Opinnäytetyö AMK

Tieto- ja viestintätekniikka

2022

Jaakko Eskelinen

TURVATTUA TIETOA

– tietoturvan toimet ja tavoitteet kansantajuisesti

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2022 | 21 sivua

Eskelinen Jaakko

TURVATTUA TIETOA

- tietoturvan toimet ja tavoitteet kansantajuisesti

Tässä työssä läpikäydään tietoturvan tarkoitus ja ne osat, joista se koostuu kansantajuisesti. Jotkin kokonaisuudet on yksinkertaistettu juuri tuosta syystä. Työn tarkoituksena ei ole vertailla protokollia tai syväluodata niiden mahdollisuuksia vaan luoda perusta, jolla jokainen käyttäjä pääsee sille tietotasolle, missä liian useat ohjeet ja opastukset olettavat lukijan olevan.

Rajan vetäminen perustiedon ja syventymisen välillä on vaikea tietotekniikassa, minkä vuoksi joitain osioita on käsitelty syvemmälti kuin toisia. Osioissa, joissa on jouduttu avaamaan teknistä koostumusta, on koitettu pitää mahdollisimman helposti ymmärrettävissä. Tämän seurauksena teknistä protokolla puolta on saateltu käsitellä vain osittain.

Jo olemassa olevia ohjeistuksia ja opastavia sivustoja on mainittu sekä esitelty työn loppupuolella. Työssä mainitut opastavat ja ohjaavat sivut auttavat kaiken tasoisissa digiongelmissa.

Työtä voisi jatkaa kokoamalla opetusmateriaalia, missä olisi koottuna arjen perusdigitarpeita vastaavat esimerkkikohdat ja tavat toimia.

ASIASANAT:

tietoturva, internet, tietotekniikka, tietosuoja

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Engineering, Information and Communications Technology

2022 | 21

Eskelinen Jaakko

SECURED INFORMATION

- acts and aims of information security in lay terms

In this thesis information security and its core elements are reviewed and interpreted.

A few protocols or methods are illustrated commonly to better serve those that do not take interest in information and communications technology. This work aims to help everybody reach a beginner level of skills in information technology.

Drawing a line between common knowledge and a deeper understanding of information technology is difficult. In few parts of this work, it was necessary to explain the underlying technical components to make it easier to understand the entirety. For this same reason, the explained technical properties and protocols might have been only partly studied to ensure that it remains simple enough for everybody to understand which is the main point of this thesis.

Existing guidance and article pages are examined at the end of the work. These webpages provide aid with various levels of problem-solving regarding information technology.

The study could be expanded by providing a set of learning material with examples covering the usual everyday information technology problems.

KEYWORDS:

security, data protection, internet, information technology

SISÄLTÖ

KUVAT

SANASTO

Wi-Fi	Kauppanimi, joka pohjautuu IEEE802.11 -ryhmän standardeihin
WLAN	IEEE802.11 -ryhmässä määriteltyjä standardeja käyttävä tietokoneen liityntäverkko
WPA2+AES	Langattoman lähiverkon salausmenetelmä, joka perustuu esijaettuun salasanaan
USB	Tietokoneen liitäntäjärjestelmä (Usb.org)
HTTPS	Suojattu verkkoliikenteen protokollatunnus
SATU	Sähköinen asiointi tunnus, joka toimii kansalaisvarmenteen yksilöivänä tunnistetietona
GHz	Gigahertsi on kansainvälisen yksikköjärjestelmän mukainen taajuuden yksikkö (SI-järjestelmä)

1 JOHDANTO

Tietokone tehtiin työkaluksi, josta se kehittyi osaksi arkea. Työkalun tehtävä on helpottaa tai vähentää työmäärää. Valitettavasti tietokoneen kohdalla tämä ei kaikille pidä paikkaansa. Usein työmäärän vähenemisen sijaan työ lisääntyy, kun työkaluna on tietokone. Liian usein tietokoneen käyttämisen ohjeet ja opastukset olettavat ohjetta lukevan jo osaavan ja ymmärtävän tiettyjä asioita. Joidenkin kohdalla se onnistuu, kun taas toisten kohdalla ohjeet jäävät ymmärtämättä, koska ohjeen tehneen tahon olettama tietämys puuttuu. Yleensä asia korjaantuu ottamalla yhteyttä työpaikan it-tukeen, mutta ongelman ollessa kotitietokoneella saattavat keinot loppua kesken.

Tiedon ja älylaitteiden lisääntyessä on tietoturvan rooli saman aikaisesti kasvanut ja vähentynyt. Kasvanut siinä mielessä, että laitteiden ja saatavilla olevan tiedon määrä kasvaa koko ajan, mutta myös vähentynyt, sillä käyttäjien tietoisuus ja ymmärrys asiasta ei ole lisääntynyt samassa tahdissa kuin tieto. Tämä on ongelma, jota tietoturvaprotokollien ja laitteiden parantaminen ei ratkaise, sillä paraskaan viruksentorjuntaohjelmisto tai palomuuri ei suojaa, mikäli käyttäjä ei niitä käytä. Ideaalisti tietoturva toimisi, kuten autolla ajaminen ajokortin saamisen jälkeen. Autoa voi ajaa ilman, että tietää, miten vaihteisto toimii tai miltä moottorin sisällä näyttää. Toki autosta saa enemmän hyötyä, kun tietää miten se toimii, mutta perustoimintoja voivat käyttää kaikki siihen opetetut. Vaikka tietoturva osaamista on parannettu lisäämällä tietotekniikka opetusta peruskoulussa, on sillä saralla vielä paljon työtä. Usean aikuisen ja nuorenkin digitaidot riittävät nettipankissa asioimiseen ja muiden arjen pakollisten asioiden hoitamiseen. Joillakin taidot eivät riitä näihinkään, mutta silti digitaalinen ja sähköinen asioiminen lisääntyy joka vuosi.

