Arjen tietoturvaa pienyrittäjille

Kaamea Oy

2022

Sisältö

Luku 1

Arjen tietoturvaa

Nykyisessä tietoyhteiskunnassa tiedonkäsittelyn ja tietoturvan merkitys korostuu jatkuvasti enemmän. Olemme niin töissä kuin arjessa kokoajan erilaisen tiedon ympäröimänä ja määrä ei ole ainakaan hidastumassa kun tietoliikenneyhteydet jatkavat nopeutumistaan. Tämä digiloikka tuo mukanaan tietysti myös haasteita ja tässä oppaassa keskitytään tiedon turvaamiseen ja hallintaan pääasiassa pien- ja mikroyrittäjien näkökulmasta. Suuri osa oppaan sisällöstä toimii tietysti sekä isompien yritysten työntekijöiden käyttöön että yksityishenkilöille.

Tietoturva käsitteenä on hyvin laaja, siihen sisältyy tietysti tekninen tietoturva virustorjuntaohjelmistoineen, mutta se kattaa myös ihan fyysisten dokumenttien turvallisuuden sekä niiden säilyvyyden että turvallisuuden. Pyrin seuraavien lukujen myötä käymään läpi ainakin oikeanlaista ajatusmaailmaa, joka tietoturvan ja tiedon käsittelyn ympärillä olisi hyvä omaksua. Ihan jokaiseen tilanteeseen sopiva ja kaiken mahdollisen kattava tämä opas ei tietenkään ole, eikä edes pyri sellaiseksi, mutta jotain konkreettisiakin käytännön vinkkejä käydään läpi.

Oppaan on toteuttanut Sievin yrittäjät r.y.:n tilauksen myötä Kaamea Oy ja uusin versio tästä oppaasta on saatavilla verkkosivuiltamme[1].

Kaamea Oy on toiminut vuodesta 2018 ja henkilökunnallamme on yhteenlaskettuna kohta 30 vuotta työkokemusta PK-sektorin IT-toimittajana. Tarjonnastamme löytyy lähes kaikki pk-yrittäjien ict-tarpeet ihan perus sähköpostipalveluista ja palomuureista virustorjuntaan sekä tietysti asiantuntijapalveluihin. Tutustu palveluihimme tarkemmin osoitteessa kaamea.fi.

Versiohistoria

1. 4.4.2022 - Versio 1.0 valmis
2. 5.4.2022 - Versio 1.1 valmis: Oikoluku, IoT-kappaleeseen selkeyttä
3. 11.4.2022 - Versio 1.2: Toinen oikolukukierros

[1] https://kaamea.fi

Luku 2

Lisenssi

[1] https://creativecommons.org/licenses/by-nc-sa/4.0

Luku 3

Tiedon määrittely ja luokittelu

Yritysten toimintaan kuuluu nykypäivänä oleellisena osana erilaisen tiedon käsittely riippumatta yrityksen toimialasta. Kirjanpitoaineisto, asiakasrekisterit yhteystietoineen, laskutustiedot, inventaariot ja muut rekisterit ovat yhtä lailla tietoa kuin IT-yrityksen ohjelmakoodi tai asiantuntijoiden tuottamat raportit. Samaten eri ympäristöjen salasanat, sähköpostin sisältö ja yrityksen käyttöön otetut valokuvat.

Omasta työhistoriasta löytyy esimerkki yrityksestä, jonka mielestä erillisen varmuuskopiointipalvelun hankinta oli täysin turhaa rahanmenoa. Yrityksen asiakasrekisteri ja tilausjärjestelmä oli ostettu pilvipalveluna ja kun ko. palveluun kuului myös tietojen varmuuskopiointi niin yrityksen sisäistä tietoa ei koettu erityisen arvokkaaksi. Yritys toimi vaate- ja muotialalla ja siten heillä oli myös melkoisen kattava kuvapankki, jota varten oli palkattu erikseen valokuvaaja, mallit ja käytetty merkittäviä määriä työaikaa kuvauksen järjestämiseen. Ensimmäinen reaktio yrityksellä oli, että kuvathan voidaan aina ottaa uusiksi jos alkuperäisille tapahtuu jotain ja kuvauspäiviä järjestettiin joka tapauksessa uusien mallistojen myötä, niin tälle datalle ei nähty kovin suurta arvoa. Lopulta kun kustannuksia laskettiin tarkemmin yhden kuvauspäivän hinnaksi tuli lähemmäs 10 tuhatta euroa, jolloin se muutaman tuhannen euron vuosikustannus tietojen varmennuksesta ei tuntunutkaan niin pahalta. Samalla yrityksessä käytiin läpi muutakin tietoa, jota yrityksen omalle palvelimelle oli tallennettu. Messuesitteiden, markkinointisuunnitelmien ja kaiken muun sisäisen tiedon määrä oli lopulta niin valtava, että jos kaikki tiedostot olisi menetetty vaikkapa ukonilman seurauksena niin yrityksen toiminta olisi pysähtynyt kokonaan vähintään viikoiksi ja pahimmillaan saattanut kaataa koko yrityksen.

On hyvin helppoa ajatella juuri siitä omasta tiedosta, että kun se on itse tuotettu niin sillähän ei ole juurikaan mitään arvoa, kun sen voi tehdä helposti uusiksi. Se on kuitenkin usein juuri sitä arvokkainta tietoa mitä yrityksellä on ja kiireisessä arjessa niiden omien dokumenttipohjien, excel-taulukoiden ja muun datan katoaminen hidastaisi useiden työnteon täysin mateluvauhtiin.

Jotta oman toiminnan tietoturvaa voi hallita ja kehittää mielekkäästi niin ihan ensimmäisenä pitää olla tiedossa kaikki se tieto, minkä olemassaolo muodossa tai toisessa on tärkeää yritykselle. Toimialasta riippuen tämän määrittelyn

vaikeus vaihtelee paljonkin, mutta asiaa voi lähteä purkamaan ihan listaksi paperille sen mukaan mitä kaikkea tietoa on pitänyt olla ennen kuin pankkitilille on saapunut rahaa.

Määrittelyn ja listaamisen jälkeen tieto on vielä hyvä luokitella sen mukaan, miten kriittistä se on. Seuraavassa kappaleessa käydään läpi muutamia yleisiä tietoturvan kanssa käytettyjä suureita, joiden mukaan omaakin tietoa voi lokeroida.

Luku 4

Tiedon ja sen turvallisuuden lajit

Kaikki tieto ei ole samanarvoista. Osa tiedosta on sellaista, että jos se ei ole käytettävissä niin koko yrityksen toiminta pysähtyy ja osa sellaista joka aiheuttaa muutaman ärräpään ja puolen tunnin työajan menetyksen.

