Työn digitalisaatio ja sen tuomat haasteet tietoturvaan eri organisaatioissa sekä parhaita käytänteitä tietoturvan varmistamiseksi

Christoffer Kavantsaari

Haaga-Helia ammattikorkeakoulu

Amk-opinnäytetyö

2022

Tradenomin tutkinto

Tiivistelmä

Tekijä(t)
Christoffer Kavantsaari

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Työn digitalisaatio ja sen tuomat haasteet tietoturvaan eri organisaatioissa sekä parhaita käytänteitä tietoturvan varmistamiseksi

Sivu- ja liitesivumäärä
27 + 14

Tiivistelmä

Opinnäytetyöni perustana on digivallankumous. Vielä 1990-luvun alussa elimme aivan erilaisessa ”digimaailmassa”. Ko. aikakautta voi nyt taaksepäin katsoen kutsua jopa esihistorialliseksi. Tänä päivänä meillä on yhden ihmiselämän aikana ollut mahdollisuus kokea todellinen vallankumous. Teknologia on muuttunut valtavalla vauhdilla. Olemme saaneet todistaa mikropiirit, kännykän, globaalin tietoverkon, esineiden ja asioiden internetin ja tekoälyn; siis useita vallankumouksia. Nämä digivallankumoukset ovat muokanneet maailmaamme. Ne ovat muokanneet jokaisen yrityksen, organisaation ja yhteisön toiminta- ja liiketoimintapoja. Globaali tietoverkko, ”netti”, on paras ja pahin asia, mikä nykysukupolville on tapahtunut. Netti on tuonut samanaikaisesti uudet mahdollisuudet ja uudet riskit ja myös viihteellisyyden koko yhteiskunnalle ja meille jokaiselle. Se on globaalia, siinä ei ole rajoja, ei maantiedettä eikä etäisyyksiä.

Haastattelin opinnäytetyötäni varten monipuolisesti eri organisaatioiden edustajia. Haastattelemani henkilöt työskentelevät seurakunnissa, nuorisotyönohjaajina, rakennus- ja sijoitusalalla, yrittäjinä ja ammattitubettajina eli vloggaajina. Kaikki haastateltavat työskentelivät organisaatioissa, joissa käsitellään arkaluonteisia tietoja. Pyrin ottamaan haastattelukysymyksissäni huomioon haastateltavien työtaustat ja laatimaan kysymykset sen mukaan. Kvalitatiivisen tutkimukseni haastattelumenetelmänä käytin teemahaastattelua. Aineiston analyysin työkaluna tutkimuksessani on sisällönanalyysi. Se voidaan ymmärtää joko yksittäisenä metodina tai väljänä metodisena tulkintakehyksenä aineistolle. Analyysissa hyödynnettiin muun muassa Mikko Hyppösen esittämiä teorioita ja malleja.

Päätarkoitukseni opinnäytetyössäni on luoda best practices-käytännöt tietoturvan osalta ja niiden jalkauttaminen eri organisaatioille. Tekemieni haastattelujen perusteella selvisi, että kaikissa organisaatioissa ei oltu onnistuttu luomaan kyseisiä käytäntöjä. Myös koulutus on ollut puutteellista ja yhteisesti sovittuja tietoturvaan liittyviä yhteisiä ohjeita ja sääntöjä ei ollut tehty. Tämä ongelma korostui erityisesti pienempien organisaatioiden osalta. Isoimmissa organisaatioissa sama ongelma ei toistunut, mutta jotkut isompien organisaatioiden työntekijöistä tyytyivät haastattelujen perusteella liian helposti nykyiseen tietoturvaosaamiseensa.

Asiasanat
Digitalisaatio, globaali tietoverkko, hallinnollinen tietoturva, best practices-käytännöt

Sisällys

1 Johdanto

Opinnäytetyöni perustana on digivallankumous. Vielä 1990-luvun alussa elimme aivan erilaisessa ”digimaailmassa”. Ko. aikakautta voi nyt taaksepäin katsoen kutsua jopa esihistoriallisiksi. Tänä päivänä meillä on yhden ihmiselämän aikana ollut mahdollisuus kokea todellinen vallankumous. Teknologia on muuttunut valtavalla vauhdilla. Olemme saaneet todistaa mikropiirit, kännykän, globaalin tietoverkon, esineiden ja asioiden internetin ja tekoälyn; siis useita vallankumouksia. Nämä digivallankumoukset ovat muokanneet maailmaamme. Ne ovat muokanneet jokaisen yrityksen, organisaation ja yhteisön toiminta- ja liiketoimintatapoja.

Tietoverkkojen symbioosit tärkeimpien teknologioiden kanssa tulevat lisääntymään huimasti. Koska teknologia on mullistavaa ja hyödyllistä, emme voi enää elää ja toimia ilman sitä. Globaali tietoverkko, ”netti”, on paras ja pahin asia, mikä nykysukupolville on tapahtunut. Netti on tuonut samanaikaisesti uudet mahdollisuudet ja uudet riskit ja myös viihteellisyyden koko yhteiskunnalle ja meille jokaiselle. Se on globaalia, siinä ei ole rajoja, ei maantiedettä eikä etäisyyksiä. (Hyppönen 2021, 9.)

Jokaisen yrityksen perusedellytyksenä on tehokkaasti toimiva digitaalinen tietoliikenne. Tämä koskee yrityksissä ja organisaatiossa sekä sisäisiä että ulkoisia verkkoja, niiden toimivuutta, nopeutta ja verkkoinfrastruktuurin toimivaa suunnittelua. Yhä lisääntynyt digitalisaatio ja pilvipalvelut edellyttävät vahvaa tietoturvaa, samoin yrityksille tärkeiden tietojen ja dokumenttien säilyttäminen. Yrityksien toimintaa on turvattava tietoturvallisuuden lisäämisellä. Tämä koskee myös jokaisen yksittäisen henkilön tietoturvaa.

1.1 Opinnäytetyön rajaus

Tutkimusmetodini on kvalitatiivinen tutkimusmenetelmä, joka sisälsi teemahaastatteluja. Työ perustuu uusimpiin tietoturvaa käsitteleviin webinaareihin ja blogeihin. Tätä desk research-vaihetta olen syventänyt teemahaastatteluilla. Aiheen ajankohtaisuuden takia työn rajaaminen oli joissakin kohdissa haasteellista. Huomasin kehittyneeni työn tekemisen aikana tietoturvan osalta monipuoliseksi aiheen osaajaksi. Aikataulutus oli haasteellista sen takia, että ko. tietoa tietoturvasta ja tietoturvarikollisuudesta tulee koko ajan lisää. Työn tavoitteena on koota best practices-työkalupakki tietoturvan takaamiseksi, mutta koska hakkerien taidot ja hakkereiden symbioosit lisääntyvät koko ajan, on tietoturvan takaaminen jatkuva prosessi.

Tavoitteena opinnäytetyössäni on tarkastella digivallankumouksen synnyttämää tarvetta kehittää erityisesti hallinnollista tietoturvaa. Tietoturvahyökkäykset ovat kehittyneet uhkaavan nopeasti ja niistä on tullut entistä hienostuneempia. Tietoturvatoimenpiteet eivät ole pysyneet tässä kehityksessä mukana. Opinnäytetyössäni esitän uusia käyttöön otettavia, konkreettisia toimenpiteitä ja toimintaohjeita hallinnollisen tietoturvan kehittämiseen. Rajaan opinnäytetyöni ulkopuolelle teknisen ja fyysisen tietoturvan, joihin sekä suomalaiset että kansainväliset tietoturvayritykset ovat vahvasti erikoistuneet. Ehdottamiani hallinnollisen tietoturvan kehittämistoimenpiteitä voi nimetä monella tavalla. Itse pidän termistä best practices-toimenpiteet hallinnollisen tietoturvan varmistamiseksi. Nämä toimenpiteet tulee sisällyttää niin yritysten kuin yhdistysten, järjestöjen, säätiöiden, vapaaehtoisjärjestöjen, seurakuntien ja yksilöiden jokapäiväisen toiminnan osaksi.

Nämä tahot kohtaavat yritysten tavoin samankaltaisia tietoturvauhkia ja tiedon väärinkäytöksiä, vaikka sitä ei ole aikaisemmin riittävästi tiedostettu. On ajoittain oletettu, että tietoturvaongelmat eivät koske näitä organisaatioita. Best practices-toimenpiteet edellyttävät jokaisen sitouttamista näiden käytänteiden noudattamiseen, jolloin edellä mainittujen toimijoiden johtotehtävissä työskentelevien tulee luoda edellytykset sille, että näistä käytännöistä tulee tärkeä osa strategista suunnittelua ja että ne jalkautetaan motivoivalla tavalla. Opinnäytetyöni rajaamiseksi en esittele best practices-toimenpiteissä myynnissä olevia, kaupallisten tietoturvayritysten tuotteita ja niiden sisältöä.

Työssäni määrittelen kyberturvallisuuden ns. virallisen määritelmän mukaan seuraavasti: tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Tässä määritelmässä kybertoimintaympäristöllä tarkoitetaan yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaa toimintaympäristöä. Tutkimusaineistoa selatessani ja opiskellessani löysin mielestäni konkreettisempia ja täydentäviä esimerkkejä määrittelyistä.

Tutkielmani keihäänkärki on hallinnollisessa tietoturvassa ja toimenpiteissä sen parantamiseksi. Haastattelujen aikana on käynyt täysin selväksi, miten tekninen ja fyysinen tietoturva on monessa tilanteessa yhdistettävä hallinnolliseen tietoturvaan. Tietoturva ei tule toimimaan, ellei sekä hallinnollista, teknistä että fyysistä tietoturvaa vahvisteta yhtäaikaisesti kaikissa organisaatioissa. Siksi työssäni käsitellään myös parannus-, ja toimenpide-ehdotuksia liittyen tekniseen ja fyysiseen tietoturvaan.

Kvalitatiivisella eli laadullisella tutkimuksella tarkoitetaan tutkimuslajia, jolla pyritään tutkimaan tutkimuskohdetta kokonaisvaltaisesti havainnoiden. Laadullisessa tutkimuksessa

lähtökohtana on todellisen elämän kuvaaminen. Tästä johtuen kvalitatiivinen tutkimusaineisto kootaan yleensä luonnollisissa eli todellisissa tilanteissa. Kvalitatiivisessa tutkimuksessa käytetään usein tutkimusmetodeja, joissa tutkittavan henkilön näkökulmat tulevat selkeästi esille haastatteluiden tai keskusteluiden muodossa. Tämä tarkoittaa, että tutkimuksen onnistumiseksi kvalitatiivisessa tutkimuksessa niin tutkijan kuin tutkittavan tulee olla aktiivisia tutkimuksen aikana. Tästä syystä kvalitatiiviseen tutkimukseen valitaan kohdejoukko yleensä tarkoituksenmukaisesti eikä satunnaisesti.

Laadullisessa tutkimuksessa ollaan usein tekemisissä tunteiden, odotusten, oletusten, kertomuksien ja merkityksien kanssa. Tutkimuksella ei ole mahdollista saada määrälliselle eli kvantitatiiviselle tutkimukselle tyypillistä tilastollisesti yleistettävää tietoa. Kvalitatiivisen tutkimuksen kohderyhmän edustajia tule käsitellä ainutlaatuisina, ja tämän vuoksi ainutlaatuisuus tulee ottaa huomioon myös aineiston tulkinnassa.

Laadullisen tutkimuksen tavoitteena on myös löytää aineistosta odottamattomia tulkintoja. Lähtökohtana laadullisessa tutkimuksessa on todellisen kokemisen ja näkemyksen kuvaaminen, jossa hallinnollista tietoturvaa pyritään kuvaamaan mahdollisimman kokonaisvaltaisesti. Laadullisessa tutkimuksessa tutkija ei voi täysin eliminoida arvolähtökohtia, jotka saattavat muokata tulkintoja. (Koppa 28.10.2021).

Käytän opinnäytetyössäni laadulliselle tutkimukselle tyypillistä harkinnanvaraista otantaa eli keskityn pienempään määrään haastateltavia, joiden teemahaastattelut pyrin analysoimaan mahdollisimman tarkasti. Aineistoni tulkinnassa korostuu siis laatu, ei määrä.

Aineistolähtöinen analyysi tarkoittaa laadullisessa tutkimuksessa pelkistetyimmillään teorian rakentamista empiirisestä aineistosta lähtien, ikään kuin alhaalta ylös. Hypoteesittomuus tarkoittaa, että minulla tutkijana ei ole lukkoon lyötyjä ennakko-oletuksia haastattelujen tuloksista. (Koppa 28.10.2021).

Kvalitatiivinen tutkimusote sopii kvantitatiivista tutkimusotetta paremmin tutkimukseni aihe huomioon ottaen. Kvalitatiivinen tutkimusote pyrkii luomaan tutkittavasta ilmiöstä mahdollisimman ymmärrettävän ja monipuolisen kuvan, kun taas kvantitatiivinen pyrkii mahdollisimman suureen yleistettävyyteen, ennustettavuuteen ja kausaaliselityksiin. (Hirsjärvi & Hurme 2000, 22.)

Kvalitatiivinen ote tarjoaa sopivia välineitä pyrkiessäni ymmärtämään tietoturvan parissa työskentelevien henkilöiden näkemyksiä ja kokemuksia hallinnollisesta tietoturvasta ja sen jalkauttamisesta osaksi organisaatioiden toimintaa. Valitsin tutkielmaani kvalitatiivisen tutkimusotteen myös teoriasta johtuvien syiden vuoksi. Tietoturvan parissa työskentelevien työntekijöiden kokemuksia on helpompi tutkia, kun otetaan huomioon tutkittavien konteksti,

yksittäisten haastateltavien tulkinnat ja yksittäisten työntekijöiden näkökulman ymmärtäminen. Tällöin saadaan muodostettua mahdollisimman kattava ja ymmärrettävä kuva ilmiöstä kadottamatta aineiston erityispiirteitä.

Tutkielma tehtiin haastattelemalla tietoturvan piirissä toimivien organisaatioiden työntekijöitä heidän näkemyksistään ja kokemuksistaan erilaisten organisaatioiden hallinnollisesta tietoturvasta. Best practices-haastattelujen yksi tavoite on kartoittaa, mitä organisaatio ja haastateltavat kokevat kuuluvan tietoturvaan erityisesti ei-kaupallisissa organisaatioissa.

Haastattelu on tutkimusmenetelmä, jonka aineistoa tutkitaan yleensä kvalitatiivisesti. Haastattelu käsitetään eräänlaisena keskusteluna, jossa ollaan suorassa vuorovaikutuksessa tutkittavan osapuolen kanssa. Haastattelussa haastattelijalla on ohjat ja hän ohjaa haastattelua esittämällä kysymyksiä tutkittavasta aiheesta. Haastattelua voidaan kuvailla toisaalta ohjatuksi, mutta kuitenkin hyvin vapaamuotoiseksi keskusteluksi. Haastattelun eduiksi voidaan luokitella joustavan aineistonkeruutavan myötäilevä haastattelu, haastatteluaiheiden järjestämisen mahdollisuus kesken haastattelun sekä haastattelun vastauksien tulkinnan vapaus, toisin kuin kvantitatiivisessa eli määrällisessä tutkimuksessa. (KvaliMOTV 2006). Haastatteluaineistoa kutsutaan primaariaineistoksi, koska tutkija on itse tuottanut sen tutkimuksen käyttöön. (Hirsjärvi & Remes & Sajavaara 1997, 73.)