Opinnäytetyöni tarkoitus on selvittää, miten tietoturva-asioita voi esittää kansantajuisesti ja miten alati lisääntyvistä digihaasteista selviää, vaikkei olisi hyvää digiosaamista.

2 TIETOTURVA

Tietoturva sanana on monelle varmasti tuttu jo peruskoulusta lähtien, mutta mitä sana tarkoittaa ja miten se näkyy arjessa. Toisille se on palomuurien ylläpitämistä ja käyttäjien hallintaa, toisille puhelimella pankkiasiointia ja kolmannelle ehkä kahvilan Wi-Fi verkossa koulutehtävien palauttamista. Kaikissa kolmessa käyttäjä on keskeisessä roolissa tietoturvan toteutumisessa. Käyttäjän roolia korostetaan useissa käyttöoppaissa ja ohjeistuksissa, mutta oikeita neuvoja tai toimia harvoin selitetään yhtä perusteellisesti.

Asioimisen verkossa ja sen ulkopuolella voi tehdä turvalliseksi monella pienelläkin keinolla. Jotkin tietoturvaa edistävistä toimista tuntuvat niin tavallisilta, ettei niitä välttämättä edes osaa yhdistää tietoturvaan. Tietoturva on kattava ja laaja termi, joka sisältää monta osaa. Tietokoneen ulkoinen pölyjen pyyhintä on yhtä lailla tiedon turvaamista siinä missä salasanasuojattu kirjautuminenkin. Tieto-sanalla viitataan tässä työssä kaikkiin mahdollisiin tiedostoihin, kuviin, sähköposteihin, linkkeihin, tallennettuihin salasanoihin sekä kaikkiin niihin toimiin, mihin puhelinta tai muuta vastaavaa laitetta tarvitaan. Tärkeimpinä ja yleisimpinä näistä mainittakoon nettipankkiasiointi sekä vahva sähköinen tunnistautuminen.

2.1 Tietoturvan koostumus

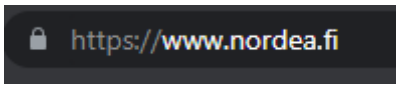
Tietoturva on toimien ja välineiden kokonaisuus, johon vaikuttavaa monet tekijät kuten: mihin käyttöön laite on tarkoitettu tai onko laitteella monta käyttäjää sekä mitä tietoja laitteella tullaan käsittelemään.

Yhtä lailla kuin kaikilla on omat pankkitunnuksensa tulisi kaikilla käyttäjillä olla omat tunnuksensa, jolla kirjaudutaan laitteelle, mikäli laite on yhteiskäytössä. Myös yhden henkilön käytössä olevalle tietokoneelle olisi viisasta tehdä kaksi järjestelmänvalvojan oikeuksilla varustettua tiliä. Tällöin mikäli yleisesti käytössä olevalle tilille tapahtuisi tietojen korruptoituminen tai lukkiutuminen, voi tietokonetta edelleen käyttää ilman suurempia palautustoimenpiteitä. Digivinkit-nimisellä verkkosivulla on perusteellinen ohje uuden paikallisen käyttäjätilin luomiseen (Digivinkit 2019).

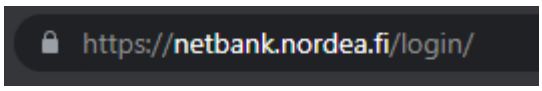
Tietoturvassa on kyse tiedon menetyksen aiheuttamasta rahallisesta tai aineellisesta menetyksestä verrattuna käytettyihin tietoturvamenetelmiin. Tämä tarkoittaa sitä, että tietoturvaan käytetty aika ja varat tulisi olla yhtä suuret kuin mahdolliset menetykset. Käyttäjälle tämä näkyy siinä, että laite, jolla asioidaan pankkisovelluksessa, on tietoturvallisesti arvokkaampi kuin pelaamiseen tai videoiden katseluun tarkoitettu tabletti. Pankkitunnuksien halutaan pysyvän turvassa, jolloin myös laite, jota käytetään niiden kanssa, tulisi olla suojattu sen mukaisesti. Tieto, jota silloin halutaan turvata, on yhteys pankkiin ja omaan pankkitiliin sekä usein myös vahvaan sähköiseen tunnistautumiseen. Arkielämässä esimerkkinä voisi toimia rahan lähettäminen postitse. Harvemmin kukaan haluaa lähettää rahaa postikorttiin teipattuna, vaan mieluummin laittaa sen kirjekuoren sisälle. Samaa ajattelutapaa käyttäen pärjää arjen digihaasteissa hyvin.