Yleisesti tietoturvaa miettiessä eri tietojen arvoa ja siten tarvittavien turvatoimenpiteiden määrää voidaan arvioida saatavuuden, luotettavuuden ja turvaamisen perusteella. Nämä kolme määrettä kuvaavat enemmän tietoturvauhkien luonnetta, mutta tämä jaottelu on yleisesti käytössä ja auttaa hahmottamaan minkälaisia uhkia vastaan mikäkin yrityksen tieto kannattaa erityisesti suojata.

Tämä lajittelu toimii yhtä lailla digitaalisen ja fyysisen tiedon lajitteluun, joskin tietysti näin informaatiotekniikan aikakautena riskit ja uhat koskevat useammin digitaalista tietoa. Fyysiseen muotoon säilytetty tieto on kuitenkin yhtä lailla tärkeää ja se on hyvä muistaa sekä tietoja määritettäessä että niitä luokiteltaessa

Tämä ei tietenkään ole ainoa mahdollinen tapa tehdä uhka-arviota ja jos toiminta sitä vaatii, voi olla hyvinkin perusteltua kehittää vaikka kokonaan oma asteikko minkä perusteella tietoturvajohtamista tehdään. Yleinen nyrkkisääntö kuitenkin on, että jaottelu pitää olla niin yksinkertainen, mutta ei yhtään sen yksinkertaisempi, kuin mahdollista. Liian moniportainen asteikko menettää äkkiä merkityksensä ja toisaalta liian yksinkertainen malli saattaa mm. aiheuttaa ylimääräisiä kustannuksia.

4.0.1 Tiedon saatavuus

Yrityksen tieto voi olla saavuttamattomissa joko hetkellisesti tai pysyvästi. Jos tarvittava tiedosto onkin toimiston verkkolevyllä, johon ei ole etäyhteyttä, tieto ei ole saatavissa, mutta se on olemassa. Ja jos se varmuuskopioimaton verkkolevy tuhoutuu tulipalossa niin tieto on menetetty pysyvästi.

Saatavuuden hetkellinen häiriö voi aiheutua myös pieleen menneestä ohjelmistopäivityksestä, haittaohjelmasta, laitteistorikosta ja monesta muusta syystä. Tällainen häiriö saattaa kestää muutamista tunneista jopa viikkoihin, riippuen valtavasti siitä miten yrityksen IT-infrastruktuuri on rakennettu ja kuinka suurista datamääristä on kysymys.

Näitä riskitasoja arvioidessa on hyvä miettiä, mitä tapahtuisi jos se oma puhelin tai läppäri jäisi auton alle tai jos ukonilma rikkoisi kaikki toimiston sähkölaitteet. Tällaisen onnettomuuden vaikutukset riippuvat tietysti paljon yrityksen muusta toiminnasta, mutta itsekin tiedän useampia tapauksia, joissa tietojen (ja tiedostojen) totaalinen menetys on vienyt koko yrityksen konkurssiin.

Saatavuuden tärkeyttä arvioitaessa yksi hyvä mittari on miettiä mitkä kaikki toiminnot pysähtyvät jos tieto ei ole saatavilla. Tällaisesta taulukosta on kohtuullisen helppoa laskea kullekin tiedolle ihan euromääräinen hintalappu ja siitä edelleen vertailla tätä hintaa varmuuskopioratkaisun kustannuksiin.

4.0.2 Tiedon luotettavuus

Näin tietoyhteiskunnassa toimiessa käytettävissä olevan tiedon luotettavuus on aivan jokaisen arjenkin sujuvuuden kannalta todella tärkeä asia. Meillä pitää olla luotettavaa tietoa siitä, milloin junat ja linja-autot liikkuvat, paljonko omalla pankkitillä on rahaa, mille tileille laskut pitää maksaa jne., ja jos tähän tietoon ei voi luottaa niin perusarjestakin tulee hyvin hankalaa.

Yrityksen oman toiminnan kannalta tilanne on ihan samanlainen. Konkreettiset vaikutukset riippuvat tietysti jälleen toimialasta, mutta hankintahinnat, toimitusajat, laskutustiedot ja muut pieniltäkin vaikuttavat tiedot voivat aiheuttaa valtavia ongelmia jos tiedot eivät ole luotettavia.

Luotettavuuden arvioinnissa kysymys kuuluukin “Mitä tapahtuu jos tämä tieto on väärin?”. Virhe tilinumerossa voi tulla todella kalliiksi, kirjoitusvirhe asiakasrekisterissä puhelinnumeron kohdalla on todennäköisesti halvempi.

4.0.3 Tiedon turvaaminen

Mitä tapahtuisi, jos sinun sähköpostisi sisältö julkaistaisiin kaikkien saataville? Tai kaikki tietokoneelta löytyvät dokumentit? Pienilläkin yrityksillä on vaitioloon liittyviä sopimuksia ja lakisääteisiä määräyksiä ja näiden rikkomisesta aiheutuvat sanktiot eivät ole aivan mitättömiä. EU:n tietosuoja-asetus (GDPR) mahdollistaa jopa 4% sakot koko konsernin liikevaihdosta, jos tietoturva on hoidettu todella leväperäisesti tai tietosuoja-asetuksen vastaisesti.

Tiedon turvaamistarvetta määriteltäessä tuleekin ottaa huomioon sekä suorat että epäsuorat kustannukset. Pienyrityksille salassapitosopimuksien rikkominen tarkoittaa usein täyttä maksukyvyttömyyttä ja jos suoraa taloudellista vahinkoa ei tietovuodosta syntyisikään niin imagohaitta tulee häiritsemään liiketoimintaa pitkään.

Pienissä yrityksissä eri turvatasoja tietojen käsittelyyn ei usein ole kovin montaa, vaan erittely on lähinnä yrittäjän itsensä ja työntekijöiden välillä. Isommissa konserneissa eri tasoja voi olla kymmenittäin ja vielä eri projekteille omansa.

Luku 5

Tietoturvauhkia ja niiden torjuntaa

Sen jälkeen kun olemassa oleva tieto on määritelty ja luokiteltu on hyvä miettiä mahdollisia riskejä mitä olemassa olevalle tiedolle voi tapahtua.

Riskien realisoituminen voi tarkoittaa tiedon katoamista, sen joutumista asiattomien käytettäväksi tai tiedon luotettavuuden menetystä. Käsiteltävästä tiedosta riippuen vahinko ja sen korjaaminen voivat olla hyvinkin kalliita. Tässä kappaleessa käyn läpi muutamia yleisimpiä riskejä ja niiden hallintaa, mutta tämä ei ole mikään kaikenkattava eikä jokaiseen tilanteeseen soveltuva malli, ajatuksena on enemmän herättää ajatuksia sen oman yrityksen tiedon tärkeydestä ja sitä uhkaavista asioista. Juuri teidän yrityksenne ratkaisut on hyvä käydä läpi luotettavan asiantuntijan kanssa, joka osaa tarjota räätälöidyn palvelukokonaisuuden tarvekartoituksen kautta.