Valitsin tutkimusaineistoni keruutavaksi teemahaastattelun. Teemahaastattelu on puolistrukturoitu haastattelumuoto, jossa käydään läpi tietyt teemat ja aihepiirit, mutta kysymysten muotoilu ja järjestys voivat vaihdella. (Ruusuvuori & Tiittula (toim.) 2009, 11.)

Perustelen teemahaastattelun valintaa tutkimusaiheen uutuuteen perustuen. Päädyin puolistrukturoituun haastatteluun eli teemahaastatteluun myös siitä syystä, että minulla oli teoriasta ohjatut tietyt teemat, joihin halusin keskittyä haastattelun avulla. Teemahaastattelun avulla on mahdollisuus tavoittaa haastateltavien elämysmaailmaa, kuten kokemuksia, ajatuksia, uskomuksia ja tunteita. Siten se tarjoaa aineistoksi tutkittavien oman äänen, mutta säilyttää haastattelujen välisen vertailtavuuden, koska jokaisen haastateltavan kanssa käydään läpi samat teemat. (Hirsjärvi & Hurme 2000, 48.)

Teemahaastattelulla pyritään saamaan merkityksellisiä vastauksia tutkimuskysymyksiin. Etukäteen mietityt teemat pohjautuvat siihen, mitä tutkittavasta aiheesta tiedetään jo etukäteen. Teemahaastattelun aihepiirit eli teemat on kirjattu ylös, mutta kysymyksiä ei ole muotoiltu tai järjestetty valmiiksi. Haastattelun osittaisella strukturoinnilla eli teemoittamisella olen pyrkinyt rajaamaan ja ohjaamaan haastattelun ennalta määriteltyihin tutkimuksen tavoitteisiin. Haastattelujen teemat perustuvat lähtökohtaisesti tutkimukseni lähdekirjallisuuden perusteella rakennettuun viitekehykseen.

2 Mitä on tietoturva?

Viestintävirasto, Huoltovarmuuskeskus ja Sanastokeskus TSK määrittelevät tietoturvan seuraavasti: Tietoturva tarkoittaa järjestelyjä ja toimenpiteitä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. (Wikipedia 22.05.2022).

Tietoturva on yksi tietosuojan toteuttamisen keino. Sen tarkoitus on suojata tietoaineisto ja tietojärjestelmät. Tietoturva tarkoittaa muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen.

Useille erityyppisille toimijoille säädetään velvollisuus huolehtia tarjoamiensa verkkojen ja palvelujen tietoturvasta sekä oikeuksia tämän toteuttamiseen. Tietoturvasääntely koskee teleyrityksiä, viestinnän välittäjiä, yhteisötilaajia, verkkotunnusvälittäjiä ja NIS-direktiivin mukaisia digitaalisia palveluita eli pilvipalveluita, verkon markkinapaikkoja ja hakukoneita. Velvoitteet säädetään pääosin laissa sähköisen viestinnän palveluista ja niitä tarkennetaan määräyksillämme. Ohjaamme ja valvomme tietoturvavelvoitteiden noudattamista.

Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus eli se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, eheys eli se, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä käytettävyys eli se, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.

2.1 Taustaa tietoturvapelureista

Netin kehittyminen on synnyttänyt uuden rikollisuuden, nettirikollisuuden. Sen uhrit ovat globaaleja. Verkkorikollisuudessa kaikki ovat uhreina samanarvoisia. Verkkorikollisuudessa pyritään pääsemään kiinni sinun, minun ja organisaatioiden verkkolaitteisiin tai dataan. Rikoksen kohteena olevaan dataan päästään mm. näppäimistönauhureilla ja keylockereilla. Verkkorikollisuudessa ei ole väliä, onko rikoksen kohteena oleva luottokortti Vietnamissa vai Utsjoella. Vuodesta 2020 lähtien olemme astuneet rajalle, jossa todennäköisyys suomalaiselle joutua verkkorikoksen uhriksi on selkeästi alkanut. Meidän tietomme ja koneemme ovat kaikkialla samanarvoisia. Netti vei pois maantiedon ja

etäisyyden. Tästä esimerkkinä Suomessa vuoden 2020 rikospiikki case Vastaamo. (Hyppönen 01.12.2020).

2.2 Tietoturvatetris ja tietoturvan näkymättömyys

Tietoturvatetriksessä on kyse pelistä, jossa pelaaja ns. yrittää estää tietoturvahyökkäyksen. Kun esto onnistuu, rivi poistuu. Jos esto epäonnistuu, rivi jää jäljelle. Kun tietoturva onnistuu sataprosenttisesti, ei näy mitään. Tietoturvassa onnistuminen on ikään kuin näkymätöntä. Kun tietovuoto tapahtuu, kaikki näkyy. Tässä kohtaa on syytä kiinnittää huomiota, kuinka suuri rooli on yrityksen tai organisaation vetäjällä, vastuuhenkilöllä tai johtoryhmällä. On sudenkuoppa todeta, että eihän meillä ole mitään tietoturvaongelmia. (Hyppönen 01.12.2020).

2.3 Tietoturvapelurit

Verkkorikolliset ovat konkreettisia vihollisia ja pelureita, jotka tekevät rikokset luottokorttivarkauksina, pankkitroijalaisina, lunnastroijalaisina, palvelunestohyökkäyksinä ja kiristyshyökkäyksinä. Nämä tietoturvan vastustajat ovat rikollisjengejä. Ne ovat jengejä, jotka eivät ehkä koskaan tapaa reaalimaailmassa. Nämä jengit ovat organisoituneita erilaisilla hierarkioilla. Niillä voi olla johto, välijohto ja suorittavat portaat jne. Nämä rikollisorganisaatiot toimivat eri forumien kautta. Rikolliset kohtaavat esim. White House Marketeissa tai Underground-klubeissa, mm. Torhideservice-palveluissa. Vaikka tuntuu abstraktilta, rikolliset voivat kohdata, rekrytoida tai myydä varastettuja tietoja tai pääsykoodeja yritysten ja organisaatioiden tietokoneisiin.

Murtauduttuaan palveluverkkoihin tietoturvarikolliset saattavat etsiä reikiä, skannata verkkoja ja myydä listoja muille tahoille. He voivat myös murtautua tietokantoihin ja myydä niistä saatua tietoa eteenpäin. Hyökkääjistä huimin on jo seitsemän vuoden ajan ollut lunnastroijalainen Cryptowall Venäjältä. Tämä hyökkääjä on ollut ensimmäinen, joka meni yrityksen koneille, salasi tiedot ja pyysi lunnaat bitcoineina lähettämänsä viestin kautta.

Bitcoineja on vaikea seurata. Siksi se on suosittu lunnaidenpyyntömuoto. Muita vastaavia lunnasmuotoja ovat olleet Monero ja Zcash. Usein se taho, jolta tiedot on viety, maksaa lunnaat ja on näin ollen verkkorikollisten kannalta paras ”asiakas”. Lunnastroijalaiset ovat nykyisin useimmiten tiettyihin organisaatioihin suunnattuja hyökkäyksiä ja ovat verkossa usein pitkään etsien heikkoja kohtia ja tietoja. Tämän jälkeen lähetetään lunnasviesti lukittujen tietojen vapauttamiseksi. Tietojen lukitseminen on erittäin haitallista terveydenhoitoalan organisaatioille, koska se lamaannuttaa täysin mm. sairaaloiden toiminnan. Tämä

johti mm. Saksassa viime elokuussa siihen, että hyökkäyksen kohteeksi joutuneen sairaalan potilaita jouduttiin siirtämään toisiin sairaaloihin.

Useimmiten hyökkäysten motiivina on rahan tekeminen ja tienaaminen, jolloin hyökkäykset kohdistuvat finanssijärjestelmiin. Tästä merkittävä poikkeus oli viimevuoden tapaus Vastaamo, jossa hyökkääjä, ransom man, alkoi kiristää potilastiedoilla sekä Vastaamoa että yksittäisiä asiakkaita. Terveys- ja potilastietojen suurin riski on siinä, että ne eivät ns. koskaan vanhene ja tiedot on pystyttävä pitämään näin ollen vuosikymmenten ajan. Tämä on iso haaste.

Hyökkääjä teki kuitenkin myös virheen. Hän kopioi koko varastamansa potilastietokannan verkkoon, jolloin saatiin tietoja hyökkääjän käyttämistä järjestelmistä. Näitä tietoja voidaan käyttää myöhemmin todistusaineistona hakkeria vastaan. Vastaamon tapauksessa kyse ei ole lunnastroijalaisesta, vaan sillä, että kiristettiin tietojen vuotamisella.

Toinen iso mullistus on Ransomware 2.0-hyökkäykset, joita on käytetty terveystietojen käyttämiseen rahan tekemiseen. Lunnastroijalaiset ovat siirtymässä uuteen vaiheeseen, koska yritykset ovat oppineet reagoimaan hyökkäyksiin. Tämä voidaan tehdä esimerkiksi varmuuskopioiden avulla. Varmuuskopioiden tulee siis olla kunnossa. Voidaan hieman kärjistäen sanoa, että lunnastroijalaisten ansiosta varmuuskopiointikulttuuri on parantunut. Tämä on johtanut siihen, että lunnastroijalaisjengit saivat vähemmän lunnaita ja ”joutuivat” kehittämään uuden hyökkäysmenetelmän. Maantieteellisesti Venäjä on yliedustettuna, kun katsotaan verkkorikollisten kotimaita. Uudessa hyökkäysmenetelmässä tiedot kopioidaan ja ne uhataan julkaista verkossa, ellei lunnaita makseta. Tällaisia kopioitavia tietoja ovat esimerkiksi sähköpostipalvelimien kopiot ja dokumenttipalvelimien kopiot.

Kaikki hakkerien käyttämät sivustot eivät ole salattuja, vaan varastettua tietoa julkaistaan myös julkisilla internetsivuilla esimerkiksi Mount Locker. Yritysten tietojen julkistamis-, ja vuototapauksissa varmuuskopiointi ei auta.

Hyvä esimerkki hyökkäyksistä ovat pankkitroijalaiset. Kaikki maksuliikenne tapahtuu nykyään tietoverkkojen kautta. Haasteeksi muodostuu yrityksen ulkopuolelle muodostuvan verkon suojaaminen. Hyökkäykset tapahtuvat pankkien asiakkaiden verkkoihin, joka on olennaisesti helpompaa kuin pankkien verkkoihin murtautuminen.

Eniten rahaa tehdään BEC eli Business Email Compromise-hyökkäyksillä. Hyökkäyksiä on vaikea huomata ja useimmiten hyökkääjä voi olla jo monien viikkojen ajan yrityksen verkkoympäristössä. Useimmiten hyökkääjä opettelee yrityksen maksuliikennekäytännöt ja alkaa ohjata sähköpostiviestien kautta esim. laskujen maksamista eri tileille. Nordfundin

tapauksessa hyökkääjät esiintyivät yrityksen henkilöinä ja pystyivät ohjaamaan omille tileilleen yli 100 miljoonaa Norjan kruunua.

Tietojärjestelmät laajenevat koko ajan. Jokainen älylaite on jatkossa haavoittuva. Jokainen firma on ”softafirma” eli digitalisaation ansiosta jokainen firma toimii tietoverkkojen ja tietotekniikan päällä. Tämän takia tietoturva koskettaa meitä kaikkia.

Tulevaisuudessa data tulee siirtymään entistä enemmän pilvipalveluihin. Pilvipalveluiden etuna on skaalautuvuus ja turvaetu. Kansainväliset pilvipalveluiden tarjoajat esim. Amazon, Microsoft ja Google, pystyvät käyttämään valtavia rahasummia jatkuvaan turvallisuuden parantamiseen. Pilvipalveluiden käyttöön siirtyminen tuo myös firmoille mahdollisia kustannussäästöjä. Yritykset voivat luopua omista datasenttereistään.

Järjestelmien auditoinnin tulee olla säännöllistä ja yrityksessä tulee tehdä myös säännöllisesti hyökkäystestauksia. Hyökkäystestauksessa palkataan joku tekemään hyökkäys yrityksen järjestelmiin, jonka jälkeen käydään läpi haavoittuvuudet.

Kommunikaatio siirtyy jatkossa sähköposteista chatteihin ja slackkeihin. Palvelujen suosion lisääntyessä myös niihin kohdistuvat hyökkäykset lisääntyvät, jolloin voidaan esimerkiksi Whatsappissa esiintyä yrityksen ylimmän johdon edustajana. Vastuun yrityksen tietoturvasta tulee olla yrityksen ylimmällä johdolla. Tietoturvan tulee olla jatkuvan kehityksen kohteena. (Hyppönen 01.12.2020).

2.4 GDPR

GDPR tulee sanoista General Data Protection Regulation (yleinen tietosuoja-asetus). Se on henkilötietojen käsittelyä sääntelevä laki, jota alettiin soveltaa kaikissa EU-maissa keväällä 2018. Tietosuoja-asetus antaa paremman suojan henkilötiedoillesi ja enemmän keinoja hallita tietojesi käsittelyä. Lainsäädäntöuudistuksen tavoitteena on ollut parantaa henkilötietojen suojaa ja tietosuojaoikeuksia**,** vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin, yhtenäistää tietosuojasääntelyä kaikissa EU-maissa ja edistää digitaalisten sisämarkkinoiden kehittymistä. (Tietosuojavaltuutetun toimisto).

2.5 Someilmiön ei-rakentavat lieveilmiöt ja sivuvaikutukset

Somemaailman ja internetverkon keskusteluryhmät ja julkaisut perustuivat alun perin ajatukselle siitä, että täydellinen sananvapaus toisi esille parhaimmat ajatukset ja toisi ihmiskunnalle lisää vapautta. Some antoi äänen niille, joilta se puuttui. Tämä ajatus muuttui vä-

hitellen 2010-luvulla, jolloin Somesta tuli erilaisten tahojen valtapyrkimysten ja heidän tavoitteidensa vaikutuskanava. Tähän haasteeseen ei tietoturvalainsäädäntö ole reagoinut riittävän ajoissa ja riittävän voimakkaasti. Mielestäni koko tietoturvan ja tietoturvalainsäädännön suuri haaste on tällä hetkellä, että reagoidaan jälkikäteen, ei proaktiivisesti ennakoiden. Kaiken lisäksi haasteiden, ongelmien ja ns. ”väärien vaikutuksien” tahti kiihtyy nopeammin kuin puolustus. Tällaiseen tilanteeseen tuovat haasteita yhä kehittyvä tekoäly, hakkereiden symbioosiyhteisöt, robotiikka ja jo olemassa olevien digijättien systemaattinen tiedon kerääminen ja tallentaminen globaalisti. Herää kysymys, pitäisikö valtion ja oikeuslaitoksen olla vastuussa digijättien sääntelystä eikä digitaalisten ”oligarkkien” itsensä. (Helsingin Sanomat 10.01.2021 ja 16.01.2021).