2.1.1 Internet ja verkko-osoitteet

Verkko-osoite kertoo jo paljon sivuston tai palvelun turvallisuudesta ja autenttisuudesta. Www.nordea.fi on verkko-osoite, joka vie Nordea verkkopankin nettisivuille. Suurin osa verkko-osoitteista alkaa kirjaimilla Www (World Wide Web). Verkko-osoitteessa voi olla pisteiden lisäksi muitakin merkkejä kuten vino- ja väliviivoja kuten kuvista 1 ja 2 käy ilmi. Yleensä virallisten tahojen nettisivujen osoitteet ovat lyhyitä ja selkeitä. Kun osoite päättyy .fi/-merkkeihin avautuu silloin hyvin todennäköisesti etusivu. Mikäli vinoviivan jälkeen on lisää tekstiä, se on yleensä osoite jollekin tietylle osiolle sivustolla.



Kuva 1. Nordean etusivun verkko-osoite.



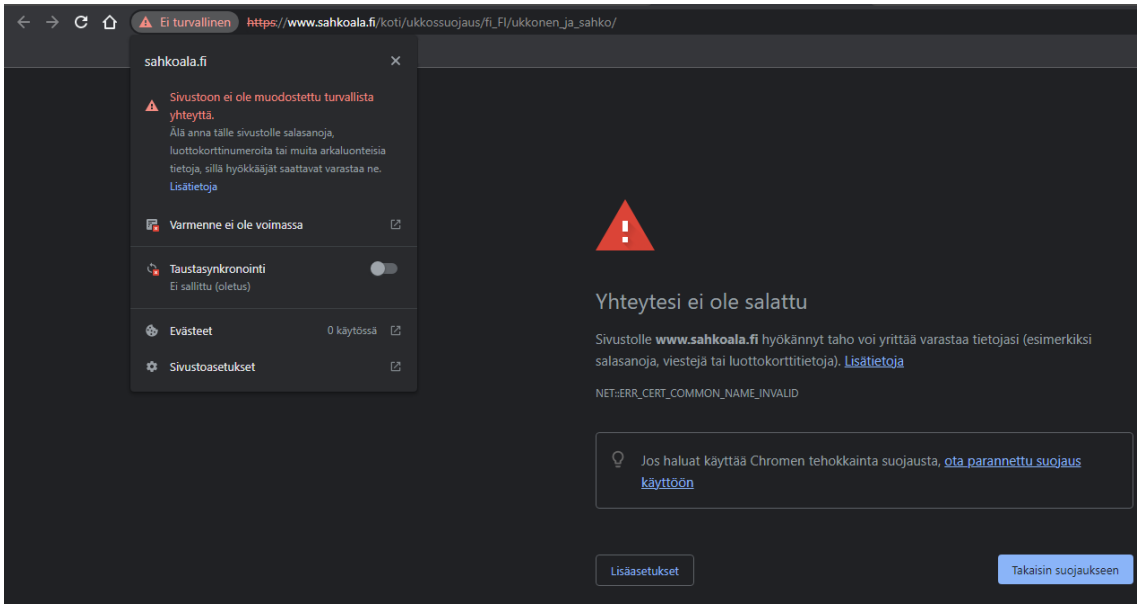
Kuva 2. Nordean nettipankin kirjautumis- verkko-osoite.

Molemmat osoitteet näyttävät turvallisilta, sillä molemmista on helposti pääteltävissä minkälaiseen sivuun ne avautuvat. Tärkeät autenttisuuden varmistavat tekijät näkyvät osoiterivin vasemmalla puolella. Suljettu lukkokuvake ja https://- alku verkko-osoitteen edessä kertovat sivuston olevan suojattu.

Https on lyhenne tietylle verkkoprotokollalle, joka on suunniteltu suojaamaan käyttäjän tietokoneen ja verkko-osoitteen välinen liikenne. Suojatulla tässä yhteydessä tarkoittaa sitä, että se informaatio, mitä käyttäjän tietokoneen ja Nordean nettisivun välillä liikkuu, on suojattu ulkopuolisilta katseilta. Postikortti ja kirjekuori vertauksena tieto nettipankkiin kirjautumisesta on kirjekuoren sisällä turvassa. Silloin se, mitä käyttäjä on siihen kirjoittanut, on täysin sama kuin vastaanottaja eli Nordean nettipankki vastaanottaa. Piilossa muilta ja sisältö salattuna pysyy myös se, mitä käyttäjä on lähettänyt vastaanottajalle. Tällöin käyttäjä voi olla varma siitä, että kaikki se, mitä nettisivulla näkyy, on autenttista tietoa, jota ei ole peukaloitu matkan varrella.

Suljettu lukkokuvake on merkkinä hyväksytystä varmenteesta. Monet tunnetut selaimet (Microsoft Edge eli entiseltä nimeltään Internet Explorer, Google Chrome ja Mozilla Firefox) auttavat käyttäjää tunnistamaan sekä varmenteen että luotetun verkko-osoitteen. Mikäli toinen näistä puuttuu, on tietoturvan taso alempi. Vanhentunut varmenne ei itsessään tee sivustosta epäluotettavaa, mutta se antaa syyn epäillä tietojen autenttisuutta. Varmenteiden päivittäminen on verkkosivun omistajan, tässä esimerkkitapauksessa siis Nordean vastuulla.