5.1 Tiedon täydellinen menetys

Tietotekniikan alalla pätee vain yksi ehdoton totuus: Kaikki laitteet rikkoutuvat. Ainoa kysymys on vain, että milloin ja mitä siitä aiheutuu. Varsinkin mukana kannettavien laitteiden rikkoutuminen fyysisesti on hyvin helppoa kuvitella, mutta myös paikoillaan olevat palvelimet ja muut isommat koneet ovat loppupelissä varsin herkkiä lopettamaan toimintansa. Ukkonen, vesivahinko ja muut ympäristöstä aiheutuvat vauriot, laitteen iän myötä tapahtuva rikkoutuminen ja käyttäjän virheet ovat kaikki lähes jokapäiväisiä ongelmia mitä tiedonkäsittelyn ja -tallennuksen kanssa tulee eteen. Myös fyysisesti esim. paperilla oleva tieto voi kadota pysyvästi ja sen varmistaminen on ihan yhtä tärkeää kuin digitaalisessa muodossa olevan tiedon hallinta.

Teknisten ja käyttäjävirheiden lisäksi verkkolevyillä ja muilla palvelimilla oleva tieto voi tuhoutua haittaohjelman seurauksena. Virustartunta yhdellekin yrityksen tietokoneelle riittää pahimmillaan hävittämään kaikki yrityksen tiedostot, joskin nykyään todennäköisempi hyökkäystapa on ns. ransomware, josta enemmän seuraavassa luvussa.

Tiedon totaalista menetystä vastaan ainoa tapa on käyttää kulloiseenkin tarpeeseen sopivaa varmuuskopiojärjestelmää. Pienimuotoiseen yritystoimintaan saattaa olla tarpeeksi varmistaa tiedot kuluttajatasoiseen pilvitallennuspalve-

luun, esimerkiksi Microsoftin OneDrive-ympäristöön, mutta nämä palvelut tarjoavat varsin rajoitetut työkalut ja turvan käyttäjän virheistä johtuvien tiedonmenetysten korjaamiseksi. Lisäksi jos käsiteltävää tietoa on merkittävän paljon tai tietoa pitää tallentaa useammasta eri järjestelmästä tämä ei välttämättä ole kustannustehokas tai ylipäätään toimiva ratkaisu.

Riippumatta käytetystä varmistusjärjestelmästä sen toimintaa tulee valvoa ja tiedon palautus on syytä testata aika-ajoin. Olen urani aikana nähnyt useita "varmuuskopioituja" palvelimia ja muita järjestelmiä, joihin on vuosikausia sitten hankittu jonkinlainen varmistuspalvelu, mutta asennuksen jälkeen sen toimintaa ei ole millään tavalla seurattu. Paras/pahin tapaus oli, että varmuuskopiointia tarjonnut yritys oli jo lopettanut toimintansa eikä asiakasyrityksen henkilöstöllä ollut tästä mitään tietoa.

Tiedonvarmistukseen liittyviä tarpeita on kuitenkin melkein yhtä monta kuin on yrityksiäkin, joten yleispätevää vastausta soveltuvasta tekniikasta tai sen toimittajasta on täysin mahdotonta antaa. Ohjeeni onkin, että ota yhteys ensin siihen omaan IT-ylläpidosta vastaavaan tahoon ja keskustele hänen kanssaan soveltuvasta ratkaisusta ja palvelutoimittajasta. Tarjonta tälläkin osa-alueella on sekä laadun että hinnan puolesta hyvin värikästä, joten oikean palvelutoimittajan etsimiseen kannattaa käyttää riittävästi aikaa.

5.2 Tiedon saatavuuden menetys

Sen lisäksi, että tieto voidaan menettää täydellisesti laitteistorikon yhteydessä tieto voi myös olla tavoittamattomissa haittaohjelman, väärin konfiguroidun palvelimen tai jopa puuttuvien salasanojen johdosta. Ns. ransomware-haittaohjelmat salaavat järjestelmän tiedot ja hyökkääjät vaativat lunnaita, yleensä bitcoin maksuna, että tiedostot saa jälleen käyttöön. Jos palvelimen tiedostot ovat salattuja ja salausavain joutuu hukkaan niin lopputulos on melkein sama kuin ransomware-hyökkäyksessä, sillä erotuksella ettei tiedostoja saa takaisin käyttöön lunnaita maksamalla. Lisäksi saatavuus voi katketa ihan vain jos se oma salasana unohtuu ja järjestelmään ei enää pääse kukaan yrityksen työntekijöistä kirjautumaan.

Haittaohjelmien mukana tulee myös haaste varmuuskopiojärjestelmälle, etenkin jos varmuuskopiointiin käytetään pelkästään pilvitallennuspalveluita, koska haittaohjelma leviää hyvin todennäköisesti myös varmuuskopioihin, etenkin jos tartuntaa ei havaita ajoissa, ja tällöin tietojen palautus saataville saattaa olla hyvinkin pitkä prosessi jonka lopputuloksesta ei ole täyttä varmuutta.

Salasanan unohtuminen ei ole erityisen harvinaista, edelleen lomakausien jälkeen IT-osastot ympäri maailmaa käyttävät valtavat määrät työaikaa salasanojen vaihtamiseen. Pienyrityksessä sen oman verkkolevyn tai pilvipalvelun pääkäyttäjän salasanat ovat kuitenkin usein vain yhden henkilön tiedossa ja jos salasana sattuu unohtumaan, tai ylläpidosta vastannut henkilö vaihtaa työpaikkaa, niin tiedostot jäävät lukkojen taakse. Tällaisissa tilanteissa tiedostojen tai sen puuttuvan salasanan palautus on kuitenkin usein mahdollista, mutta epäpätevissä käsissä tilanne on hyvinkin riskialtis. Unohtuneen salasanan ohittaminen kun on teknisesti ottaen järjestelmän turvajärjestelmien murtamista ja osaamaton tekee helposti vielä lisää vahinkoa. Samaan tapaan kuin osaava lukkoseppä saa oven siististi auki hukkuneen avaimen jäljiltä, mutta amatööri rikkoo ikkunan ja ovenkarmit mennessään.