2.6 Tekoäly ja älylaitteet

The Guardian pohti jo vuonna 2019, olisiko Jeff Bezoksen johtaman Amazonin kehittämä älykaiutin Alexa hyvä laite ajan säästämistä varten vai alku Orwellilaiselle yhteiskunnalle, jossa älylaitteet valvovat ja vakoilevat käyttäjiään, vaikka Amazon onkin vakuuttanut, että se suhtautuu asiakastietoihinsa vakavasti. Vuonna 2018 saksalainen Amazon-asiakas sai vahingossa noin 1700 äänitiedostoa jonkun toisen Echo-laitteelta. Saamansa tiedon avulla kyseinen asiakas sai valtavan määrän tietoa kyseisen Echo-laitteen käyttäjästä ja hänen tyttöystävästään. Amazonin mielestä kyse oli inhimillisestä erehdyksestä. (Lynskey 09.10.2019).

3 Aiemmat tutkimukset

Useimmat aiemmat tutkimukset, joita löysin tätä tutkielmaa varten, olivat webinaarit ja internetistä löytyvät julkaisut. Tietoturvasta on myös julkaistu paljon kirjallisuutta, mutta useimmissa löytämissäni kirjallisissa lähteissä oli vanhentunutta tietoa tietoturvan osalta, joten otin tavoitteekseni löytää ajankohtaisempia teoksia, jotka sopisivat aiheeltaan opinnäytetyöni aiheeseen. Tehdessäni opinnäytetyötäni huomasin, että F-Securen (nykyinen WithSecure) tutkimusjohtaja Mikko Hyppönen oli kirjoittanut Internet-nimisen kirjan, joka on julkaistu vuonna 2021. Kirjassaan Hyppönen kuvaa yhtenä oman alansa huippuasiantuntijana internetin ja sitä kautta tapahtuvien tietoturvahyökkäysten historiaa ja kehitystä. Hyppönen toteaakin kirjassaan osuvasti: ”Internet on parasta ja pahinta, mitä meille on tapahtunut. Digitalisaation vallankumous näkyy kaikkialla arjessamme. Netti tuo meille merkittäviä uusia hyötyjä, mutta samalla kylmääviä riskejä. Tämä vallankumous on vasta alussa”. (Hyppönen 2021, 9.)

4 Digitalisaatio

Digitalisaatio, somepalveluiden käyttö esim. Google, Spotify ja Facebook ovat lisääntyneet ”valonnopeudella”. Omien työkokemuksieni perusteella ja viimeaikaisten tietoturvahyökkäyksien takia voidaan väittää, että eri hyvinvointi-, terveys- ja terapiapalveluja tarjoavat organisaatiot samoin kuin vapaaehtoisjärjestöt, koulutusorganisaatiot, hyväntekeväisyysjärjestöt, seurakunnat ja monet vastaavat toimijat tulevat kohtaamaan omat tietoturvahaasteensa samalla tavalla kuin kovimmat voittoa tekevät business-yritykset tai valtiot.

4.1 Hallinnollinen tietoturva

Hallinnollinen tietoturva ei suojaa lähtökohtaisesti vain tietoturvahyökkäyksiltä. Hallinnollisessa tietoturvassa on kyse usein tietoturvan ja toimintojen opettamisesta, sitouttamisesta ja jalkauttamisesta. Hallinnollinen tietoturvauhka on usein osaamattomuutta ja huolimattomuutta, joskus jopa tahallista. Keinona hallinnollisen tietoturvan edistämiseksi voidaan käyttää kokeiluina ns. tietojenkalastelu (phishing) sähköpostitestejä ja jopa hallittuja tunkeutumistestauksia. Tärkeä osa tätä testausta on tulosten ja organisaation reagoinnin välitön raportointi sekä jatkuva valvonta.

4.2 Pilvipalvelut

AWS:ssä eli Amazon Web Servicessa eräs pilvipalvelun tietoturvan kannalta tärkeä asia on jaetun vastuun malli. Mallissa vastuut jaetaan asiakkaan ja pilvipalvelun tarjoajan välillä.

Asiakas on vastuussa tietoturvasta pilvipalvelussa, ns. pilvipalvelun sisällä ja hänen tulee huolehtia asiakastiedoista, sovellusten, identiteettien ja käyttöoikeuksien hallinnasta, käyttöjärjestelmien, verkkojen ja palomuurin konfiguraatioista, asiakkaiden tiedoista, salauksesta, tietojen eheydestä ja todentamisesta, palvelinten salaamisesta koskien tiedostojärjestelmää ja dataa sekä verkkoliikenteen suojaamisesta, johon kuuluvat mm. salaus ja eheys.

Palveluntarjoaja on vastuussa pilvipalvelun turvallisuudesta ja heidän tulee huolehtia ohjelmistojen osalta tietojen tallentamisesta, tietokannoista ja verkosta sekä laitteistojen ja AWS:n globaalista infrastruktuurista.

AWS on pilvipalvelun tuottajana vastuussa tuottamansa palvelun turvallisuudesta. Se vastaa mm. palvelinkeskusten fyysisestä turvallisuudesta, laitteisto- ja ohjelmistoinfrastruktuurista ja verkkoinfrastruktuurista.

Asiakkaan tehtävänä on huolehtia tietoturvasta pilvipalvelussa ns. palvelun sisällä. Hänen tulee huolehtia Amazon Elastic Compute Cloudin (Amazon EC2:n) toimivuudesta, sovellusten tietoturvan varmistamisesta erityisesti salasanojen ja käyttöoikeuksien osalta. Asiakkaan tulee myös huolehtia suojausryhmän kokoonpanosta, otetaanko käyttöön käyttöjärjestelmä tai isäntäpohjaiset palomuurit, joiden avulla estetään mahdolliset tunkeutumisyritykset, verkkokokoonpanoista ja tilien hallinnasta.

Asiakas vastaa myös asiakastietojen, sovellusten, pääsynhallinnan, käyttöjärjestelmän, verkon ja palomuurin kokoonpanon, asiakkaiden tietojen salauksen ja tietojen eheyden todennuksen, palvelinten salaamisen sekä verkkoliikenteen suojauksen konfiguroinnista.

4.3 Muutamia parhaita käytäntöjä, jotka organisaation tulisi ottaa käyttöön pilvipalveluun siirryttäessä

On tärkeää ymmärtää, että sekä asiakas että palveluntarjoaja ovat vastuussa pilvipalvelun turvallisuudesta. Tehdessään sopimusta pilvipalveluntarjoajan kanssa, siinä tulisi määritellä, mistä pilvipalveluturvallisuuden palveluista on kyse, mikä on asiakkaan vastuu ja mikä palveluntarjoajan.

Kun tiedot tallennetaan pilveen, ne on suojattava asianmukaisesti. Pilvipalvelun tulisi tukea tietojen salausta pilvipalveluun ja pilvestä siirtyville tiedoille.

Yritysten on luotava tietojen poistokäytännöt, jotka poistavat tiedot turvallisesti valitusta järjestelmästä säilyttäen samalla vaatimustenmukaisuuden.

Pääsynvalvontakäytäntöjen avulla yritys voi hallita pilviympäristöön tulevia käyttäjiä. Pilviympäristöä on valvottava jatkuvasti turvallisuusuhkien varalta, uhat on eliminoitava niin nopeasti kuin mahdollista ja rutiinitunkeutumistestaukset tulee suorittaa.

Hyvin usein suurin uhka pilvipalveluille on oma yritys ja sen työntekijät. Yritysten pitäisi kouluttaa kaikki työntekijät, jotka käyttävät pilvipalvelua, parhaiden tietoturvakäytäntöjen mukaan. Näin pystymään estämään sisäiset turvallisuusuhat samalla kun valmistaudutaan ulkoisiin. (Haaga-Helia ammattikorkeakoulu 2021. Cloud Service Technologies, ICT4TF024. Module 4. 28.02.2021).

5 Tor-verkko

Tor-ohjelmisto mahdollistaa internetin anonyymin käytön, minkä vuoksi Tor-verkko on ollut myös rikollisten suosiossa. Maailmanlaajuisesti Tor-verkolla on noin kaksi miljoonaa käyttäjää. Tor-verkon ohella internetissä on muitakin anonymiteetin takaavia järjestelmiä, mutta Tor on näistä järjestelmistä suosituin.

Tor-verkkoa käytetään yleensä Tor-selainohjelmalla, jonka avulla voi selata normaaleja verkkosivuja anonyymisti sekä selailla vain Tor-verkossa toimivia anonyymejä, onion-päätteisiä verkkosivuja. Vaikka Tor-verkossa toimii myös runsaasti rikollisia, asiantuntijat arvioivat, että enemmistö verkon toiminnasta on laillista.

Tor-verkossa on tarjolla muun muassa blogeja, keskustelufoorumeita ja uutissivustoja. Esimerkiksi BBC tarjoaa sisältöjään Tor-verkossa. BBC haluaa Tor-verkossa olemisellaan helpottaa uutistensa lukemista maissa, joissa BBC:tä sensuroidaan tai sen lukeminen estetään kokonaan. Esimerkiksi Kiinan viranomaiset, jotka ovat tunnettuja nettisensuuristaan, eivät pysty puuttumaan Tor-verkon sisältöihin. Juuri tällaisten humanitaaristen syiden vuoksi Tor-verkko pystyy löytämään itselleen rahoitusta ja olemaan olemassa. Monet toimittajat käyttävät ulkomailla ollessaan paljon Tor-selainta, sillä sen avulla he pääsevät ohi paikallisesta sensuurista ja ovat toisaalta suojassa verkkovakoilulta, jota kohdistetaan helposti journalisteihin. Tor-verkon varjopuolena on se, että se mahdollistaa internetin anonyymin käytön. Tästä johtuen Tor-verkko on ollut ja on edelleen rikollisten suosiossa.

Useimmiten Tor-verkko nousee tiedotusvälineissä esille yleensä vain rikostapausten yhteydessä, jolloin yleinen kuva Tor-verkosta vääristyy helposti. Tämä johtaa siihen, että Torin lailliset käyttötarkoitukset eivät yleensä nouse otsikoihin. Asiantuntijat arvioivat Tor-verkon olevan yleiskäyttöinen teknologia ja vähän niin kuin veitsi, koska Tor-verkon avulla voidaan tehdä sekä hyviä että pahoja asioita. Rikolliset hyödyntävät Tor-verkkoa mm. huumeiden, aseiden ja palkkamurhien myymiseen. Toinen rikollisten Tor-verkossa usein myymä artikkeli ovat erilaiset tietomurroissa varastetut tiedot. Tor-verkossa on useita kauppapaikkoja, joissa rikolliset myyvät henkilötietoja, luottokorttitietoja ja muita tietomurroissa haltuun saatuja tietoja. Tämän tyyppisiä tietoja voidaan käyttää tietomurtojen tekemisiin, yritysten huijaamiseen ja yksityisiin ihmisiin kohdistuviin identiteettivarkauksiin. (STT - Savonen 30.10.2020).

Tämän vuoden puolella Tor-verkko ja tietoturvaiskut ovat nousseet taas otsikoihin Venäjän hyökättyä Ukrainaan. Hakkerien kollektiivi Anonymous julisti kybersodan Venäjän hallintoa vastaan kohdistamalla hyökkäyksiään mm. venäläismediaan. Kollektiivin hyökkäyksien kohteeksi ovat joutuneet uutistoimisto Tass, taloussanomalehti Kommersant ja sano-

malehti Izvestiya. Tämän lisäksi Anonymous-kollektiivin suorittamien hakkeri-iskujen kohteeksi olisivat joutuneet ainakin Kremlin, duuman sekä Venäjän puolustusministeriön sivut. Business Insiderin mukaan hakkeri-iskujen kohteeksi olisivat joutuneet ainakin Kremlin, duuman sekä Venäjän puolustusministeriön sivut.

F-Securen (nykyinen WithSecure) tutkimusjohtajan Mikko Hyppösen mukaan ryhmältä on nähty tähän mennessä runsaasti erilaisia hyökkäyksiä. Osa hyökkäyksistä on ollut DDoS-hyökkäyksiä eli palvelunestohyökkäyksiä, joilla pyritään hidastamaan jonkun verkkosivuston tai vaikka sähköpostipalvelimien toimintaa. Palvelunestohyökkäyksien lisäksi Anonymous on aiheuttanut tietovuotoja murtautumalla sisään erilaisiin valtion hallinnon järjestelmiin. Kollektiivi varastaa näistä hallinnon järjestelmistä tietoja ja vuotaa niitä julkisuuteen. Hyppösen mukaan ryhmän kybersodalla on ideologisia vaikutuksia meneillään olevaan sotaan Venäjän ja Ukrainan välillä. Hän arvioi ryhmän tekemien iskujen olevan aika näyttäviä ja näkyviä hyökkäyksiä, jotka vaikuttavat siihen mielikuvaan, mikä ihmisille syntyy kyseisestä sotatilanteesta. (MTV Uutiset 28.02.2022).

6 Haastattelut

Haastattelin opinnäytetyötäni varten monipuolisesti eri organisaatioiden edustajia. Haastattelemani henkilöt työskentelevät tietoturva-asiantuntijoina, seurakunnissa, nuorisotyönohjaajina, rakennus- ja sijoitusalalla, yrittäjinä ja ammattitubettajina eli vloggaajina. Kaikki haastateltavat työskentelivät organisaatioissa, joissa käsitellään arkaluonteisia tietoja. Pyrin ottamaan haastattelukysymyksissäni huomioon haastateltavien työtaustat ja laatimaan kysymykset sen mukaan. Haastattelut suoritettiin vallitsevan koronatilanteen vuoksi etänä Microsoft Teamsin kautta, puhelimitse tai sähköpostitse. Ennen haastattelun aloittamista kysyin haastateltavilta lupaa haastatteluun nauhoittamiseen. Useimmat haastateltavista suostuivat tähän. Vain yksi haastateltavista kielsi nauhoittamisen, joten haastattelin häntä puhelimitse ja kirjoitin vastaukset ylös koneelleni. Yksi haastatteluista tapahtui sähköpostin välityksellä. Haastattelua varten laadin tietyt peruskysymykset, jotka lähetin jokaiselle haastateltavalle sähköpostitse ennen haastattelua. Viimeistä haastattelua varten laadin erityiskysymykset haastateltavalle. Kyseinen haastateltava oli F-Securen (nykyinen WithSecure) tutkimusjohtaja Mikko Hyppönen. Sain häneltä luvan mainita hänet nimeltä tutkielmassani.

6.1 Tutkimuksen tulokset

Esittelen tutkimustulokseni yhteenvetoina kaikkien haastateltavien vastauksista. Olen litteroinut ja analysoinut tulokset siten, että jokaista yksittäistä kysymystä vastausvaihtoehtoineen ei käydä läpi. Edellä mainittu tuloksien käsittelytapa on perusteltu, koska useat haastateltavien vastaukset toistivat samoja vastauksia ja vahvistivat monen kysymyksen osalta heidän yhteistä näkökantaansa.