Yleensä yritykset ostavat verkkosivujen turvallisuuteen ja päivityksiin sekä ylläpitoon palvelun joltain verkkosivuihin erikoistuneelta yritykseltä. Yritysten verkkosivujen tietoturvallisuuteen liittyvissä kysymyksissä kannattaa aina olla yhteydessä suoraan kyseiseen yritykseen. On myös yrityksen etu, että heidän sivustonsa vaikuttavat asiakkaalle turvallisilta. Internet-selain ilmoittaa yleensä hyvin selvästi, mikäli varmenne on vanhentunut tai muutoin epäkelpo. Esimerkiksi, jos nettisivun osoite tai nimi on muuttunut, silloin uuden nettisivun varmenne ei toimi vanhan nettisivun osoitteessa. Kuvassa 3 on Chrome internet -selaimen ilmoitus tietosuojavirheestä.



Kuva 3. Tietosuojavirhe.

Selain antaa varoituksen heti, kun valittua sivua yrittää avata, sekä selityksen, miksi sivu estettiin. Myös yliviivattu ja punaiseksi maalattu https-osoitteen alussa kertoo tietojen olevan vaarassa. Kun klikkaa punaista kolmiota osoiterivin alussa, tulee esiin kuvassa auki oleva pienempi tietoikkuna, joka selventää lisää, miksi yhteys ei ole salattu. Yleensä jos tämmöinen varoitus tulee vastaan, on kyseessä väärä nettisivun osoite tai osoite on vanhentunut. Tässä tapauksessa kyseessä on väärä osoite. Sivusto oli vaihtunut sahko-maailma.fi-nimiseksi, minkä vuoksi varmenne ilmeni selaimelle viallisena. Kun saman osoitteen kirjoitti hakukoneeseen, löytyi heti uuden sivuston linkki.

2.1.2 Fyysiset laitteet

Tietokoneen keskusyksikön sekä oheislaitteiden siivoaminen on osa tietoturvaa. Nyky-aikana useimmilta löytyy tietokoneen lisäksi puhelin tai tabletti, jolla arkipäivän asioita hoidetaan netissä ja tällöin myös näiden laitteiden huoltaminen on osa tietoturvaa.

Jos tietokoneen keskusyksikkö ylikuumentuu laitteen sisään päässeen pölyn vuoksi tai tabletti kostuu sade säässä, ovat tiedot silloin vaarassa. Ja kuten aikaisemmin jo todettiin, tieto tarkoittaa kaikkea sitä, mihin laitetta käytetään.

Tietokoneen keskusyksikköä ei tarvitse päivittäin puhdistaa, mutta viikoittainen pölyjen pyyhintä ja imurointi tietokoneen läheisyydestä pidentää laitteen elinikää sekä takaa sen

toiminnan. Laiteen tulee olla pois päältä, kun itse laitetta puhdistetaan imurilla tai paineilmalla. Mikäli laite on päällä, kun sen sisältä imuroidaan tai puhalletaan paineilmaa, voivat elektroniset osat vaurioitua ja pahimmassa tapauksessa rikkoutua.

Sama pätee kannettavaan tietokoneeseen. Kannettavan tietokoneen tuuletusaukon kohdalta voi imurilla poistaa sisään mennyttä pölyä. Kannettavaa tietokonetta ei kannatta pitää pitkiä aikoja kankaisella alustalla, sillä useimmissa malleissa tuuletusaukot sijaitsevat reunassa tai kannettavan tietokoneen pohjassa, jolloin laitteeseen joutuu tekstiilipölyä. Laite kuumenee nopeammin, ja sen suorituskyky hidastuu pölyn täyttäessä laitteen elektronisten osien pinnat ja ilmatiet. Myös tulipalon riski kasvaa, kun syttyvää ainetta joutuu laitteen kuumeneville pinnoille.

Kotiin olisikin hyvä hankkia palopeite, jolla pienet sähkölaitepalot saadaan sammutettua. Paloturvallisinta on pitää tietokoneen ympärillä tarpeeksi vapaata tilaa, jotta sammuttaminen palopeitteellä tarvittaessa onnistuu. Palopeitteellä sammuttaminen perustuu hapen poistamiseen palavan laitteen ympäriltä. Hapen pääsy tulee estää täysin palavaan laitteeseen, jotta palo sammuu. Palopeite pitää kietoa palavan laitteen ympärille tiivisti joka puolelta ja painaa sen reunat vasten pöytää tai tasoa, jonka päällä palava laite on. Tämä ei ole mahdollista, mikäli laitteen ympärillä on muita esineitä tai laite sijaitsee pienessä tilassa. Kun tilaa on laitteen ympärillä tarpeeksi, on sammutus ja siivoaminen helpompaa. (Kodinturvaopas).

Puhelinten ja tablettien kanssa paloturvallisuus on tärkeintä laitteita ladattaessa. Nykyajan akut, joita puhelimissa ja tableteissa käytetään, harvoin hyötyvät täyteen lataamisesta. Usein uudet laitteet on varustettu helppokäyttöisillä akun terveydentilan seuranta sovelluksilla, jotka kertovat akun varaustason ja kunnon. Jotkin laitteet myös seuraavat latauksen aikana akun toimintaa ja rajoittavat latausta, mikäli akku tai laite kuumenee liiaksi. Vaikka useimmissa uusissa laitteissa onkin tämä ominaisuus, on hyvä olla jättämättä laitetta turhaan latautumaan. Puhelimen yön yli latauksessa on vaarana akun ylikuumeneminen ja siten mahdollinen tulipalon riski, koska puhelin latautuu yleensä pöydällä tai muulla palavalla alustalla, jolloin ylikuumentunut akku saattaa sytyttää alustan palamaan.