Haittaohjelmia vastaan nykyaikaiset virustorjuntaohjelmistot toimivat varsin hyvin, kunhan ne päivitetään säännöllisesti. Täydellisiä ne eivät kuitenkaan ole, vaan niiden rinnalle tarvitaan loppukäyttäjältä vähän järjenkäyttöä. Linkkejä tietojen kalasteluun, haittaohjelmien levittämiseen ja muuhun kiusantekoon tulee meille kaikille sähköpostiin, tekstiviesteihin ja nykyään myös pikaviestimiin kuten Whatsapp ja Telegram ja näitä linkkejä availemalla riskeeraat omien laitteidesi tietoturvan. Lisäksi haittaohjelmia yritetään syöttää järjestelmiin myös kohdistettujen hyökkäysten avulla, esimerkiksi väärentämällä sähköpostin lähettäjätiedot tai käyttämällä varastettuja tunnuksia, jolloin turvallisen näköisestä osoitteesta saapuva posti saattaakin olla haitallinen. Yhteistä näille kaikille hyökkäyksille on kuitenkin se, että loppukäyttäjältä vaaditaan toimenpiteitä jotta hyökkäys onnistuu. Eli hyvä viruksentorjuntaohjelmisto on vasta toinen porras turvaketjussa ja ensimmäisenä on se hyvin koulutettu käyttäjä joka ei availe kaikkia eteen tulevia linkkejä.

Salasanojen hallinta on kokonaan oma taiteenlajinsa ja siitä on tässä oppaassa oma kappale, mutta tiedon saatavuuden kannalta talon sisällä oleviin järjestelmiin yleisesti käytetty ratkaisu on luoda järjestelmiin oma, täysin erillinen, ylläpitotunnus. Tälle tunnukselle luodaan vahva salasana ja sitä säilytetään ihan paperilla, suljetussa kirjekuoressa ja se vaihdetaan aina käytön jälkeen. Verkkopalveluna toimivissa järjestelmissä salasanan nollaus yleensä onnistuu joko asiakaspalvelun tai itsepalveluliittymän kautta, mutta näidenkin toiminta on syytä varmistaa ennen kuin todellinen tarve tulee eteen.

5.3 Tiedon luotettavuuden menetys

Pienyrityksissä yrityksen sisällä käsiteltävän tiedon luotettavuus on yleisesti varsin hyvällä tasolla. Tietoja käsittelee hyvin harva ja esimerkiksi uutisissa monena kesänä pyörineet huijauslaskut harvemmin menevät pienillä yrityksillä läpi. Tämä ei kuitenkaan tarkoita, etteikö tiedon luotettavuus pienyrityksen toiminnassa olisi yhtä oleellinen osa kuin isoilla konserneillakin.

Kohdistettuja tietoturvahyökkäyksiä tehdään jatkuvasti enemmän myös pieniä yrityksiä kohtaan ja jos tällainen hyökkäys jatkuu huomaamatta pidempään sillä voi olla todella vakavat vaikutukset ihan yrityksen sisäiseenkin toimintaan. Muutaman tietokoneen täydellinen haltuunotto kun voi pahimmillaan tarkoittaa esimerkiksi sitä, että pankkiliikenne ohjautuukin hyökkääjän oman ympäristön kautta ja maksut lähtevät väärille tileille.

Isommissa yrityksissä tiedon luotettavuus on sitten kertaluokkaa haastavampi asia hallinnoitavaksi, kun samaa tietoa käsitellään useissa eri paikoissa ja kenelläkään ei ole täydellistä kuvaa kaikesta siitä tiedosta mitä yrityksen sisällä liikkuu. Yksittäisen työntekijän salasanojen joutuminen vääriin käsiin saattaakin aiheuttaa todella vakavat seuraamukset muille työntekijöille. Asiattomien pääsy esimerkiksi henkilöstöhallinnon tietoihin voi aiheuttaa mittavaa haittaa paitsi itse yritykselle niin myös sen työntekijöille.

Varsinaisten tietoturvahyökkäysten lisäksi tiedon luotettavuutta pitää arvioida esimerkiksi IT-ympäristön valvontatyökalujen osalta. Väärin konfiguroitu varmuuskopiointijärjestelmä voi antaa virheellistä turvallisuudentunnetta ilmoittamalla että tiedostot ovat tallessa. Päivittämättä jäänyt virustorjunta voi näyttää "vihreää valoa" ja järjestelmä voi siitä huolimatta olla haavoittuvainen. Lisäksi huono IT-kumppani voi säästää omaa vaivaansa väittämällä, että pa-

lomuuri on kunnossa tekemättä konkreettisesti asian eteen mitään. Vastaava huolimattomuus pätee tietysti myös yrityksen omiin työntekijöihin ja sisäisen tiedon luotettavuus onkin hyvin pitkälle sen varassa miten luotettavia työntekijöitä palkkalistoilta löytyy.

5.4 Tiedon vuotaminen ulkopuolisille

Tietojen menetyksen rinnalla toinen, usein vielä pahempi, uhka yrityksen tietoturvalle on tietojen vuotaminen ulkopuolisten käsiin. Tietovuoto, laajuudesta riippumatta, aiheuttaa aina vakavia ongelmia paitsi yrityksen toimintaan niin myös sen imagoon. Erilaisia tietovuotoja uutisoidaan ympäri maailmaa viikoittain ja niiden vaikutukset voivat olla todella vakavia, kuten Vastaamon tapaus vuonna 2020 on osoittanut.

Imagohaitan lisäksi tietovuodosta voi koitua merkittävän suuret taloudelliset vahingot. Salassapitosopimusten korvaussummat ovat usein varsin mittavia ja ääritilanteissa tietovuodolla voi olla myös rikosseuraamuksia. Lopullinen vahinko riippuu tietysti siitä, mitä tietoa on loppupelissä vuotanut, mutta lähes yhtä paljon myös siitä, miten tietovuotoon reagoidaan. Tietoturvaloukkauksesta on myös lakisääteinen velvoite ilmoittaa [1], mutta asiakkaiden suuntaan tehokas viestintä on usein paljon merkittävämpää jatkon kannalta kuin lain vaatimat toimenpiteet.

Tietovuoto voi tapahtua esimerkiksi haittaohjelman, onnistuneen tietojen kalastelun, vahingon, huolimattomuuden tai osaamattomuuden johdosta. Ehkä yleisin tapa tietovuodoille on sähköpostin salasanan joutuminen vääriin käsiin, jolloin sähköpostin koko sisältö päätyy pahantahtoisiin käsiin. Vuodettuja sähköpostin salasanoja käytetään toki suurelta osin "vain" erilaisten haittaohjelmien ja muiden hyökkäysten levittämisen, mutta samalla mm. asiakkaiden sähköpostiosoitteet päätyvät roskapostittajien käsiin.

Tätäkin hyökkäystä vastaan paras väline on se hyvin koulutettu loppukäyttäjä, joka osaa jättää kalasteluviestit huomiotta ja noudattaa hyviä salasanakäytäntöjä. Heikko ja monessa palvelussa käytetty sama salasana on melkein yhtä hyvä tapa päästää asiattomia omaan sähköpostiin käsiksi kuin kirjautumistietojen suora jakaminen sosiaalisessa mediassa. Tekniset apuvälineet tietysti estävät oman osansa, mutta pelkästään tiedonkalasteluun on niin paljon erilaisia tekniikoita ja mahdollisuuksia, ettei mikään tekninen järjestelmä takaa täydellistä onnistumista. Tästä huolimatta salasanamanagerin, 2-vaiheisen tunnistautumisen ja muiden tekniikoiden käyttö on enemmän kuin suositeltavaa, näistä enemmän omissa kappaleissaan.