Pääkriteereitä haastateltavien valinnalle oli yksi. Haastateltavat kartoitettiin edustamaan laajasti ja edustavasti erilaisia organisaatioita, joissa käsitellään arkaluonteisia asioita ja pyritään suojelemaan niitä organisaation ulkopuolisilta henkilöiltä. Lähetin näille valituille haastateltaville haastattelukysymykset sähköpostitse ja tiedustelin, suostuvatko he haastateltaviksi tutkielmaani varten. Suurin osa heistä suostui. Yksi haastateltavista meinasi ensin kieltäytyä, mutta sain hänet lopulta suostumaan haastatteluun.

Vallitsevan Covid 19-viruksen aiheuttaman poikkeustilanteen vuoksi suoritin haastattelut etänä Microsoft Teamsin avulla. Ensimmäisissä haastatteluissa noudatin etukäteen valmistamaani teemahaastattelurunkoa. Toisen haastattelun aikana ja sitä seuraavissa haastatteluissa pystyin tarpeen mukaan soveltamaan valmiita kysymyksiä ja tekemään tarkentavia lisäkysymyksiä. Näin syvensin näkökulmaa, jonka haastateltava oli avannut. Kaikissa haastatteluissa kävin läpi samat teemat haastattelurungon pohjalta, joskin esitin kysymyksiä siinä järjestyksessä mikä

tuntui luontevalta kunkin haastateltavan osalta. Kun suoritin viimeisiä haastatteluja, koin vahvasti, että aineiston saturaatio eli kyllääntyminen toteutui. Saturaation saavuttaminen tarkoittaa sitä, että uudet haastattelut eivät enää tuo tutkimusongelman kannalta olennaista uutta tietoa. (Hirsjärvi & Remes & Sajavaara 2003, 169.)

6.2 Haastattelut

H5 arvioi organisaationsa tietoturvan nykytilan olevan todennäköisesti ihan okei. Hän totesi vielä, että organisaatiossa on pyritty noudattamaan peruskäytäntöjä, joita ovat esimerkiksi kaksivaiheinen tunnistautuminen ja että organisaatiossa voisi järjestää lyhyen koulutuksen tai ottaa käyttöön jonkin työkalun, jonka avulla pyrittäisiin estämään esimerkiksi sähköpostin kautta tapahtuvat tietoturvariskit. Lopuksi haastateltava totesi, että parannettavaa varmasti on.

H7 totesi, että hänen organisaatiossaan tietoturvan nykytila on suhteellisen hyvä ja sitä on pyritty parantamaan. Suurin osa hänen organisaationsa palveluista tulee Googlen kautta ja suurin osa organisaation dokumenteista on tallennettuna Googlen pilvipalvelimelle. Organisaatiossa on käytössä sähköpostien ja muiden ohjelmien osalta kaksivaiheinen tunnistautuminen. Organisaatiossa on myös määritetty sallitut laitteet ja organisaation puhelimissa on käytössä Elisan tietoturva kuten myös tietokoneissa. Kaikissa ohjelmissa on käytössä kaksivaiheinen tunnistautuminen ja kännykkään tulee Googlen kautta vastanumero tai pitää käyttää Googlen-authenticator-ohjelmaa tai siitä saatavaa tunnusnumeroa.

H6:n organisaatiossa työntekijöiden ohjeistuksen kannalta oli hyvää se, että salasanat pitää vaihtaa tietyin väliajoin. Lisäksi organisaatiossa on ohjeistuksia siitä ja selkeät tietosuojalausekkeet siitä, mitä aineistoa kirjataan ja mitä aineistoa siinä kerätään. Siinä mielessä organisaation IT-puoli oli hyvin hallussa. Organisaatiolla on myös käytössä kaksivaiheinen tunnistautuminen.

H4 totesi samaan asiaan liittyen, että organisaatio, jossa hän työskentelee, on iso konserni ja organisaatiolla on erittäin iso IT-osasto. Hänen organisaatiossaan tietoturva-asiat olivat keskimäärin hyvin hoidettu, ja heillä on tarpeeksi resursseja niiden hoitamiseen. Haastateltava itse ei ollut tietoturva-asiantuntija. Hän työskentelee muissa tehtävissä kuin tietoturvan parissa mainitsemassaan organisaatiossa, joten hän ei tuntenut teknisiä asioita tietoturvan hoitamisen suhteen.

Haastatteluiden perusteella suurimmat organisaatiot pystyvät panostamaan hallinnolliseen tietoturvaan huomattavasti paremmin kuin pienemmät organisaatiot. H2 totesi, että hänen

organisaatiossaan hallinnolliseen tietoturvaan on panostettu useampia vuosia melko paljon ja hänen käsittääkseen hallinnollisen tietoturvan nykytila organisaatiossa on hyvä. Tämä tuli ilmi myös H7:n vastauksessa tietoturvan nykytilasta hänen organisaatiossaan.

H3:sen organisaatiossa, joka on hänen perustamansa yritys, noudatetaan parhaita käytäntöjä, joita organisaation asiakkaat ja kumppanit edellyttävät heiltä. Lisäksi he käyttävät monia AWS:n, Googlen, F-Securen, Oneloginin ja muiden tahojen tarjoamia työkaluja.

H8, joka on ammatiltaan vloggaaja ja tubettaja, totesi tietoturvan nykytilanteen osalta Youtuben kannalta seuraavaa: Tubettajien joukossa ja Suomen Tubettajat ry:ssä kyseistä asiaa on mietitty. Alustatietoturva on hyvä, koska tubettajilla on käytössä maailman suurin tietotekniikka eli Google ja Google tarjoaa käyttäjilleen hyvät tietoturvavälineet mm. kaksivaiheisen tunnistautumisen. Se suojaa tilit hyvin ja kaikki muut systeemit, joista henkilö ei tiedä.

Ongelmana on se, että kaikki tubettajat eivät välttämättä käytä kyseisiä palveluja. Esimerkiksi joillakin tubettajilla ei ole käytössä kaksivaiheista varmennusta, mikä on johtanut ongelmiin. Yhden tubettajan kanava poistui ja ilmeni, että sitä vastaan oli tehty phishing-tyylinen hyökkäys. Hyökkäys oli toteutettu siten, että tubettajaa oli pyydetty lataamaan haittaohjelma. Kyseinen tubettaja otti ongelman huomattuaan yhteyttä Googleen ja sai apua. Hyökkäys olisi ollut estettävissä, jos käyttäjällä olisi ollut käytössä kaksivaiheinen varmennus. Käytännössä, kun tunkeutujat saivat selville salasanan, niin se oli siinä.

Lisäksi isossa organisaatiossa työskentelevä H4 totesi, että hänen organisaatiossaan jalkauttamista ei tapahdu sillä tavalla, että tietoturva-asioita käytäisiin säännöllisin väliajoin yhdessä läpi ja tämän jälkeen otettaisiin käytäntöön. Vaikuttaa siltä, että tämä on isommissa organisaatioissa yksi suurimmista haasteista liittyen parhaiden käytäntöjen jalkauttamiseen organisaation ja tiimien koon takia. Pienemmissä organisaatioissa sama ongelma ei toistunut.

Haastateltavat H1 ja H2 eivät osanneet vastata tietoturvariskien kartoitukseen liittyvään kysymykseeni. Tässä korostuu mielestäni koulutuksen puutteellisuus ja mahdollinen resurssipula koulutuksen järjestämisen suhteen.

Haastateltavien vastauksissa korostuivat tietyt best practices-käytännöt hallinnollisen tietoturvan osalta. Näitä olivat mm. sen varmistaminen, että vain tietyillä henkilöillä on pääsy arkaluontoiseen tietoon. H2 ei osannut vastata kysymykseen. Hän totesi, että pitäisi kysyä näkemystä tietoturvaosaajalta. (Haastattelut H1-H8.)

6.3. Mikko Hyppösen ja tutkijan välinen vuoropuhelu, räätälöidyn haastattelun viisaita sanoja ja opetuksia

Viimeisin suorittamani haastattelu oli ns. spesiaalihaastattelu, sillä pääsin haastattelemaan tuttavani suosituksen avulla F-Securen (nykyinen WithSecure) tietoturvajohtajaa ja oman alansa huippuasiantuntijaa ja gurua Mikko Hyppöstä. Laadin haastattelua varten erityiskysymykset pyrkien ottamaan huomioon Hyppösen pitkän kokemuksen ja asiantuntijuuden tietoturva-alalta. Kysymykset liittyivät Covidin myötä lisääntyneen etätyön aiheuttamiin muutoksiin organisaatioiden tietoturvakäytäntöihin, tietoturvahyökkäysten uusiin muotoihin ja uhkiin, organisaatioiden keinoihin valmentaa ja motivoida työntekijöitään sovittujen tietoturvakäytäntöjen noudattamiseksi, ja mitkä ovat Hyppösen mielestä tietoturvan 5–10 best practices-käytäntöä, joihin kaikkien organisaatioiden tulisi pyrkiä erityisesti hallinnollisen tietoturvan osalta.

6.4 Covid 19-viruksen aiheuttama poikkeustilanne

Covidin aiheuttaman poikkeustilanteen osalta muutos oli selvä. Suurimmat muutokset olivat tulleet sellaisten työntekijöiden arkeen, jotka eivät ole perinteisesti tehneet koskaan etätöitä. Suurin haaste on siinä mitä on tapahtunut niille laitteille, joita ei ole koskaan viety ns. pois konttorilta. Laitteissa ei ollut etämahdollisuuksia ja niihin ei oltu asennettu VPN:nää eli Virtual Private Networkia, joka mahdollistaa yksityisen ja ulkopuolisilta suojatun internetin käytön. Pandemian aikana työntekijät ovat vieneet laitteitaan kotiin eikä heillä ollut osaamista, työkaluja, lisenssejä työkaluihin ja VPN:niin. Kaikki tämä jouduttiin rakentamaan pandemian aikana nollasta.

Tämä on ollut Hyppösen mukaan suurin Covidin aiheuttaman poikkeustilanteen muutos. Se on myös johtanut moniin väliaikaisiin ratkaisuihin eivätkä kyseiset ratkaisut yleensä ole tietoturvallisia ratkaisuja. Tässä ilmenee mielestäni hyvin se haaste, joka tuli ilmi aiempien haastattelujen yhteydessä. Organisaatioiden työntekijät ovat tyytyneet liian helposti ja nopeasti nykyiseen tietoturvaosaamiseensa ja mahdollisesti kokeneet, että lisäkoulutukselle ei ole tarvetta tai sen järjestäminen on liian vaivalloista ja kallista. Covidin aiheuttaman poikkeustilanteen aikana uudelle osaamiselle ja lisäkoulutukselle on entistä enemmän tarvetta ja erityisesti siksi, että tietoturva muuttuu koko ajan ja hakkereiden tekemät hyökkäykset ovat entistä hienostuneempia ja vaikeampia havaita.

6.5 Tietoturvahyökkäysten uudet muodot ja uhat

Tietoturvahyökkäysten uusien muotojen ja uhkien osalta Hyppönen nosti esiin kolme erilaista trendiä. Ensimmäinen on hyvin tiedossa ja jo pitkään käytössä ollut hyökkäysmenetelmä eli kiristyshyökkäykset, jolloin kyseessä ei ole pelkästään lunnastroijalainen. Viimeisin esimerkki tästä oli psykoterapiakeskus Vastaamoon tehty hyökkäys. Tuolloin kyseessä ei ollut lunnastroijalainen, vaan arkaluontoisten tietojen vuotamisella kiristäminen. Kyseessä on trendi, joka lähtee siitä, että verkkorikolliset ovat aina tehneet rahaa sillä logiikalla, että he varastavat tietoa ja myyvät sen eniten tarjoavalle. Jossain vaiheessa rikolliset tajusivat, että eniten lunnaita tarjoava taho onkin tiedon alkuperäinen omistaja. Tieto varastetaan ja myydään takaisin sen omistajalle lunnaita vastaan. Kyseinen taktiikka korostuu erityisesti kiristyshyökkäyksissä ja erityisesti lunnastroijalaisissa. Hakkerit vaativat maksun yleensä bitcoineina, koska niitä on lähes mahdotonta jäljittää ja hakkereiden kiinnijäämisriski pienenee. Tällä hetkellä tärkeimpänä kryptovaluuttana on edelleen Bitcoin, mutta myös uusia digitaalisia valuuttoja on nousemassa markkinoille. Näitä valuuttoja ovat muun muassa Monero ja Zcash. Tässä kohtaa voidaan aiheellisesti kysyä, miten eri organisaatiot suhtautuvat lunnaiden takaisinmaksamiseen. Myös Hyppönen korosti tätä dilemmaa. Hänen mukaansa organisaatiot joutuvat miettimään, haluavatko he maksaa lunnaat, kykenevätkö ne siihen ja onko lunnaiden takaisinmaksaminen edes laillista?

Hyppösen keskustellessa organisaatioiden kanssa, jossa tätä asiaa mietitään, todettiin, että heillä on usein varmuuskopiot ja on testattu, että tiedot saataisiin nopeasti palautettua. Eli tietojen takaisin saamiseksi ei usein tarvitse maksaa lunnaita. Organisaatiot pohtivat, voivatko ne antaa rikollisten vuotaa esim. patenttihakemukset, sopimusneuvottelut ja sähköpostihistorian verkkoon. Hyppösen mukaan aluksi monet organisaatiot ovat todenneet, että se kirpaisee, mutta sen annetaan tapahtua kuitenkin. Tilanne on eri työntekijöiden henkilökohtaisten tietojen osalta esim. kirjeenvaihdossa on mukana sellaisia asioita kuin henkilökunnan sähköpostikirjeenvaihtoa työterveyshuollon kanssa. Tällöin organisaatio ei voi sallia vuotaa tietoja henkilökunnan sairauksista verkkoon. Tällaisessa tilanteessa on usein pakko maksaa lunnaat. Tämä trendi on johtanut siihen, että lunnaat yleensä maksetaan henkilöihin liittyvien tietojen pelastamiseksi.

Terveystiedot ovat muuttuneet hyökkäysten kohteeksi. Terveystietoja käsittelevät järjestelmät eivät ole missään päin maailmaa kauhean hyvin suojattu. Se ei ole ollut Hyppösen mukaan kauhean iso ongelma, koska valtaosa hyökkääjistä on rahan perässä. Historiallisesti eli ns. perinteisesti on ajateltu, että jos hyökkääjät ovat rahan perässä, niin he hyökkäävät pankkijärjestelmiin, maksujärjestelmiin, maksupäätteisiin, luottokorttitietoihin, palkanmaksujärjestelmiin ja finanssisysteemeihin eli paikkoihin, missä raha liikkuu. Voidaankin kysyä, miksi hyökkääjät menisivät varastamaan terveystietoja. Nyt tämä ns. vanha

trendi alkaa vähitellen hajoamaan ja terveystiedoista tulee tulevaisuudessa yhä suurempaa valuuttaa hakkereille.