Yleensä liian korkea lämpötila laitteen tai akun sisällä saattaa johtua täysin normaalista käytöstä, mutta mikäli laite itsessään tuntuu useasti erittäin kuumalta latauksen aikana, on syytä tarkistuttaa laitteen akku jälleenmyyjällä tai viedä laite huoltoon akun vaihtoon.

2.1.3 Langalliset laitteet

Langallisissa laitteissa USB-johto toimii tiedon kuljettamisessa näppäimistön ja tietokoneen välillä. USB-johdoista löytyy eri liitinpäillä varustettuja versioita. Suurin osa kuluttajista käyttää päivittäin USB versio-C:tä. Tällä yleisimmällä johdolla ladataan mm. polkupyörän valot, tabletit ja puhelimet. Toki tuotteen mallista ja valmistajasta riippuu, minkälaista johtoa on käytettävä ja toimitetaanko sellainen uuden laitteen mukana. Euroopan parlamentti ehdotti syyskuussa 2021 USB versio-C:n standardisoimisesta osana toimiaan vähentää elektroniikka jätettä niin luonnon kuin kuluttajienkin kannalta. 6.10.2022 julkaistu artikkeli Euroopan parlamentin nettisivuilla kertoo, mitä muutoksia on odotettavissa kuluttajille lain tullessa voimaan. (Euroopan parlamentti 2022).

Langallisten laitteiden ollessa suoraan kiinni kytkettyjä tietokoneeseen ei salakuuntelu painetuista näppäimistä tai hiiren liikkeistä ole mahdollista ilman, että joko laitteen sisällä tai johdon ja tietokoneen välissä on kuuntelulaite. Tämä urkintaan tehty laite voi olla sisäänrakennettu USB-johdon liittimen osaan, jolloin on mahdotonta sitä paljain silmin nähdä. Sama pätee, mikäli laite olisi näppäimistön tai hiiren sisällä, jolloin ylimääräisen osan huomaaminen olisi suurimmalle osalle käyttäjistä mahdotonta. Mikäli laite on hankittu tunnetusta ja luotettavasta jälleenmyyntipisteestä ei ole todennäköistä, että urkintavälineitä olisi piilossa laitteessa. Harvalla käyttäjällä on pääsyä rikollisia kiinnostaviin niin arvokkaisiin tietoihin, että se maksaisi vaivan asentaa urkintalaitteita tuhansiin ja taas tuhansiin laitteisiin. Fyysisesti paikallaan pysyvät laitteet kuten pöytäkoneet ja niiden oheislaitteet ovat muutenkin vaikeasti joka roiston saavutettavissa. Toki tämä pätee vain fyysisten laitteiden seurantaan, internetissä tapahtuvaa rikollisuutta voi tehdä mistä käsin vain. Yleisesti käytössä olevista tietokoneista harvoin voi varmuudella sanoa niiden olevan tietoturvallisia, joten on syytä välttää henkilötietojen käsittelyä tällaisilla laitteilla.

2.1.4 Langattomat laitteet

Langattomat laitteet toimivat yleensä Bluetooth- nimisellä menetelmällä, joka perustuu radioaaltoihin. Radioaaltojen taajuus vaihtelee 2,402GHz – 2,480GHz. Bluetoothin langaton tiedonsiirto on kasvattanut suosiotaan oheislaitteissa, kun sen tiedonsiirtonopeus on noussut tekniikan kehittyessä. Bluetooth menetelmällä toimii niin näppäimistöjä, hiiriä, kaiuttimia kuin kuulokkeitakin. Näissä laitteissa saattaa joskus tulla mukana pieni USB-liitin, joka toimii Bluetooth-vastaanottimena päätelaitteelle. Useimmissa tietokoneissa,

niin kannettavissa kuin pöytäkoneissakin, on sisäänrakennettu Bluetooth -vastaanotin, mutta jotkin laitteet tarvitsevat oman erillisen liittimen, jossa on myös mukana tarvittava ohjelmisto tai koodi, jolla tietokone osaa tulkita liitetyn laitteen oikein. Kuulokkeissa ja kaiuttimissa usein laite valitaan puhelimesta tai vastaavasta laitteesta, jolla musiikkia halutaan toistaa, mutta hiiren tai näppäimistön kanssa erillinen liitin on pakollinen. Hiiren tai näppäimistön mukana tuleva liitin on jo yhdistetty toimimaan päätelaitteen kanssa, jolloin juuri se hiiri tai näppäimistö lähettää tietoa vain tiettyyn vastaanottimeen. Tällöin näppäimistöllä painellut näppäimet liikkuvat radioaaltoja pitkin tietokoneelle tulkittavaksi. Kun tieto liikkuu ilmassa radioaaltoja pitkin, on myös sen kaappaaminen helpompaa kuin lankaa pitkin kulkevan. Tämän vuoksi julkisilla paikoilla, kuten kahviloissa, kirjastoissa ja etätyöpisteissä, olisi turvallisempaa käyttää langallista näppäimistöä ja hiirtä. Bluetooth-tekniikan suurin kantama on vain 10 m, mutta sen kokoisen alueen tarkistaminen vaikkapa kahvilassa olisi sekä aikaa vievää, että usein liki mahdotonta.