[1] https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta

Luku 6

Käytännön toimintaohjeita 101

Edellisissä kappaleissa olemme nyt käsitelleet tietoa ja sen turvaamista varsin abstraktilla tasolla. Tähän kappaleeseen on sitten kerätty varsin käytännönläheisiä asioita, joilla liiketoimintoja saa näin tietoyhteiskunnan aikana hoidettua turvallisemmin. Lista ei edes yritä olla kaiken kattava, vaan ennemminkin "vähintään nämä pitäisi olla kunnossa" -tyylinen luettelo. Lista ei myöskään ole missään erityisessä tärkeysjärjestyksessä.

Osa esimerkkiratkaisuista ei tietenkään sovellu ihan jokaiseen tarpeeseen, mutta otsikkotasolla listan pitäisi olla varsin yleispätevä. Soveltuvien tekniikoiden valinta siihen oman yrityksen toimintaan riippuu kuitenkin niin monesta tekijästä, että ennen lopullista valintaa suosittelen vaihtoehtojen läpikäyntiä luotettavan kumppanin kanssa.

6.1 Salasanan käyttö sekä mobiililaitteessa että tietokoneella

Uusimmissa älypuhelimissa on sisäänrakennettuna tallennettujen tiedostojen salaaminen, jolloin laitteen joutuminen vääriin käsiin ei ole automaattisesti tietovuoto. Android ja iOS laitteet käyttävät näytön lukituksen salasanaa salausavaimena, tarkempia ohjeita varten tutustu oman laitteesi käyttöohjeeseen.

Etenkin nykyään, kun siinä kännykässä kulkee mukana sähköposti, rahat, yhteystiedot, sosiaalisen median tilit ja ihan kaikki muukin voisi kuvitella, että ihmiset olisivat hyvin tarkkoina siitä, kuka laitteen tietoihin pääsee kiinni. Mutta edelleen on sekä hämmästyttävän että huolestuttavan yleistä ettei minkäänlaista lukitusta ole otettu käyttöön.

Kasvojentunnistukseen perustuvat tekniikat (esim. Applen FaceID) eivät ole yhtä turvallisia kuin sormenjälki tai salasanat (joista jälkimmäinen on parempi), mutta senkin käyttöönotto on paljon parempi kuin laitteen pitäminen täysin avoimena kenelle tahansa kuka sen sattuu käsiinsä saamaan baaritiskiltä, kaupan kassahihnalta, narikkaan jätetystä takista tai mihin nyt itse kukin sattuu kännykkänsä toisinaan hukkaamaan.

Sama pätee tietysti tietokoneisiin, läppärin varastaminen on vain vähän vai-

keampaa kuin puhelimen ja yrityskäytössä kannettavissa on jopa enemmän tietoa käytettäväksi pahantahtoisiin tarkoituksiin. Selain täydentää salasanat automaattisesti kaikkialle ja kirjanmerkeistä löytyy suoraan lista mihin palveluihin salasanoilla pääsee käsiksi. Tietokoneiden kanssa tietojen salaus ei ole vastaavaan tapaan sidottu salasanaan kuin mobiililaitteissa, eli sen käyttöönotto pitää tehdä erikseen. Tarkat ohjeet riippuvat käyttöjärjestelmän versiosta, keskustele oman IT-tukesi kanssa salauksen käyttöönotosta.

6.2 Salasanamanagerin käyttö ja salasanakäytännöt

Lähes viikoittain uutisista voi lukea miten milloin minkäkin verkkopalvelun käyttäjätietoja on varastettu ja salasanoja on vuotanut maailmalle. Jos käytät samaa sähköpostiosoitetta ja salasanaa useammassa eri palvelussa niin yhdenkin palvelun tietomurto altistaa kaikki käyttäjätilisi väärinkäytöksille samantien vaikka valitsemasi salasana olisi miten pitkä ja monimutkainen tahansa.

Heikkojen salasanojen käyttö puolestaan altistaa käyttäjätilit ns. brute-force hyökkäyksille. Nykyiset tietokoneet kykenevät käymään läpi aivan kaikki 8 merkkiä pitkät yhdistelmät (isot ja pienet kirjaimet, numerot, erikoismerkit) läpi reilussa puolessa tunnissa. Tämänhetkinen yleinen nyrkkisääntö on käyttää vähintään 12 merkkisiä salasanoja, joissa on pieniä ja isoja kirjaimia sekä numeroita, lisäksi vahvasti suositellaan erikoismerkkien käyttöä.

Salasanamanagerin avulla voit helposti käyttää jokaisessa palvelussa eri salasanaa ja salasana voi olla miten monimutkainen tahansa, koska manageriohjelma huolehtii siitä. Tällöin tarvitsee pitää huoli vain yhdestä, riittävän turvallisesta, salasanasta, jolla saat oman salasanahallinnan auki ja ohjelma huolehtii loput. Suurimmassa osassa verkkoselaimia on oma sisäänrakennettu salasanamanageri, mutta se toimii tietysti vain verkkosivujen kanssa. Erillinen manageri mahdollistaa salasanojen turvallisen hallinnan mihin tahansa ohjelmistoon ja miltä tahansa laitteelta käsin.

Ohjelmia ja palveluntarjoajia tähän tarpeeseen on nykyään aivan käsittämättömän paljon ja valinta niiden välillä voi olla vaikeaa. Internetin keskustelupalstoilla vastaukseksi tarjotaan useimmiten BitWarden[1] ja LastPass[2] palveluita. Lisäksi kotimainen F-Secure[3] tarjoaa omaa ID Protection -tuotettaan. Näiden lisäksi tarjolla on erillisiä ohjelmia ostopalvelun sijaan, esimerkiksi avoimen lähdekoodin KeePassXC[4].

Kattavan vertailun tekeminen eri ratkaisuista vaatii kuitenkin kokonaan oman oppaansa. Valitsitpa minkä tahansa palvelutoimittajan tai ohjelmiston niin selvitä ensin kunkin ratkaisun hyvät ja huonot puolet. Hyvä IT-kumppani osaa neuvoa tämänkin kanssa.