Kolmas trendi Hyppösen mukaan on se, että kaikki tieto menee verkkoon. Ensimmäinen internet vallankumouksen aalto oli se, että kaikki tietokoneet menivät verkkoon ja se on jo tapahtunut eli se on jo historiaa. Käynnissä oleva toinen aalto vie kaiken muun myös esineet verkkoon. Ennen pitkää kaikki, mikä menee sähköverkkoon, menee myös tietoverkkoon. Suojautuminen on kovin vaikeata sen takia, koska kyseessä on usein tuotteita, joissa halvin tuote voittaa. Kun ostat esimerkiksi vatkainta, niin tärkein myyntiargumentti on hinta. Kukaan ei kysy, minkälainen tietoturva vatkaimessa on.

Se valmistaja, joka pistää vähiten rahaa tietoturvaan, saa halvimman tuotteen ja voittaa. Tämä on Hyppösen mielestä tietoturvan osalta vaikea yhtälö. Ainoa ratkaisu tähän, jonka Hyppönen keksi, on regulaatio. Hyppönen ei pitänyt regulaatiota optimaalisena vastauksena, koska hän ei pidä regulaatiosta, sillä se epäonnistuu usein. Miksi regulaatio sitten usein epäonnistuu? Tämä liittyy regulaation jäykkään rakenteeseen. Kun komitea miettii, miten me suojaamme kuluttajia tätä ongelmaa vastaan, niin lopputulos on yleensä aina puutteellinen tai epäonnistunut. Otetaan esimerkkinä evästelaki. Luultavasti sen tuloksena tullut popup-ikkuna vain harmittaa kuluttajaa. Ajatus on hyvä, mutta lopputulos on usein epäonnistuminen regulaatiossa. Regulaatio voi silti olla looginen IOT:n (Internet of Things) puolella. Kaikkea muuta reguloidaan vahvasti, mutta ei tietoturvallisuutta. Suomessakin on tehty töitä asian suhteen ja sen tuloksena on ns. Figoran tietoturvamerkki, joka mm. Philipsillä käytössä. Haasteena siinä on se, että se on saatavilla vain Suomessa ja se on vapaaehtoinen.

6.6 Organisaatioiden haasteet tietoturvakäytäntöjen noudattamisen valmentamiseen ja motivointiin

Hyppösen mukaan selkeänä haasteena on se, että käyttäjät eivät aina opi mitään. Minkä he oppivat, he unohtavat helposti saman tien. Saman opin tai ohjeen saa kertoa useaan kertaan, esimerkkinä älä käytä samaa salasanaa, joka paikassa ja kuitenkin ihmiset käyttävät samaa salasanaa monessa paikassa. Organisaatioissa monet menevät joka phishing-hyökkäykseen ja avaavat kaikki liitteet. Hyppösen mukaan rakennamme tietoturvaa sillä logiikalla, että käyttäjät suojelevat meitä hyökkäyksiltä ja me epäonnistumme joka kerta. Hyppösen mukaan pitäisi mahdollisimman paljon ottaa valtaa pois yksittäisiltä käyttäjiltä ja riskit pois käyttäjiltä. Järjestelmät tulisi ideaali tilanteessa rakentaa sellaisiksi, että käyttäjät saavat tehdä ns. virheklikkauksia, mutta vahinkoa ei synny. Tämä ei silti ole mahdollista, koska käyttäjät tekevät aina virheitä ja koska tällaisia systeemejä ei pystytä tekemään eikä käyttäjiin voida ikinä täydellisesti luottaa. Joudutaan miettimään parhaita käytäntöjä siitä, miten käyttäjiä voidaan motivoida ja kontrolloida.

Tiheästi toistuvat koulutukset ja testaaminen ovat Hyppösen mukaan ns. keppiratkaisuja. Porkkanaratkaisut, joita Hyppönen ja allekirjoittanut ovat nähneet, on se, mitä tehdään tietoturvafirma Hoxhuntissa, jossa tehdään hallittuja ja simuloituja tunkeutumistestausharjoituksia eli koulutetaan käyttäjiä tunnistamaan esim. phishing-sähköpostit, toimitusjohtajahuijaukset tai huijauspuhelinsoitot. Hoxhunt on yksi tietoturvapalvelujen tarjoaja, joka on pelillistänyt tunkeutumistestausharjoitukset.

6.7 Mikko Hyppösen best practices-käytännöt, joihin kaikkien organisaatioiden tulisi pyrkiä erityisesti hallinnollisen tietoturvan osalta

Hyppönen korosti erityisesti seuraavia best practices-käytäntöjä: päivitä, backuppaa, passwords eli lyhenteenä pbp. On tärkeää, että organisaatioissa tiedetään, mitä järjestelmiä niillä on käytössä ja mitä ohjelmistoja ajetaan. On tärkeää, että tiedetään työasemien lukumäärä ja tiedetään, mitä kaikkea niissä käytetään. On tärkeä tietää, mitkä softat ovat edelleen tuen piirissä, mitkä eivät ole. On tärkeää myös hankkiutua niistä ohjelmistoista aktiivisesti eroon, jotka eivät enää päivity. Muista järjestelmistä päivitetään ne, mitä voidaan ja tehdään se mahdollisimman nopeasti. Vain näillä päivityksillä on ensisijaisesti merkitystä.

Monessa organisaatiossa esim. Windows-päivitykset tulevat jopa puolen vuoden viiveellä. Silloin ei ole kauheasti enää väliä, jos joku hyökkäys on ollut 5 kuukautta aktiivisena. Laitteistoista luopuminen on paljon vaikeampaa ja järjestelmistä eroon pääseminen on todella vaikeaa. Järjestelmistä eroon pääseminen pitää tehdä oikein ja ne järjestelmät, jotka ovat vielä aktiivisessa käytössä, tulee päivittää säännöllisesti. Tähän tiivistyy Hyppösen ehdottama ensimmäinen toimenpide hallinnollisen tietoturvan varmistamisen osalta.

Toinen toimenpide on varmuuskopiointi eli backups. Varmuuskopiointi tuntuu itsestään selvältä toiminnalta, mutta sitä se ei Hyppösen mukaan todellakaan ole. Isoissakin organisaatioissa mennään pieleen tässä asiassa ja siihen ei ole kiinnitetty riittävästi huomiota ennen kuin nyt. Lunnastroijalaiset ovat pakottaneet testaamaan varmuuskopiot / backupit. Kun organisaatioilla on useita työasemia, kannettavia tietokoneita, palvelimia, AD-palvelimia, kännyköitä ja tabletteja, jotka on kryptattu, niin organisaatioille muodostuu ongelmaksi, miten tämä kokonaisuus nyt varmuuskopioidaan ja tarvittaessa palautetaan. Organisaatioilla ei välttämättä olekaan backuppeja kännyköistä, vaan pelkästään tietokoneista. Myös tyypillinen tilanne on, että backuppeja, voi olla hyvinkin kattavasti. Kun tulee tarve käyttää ja niitä lähdetään palauttamaan. Kun tietoja on palautettu pari päivää, niin havaitaan, että kauanko tässä oikein kestää tällä tahdilla ja huomataan, että palauttaminen vie merkittävästi aikaa esim. suuren tietomäärän palauttamisessa voi mennä 2 vuotta.

Organisaatioissa ei ole riittävästi testattu isojen palautusten kestoa. Riippuu, miten palauttaminen on toteutettu, mutta tämä 2 vuotta ei ole vitsi, vaan yhden suuren organisaation ihan oikea lopputulos. Kyseinen organisaatio päätyi maksamaan lunnaat, jotta tiedot saatiin nopeasti takaisin ja ettei tarvitse odottaa 2 vuotta. Tässä tapauksessa tiedot saadaan takaisin viikossa, kun maksetaan lunnaat. Silti, vaikka lunnaat maksetaankin ja saadaan purkutyökalut ja purkuavaimet, niin tietojen palauttaminen saattaa kestää kuukauden. Hyppösen toinen best-practice käytäntö liittyy siis Backup-kulttuuriin, varmuuskopioiden käyttöönottoon ja niiden palauttamisen testaamiseen.

Seuraavaksi keskitytään salasanaan eli Password. Hallinnollisen tietoturvan kannalta puhutaan enemmän autentikaatiokulttuurista. Miten työntekijät autentikoituvat eri verkkoihin, minkälaisia autentikaatioratkaisuja organisaatiolla on käytössä, minkälaiset single sign in-järjestelmät meillä on, minkälaisia autentikaatio-tokeneita tai sovelluksia käytetään, miten biometriikkaa voidaan hyödyntää. Autentikaatio on tärkeä aihe kokonaisuudessaan ja ytimenä miten yksittäinen käyttäjä saadaan irti siitä, että pitää keksiä itse salasanoja.

Mitä muuta organisaatioissa pitäisi tehdä? Läpinäkyvyys organisaation toimintoihin on tärkeää. Mitä meidän organisaatiossamme tapahtuu? Kuinka paljon koneita verkossa on juuri nyt? Mitä ne tekevät ja mikä on normaali tilanne organisaation verkossa? Hyppönen ajoi tässä takaa sitä, että organisaatiossa on selkeä ymmärrys siitä mikä on normaalia ja tapahtuuko verkossa jotain epänormaalia? Epänormaalia ei voida löytää, jos ei tiedetä, mikä on normaalia. Näkyvyys organisaatioissa ja sen verkon toiminnassa on tärkeää ja sisäverkkoajattelu on historiaa. Jotta näkyvyyttä pystytään hyödyntämään, pitää olla selkeät suunnitelmat, mitä tehdään, kun tulee poikkeustilanne, eli Incident response-suunnitelma. Tärkeintä Hyppösen mukaan, että mietitään organisaation sisällä, mitä tehdään ennen kuin on paniikki päällä.

Dokumentointi olisi hyvä best practices-käytäntöjen osalta. Kun firmaan tulee uusi CISO, (chief information security officer, tietoturvajohtaja), niin hänen ei tarvitse muuta kuin lukea dokumentointi manuaalit läpi ja ymmärtää, miten organisaatiossa toimitaan ja miten turvajärjestelmät toimivat, miten software lifecycle management on toteutettu organisaatiossa ja dokumentoitu. Näin ei ole Hyppösen mukaan monessakaan organisaatiossa ja kaikkea ei usein ole dokumentoitu riittävän hyvin.

Organisaatioissa pitäisi päästä siirtymään yhä enemmän sellaiseen malliin, että luottamus käyttäjän organisaation dataan tekemiin asioihin toimii. Tiettyjen laitteiden oikeudet ja kehittyneempi käyttäjän hallinnan malli ovat avainasioita tässä. Pitäisi siirtyä enemmän käyt-

täjä, - ja tilannelähtöiseen malliin. Esimerkkinä käyttäjä saa tehdä tietyn asian tietyssä järjestelmässä tiettyyn aikaan, mutta sama käyttäjä ei esim. aamuneljältä saa tehdä tiettyä asiaa. (Haastattelu H9.)

7 Yhteenveto ja mitä opin opinnäytetyötä tehdessäni

Pienemmät organisaatiot eivät pysty panostamaan hallinnolliseen tietoturvaan samalla tavalla kuin isommat organisaatiot. Pienemmissä organisaatioissa kyllä järjestettiin tietoturvakoulutus ja useimmiten organisaatio oli palkannut tietoturvavastaavan huolehtimaan tietoturvasta, mutta ei oltu aina täysin varmoja lisäkoulutuksen tarpeesta. Pienemmissä organisaatioissa ei oltu aina täysin varmoja organisaation tietoturvan nykytilasta.

Suurin osa pienempien organisaatioiden työntekijöistä ei tehnyt töitä tietoturvan parissa, vaan he olivat enemmänkin ns. rivityöntekijöitä. Tämä ei kuitenkaan koskenut vain pienempiä, mutta myös isompia organisaatioita.

Kahdeksasta haastateltavasta kolme arvioi organisaatioidensa tietoturvan nykytilan olevan todennäköisesti ihan ok, suhteellisen hyvä ja hyvin hallussa. Heidän organisaatioissaan oli myös käytössä kaksivaiheinen tunnistautuminen. Suurimmat organisaatiot pystyvät panostamaan hallinnolliseen tietoturvaan huomattavasti paremmin kuin pienemmät organisaatiot.

Tietomurron sattuessa toimintatavat poikkesivat huomattavasti toisistaan eri organisaatioissa. Kaikille organisaation työntekijöille ei oltu myöskään annettu selkeitä toimintaohjeita. Tämä vaihteli eri organisaatioiden välillä. Haastattelujen perusteella suurimmilla organisaatioilla oli toimintaohjeet tietomurron varalta. Kaksi haastateltavaa korostivat yhteydenoton tärkeyttä esimieheen, asiakastietojärjestelmään, sähköpostitarjoajaan ja IT-tukeen tietomurron sattuessa. Myös hyökkäyksen kohteeksi joutuneen henkilön informoinnin tärkeyttä korostettiin. Tärkeimpinä toimenpiteinä korostettiin myös salasanojen vaihtamista, uloskirjautumista kaikilta tileiltä ja kaksivaiheisen tunnistautumisen käyttöönottoa.

Suurimmissa organisaatioissa työntekijöille järjestettiin kaikille työntekijöille pakolliset yritysturvallisuuden ja tietoturvallisuuden verkkokurssit. Tämän lisäksi useimmissa suurimmissa organisaatioissa toimi erillinen turvallisuudesta vastaava tiimi. Tämä ei ollut mahdollista kaikkien organisaatioiden osalta. H6 totesi, että hänen työpaikallaan luotetaan työntekijöihin tietoturvaan liittyvissä asioissa. Mielestäni tässä on havaittavissa sekä mahdollisuus että uhka. Mahdollisuutena on, että jos työntekijöille on annettu selkeät ohjeet ja he noudattavat niitä, niin tietomurtoja ei tapahdu ja ulkopuolista apua ei tarvita. Uhkana on se, että jos työntekijöille ei olla annettu selkeitä toimintaohjeita tietoturvan osalta ja he eivät tiedä, mitä tulee tehdä tietomurron sattuessa, luotto työntekijöihin ja organisaatioon kärsii ja tietoturvaiskujen riski kasvaa.

Organisaatioiden parhaiden tietoturvakäytäntöjen osalta useimpien haastateltavien vastauksissa korostuivat kaksivaiheinen tunnistautuminen ja vahvojen salasanojen käyttö. Lisäksi korostettiin koulutuksen tärkeyttä tietoturvan osalta sekä työntekijöiden vastuuta oman yksikkönsä toimintatavoista ja periaatteista.

Useimmissa organisaatioissa parhaat käytännöt jalkautettiin koulutuksen avulla. Tosin kaikissa organisaatioissa koulutuksia ei ollut järjestetty ja kaksi haastateltavaa ei tiennyt, tapahtuuko heidän organisaatiossaan parhaiden käytäntöjen jalkauttamista organisaation toimintaan. Useimmissa tapauksissa tietoturvaan liittyvät asiat ja päivitykset tulivat organisaation IT-osastolta tai IT-taholta. Koulutuksen tarpeesta oli myös puhuttu muutamissa organisaatioissa, mutta sitä ei vielä ollut järjestetty.