Tästä syystä työpaikoissa, joissa käsitellään henkilötietoja tai muuta arkaluonteista asiaa, voidaan langattomien laitteiden käyttö kieltää tietoturvauhan perusteella. Myös tavallisen käyttäjän tietojen kaappaaminen kiinnostaa rikollisia. Rikolliset yrittävät kaapata salasanoja urkkiakseen mm. henkilöiden tilitietoja. Käyttäjätilitiedoissa yleensä on nimitietojen lisäksi osoite, pankkikortin tiedot sekä puhelinnumero. Tästä syystä olisi hyvä poistaa maksukorttien tiedot käyttäjätileiltä maksun jälkeen, tai muutoin varmistaa, ettei tili voi suora veloittaa ilman vahvaa tunnistautumista. Tällöin tilin salasanan saaminen ei vielä tuota taloudellista menetystä tilin alkuperäiselle omistajalle.

2.2 Tietoturvan mittaaminen

Miten sitten voi kotona mitata oman tietokoneensa tietoturvan vastaavuuden mahdollisiin menetyksiin? Yksi tapa on miettiä, kuinka paljon aikaa ja työtä kuluisin tilanteen korjaamiseen identiteettivarkauden, tietovuodon, tietojen korruptoitumisen tai haitallisen ohjelman jälkeen. Jos on hyvät tietotekniset taidot ja ymmärtää, miten tilanteessa pitää toimia, hoituu tilanteen korjaaminen helposti. Mikäli taidot riittävät vain jokapäiväisten asioiden hoitoon tietokoneella on mahdollista, ettei käyttäjä edes tiedä mistä aloittaisi. Seuraavaksi käydään läpi mahdollisten arkipäiväisten tietoturvauhkien torjumista ja niiden seurausten korjaamisesta.

2.2.1 Lähiverkot

Langaton lähiverkko eli WLAN löytyy nykyään melkein jokaisesta kodista ja kauppaliikkeestä. WLAN on standardisoitu tekniikka, josta käytetään myös kauppanimenä Wi-Fi:ä. Kuten Bluetooth WLAN perustuu radioaaltoja pitkin kulkevaan tietoon. WLAN-laitteet toimivat 2,4GHz:n sekä 5GHz:n radiotaajuusalueella. (IEEE802.11) Nämä merkinnät saattavat olla tuttuja mm. tulostinten, tablettien sekä kannettavien tietokoneiden yhteydestä. Kaikki laitteet eivät välttämättä pysty toimimaan molemmissa taajuuksissa, niiden rakenteellisten ominaisuuksien takia. Esimerkiksi jotkin tulostimet tukevat vain 2.4GHz:n radiotaajuuden WLAN-verkkoyhteyttä. WLAN on hyvin yleistynyt standardi, mikä tekee siitä helppokäyttöisen käyttäjälle, mutta myös helpon kohteen rikollisuudelle.

WLAN toimii pintapuolin tarkasteltuna kuin radiopuhelin. Mikäli puhuu radiopuhelimeen tietyllä taajuudella, niin kaikki samalla taajuudella olevat kuulevat puhujan. Yhtä lailla WLAN-verkossa liikkuva tieto on kaikkien samalla taajuudella olevien kuultavissa. Tämän vuoksi vapaasti etenevä tieto pitää olla salakirjoitus algoritmilla suojattu. Koska joitain aikaisemmin käytettyjä tiedon suojaustapoja on pystytty murtamaan, on WPA2+AES-salaus yleistynyt kotikäyttäjillä. WPA2+AES on tietoturvaprotokolla, joka on tullut standardiksi langattomiin lähiverkkoihin. Protokolla muuttaa langattomassa lähiverkossa liikkuvan tiedon salatuksi niin, että ilman käännösohjetta eli teknisellä termillä avainta (engl. pre-shared key) tieto on käyttökelvotonta. Protokolla antaa reitittimelle ja päätelaitteelle käännösohjeen. Tällöin vain halutut laitteet ymmärtävät taajuudella liikkuva tiedon. Protokollan käyttöönottoon ja asetuksiin palataan seuraavassa kappaleessa.

Suojaamattomien lähiverkkojen käyttö ei ole rangaistava teko, mutta riitojen välttämiseksi olisi muiden omistamien verkkojen käyttö pidettävä mahdollisimman vähäisenä. Mikäli suojaamattoman lähiverkon kautta muodostetaan yhteys sen sisällä toimiviin palvelimiin tai laitteisiin voi kyseessä olla rangaista luvaton käyttö. Mikäli salasana suojatun lähiverkon salaus murretaan, on silloin mahdollisesti kyse rikoslain 8:8a:ssa tarkoitetusta tietomurrosta. Myös tietomurron yritykset ovat rangaistavia. Harvemmin käyttäjä huomaa luvatonta lähiverkon käyttöä. Mikäli luvaton käyttö on edennyt poliisin tutkittavaksi, selviää asia käyttäjälle vasta silloin. Langattoman lähiverkon luvaton käyttö on helpointa estää vahvalla ja tarpeeksi pitkällä salasanalla.