[1] https://bitwarden.com/
[2] https://www.lastpass.com/
[3] https://www.f-secure.com/fi/home/products/id-protection
[4] https://keepassxc.org

6.3 2-vaiheisen tunnistautumisen käyttöönotto

Lyhenne MFA[5] ei välttämättä sano vielä mitään, mutta moni meistä käyttää jo 2-vaiheista tunnistautumista tiedostamattaan. Pankkitunnuksilla tai mobiilivarmenteella (jotka ovat 2-vaiheisia tunnistustapoja) kirjautuminen toimii omaveroon, vakuutusyhtiöihin, pankkeihin ja puhelinoperaattoreiden palveluihin.

2-vaiheisella tunnistautumisella tuodaan salasanan lisäksi toinen varmistuskeino, jolla estetään palveluiden luvaton käyttö, josta nimikin juontaa juurensa. Mobiilivarmenteen lisäksi 2-vaiheisen tunnistautumisen voi suorittaa sähköpostilla, tekstiviestillä tai erillisellä todentajasovelluksella, kuten Microsoft Authenticator. Näitä käyttämällä pelkkä salasanan vuotaminen vääriin käsiin ei vielä riitä väärinkäytökseen, vaan sen lisäksi tarvitaan tuo toisen vaiheen tunnistautuminen. Puhelimen kanssa molempien vaiheiden tiedot ovat usein samassa laitteessa, joten sen turvaaminen on entistä tärkeämpää, mutta pelkän salasanan vuotaminen tai arvaaminen bruteforce -menetelmällä on paljon todennäköisempää kuin koko kännykän varastaminen.

Tunnistautumista voi käyttää lähes kaikissa isoissa palveluissa, kuten GMail, Outlook ja Facebook. Osa näistä palveluista on jo siirtynyt pakottamaan 2 vaiheisen tunnistautumisen käyttöä ja kokoajan kasvava osa eri verkkopalveluista tukee sitä muodossa tai toisessa.

MFA on tällä hetkellä ehkä suurin muutos mitä verkkopalveluiden käyttöön on tulossa ja sen käyttöönotto aina kun mahdollista on ehdottomasti suositeltavaa. Tekniset yksityiskohdat ja jokaisen eri palvelun läpikäynti on kuitenkin liian iso urakka tämän oppaan sivuilla, joten suosittelen edelleen kääntymään sen oman IT-kumppanin puoleen.

6.4 VPN ei ole tietoturvaa, välttämättä

VPN-yhteyksiä tarjotaan nykyään joka puolella ja myyntivideot lupaavat että sillä korjautuu kaikki maailman ongelmat. VPN-yhteyksille on tietysti paikkansa ja niiden avulla voidaan parantaa myös tietoturvaa, mutta VPN-yhteyksillä ratkaistaan enemmän muita kuin tietoturvaan liittyviä ongelmia.

Etenkin Amerikassa VPN-yhteyksiä mainostetaan turvallisuuteen liittyvinä työkaluina, mutta sikäläinen tietosuojakulttuuri poikkeaa valtavasti meidän versiosta. Internet-operaattoreilla on siellä mahdollisuus (ja yleinen käytäntö) seurata kuluttajiensa verkkokäyttäytymistä ja tätä tietoa käytetään mm. mainostamiseen. Tällaisen liikenneseurannan estämiseen useimmat kaupalliset VPN-palvelut toimivatkin aivan hyvin. Toinen kuluttajille myytävä käyttökohde on maarajoitteiden kiertäminen mm. suoratoistopalveluiden osalta. Tähänkin tarkoitukseen VPN on ihan toimiva, joskin käyttöehtojen kannalta usein kyseenalainen, ratkaisu.

Meillä Suomessa tilanne on kuitenkin aivan toinen. Tietoliikenneyhteydet nauttivat samaa suojaa kuin mm. postin palvelut, joten vastaavanlaista tarvetta suojautua sen oman palveluntarjoajan seurantaa vastaan ei ole edes olemassa.

VPN-yhteydet eivät tietysti ole tarpeeton työkalu täällä meilläkään. Useimmiten yrityksissä käytetään erilaisia VPN-toteutuksia sallimaan pääsy yrityksen omiin palveluihin, joka on etenkin näin etätyöaikana ollut aivan ehdoton välttämättömyys. Tällä ei kuitenkaan ole suoranaisesti tietoturvan kannalta niin

[5] Multi Factor Authentication

isoa merkitystä, VPN-liikenne kun on turvallisuuden kannalta ihan vastaavaa, kuin kaikki muukin yrityksen sisäinen liikennöinti ja sen hallintaan on omat työkalunsa jo olemassa.

Jos kuitenkin käytät usein hotellien, lentokenttien tai muiden yleisesti käytössä olevien verkkojen yhteyksiä niin VPN-yhteyksien käyttö on myös osa tietoturvaa. Yleisesti käytössä olevien verkkojen liikennettä on mahdollista analysoida, etenkin jos langaton verkko on salaamaton ja tällaisia verkkoja käyttäviä laitteita on mahdollista huijata ottamaan yhteys hyökkääjän laitteisiin. Jos tällainen huijaus onnistuu hyökkääjä voi analysoida ja uudelleen ohjata liikennettä miten tahansa haluaa, jolloin maailma on auki erilaisille huijauksille ja tietojen varastamiselle. Oikeinkäytettynä VPN-palvelut suojaavat tällaisia hyökkäyksiä vastaan varsin tehokkaasti.

6.5 Laitteiden elinkaari ja tietoturvallinen hävitys

Kuten jo todettua, kaikki laitteet hajoavat, mutta osa niistä säilyy toimintakykyisinä pidempään kuin ne soveltuvat yrityksen tarpeisiin. Huolimaton vanhojen laitteiden hävittäminen saattaa kuitenkin aiheuttaa tietovuodon yrityksessä. Varmin tapa tähän on laittaa vanhat koneet sellaisenaan myyntiin kirpputorille, ja tätä tapahtuu useammin kuin äkkiseltään voisi kuvitella.

Mekaaninen tuhoaminen on tietysti varma tapa hävittää arkaluontoiset tiedot laitteista, mutta koko koneen tuhoaminen on usein tarpeetonta energiantuhlausta ja toisekseen vanhoillekin laitteille voi löytyä edelleen hyötykäyttöä muualla vaikka ne eivät yritystoimintaan enää olisikaan soveltuvia. Tietokoneiden kohdalla massamuistin, eli kiintolevyjen, poisto ja tuhoaminen säilyttää muun koneen käyttökelpoisena, jolloin ne voi myydä tai lahjoittaa eteenpäin ja (ellei sopimusteknisesti ole tarvetta) koneen voi tyhjentää myös ohjelmallisesti, jolloin se on käyttöön otettavissa seuraavan omistajan toimesta ilman osien hankintaa.

Mobiililaitteista massamuistien irrotus on käytännössä mahdotonta, joten jos sopimukset vaativat tietojen mekaanista tuhoamista niin silloin ei auta kuin heittää koko puhelin murskaimeen. Mobiililaitteetkin on kuitenkin mahdollista tyhjentää ohjelmallisesti, jolloin käytöstä poistuneet laitteet voi kierrättää ilman tietoturvariskejä.

