing 101: What is spear phishing? Viitattu 1.4.2018. Saatavissa: Saatavissa: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/spear-phishing-101-what-is-spear-phishing

Trend Micro n.d. Data Breach. Viitattu 30.3.2018. Saatavissa: https://www.trendmicro.com/vinfo/us/security/definition/data-breach

Tuulinen, T. 2017. Tietoturvan vahvistaminen Zero Trust- politiikan ja mikrosegmentoinnin avulla. Viitattu 4.4.2018 Saatavissa: https://www.cinia.fi/blogi/tietoturvan-vahvistaminen-zero-trust-politiikan-ja-mikrosegmentoinnin-avulla.html

Twitterin tutkimus 2019. Retrospective Review Twitter, Inc. and the 2018 Midterm Elections in the United States Viitattu 2.5.2019. Saatavissa: https://blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf

Van Zadelhoff, M. 2016. The biggest cybersecurity threats are inside your company. Viitattu 4.4.2018. Saatavissa: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

Viestintäviraston www-sivut 2016. Yahoo!-tietomurrosta yli miljardin käyttäjän tiedot: vaihda salasana. Viitattu 30.3.2018. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/09/ttn201609231341.html

Virgillito, D. 2014. A Physical security policy can save your company thousands of dollars. Viitattu 6.4.2018. Saatavilla: http://resources.infosecinstitute.com/physical-security-policy-can-save-company-thousands-dollars/#gref