Tietoturvariskien kartoittamisen osalta vain kahdessa organisaatiossa oli toteutettu tietoturvariskien kartoitus. Useimmat haastateltavista eivät tienneet, onko heidän organisaatiossaan toteutettu tietoturvariskien kartoitusta tai onko siitä olemassa jonkinlaista suunnitelmaa.

Useimmissa organisaatioissa oli olemassa kirjalliset ohjeet tai hallintasuunnitelma tietoturvariskien varalta. Vain osassa organisaatioissa ei ollut ohjeita tai haastateltavat eivät olleet varmoja siitä, onko niitä olemassa. Tämä on mielestäni iso ongelma ja haaste, johon organisaatioon olisi syytä panostaa. Työntekijöiden tulee tietää, onko heidän organisaatiossaan olemassa tietoturvariskien hallintasuunnitelma tai jotain muuta kirjallista ohjeistusta tietoturvariskien osalta.

Vain kahdessa organisaatiossa oli toteutettu tietoturvauhkiin liittyviä käytännön harjoituksia. Osa haastateltavista kannatti kyseistä koulutusmallia, kun taas osa ei ollut varma siitä, pitäisikö kyseisiä koulutuksia järjestää vai ei. Heidän vastauksissaan korostui epävarmuus koulutusmallin osalta.

Yhteisesti sovittujen tietoturvakäytänteiden noudattamista ei haastattelujen mukaan seurattu useimmissa organisaatioissa. Heidän mukaansa seurantaa ja mittaamista pitäisi tapahtua organisaatioissa. Vain kahdessa organisaatioissa seuraamista tapahtui jatkuvan koulutuksen ja erilaisten mittarien avulla kuten myös sekä sisäisten että ulkoisten auditointien kautta. Herää kysymys, miksi tietoturvakäytänteiden noudattamista ei seurattu useimmissa organisaatioissa?

Useimmat haastateltavat eivät tienneet, mitataanko heidän organisaatioissaan yhteisesti sovittujen tietoturvaohjeiden noudattamisen vaikuttavuutta. Vain yhdessä organisaatiossa mittaamisessa hyödynnettiin testejä osana jatkuvaa koulutusta. Miksi haastateltavat eivät

tienneet, tapahtuuko heidän organisaatioissaan yhteisesti sovittujen tietoturvaohjeiden noudattamisen vaikuttavuuden mittaamista?

Useimmat haastateltavat kokivat tietoturvavalmennuksen tarpeellisena. Kaksi haastateltavista olivat tyytyväisiä heidän organisaatioissaan olemassa oleviin koulutuksiin ja käytäntöihin ja niiden arveltiin riittävän. Tämä on mielestäni iso tietoturvariski, sillä koronan aiheuttaman poikkeustilanteen takia hakkereiden tekemät tietoturvahyökkäykset ovat lisääntyneet ja hyökkäyksistä on tullut entistä hienostuneempia ja vaikeampia havaita. Ovatko olemassa oleva koulutus ja käytännöt riittäviä?

Useimmissa organisaatioissa oltiin varauduttu tietoturvauhkien jatkuviin muutoksiin koulutuksen avulla. Muutamissa organisaatioissa oli käytössään tietoturvasta vastaava tiimi tai tietoturvasta vastaava yksittäinen taho kuten esimerkiksi yritysturvallisuuspäällikkö. Näen myös tässä sekä mahdollisuuden että uhan. Mahdollisuutena on, että organisaation työntekijöiden ei tarvitse huolehtia tietoturvasta, sillä ulkopuolinen henkilö tai tiimi hoitaa sen heidän puolestaan. Uhkana taas on, että jos ulkopuolinen henkilö tai taho hoitaa tietoturvaan liittyvät asiat heidän puolestaan, he eivät opi itse huolehtimaan tietoturvaan liittyvistä asioista ja saattavat sortua ns. amatöörin virheisiin tietoturvaan liittyen. Myös tietoturvasta vastaava tiimi tai tietoturvasta vastaava yksittäinen taho kuten esimerkiksi yritysturvallisuuspäällikkö saattavat tehdä virheitä ja virhearvioita tietoturvan osalta ja jos työntekijät luottavat heihin sokeasti, niin he saattavat koko organisaationsa vaaraan tietoturvan osalta.

Useimmilla organisaation työntekijöiden tehtävänä oli seurata yhteisistä sovittuja ohjeita. Useimmiten organisaatioissa ei ollut tietoturvavastaavaa, jolloin kaikki työntekijät joutuvat kantamaan oman vastuunsa tietoturvasta. Tässä haasteena on se, että jos työntekijöitä ei ole koulutettu riittävästi ja yhteisesti sovittuja tietoturvaohjeita ei ole, niin he todennäköisesti tekevät jotain, joka vaarantaa pahimmassa tapauksessa koko organisaation tietoturvan.

Useimmat haastateltavista olivat tyytyväisiä organisaationsa tietoturvan nykyiseen tasoon. Vain kaksi heistä toivoi, että heidän hallinnolliseen tietoturvaosaamiseensa panostettaisiin enemmän. Herää kysymys, tyytyvätkö organisaatioiden työntekijät liian helposti nykyiseen osaamiseensa ja kokevat he, että lisäkoulutukselle ei olisi tarvetta tai sen järjestäminen koetaan liian vaivalloiseksi tai kalliiksi. Osa haastateltavista tyytyi myös mielestäni liian helposti nykyiseen tietoturvaosaamiseensa eivätkä kokeneet tarvetta lisäkoulutukselle. Tämä on erittäin suuri haaste, sillä jo nyt tietoturvan merkitys on kasvanut valtavasti ja tulee kasvamaan tulevaisuudessa entistä suuremmaksi.

Haastattelujen perusteella tietoturvauhat ovat helposti edellä tietosuojatoimenpiteitä. Yksi hyvä keino uhkien estämiseksi on valkohattuhakkerointi. Haastateltavat korostivat vastauksissaan yleisiä ohjeita tietoturvaan liittyen: älä koskaan jaa salasanoja ja käyttäjänimiä, käytä aina kaksivaiheista tunnistautumista, organisaation tulee laatia kaikkia tiimin jäseniä koskevat kirjalliset ohjeet ja käytännöt, joita tulee noudattaa, organisaation tulee kouluttaa kaikki työntekijänsä. Organisaatiossa on myös tiedotettava tietoturvaongelmista.

Vain yksi haastateltava tiesi, minkälaisia työkaluja on olemassa tunkeutumistestauksen simulointia varten. Miksi näin on? Eivätkö organisaatioiden tietoturva-vastaavat kerro organisaatioiden työntekijöille, minkälaisia työkaluja heillä on käytössä tunkeutumistestauksen simulointia varten vai onko niitä ollenkaan?

Päätarkoitukseni opinnäytetyössäni oli luoda best practices-käytännöt tietoturvan osalta ja niiden jalkauttamisen osalta eri organisaatioille. Tekemieni haastattelujen perusteella selvisi, että kaikissa organisaatioissa ei oltu onnistuttu luomaan kyseisiä käytäntöjä. Myös koulutus on ollut puutteellista ja yhteisesti sovittuja tietoturvaan liittyviä yhteisiä ohjeita ja sääntöjä ei ollut tehty. Tämä ongelma korostui erityisesti pienempien organisaatioiden osalta. Isoimmissa organisaatioissa sama ongelma ei toistunut, mutta jotkut isompien organisaatioiden työntekijöistä tyytyivät haastattelujen perusteella liian helposti nykyiseen tietoturvaosaamiseensa. Useimmissa haastateltavieni organisaatioissa oli selkeät tietoturvasäännöt ja ohjeet, joita kaikki noudattivat ja hallinnollisen tietoturvan jalkautus oli onnistunut hyvin. Tosin kaikissa organisaatioissa tietoturvan yhteisten sääntöjen ja ohjeiden jalkauttaminen ei ollut onnistunut hyvin tai se oli jäänyt puolitiehen. Eräät organisaatioiden edustajat eivät olleet myöskään tietoisia siitä, oliko tietoturvan jalkauttaminen organisaatioon onnistunut ja oliko organisaatioissa yhteisesti sovittuja tietoturvakäytäntöjä- ja ohjeita.

Lähteet

Cox BLUE/Cyber Security. Luettavissa: https://www.coxblue.com/category/cyber-security/ Luettu: 09.02.2022.

CYBEREXPERTS.com/Cyber Security. Luettavissa: https://cyberexperts.com/category/cybersecurity/ Luettu: 09.02.2022.

Grönfors, Matti
1985 Kvalitatiiviset kenttätyömenetelmät. Juva: WSOY 1985.

Haaga-Helia ammattikorkeakoulu 2021. Cloud Service Technologies, ICT4TF024. Module 4. Luettu: 28.02.2021.

Haastattelut H1-H9. Tutkijan hallussa.

Helsingin Sanomat 10.01.2021 ja 16.01.2021. Luettu: 02.02.2022.

Hirsjärvi, Sirkka & Hurme, Helena
2000 Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino 2000.

Hirsjärvi, Sirkka & Remes, Pirkko & Sajavaara, Paula
2003 Tutki ja kirjoita. Helsinki: Tammi 2003.

Hyppönen, Mikko
2020 Tietoturva tänään-webinaari. Katsottavissa: https://www.youtube.com/watch?v=YNvur8b3Q9s Katsottu: 01.12.2020.

Hyppönen, Mikko
2021 Internet. Werner Söderström Osakeyhtiö Helsinki 2021.

KvaliMOTV. Luettavissa: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_3.html Luettu: 14.11.2021.

Kyberturvallisuus. Luettavissa: https://fi.wikipedia.org/wiki/Kyberturvallisuus Luettu: 02.01.2021.

Laadullinen tutkimus – Jyväskylän yliopisto. Luettavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus Luettu: 14.11.2021.

Lynskey, D. 09.10.2019. 'Alexa, are you invading my privacy?' – the dark side of our voice assistants. Luettavissa: https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants Luettu: 02.02.2022.

MTV Uutiset 28.02.2022 Anonymous hakkeroi venäläisiä uutismedioita – lue sanasta sanaan, millainen viesti ilmestyi yhtäkkiä ruudulle. Luettavissa: https://www.mtvuutiset.fi/artikkeli/anonymous-hakkeroi-venalaisia-uutismedioita-lue-sanasta-sanaan-millainen-viesti-ilmestyi-yhtakkia-ruudulle/8366510 Luettu: 06.03.2022.

Norton. Luettavissa: us.norton.com Luettu: 09.02.2022.

TIETOSUOJAVALTUUTETUN TOIMISTO/Tietosuoja. Luettavissa: https://tietosuoja.fi/gdpr Luettu: 02.02.2022.

Ruusuvuori, Johanna & Tiittula, Liisa (toim.)
2009 Haastattelu. Tutkimus, tilanteet ja vuorovaikutus. Osuuskunta Vastapaino, Tampere 2009.

Savonen, T. 30.10.2019. Tor-verkko nousee esiin rikosten yhteydessä – Useimmat käyttötavat laillisia. Luettavissa: https://www.kansanuutiset.fi/artikkeli/4356780-tor-verkko-nousee-otsikoihin-rikosten-yhteydessa-useimmat-kayttotavat-laillisia Luettu: 06.03.2022.

Tuomi, Jouni & Sarajärvi, Anneli
2006 Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi 2006.

Liitteet

Liite 1 Haastattelukysymykset/kaikki muut haastateltavat paitsi Mikko Hyppönen

Miten kuvaisitte organisaationne tietoturvan nykytilaa?

Jos yritykseenne tehtäisiin tietomurto, miten sinä toimisit ja onko sinulle/teille annettu toimintaohjeet?

Mitkä ovat mielestänne organisaationne parhaat tietoturvakäytännöt?

Miten organisaationne parhaat käytännöt jalkautetaan organisaationne hyväksi?

Kuvaile miten organisaatiossanne on suoritettu tietoturvariskien kartoitus? Jos koette, että kartoituksessa olisi parantamisen varaa, mitä ehdottaisitte?

Onko organisaatiossanne tietoturvariskien hallintasuunnitelmaa tai valmista vastaavaa kirjallista ohjeistusta tietoturvariskien osalta?

Kuvaile miten organisaatiossanne on toteutettu tietoturvauhkiin liittyviä käytännön harjoituksia? Jos koette, että tietoturvauhkiin liittyvissä käytännön harjoituksissa olisi parantamisen varaa, mitä ehdottaisitte?

Miten organisaatiossanne seurataan yhteisesti sovittujen tietoturvakäytänteiden noudattamista?

Miten mitataan noudattamisen vaikuttavuutta?

Jos organisaatiossanne yhdistettäisiin koulutus, jalkauttaminen ja mittaaminen ja ne suoritettaisiin tietoturvavalmennuksena, kokisitteko sen tarpeelliseksi?

Miten organisaatiossanne on varauduttu tietoturvauhkien jatkuviin muutoksiin?

Mikä on roolisi organisaationne tietoturvan osalta?

Haluaisitko, että sinun hallinnolliseen tietoturvaosaamiseesi panostettaisiin enemmän?

Ovatko tietoturvauhat aina helposti edellä tietosuojatoimenpiteitä? Miksi? Jos näin on, mitä ehdottaisit, että pitäisi tehdä?

Mitä best practices-käytäntöjä tietoturvan osalta ehdottaisit kaikkiin organisaatioihin (yhtiöt, säätiöt, seurakunnat)? Miksi?

Mitä valmiita työkaluja on tunkeutumistestauksen simulointia varten?

Minkälaista checklistiä ehdottaisit jokaiseen organisaatioon tietoturvatoimenpiteiden osalta?

Liite 2

Haastattelukysymykset Mikko Hyppöselle

Covid on lisännyt etätyön merkitystä huomattavasti ja mahdollisesti pysyvästi. Mitkä ovat mielestäsi Covidin myötä lisääntyneen etätyön aiheuttamat merkittävimmät muutokset organisaatioiden tietoturvakäytäntöihin? Tai mitä niiden tulisi ideaali tilanteessa olla?

Minkälaisia uusia tietoturvahyökkäyksien muotoja ja uhkia on odotettavissa tai trendejä havaittavissa tällä hetkellä? Miten niihin tulisi valmistautua erityisesti hallinnollisen tietoturvan näkökulmasta?

Miten organisaatioiden tulisi valmentaa ja motivoida työntekijöitään sovittujen tietoturvakäytäntöjen noudattamiseksi?

Yhteenvetona, mitkä ovat mielestäsi tietoturvan 5–10 best practices-käytäntöä, joihin kaikkien organisaatioiden tulisi pyrkiä, erityisesti hallinnollisen tietoturvan osalta?