Useat leasing-yritykset tarjoavat tietojen turvallista poistoa elinkaaripalvelun yhteydessä ja jokainen asiansa osaava IT-palveluita tarjoava yritys voi tehdä tietojen poistoa palveluna siinä kuin käyttäjätukeakin. Olipa valittu tapa hävitykselle mikä tahansa niin tietoturvan huomiotta jättäminen laitteiden uusimisessa on yksi tapa kirjaimellisesti ojentaa omat tiedot ulkopuolisten käsiin.

6.6 IoT ja älylaitteet

Nykyään jo vanhaksi luokiteltava vitsi on, että IoT-lyhenteessä S-kirjain tarkoittaa 'security':a. Markkinoille tulee yhä kiihtyvämmällä vauhdilla erilaisia valaisimia, jääkaappeja, televisioita, leivänpaahtimia ja astianpesukoneita jotka voi kytkeä internetiin. Tästä trendistä voi olla itse kukin mitä mieltä haluaa, mutta usein erilaisia älylaitteita käyttöön otettaessa tietoturva ei ole ensimmäinen mietittävä asia.

Useat IoT-laitteet sisältävät käytännössä ihan täyden tietokoneen verkkoyhteydellä ja osa näistä osaavat kommunikoida myös mm. bluetoothin välityksellä. Näistä laitteista löytyy lisäksi erilaisia tietoturvahaavoittuvuuksia lähestulkoon päivittäin kun laitevalmistajilla ei ole joko osaamista taikka intressiä huolehtia myymiensä järjestelmien turvallisuudesta. Osassa laitteista se varsinainen "äly" on alihankintana ostettu komponentti ja se itse laite on perinteisemmän elektroniikkatehtaan tuottama. Näiden laatu niin teknisesti kuin turvallisuuden kannalta on vähintään yhtä kirjava kuin erilaisten älylaitteiden määrä. Internetistä löytyy mitä uskomattomimpia tarinoita siitä, miten isojenkin yritysten tietoturva on saatu murrettua kahvinkeittimellä tai ilmalämpöpumpulla, eli mistään teoreettisesta uhasta ei ole kysymys. Ja jos tällainen tietoturvariskin sisältävä laite kytketään sinne omaan lähiverkkoon, niin samalla ohitetaan mm. verkon oma palomuuri ja pahimmillaan avataan suora reikä hyökkäyksille verkon turvajärjestelyiden ohi.

Tieto- ja yksityisyydensuoja näissä laitteissa on lisäksi usein varsin kyseenalainen ja mm. monet halvemmat ja "helposti käyttöönotettavat" valvontakamerat toimivat siten, että kuva ja ääni kiertävät ensin valmistajan palvelimille (lähes aina Kiinaan) ennenkuin ne välitetään sinne loppukäyttäjän matkapuhelimeen. Lisäksi laitteiden hallintaan ja ohjaukseen liittyvät mobiilisovellukset haluavat usein kyseenalaiset oikeudet laitteen tietoihin ja loppukäyttäjälle tulee harvoin erityisen selväksi mihin tietoja käytetään. Lisäksi GDPR ja muut yksityisyydensuojaa turvaavat lait ja asetukset ovat kiinalaisia yrityksiä vastaan varsin hengettömiä.

Älykkäälle valaistuksen ohjaukselle ja muulle automaatiolle on yrityksissäkin kuitenkin kysyntää ja niillä voidaan saada ihan selviä säästöjäkin mm. energiankulutuksen hallinnassa. Automaatiota hankkiessa on kuitenkin tärkeää pitää tietoturva yhtä lailla hallinnassa kuin varsinaista tietotekniikkaa ostaessa.

6.7 Kaikki hyökkäykset eivät tapahdu pelkästään verkossa

Laitteiden tietoturva käsittää myös fyysisen turvallisuuden. Jos hyökkääjällä on fyysinen pääsy laitteisiisi niin erilaisten etäkäyttö- ja haittaohjelmien asentaminen on paljon helpompaa kuin verkon yli. Täysin valvomaton pääsy laitteeseen on tietoturvan kannalta tietysti pahin mahdollinen tilanne, mutta haittaohjelmia voi istuttaa myös esim. muistitikulle jolloin käyttäjä itse saastuttaa laitteensa tietämättään.

Fyysisten hyökkäysten kanssa ainoastaan ihmisen kekseliäisyys on rajana hyökkäysten naamiointiin. Matkapuhelimen laturin kuoriin on mahdollista sisällyttää haittaohjelmaa levittävä tietokone siten, että laite toimii edelleen laturina. Lähiverkkoon voidaan kytkeä kiinni hyvinkin pieniä laitteita, joita voidaan käyttää myöhemmin verkon yli tietojen varastamiseen ja muuhun haitantekoon.

Suoraan yrityksen toimitiloihin tehtävän hyökkäyksen lisäksi laitteisiin voidaan päästä käsiksi melkein missä tahansa julkisella paikalla. Kahvilan pöytään jätetty kannettava on suorastaan houkutteleva kohde ja kaupan kassalle jäänyt matkapuhelin on helppoa varustaa omilla "valvontatyökaluilla" ennen palauttamista.

Pienissä yrityksissä täysin tuntemattomia harvemmin päästetään verkkolait-

teiden pariin vain kysymällä, mutta toimistohotelleissa tietoturvan taso on usein suorastaan järkyttävä ja jaettuihin kytkentäkaappeihin pääsee kunhan vain pyytää talonmiestä avaamaan oven. Yleisradiokin on tehnyt aiheesta jutun muutama vuosi sitten, jossa toimittaja kokeili pääsyä erilaisiin toimistoihin ja tuotantotiloihin pelkästään huomioliivin ja muistiinpanovälineiden avulla. Ihmiset kun ovat luonnostaan hyvää tahtovia ja avuliaita niin pahantahtoisellekin teknikolle pidetään ovi auki ja parhaimmillaan tarjotaan vielä kahvit kaupanpäälle.

6.8 Käytännön maalaisjärki ja lähdekriittisyys

Tämä on jo otsikkotasolla varsin laaja käsite ja sitä on hyvin hankala tiivistää mihinkään lyhyeen nyrkkisääntöön. Fakta kuitenkin on, että niin pitkään kun ihmiset ovat minkäänlaista kanssakäymistä toistensa kanssa harrastaneet niin sekaan on aina mahtunut niitä, jotka yrittävät jollain tapaa hyötyä muista. Käärmeöljykauppiaita ei enää toritapahtumissa juurikaan näy, mutta niitä ja kaikkia muita huijareita nigerialaisista prinsseistä väärennettyihin postin kuljetuksiin löytyy verkosta enemmän kuin kukaan ehtii laskemaan.