WPA2+AES-protokolla suojaa vain langattomassa lähiverkossa liikkuvan tiedon eli sen mikä liikkuu reitittimen ja päätelaitteen eli esim. tietokoneen välillä. Reitittimestä eteenpäin tieto liikkuu internet johtoa pitkin isompiin välityspalvelimiin ja sitä kautta internettiin. Suojattu langaton lähiverkko muuttuu siis suojaamattomaksi, kun se muuttuu reitittimen jälkeen langalliseksi. Tämän takia salattu liikenne päätelaitteen ja verkkosivun välissä on tärkeä. Kuten aikaisemmin todettiin verkko-osoitteen turvallisuudesta, päästä päähän salattu liikenne ilmaistaan verkkoselaimessa suljettuna lukko- kuvakkeena sekä https-alkuna osoitteessa. Nämä tekijät jatkavat langattoman lähiverkon suojausta ja siten turvaavat tiedon.

2.2.2 Reititin

Reititin on kuin pieni tietokone, joka toimii kodin tietoliikenteen ja internetin välisenä viestinviejänä. Reititin jakaa internetosoitteet kaikille laitteille, joihin se on kytketty. Wi-Fi:n kautta yhdistetty älypesukone, internetjohdolla yhdistetty televisio sekä pöytätietokone ovat kaikki saaneet internetyhteytensä sekä osoitteensa reitittimeltä. Internetosoitteet toimivat hiukan kuten asuntojen osoitteet. Niiden avulla reititin osaa ohjata tiedon oikealle laitteelle. Yleensä reitittimet antavat ennalta määrätystä joukosta vapaan osoitteen sen hetkisille laitteille, jotka ovat aktiivisia. Tästä syystä esimerkiksi televisio voi joskus valittaa internet yhteyden puuttumisesta, koska osoite, jonka televisio oli saanut viimeksi oltuaan päällä, onkin osoitettu toiselle laitteelle. Tämä korjaantuu sammuttamalla reitittin sen omasta virtanappulastaan ja kun kaikki laitteessa olevat valot ovat sammuneet, käynnistämällä se uudelleen. Tällöin reititin antaa kaikille aktiivisille laitteille uudet osoitteet ja palauttaa internet yhteyden.

Reitittimet saavat yleensä järjestelmäpäivityksensä käytössä olevalta operaattorilta etäyhteyden kautta. Laitteissa on tehdasasetuksissa jo kaikki tarvittava valmiina. Tämä sisältää mainitun WPA2+AES suojauksen. Laitteen kyljessä olevasta tarrasta yleensä selviää laitteen malli, valmistaja sekä langattoman lähiverkon salausavain eli salasana. Reitittimen käyttöliittymään pääset kirjoittamalla internetselaimeen samaisesta tarrasta löytyvän IP-osoitteen. Laitteen mukaan osoite saattaa vaihdella, mutta esimerkkinä tässä Zyxel-merkkisen reitittimen oletus IP-osoite: 192.168.10.1. Osoite kirjoitetaan samalle osoiteriville kuin normaalistikin. Osoitteen takaa avautuu kirjautumisikkuna, johon käyttäjätunnus on oletuksena admin ja salasana joko verkon salasana tai erikseen mainittu kirjautumissalasana. Nämä oletussalasanat olisivat turvallista aina vaihtaa. Mikäli

laitteen mukana ei ole tullut käyttöohjetta, sellaisen voi pyytää jälleenmyyjältä tai hakea valmistajan omilta sivuilta. Verkon salasanan ei tarvitse olla helposti muistettavissa, koska mitä pidempi salasanan on, sen parempi. Esimerkiksi 20-merkkisen salasanan voi kirjoittaa paperille ja pitää sitä turvassa, sillä jos rosvo sen pöytälaatikosta löytää, silloin on suurempiakin puutteita turvallisuudessa kuin lähiverkon salasana.

2.2.3 Sähköinen kirjautuminen ja todentaminen

Salasanat ja pääsykoodit ovat osa todentamista, jolla kerrotaan tietokoneelle tai verkkosivulle, että sisään kirjautuva käyttäjä on tilin oikeaomistaja. Vahva tunnistautuminen on ollut esillä paljon viime vuosina koronan myötä. Vahvalla tunnistautumisella kirjaudutaan mm. useiden virastojen sivustoille kuten Kela, Verohallinto, Omakanta ja kunnallisen terveydenhuollon yhteydenotto sivustot. Vahva tunnistautuminen suojaa käyttäjien tietoja, mutta saattaa myös hidastaa tietoihin käsiksi pääsyä. Kaikille käyttäjille ei ole itsestään selvää mitä vahva tunnistautuminen tarkoittaa tai miksi sellainen on tarpeen kirjauduttaessa edellä mainittuihin palveluihin.