Liite 3

Ehdotuksia tietoturvan best practices-käytännöistä organisaatioille

Suojaa tietosi

Päivittäisessä elämässäsi vältät todennäköisesti henkilökohtaisten tunnistetietojen jakamista, kuten sosiaaliturvatunnuksesi tai luottokorttinumerosi, kun vastaat ei-toivottuun

sähköpostiin, puheluun, tekstiviestiin tai pikaviestiin. On tärkeää noudattaa samaa varovaisuutta työssä. Muista, että verkkorikolliset voivat luoda sähköpostiosoitteita ja verkkosivustoja, jotka näyttävät laillisilta. Huijarit voivat väärentää soittajan tunnistetietoja. Hakkerit voivat jopa ottaa haltuunsa yrityksen sosiaalisen median tilit ja lähettää näennäisesti laillisia viestejä.

On tärkeää olla vuotamatta yrityksesi tietoja, arkaluontoisia tietoja tai immateriaalioikeuksia. Jos esimerkiksi jaat kuvan verkossa, joka näyttää taulun tai tietokoneen näytön taustalla, saatat vahingossa paljastaa tietoja, joita yrityksen ulkopuolisten ei pitäisi nähdä.

Kunnioita samalla tavalla myös muiden yritysten henkistä omaisuutta. Vaikka se olisikin vahinko, niin muiden yritysten IP-osoitteen tai liikesalaisuuksien jakaminen tai käyttäminen voi saada sinut ja yrityksesi vaikeuksiin.

Yrityksesi voi auttaa suojaamaan työntekijöitään, asiakkaitaan ja tietojaan luomalla ja jakamalla liiketoimintakäytäntöjä, jotka kattavat aiheita, kuten miten tuhota tarpeettomia tietoja ja kuinka ilmoittaa epäilyttävistä sähköposteista tai lunnasohjelmista.

Vältä pop-up ikkunoita, tuntemattomia sähköposteja ja linkkejä

Varo tietojenkalastelua. Tietojenkalastelijat yrittävät huijata sinua klikkaamaan linkkiä, joka voi johtaa tietoturvaloukkaukseen.

Tietojenkalastelijat saalistavat työntekijöitä toivoen, että he avaavat ponnahdusikkunoita tai muita haitallisia linkkejä, joissa voi olla viruksia ja haittaohjelmia. Siksi on tärkeää olla varovainen lähettäjien lähettämien sähköpostiviestien linkkien ja liitteiden suhteen. Yhdellä klikkauksella voit antaa hakkereille mahdollisuuden tunkeutua organisaatiosi tietokoneverkkoon.

Älä koskaan kirjoita henkilökohtaisia tietoja tai yritystietoja vastauksena sähköpostiin, ponnahdusikkunan verkkosivustoon tai muuhun viestintämuotoon, jota et ole aloittanut. Tietojenkalastelu voi johtaa identiteettivarkauteen. Se on myös tapa, jolla useimmat ransomware-hyökkäykset tapahtuvat.

Yrityksesi voi auttaa käyttämällä sähköpostitodennustekniikkaa, joka estää nämä epäilyttävät sähköpostit. Sinulle ilmoitetaan yleensä, että sähköposti on lähetetty karanteenikansioon, jossa voit tarkistaa, onko se laillinen vai ei.

Ole varovainen. Jos et ole varma sähköpostin tai muun viestin laillisuudesta, ota aina yhteyttä turvallisuusosastoon tai turvallisuusjohtoon.

Käytä vahvaa salasanasuojausta ja vahvaa tunnistautumista

Vahvat, monimutkaiset salasanat voivat estää kybervarkaita pääsemästä yrityksen tietoihin. Yksinkertaiset salasanat helpottavat kybervarkaiden sisäänpääsyä. Jos kyberrikollinen selvittää salasanasi, se voi antaa heille pääsyn yrityksesi verkkoon. Tästä syystä monimutkaisten salasanojen luominen on tärkeää.

Vahva salasana sisältää vähintään 10 merkkiä ja se sisältää numeroita, symboleita kuten myös isoja ja pieniä kirjaimia. Yritysten tulisi pyytää työntekijöitään vaihtamaan salasanoja säännöllisesti. Salasanojen muuttaminen ja muistaminen voi olla hankalaa. Salasanojen hallintaohjelmasta voi olla hyötyä niiden muistamisessa.

Yritykset voivat myös vaatia vahvaa tunnistautumista, kun työntekijä yrittää käyttää arkaluontoisia verkkoalueita. Se voi olla esimerkiksi väliaikainen koodi, joka löytyy työntekijän puhelimesta. Tämä parantaa yrityksien tietoturvaa.

Käytä varmistettua Wi-Fi-yhteyttä

Wi-Fi-yhteyksien tulisi olla turvattuja, salattuja ja piilotettuja. Jos työskentelet etänä voit suojata tietosi käyttämällä VPN:nää eli virtuaalista ja yksityistä verkkoa. VPN on elintärkeä työskenneltäessä toimiston ulkopuolella tai liikematkalla. Julkiset Wi-Fi-verkot voivat olla riskialttiita ja ne voivat vaarantaa tietojesi turvallisuuden.

On hyvä pitää mielessä, että jotkut VPN:nät ovat turvallisempia kuin toiset. Jos yrityksellläsi on VPN, pidä huoli siitä, että osaat käyttää sitä oikein. Muun muassa Norton Secure VPN tarjoaa vahvaa VPN-suojausta, joka auttaa pitämään tiedot yksityisenä julkisessa Wi-Fi-verkossa.

Varmista palomuurisuojaus töissä ja kotona

Palomuurin hankkiminen on yksi tärkeimmistä hankinnoista tietoturvan kannalta ja yksi tärkeimmistä puolustustekniikoista kyberhyökkäyksessä. Palomuurit estävät luvattomat pääsyt nettisivuille, sähköpostipalvelimille ja muille netin kautta saavutettaville tiedon lähteille. Se estää tietoturvarikollisia pääsemästä yrityksesi verkkosivuille ja tietokantoihin. Älä luota pelkästään siihen, että yrityksellläsi on palomuuri. On suositeltavaa asentaa palomuuri myös kotiverkkoon.

Kaikkien organisaatioiden tulisi asentaa palomuuri, joka estää tietojen päätymisen vääriin käsiin. Ulkoisen palomuurin lisäksi monet yritykset ovat alkaneet asentaa sisäisiä palomuureja lisäsuojan tarjoamiseksi. On myös tärkeää, että ne yrityksen työntekijät, jotka työsken-

televät kotona, asentaisivat palomuurin myös kotiverkkoonsa. Internetin turvallisuuspalveluiden tarjoajilta saa tietoa erilaisista palomuureista. Myös yritykset tarjoavat työntekijöilleen palomuurin asennuspalveluja.

Sijoita tietoturvajärjestelmiin

Pienemmät yritykset saattavat epäröidä, kun on kyse investoinnista tietoturvaan. Tämä sisältää yleensä vahvat virusten ja haittaohjelmien havaitsemiseen tarkoitetut ohjelmat, ulkoiset kovalevyt varmuuskopiointia varten ja säännölliset tietoturvaprotokollan läpikäynnit. Tämän sijoituksen tekeminen voi pelastaa yrityksiä ja työntekijöitä mahdollisilta taloudellisilta ja oikeudellisilta haitoilta.

Kaikissa laitteissa, joita käytetään töissä ja kotona, tulisi olla päivitetty tietoturvaohjelmisto. Yritykselle on tärkeää tarjota tietoturvaa työpaikalla ja ottaa tarvittaessa yhteyttä IT-osastoon tai tietoturvavastaavaan, mikäli rikkeitä ilmenee. Mitä nopeammin rikkeet raportoidaan, sitä parempi.

Asenna tietoturvasoftan päivitykset ja varmuuskopioinnit

Tietoturvan parhaimpien käytäntöjen seuraaminen tarkoittaa sitä, että tietoturvapalvelimia, Internet-selaimia ja käyttöjärjestelmiä päivitetään jatkuvasti, jotta ne pystyvät torjumaan kaikki kyberuhat.

Mikäli yrityksesi lähettää ohjeita tietoturvapäivityksistä, ne tulisi asentaa välittömästi. Tämä koskee myös työpaikalla käytettäviä henkilökohtaisia laitteita. Säännölliset päivitykset torjuvat kyberuhkia.

Tietoturvan ja omien henkilökohtaisten tietojen varmuuskopioiminen ja turvaaminen on olennaisen tärkeää turvallisuuden varmentamiseksi ja tietoturvaiskujen välttämiseksi. Yrityksellä tulisi olla ohjeet siitä, miten ja minne tieto tallennetaan. Tärkeät tiedostot ja kansiot voidaan tallentaa mm. pilveen tai ulkoiselle kovalevylle.

Koulutuksen ja vuoropuhelun jatkuva järjestäminen IT-osaston kanssa

IT-osastosi on ystäväsi. Vuoropuhele yrityksesi tukitiimin kanssa tietoturvasta. Teillä saattaa olla paljon puhuttavaa.

IT-osaston kanssa työskenteleminen kannattaa esimerkiksi silloin, kun palvelimeen kohdistuva päivitys ei onnistu. Ei pidä tehdä yksinkertaisesta ongelmasta vielä monimutkaisempaa yrittämällä korjata sitä itse. Sen sijaan kannattaa antaa IT-osaston hoitaa asia. On myös

fiksua raportoida kaikki mahdolliset tietoturvaan liittyvät vaarat IT-tuelle, sillä he eivät välttämättä ole tietoisia kaikista mahdollisista uhista.

Matkustaessa on tärkeää olla yhteydessä IT-tukeen. Ennen kuin lähdet, kannattaa asiasta mainita IT-osastolle erityisesti silloin, jos käytät julkista Wi-Fi-yhteyttä. Nauti matkastasi, mutta älä unohda VPN:nää.

Varmista myös, että IT-tukiosasto on oikea. Varo huijareita, jotka teeskentelevät olevansa yrityksesi IT-tuen edustajia. Saatat saada tietojenkalastelusähköpostin joltakulta, joka väittää olevansa yrityksesi IT-tuen edustaja. Tavoitteena on saada sinut asentamaan haittaohjelma koneellesi tai mobiililaitteellesi tai luovuttaa yrityksen kannalta elintärkeää tietoa. Tällaisissa tilanteissa heille ei tule tarjota mitään informaatiota. Sen sijaan tulee ottaa yhteyttä IT-tukeen välittömästi.

Säännöllinen auditointi; kolmannen osapuolen suorittama valvonta

Yleensä tietoturvaongelmat alkavat yritysten sisällä. Tästä syystä yritysten on tarkkaan harkittava sitä, mitä tietoja työntekijät saavat käsitellä ja mihin heillä on pääsy.

Yrityksen työntekijänä saatat olla vastuussa yrityksen asiakkaiden ja työntekijöiden tiedoista. Mikäli näin on, sinun tulee noudattaa yrityksen ohjeita siitä, miten arkaluontoista tietoa tulee käsitellä. Mikäli olet vastuussa tietojen varmuuskopioiden suojelemisesta, sinun tulee suojella kyseisiä tietoja yrityksen ulkopuolisilta henkilöiltä.

Yritykset ja niiden työntekijät saattavat joutua myös valvomaan kolmansia osapuolia kuten konsultteja tai aiempia työntekijöitä, joilla on väliaikainen pääsy yrityksen tietoverkkoon. On tärkeää rajoittaa näiden henkilöiden pääsyä tietyille alueille ja deaktivoida pääsy välittömästi, kun he ovat saaneet työnsä valmiiksi.

Organisaation itse järjestämät säännölliset hyökkäykset

Viisaat yritykset käyttävät aikaa työntekijöidensä kouluttamiseen. Työntekijänä sinun tulee tietää yrityksesi tietoturvaohjeistukset, yrityksesi odotukset tietoturvan osalta ja seurata niitä.

Tässä on esimerkki. Saatat käyttää älykelloa työpaikallasi. On tärkeää suojella henkilökohtaisia laitteitasi päivitetyllä tietoturvalla. Sinun tulee myös tietää ja seurata yrityksesi ohjeita hyväksytyistä elektronisista välineistä. Kun tuot työpaikallesi oman laitteesi, kysy IT-osastoltasi, onko sinulla oikeutta käyttää yrityksen tietoja omalla koneellasi ennen niiden lataamista. Käytä aina laillisia applikaatioita tutkiessasi yrityksen kannalta tärkeitä dokumentteja.

Se, miten tietotekniikka voi muodostaa yhteyden sinun laitteisiisi, on hyvä osata. Tämä tieto voi säästää aikaa ottaessa yhteyttä IT-tukeen omien laitteiden osalta.

Mikäli haluat tallentaa tietoja pilveen, keskustele ensin IT-tuen kanssa siitä, mitkä pilvipalvelut ovat hyväksyttyjä. Jos tallennat tietoja pilvipalvelimeen, jota yritys, jossa työskentelet, ei hyväksy, voit joutua vaikeuksiin. (us.norton.com).

Dokumentoi tietoturvatoimenpiteet ja käytännöt

Vaikka pienyritykset toimivat usein suullisesti ja intuitiivisesti, kyberturvallisuus on yksi alueista, jonka osalta on välttämätöntä dokumentoida protokollat. Pienyritysten hallinnon kyberturvallisuusportaali tarjoaa verkkokoulutusta, tarkistuslistoja ja tietoja verkkoyritysten suojaamiseksi. FCC:n Cyberplanner 2.0 tarjoaa lähtökohdan suojausasiakirjallesi. Harkitse myös osallistumista pienyritysten vapaaehtoiseen C3-ohjelmaan, joka sisältää yksityiskohtaisen työkalupakin kyberturvallisuuden parhaiden käytäntöjen ja tietoturvakäytäntöjen määrittämiseksi ja dokumentoimiseksi.

Suunnitelma/ohjelma mobiililaitteille

59 prosenttia yrityksistä sallii tällä hetkellä BYOD:n eli ajatuksen siitä, että työpaikalle saa tuoda omia laitteita. Siksi onkin välttämätöntä, että yrityksillä on dokumentoitu BYOD-käytäntö, joka keskittyy turvatoimiin. Erilaisten älylaitteiden suosion lisääntyessä on tärkeää sisällyttää nämä laitteet osaksi yritysten tietoturvakäytäntöjä. Symantecin Norton suosittelee myös, että pienyritykset vaativat työntekijöitä asentamaan automaattiset tietoturvapäivitykset ja että yrityksen salasanakäytäntö koskee kaikkia verkkoon pääseviä mobiililaitteita.

Kouluta kaikki työntekijät

On välttämätöntä, että kaikille verkkoon pääseville työntekijöille annetaan koulutusta yrityksen verkkoturvallisuuden ja tietoturvan käytännöistä.

Koska käytännöt kehittyvät, on välttämätöntä saada säännölliset päivitykset uusiin protokolliin. Pyydä työntekijöitä pitämään huolta siitä, että jokainen heistä allekirjoittaa asiakirjan, jossa ilmoitetaan, että heille on ilmoitettu käytännöistä, ja ymmärtää, että toimenpiteisiin voidaan ryhtyä, jos he eivät noudata turvallisuuskäytäntöjä.