Näiden tunnistaminen ja oikeaoppinen reagointi on kuitenkin avainroolissa sekä yritysten että ihan henkilökohtaisenkin tietoturvan varmistamiseksi. Huijaukset kehittyvät kokoajan paremmiksi ja huijarit kehittävät kokoajan uusia keinoja joilla saada uusia uhreja tarttumaan syöttiin. Tämä tarkoittaa myös sitä, että meidän kaikkien täytyy jatkuvasti ylläpitää taitoja tunnistaa huijareita.

Pienissä yrityksissä kaikki pääasiassa tuntevat toisensa, eli riski sille, että Whatsapissa toimitusjohtajan nimissä lähetetty viesti aiheuttaisi toimenpiteitä on aika pieni. Suuret yritykset etenkin kansainvälisillä markkinoilla taistelevat kuitenkin kokoajan näitä hyökkäyksiä vastaan. Usein käytetty huijaus on esittää yrityksen johtohenkilöä, joka on kokouksessa asiakkaan kanssa ja neuvotteluissa on herännyt yhtäkkiä tarve siirtää rahaa tilille tai hankkia asiakkaille kiitokseksi lahjakortteja. Huijari lupaa, että työnantaja kyllä maksaa kulut, kunhan uhri nyt äkkiä hoitaa maksun kuntoon vaikka sitten henkilökohtaisella kortillaan. Ei tarvinne kertoa, että miten rahoille käy jos tällaiseen sattuu lankeamaan.

Kaikkia mahdollisia versioita kuitenkin liikkuu varsinkin sähköpostissa suunnilleen yhtä paljon kuin ihan oikeaakin postia. Roskapostisuodattimet toki syövät näistä suurimman osan, mutta aina toisinaan jotain pääsee läpi.

> Johnson Philip tarjoaa varsin mukavaa summaa provisiopalkkiota, kunhan järjestelen hänen kanssaan 12,5 miljoonaa dollaria Ukrainan kriisin myötä takavarikoituja Venäjän varoja länsimaiselle pankkitilille. John kertoo että olen päässyt Kuka kukin on -kirjaan ja Amerikan verovirasto kertoo että minulla on kymmenien tuhansien veronpalautukset odottamassa.

Kaikissa esimerkeissä on tietysti linkit mukana, joita pitää klikata juuri nyt tai nämä valtavan hienot tilaisuudet valuvat seuraaville.

Täällä Suomessa olemme toistaiseksi olleet aika hyvin turvassa ihan pelkästään kielimuurin takia, huijarit kun toimivat pääasiassa englanniksi, mutta täysin oikeaoppista suomeakin alkaa eri huijauksissa näkymään. Edelliset esimerkit ovat tietysti aivan ilmeisiä, mutta muutaman kerran on ollut hyvin lähellä etten ole itsekin langennut rahtiliikenteen (Posti, Fedex, UPS) nimissä lähetettyihin huijauksiin ja Postin osalta näitä huijauksia on käsitelty ihan Ylen uutisissakin.

Tarkkana siis pitää olla. Ihan ensimmäisenä on hyvä käydä läpi, että onko viesti nyt jollain tapaa ajankohtainen ja että täsmääkö viestin lähettäjätiedot sisällön kanssa. Esimerkiksi postin nimissä lähetetyt ilmoitukset, että paketin toimituksessa on jotain vikaa on helppo poistaa katsomatta jos voi olla varma ettei postin kyydissä ole mitään lähetystä yritykselle tulossa. Toiseksi ennen linkkien avaamista tulee katsoa että onhan osoite nyt oikea. Verkkosivut saadaan näyttämään täysin autenttisilta hyvinkin helposti, mutta itse osoitteen väärentäminen on nykyään hyvin hankalaa, joskin postii.com saattaa nopeasti vilkaisemalla mennä läpi.

Luku 7

Lisää luettavaa ja katsottavaa

Kuten jo moneen kertaan olen todennut, tämä opas ei ole mikään kaikenkattava kokonaisuus vaan ennemminkin tönäisy oikeantyyppiseen ajatusmaailmaan. Verkosta löytyy hyviä resursseja joilla syventää omaa ymmärrystä tietoturvankin osalta, mutta lähdekriittisyys ja medialukutaito on näidenkin osalta ihan avainasemassa ettei omaa toimintaansa pohjaa väärällä tapaa painotettuun tai suoraan virheelliseen tietoon.

Tässä muutamia luotettavaksi todettuja resursseja.

- Kyberturvallisuuskeskuksen oppaat
  - https://www.kyberturvallisuuskeskus.fi/fi/ohjeet
  - Kyberturvallisuuskeskus on Traficomin (Liikenne- ja viestintävirasto) ylläpitämä palvelu ja sivustolta löytyy ohjeiden lisäksi ajankohtaisia uutisia tietoturvasta. Kyberturvallisuuskeskus myös vastaanottaa ilmoituksia tietoturvaloukkauksista ja yleisesti ylläpitää valtion tuottamia tietoturvapalveluita.
- Ylen digitreenit
  - https://yle.fi/aihe/digitreenit
  - Ylen digitreeneissä on ohjeita laidasta laitaan ja painotus on enemmän yksityishenkilöiden tietoturvassa, mutta samat ohjeet pätevät yhtä lailla yritysmaailmaan. Samalta sivustolta löytyy myös ohjeita mm. mobiililaitteiden käyttöön ja tekijänoikeusasioihin. Digitreenien lisäksi suosittelen katsomaan Areenasta Team Whack -juttusarjan, jossa tietoturvan ammattilaiset näyttävät ihan konkreettisesti miten nopeasti osaava tekijä pääsee heikosti suojattuihin järjestelmiin käsiksi.
- Suomen yrittäjien tietopankki
  - https://www.yrittajat.fi/tietopankki/turvaa-yrittamiseen/riskinhallinta/tietoturva/
  - Yrittäjäyhdistys tarjoaa myös jäsenilleen ohjeita ja artikkeleita tietoturvasta ja sen hallinnasta. Painotus on vähän enemmän lakien ja säännösten huomioinnissa kuin käytännönläheisessä tietoturvassa, mutta mm. GDPR asettaa omat vaatimuksensa yritystoimintaan ja niiden noudattaminen on yhtä lailla tärkeää yritystoiminnassa.

- Hakukoneet
  - Hakukoneet ovat äärettömän tehokkaita työkaluja myös tietoturvakysymyksiä selvitettäessä. Etenkin IoT-laitteiden kanssa 'laitteen nimi + tietoturva' -haku paljastaa usein hyvin nopeasti minkälaisesta älylampusta tai kahvinkeittimestä on kysymys ja että kannattaako sitä kytkeä omaan verkkoon kiinni.