Varmista turvalliset salasanakäytännöt

Moni työntekijä pitää salasanojen vaihtamista vaivalloisena. Salasanoja tulisi kutenkin vaihtaa säännöllisesti, sillä 63 prosenttia tietoturvaloukkauksista tapahtui kadonneiden, varastettujen tai heikkojen salasanojen takia. Tästä huolimatta 65 prosenttia salasanakäytäntöä käyttävistä pk-yrityksistä ei vaadi työntekijöiltään salasanojen säännöllistä vaihtamista. Tämän päivän Tuo Omat Laitteesi-maailmassa on välttämätöntä, että kaikki yritysverkkoon pääsevät työntekijöiden laitteet on suojattu salasanalla.

Viimeisimpien käytäntöjen ja ohjeiden mukaan salasanojen tulisi sisältää isoja ja pieniä kirjaimia, numeroita ja symboleita. Pk-yritysten tulisi vaatia kaikkien salasanojen vaihtamista 60–90 päivän välein.

Varmuuskopioi säännöllisesti kaikki data

On tärkeää estää mahdollisimman monta tietoturvahyökkäystä. Tästä huolimatta niitä voi silti tapahtua. Suositeltavaa on tekstinkäsittelyasiakirjojen, sähköisten laskentataulukoiden, tietokantojen, rahoitustiedostojen, henkilöstötiedostojen ja myyntisaamisten / maksettavien tiedostojen varmuuskopioiminen. Myös kaikki pilveen tallennetut tiedot tulisi varmuuskopioida. Varmuuskopiot tulee tallentaa erilliseen paikkaan esimerkiksi tulipalon tai tulvan varalta.

Varmuuskopiointi on paras ratkaisu henkilökohtaisten tietojen ja yritystietojen turvaamiseen. Yksi suurimmista tietoa uhkaavista tekijöistä on haittaohjelma eli ns. lunnasohjelma. Kyseessä on ohjelma, joka aktivoituu, kun työntekijä klikkaa haitallisia linkkejä. Ohjelma ikään kuin ottaa tietoja panttivangikseen. Saadakseen tietonsa takaisin uhrin on maksettava lunnaat. Useimmiten lunnasohjelmien kohteena ovat yritykset, mutta viime aikoina niiden kohteena ovat olleet myös yksittäiset henkilöt. Nämä hyökkäykset voidaan välttää ainoastaan varmuuskopioinnin avulla.

Asenna virustorjuntaohjelma

On väärin olettaa, että työntekijät tietävät, ettei tietojenkalastelusähköposteja saa koskaan avata. Vuonna 2016, 30 prosenttia työntekijöistä avasi verkkourkintasähköpostit. Tämä on 7 prosenttia enemmän kuin vuonna 2015. Koska tietojenkalasteluhyökkäykset sisältävät haittaohjelmien asentamisen työntekijän tietokoneelle, kun linkkiä klikataan, on tärkeää, että työntekijöillä on haittaohjelmien torjuntaohjelmisto asennettuna kaikkiin laitteisiin. Tietojenkalasteluhyökkäykset kohdistuvat usein tiettyihin pk-yritysten työntekijöihin.

Virustorjuntaohjelmat ovat varma tapa estää haitallisten ohjelmien pääsy tietokoneellesi. Virustorjuntaohjelmat tulisi asentaa kaikille laitteille, jotta ne pystyvät havaitsemaan haitalliset verkkosivut ja viestit. Virustorjuntaohjelmat tarjoavat jatkuvan suojan tietoturvauhilta ja haittaohjelmilta. Niiden avulla pystytään takaamaan yrityksien tietoturva ja suojaamaan yrityksien tietoja tietoturvahyökkäyksiltä.

Käytä monipuolista ja vahvaa tunnistautumista

Varotoimista huolimatta työntekijä tekee todennäköisesti tietoturvaloukkauksen, joka voi vaarantaa tietosi. Tästä syystä yritysten työntekijöiden tulisi käyttää kaksivaiheista tunnistautumista. Kaksivaiheisen tunnistautumisen käyttäminen useimmissa suurimmissa verkko- ja sähköpostituotteissa on helppoa ja hyödyllistä tietoturvan kannalta.

Turvallisuus on liikkuva kohde. Verkkorikolliset kehittyvät päivittäin. Tietojen suojaamiseksi on tärkeää. Jokaisen työntekijän tulee asettaa kyberturvallisuus etusijalle ja pysyä ajan tasalla hyökkäysten ja uusimman ennaltaehkäisytekniikan uusimmista suuntauksista. (coxblue.com).

Ole varovainen tuntemattomien USB-laitteiden kanssa

USB-laitteista on tullut yksi yleisimmistä tiedonsiirron menetelmistä. Tästä syystä niihin tulisi suhtautua laitteina, jotka sisältävät viruksia tai haittaohjelman ja niitä ei tulisi koskaan liittää välittömästi yrityksen tietokoneisiin, tulivatpa ne mistä tahansa. Yksi yleisimmistä USB-laitteissa olevista haittaohjelmista on ns. keystroke detector-haittaohjelma, joka tuhoaa minkä tahansa tietokoneen heti, kun USB-laite liitetään siihen.

IT-osaston tulisi tarkistaa USB-laitteet, ennen kuin niitä käytetään yrityksessä. Mikäli tätä tarkistusta ei tehdä, voivat yrityksen kaikki tietokoneet olla vaarassa.

Pidä mobiililaitteet turvallisina

Teknologisen kehityksen myötä mobiililaitteista on tullut minitietokoneita ja niihin voidaan tallentaa valtavasti tietoa. Kehityksen myötä matkapuhelimista ja kannettavista on tullut entistä pienempiä. Tämä on johtanut siihen, että näitä laitteita on entistä vaikeampi jäljittää ja osa niistä katoaakin. Jos hyökkääjä pääsee käsiksi tällaisiin laitteisiin, hän saattaa päästä helposti sisään yrityksen tietoverkkoon teeskentelemällä olevansa laitteen omistaja.

Työntekijöiden tulee olla aina tietoisia mobiililaitteidensa sijainnista. Niiden valvomatta jättämisellä voi olla vakavia seuraamuksia.

Varmista tietosuoja

Usein olemme tarkkoja sen suhteen, mitä tietoja jaamme itsestämme sosiaaliseen mediaan. Sama tarkkuus tulisi liittää myös osaksi työelämää. Lataamalla huolimattomasti tietoja verkkoon, saatat vahingossa jakaa yksityiskohtaisia tietoja, joita voidaan käyttää yritystäsi vastaan. Nämä tiedot saattavat mahdollistaa hakkereille pääsyn yrityksesi tietoverkkoon ja antavat mahdollisuuden kilpaileville yrityksille käyttää vuodettuja tietoja hyväkseen. Tämän välttämiseksi voidaan kehittää erilaisia tiedonsuojaamistyökaluja. Työntekijöiden tulisi aina tarkistaa esimerkiksi kaikki heidän työpaikkaansa liittyvät videot ja valokuvat ennen niiden julkaisemista sosiaalisessa mediassa. Mikäli he eivät toimi niin, he saattavat tahtomattaan vuotaa yritykseen liittyvää arkaluontoista tietoa hyökkääjille ja hakkereille. Työntekijöiden tuleekin noudattaa erityistä varovaisuutta sen suhteen, mitä he jakavat nettiin.

Asenna tietoturvaohjelmistoon liittyvät päivitykset

Internetin turvallisuuspalveluiden tarjoajat päivittävät säännöllisesti heidän ohjelmistojaan vastatakseen jatkuvasti kasvavaan ja hienostuneempaan tietoturvauhkaan. Jos päivitysohjeet ovat tulleet yrityksesi IT-osastolta, on sinun tehtäväsi asentaa kyseiset päivitykset.

Internetin turvallisuuspalveluiden tarjoajat tekevät jatkuvasti töitä torjuakseen uusimmat tietoturvauhat ja pitääkseen asiakkaat turvassa. Sen takia he lähettävät asiakkailleen säännöllisesti päivitystiedotteet. Mikäli et noudata näitä päivitystiedotteita, asetat itsesi alttiiksi uusimmille tietoturvauhille. Sama käytäntö pätee muihinkin työpaikalla käytettäviin älylaitteisiin.

Syleile tietoturvakoulutusta

Useimmat yritykset valmentavat työntekijöitään tietoturvan osalta. He tekevät tämän vähentääkseen inhimillisistä virheistä ja työntekijöiden laiminlyönneistä johtuvia tietoturvahyökkäyksiä. Kaikkien työntekijöiden tulisi olla tietoisia siitä, mitä tietoturvahyökkäykset voivat aiheuttaa yritykselle ja sen työntekijöille.

Osallistumalla näihin valmennuksiin työntekijät oppivat havaitsemaan tietojenkalastelusähköposteja ja pop up-verkkosivuja. Tämän osaamisen avulla he pystyvät estämään mahdolliset tietovuodot.

Valmennuksen tehtävänä on pitää työntekijät ajan tasalla uusimmista tietoturvahyökkäyksien muodoista. Työntekijän tulee noudattaa yrityksen tietoturvaohjeita ja soveltaa niitä oikein. Työntekijöillä tulisi olla myös IT-osaamista erityisesti etätyöskentelytilanteissa.

Ole tietoinen valesähköposteista ja toimitusjohtajahyökkäyksistä

Hyökkääjät saattavat väittää edustavansa yrityksen johtohenkilöitä. Matkimalla toimitusjohtajien lähettämiä sähköposteja hakkerit saattavat huijata työntekijöitä luovuttamaan heille yrityksen kannalta tärkeitä tietoja esimerkiksi yrityksen tilisiirroista. Toimitusjohtajina esiintyvät hakkerit saattavat olla yhteydessä työntekijöihin vaatimalla heitä suorittamaan kiireisiä tehtäviä, siirtämään rahaa tai hankkimaan lahjoja.

Tietovuotojen välttämiseksi työntekijöiden ei tulisi koskaan vastata tällaisiin sähköposteihin. Sen sijaan heidän tulisi tarkastaa sähköpostiosoite. Hakkerit matkivat sähköpostiosoitteita tavoilla, joita on vaikea havaita välittömästi. Huomaamattomat erot esimerkiksi sähköpostiosoitteissa eivät ole helposti havaittavissa.

Varmista kunnollinen laitteiden hallinta

Pystyäkseen parhaiten noudattamaan yrityksen tietoturvakäytänteitä ja sääntöjä työntekijöiden on hallittava laitteitaan. Yhdistämällä yrityksen laitteet tietoturvasäännösten kanssa edistää tietoturvan käyttöönottoa entisestään. Estääkseen tietoturvarikollisten pääsyn yrityksen tietoverkkoihin siihen yhdistettyjen laitteiden kautta työntekijöiden on asennettava nämä laitteet valmistajien ohjeiden mukaisesti.

Varmista ohjelmistojen laillisuus

Kaikki ohjelmistot eivät ole turvallisia. Varomattomasti ladatut ja asennetut ohjelmat voivat aiheuttaa vakavia uhkia sekä yrityksen tietoverkolle että yritykselle. On oltava varovainen sen suhteen, miltä internetsivuilta lataa ohjelmia kuten myös sen yrityksen valinnassa, jolta ohjelmat tilataan. Tänä päivänä ohjelmistoja voi ladata ilmaiseksi monilta eri internet-sivuilta. Tämä on johtanut siihen, että hakkerit ovat ladanneet omia ohjelmiaan Internetiin. Monet näistä ohjelmista sisältävät haittaohjelmia kuten esimerkiksi troijalaisia.

Työntekijöiden tulee ymmärtää ja noudattaa työpaikkansa sääntöjä siitä, mitä ohjelmia tietokoneille saa ladata. Latauksia saisi tehdä vain yrityksen koneille. Ohjelmistojen laillisuus ja turvallisuus varmistetaan ajamalla ne virustorjuntaohjelmien läpi.

Ole tarkka sosiaalisen suunnittelun suhteen

Sen sijaan, että hyödyntäisi ohjelmistojen ja asennettujen käyttöjärjestelmien haavoittuvuuksia, sosiaalinen suunnittelu hyötyy inhimillisistä virheistä. Verkkorikolliset keräävät tietoja uhreistaan sosiaalisten alustojen kautta voidakseen imitoida heitä. Hyökkääjät manipuloivat ja huijaavat psykologisesti uhrejaan jakamaan arkaluonteista tietoa. Käyttämällä hyvin jäsennettyä tutkimusta aiotun uhrin tiedoista ja taustatiedoista rikoksen tekijät voivat

saada uhriensa luottamuksen. Kun haitalliset toimijat ovat antaneet näennäisesti harmittoman syyn, työntekijät luovuttavat helposti arkaluontoista tietoa yrityksestä.

Työntekijät voivat helposti välttää tällaiset ansat olemalla erityisen varovaisia verkossa. Vältä kaikkia tarjouksia, jotka kuulostavat liian hyviltä ollakseen totta. Suurin osa niistä on huijauksia.

Käytä hallittua palveluntarjoajaa

Inhimilliset virheet ovat väistämättömiä, vaikka ne ovatkin vältettävissä. Loppukäyttäjän virheitä voidaan vähentää hallitun palveluntarjoajan avulla. Sen avulla voidaan löytää kadonneet laitteet ja pyyhkiä niiden muistot etäyhteyden kautta, jotta voidaan estää kadonneen laitteen aiheuttamat tietorikkomukset. Hakkerit toteuttavat monia hyökkäyksiä saatuaan tietoja kadonneiden laitteiden kautta. Hankkimalla tietoja laitteen sijainnista se voidaan saavuttaa manuaalisesti ja ilmoittaa asiasta viranomaisille.

Salaa tietosi

Tietojen salaus estää luvattomia henkilöitä pääsemästä tietoihisi. Käyttäjät voivat salata tietoja muuntamalla ne toiseen muotoon, jolloin vain salausavaimen omaava henkilö pääsee käsiksi viestiin. Tietojen salaus on tällä hetkellä yksi suosituimmista tietosuojamenetelmistä, joita yritykset käyttävät. Tietojen salauksen tarkoituksena on suojata digitaalisen datan luottamuksellisuus. Työntekijöiden tulisi omaksua tietojen salaus.

Vältä sotkuista työpöytää

Niin ilmeiseltä ja yksinkertaiselta kuin se kuulostaakin, sotkuinen työpöytä voi olla monien pienten tärkeiden tietojen lähde. Tyypillisen työpäivän aikana työntekijöiden työpöydälle saattaa päätyä paljon tärkeitä tietoja sisältäviä papereita. Pomosi muistiinpanot, paperit, joihin on kirjoitettu salasanoja, ja laskut ovat tärkeitä tietolähteitä, jotka voidaan helposti jättää makaamaan sotkuiselle pöydälle. Jotkut tietoturvan parhaista pöydänhallintakäytännöistä ovat hyvin yksinkertaisia noudattaa. Älä jätä flash-asemia tai digitaalisia tallennuslaitteita lojumaan pöydällesi. Lukitse kaapit tai laatikot. On tärkeää varmistaa, ettet jätä luottamuksellisia papereita työpöydällesi pitkäksi aikaa. Hyvin harjoitellulla pöydänhallinnalla voi olla suuri vaikutus yritysten tietoturvan vahvistamiseen. (cyberexperts.com).