Sähköinen kirjautuminen on korvannut useita käyntejä asiakaspalvelijalla paikan päällä. Kuten tiskilläkin asioidessa on oltava todiste henkilöllisyydestä, useimmiten henkilökortti tai joissain tapauksissa passi. Tällöin henkilötodistuksesta käy ilmi henkilötietojen lisäksi kuva kortin omistajasta, jolloin voidaan varmistua käyttäjän identiteetistä. Tässä tapauksessa tunnistautuminen perustuu kahteen erilliseen tekijään: fyysiseen objektiin, mikä löytyy käyttäjältä eli henkilötodistus, ja henkilön yksilölliseen ominaisuuteen eli ulkonäköön, joka vastaa henkilötodistuksen kuvaa. Tällaista kahteen eri tekijään perustuvaa tunnistautumista kutsutaan vahvaksi tunnistautumiseksi. Sama periaate pätee sähköisessäkin asioimisessa. Vaikeutta tunnistautumiseen tuo tietokone. Sivusto, jota kautta kirjaudutaan, toimii sille annettujen ohjeiden mukaisesti. Tietokone ei voi verrata passissa olevaa kuvaa ja käyttäjän kasvoja kuten asiakaspalvelija vaan se toteaa tunnistautumisen onnistumisen muilla keinoin. Tietokone tarvitsee tiedot siitä, mitkä ovat hyväksyttyjä tunnistautumisen menetelmiä. Sähköpostipalveluihin, kuten Gmail tai Outlook, käyttäjän luoma salasana on hyväksytty metodi.

Salasanan suojaus perustuu käyttäjän tietämään asiaan. Salasanojen suurin uhka on väsytyshyökkäys. Väsytyshyökkäys (engl. brute-force attack) on rikollisten käyttämä keino saada muiden käyttäjätilien tiedot hallintaansa. Väsytyshyökkäyksessä erilaisia merkkiyhdistelmiä syötetään sähköpostin tai käyttäjänimen kanssa niin kauan, kunnes

salasana löytyy koetetuista vaihtoehdoista. (Kyberturvallisuuskeskus). Tämä hyökkäysmetodi on helpottunut tietokoneiden laskentatehon nousun myötä. Manuaalisesti tämmöinen hakkerointi veisi liian kauan aikaa verrattuna hyötyyn, jonka voro saavuttaisi, mutta automatisoituna tietokoneen laskentatehon kanssa asian laita on aivan toinen. Vaikka murretun salasanan takana ei olisikaan mitään rahanarvoista hyötyä, saattaa muilla vastaavilla tileillä löytyä pankkikortti tai muut maksutiedot. Tämän vuoksi jokaiselle käyttäjätilille tulisi olla oma salasanansa, jotta tietomurto ei leviä sen sattuessa.

Yhä useammissa sovelluksissa tai nettisivuissa on otettu kaksivaiheinen todistautuminen käyttöön. Yleensä toisena osana kaksivaiheista tunnistautumista on salasana. Toinen osuus tunnistautumisesta on jokin semmoinen fyysinen esine, mikä henkilöllä on hallussaan esim. avain tai kortti tai se voi perustua johonkin henkilön yksilölliseen ominaisuuteen kuten ääni, ulkonäkö tai olemus. Joissain työpaikoissa on käytössä varmennekortti, millä kirjaudutaan työtietokoneelle. Tällöin vahva tunnistautuminen perustuu henkilön hallussaan olevalle varmennekortille ja siihen liitettyyn salasanaan, jonka kortin omistaja tietää. Varmennekortti on työpaikan antama henkilökohtainen sirukortti, joka toimii kuten henkilökortin kansalaisvarmenne.

2.2.4 Sähköinen henkilöllisyys

Kansalaisvarmenne on Suomen poliisin myöntämän henkilökortin mukana tuleva sähköinen henkilötodistus. Se sisältää tavallisten henkilötietojen lisäksi SATU:n eli sähköisen asiointitunnuksen. SATU on juokseva sarjanumero eikä se kerro mitään käyttäjän tietoja numerosarjassa toisin kuin HETU eli henkilötunnus. Asiointitunnuksen käyttämiseen sähköiseen kirjautumiseen vaaditaan tietokoneen lisäksi kortinlukija laite sekä kortinlukija ohjelmisto. Kortinlukija laitteita on myynnissä isoissa marketeissa sekä elektroniikkaan erikoistuneissa kaupoissa. Kortinlukijaohjelmiston saa ladattua ilmaiseksi Digi- ja väestöviraston sivuilta. Samalta sivulta löytyy suomenkielinen ohje ohjelmiston asentamiseen ja käyttöönottoon. SATU:n aktivointiin tarvitaan henkilökortin mukana tullut aktivointitunnus. Mikäli tämä on kadonnut, on poliisin lupahallinnosta mahdollista tilata uusi aktivointitunnus. Aktivointitunnuksen mukana on myös PUK-koodi, jota tarvitaan, jos PIN-koodi lukkiutuu eli koodi kirjoitetaan väärin viisi kertaa peräkkäin. Kansalaisvarmenne on asennuksen jälkeen helpoimpia sähköisen tunnistuksen metodeja. Sillä voi kirjautua kaikkiin palveluihin samalla tavalla ja useammalle varmasti tärkeimpänä, samalla PIN-koodilla. Varmenteella voi lisäksi tehdä sähköisen allekirjoituksen sekä salata

sähköpostiviestejä. Digi- ja väestöviraston sivuilla voi testata sähköistä allekirjoitusta sekä kirjautumista turvallisesti. (DVV)

Sähköistä henkilöllisyyttä on vaikeampi pitää turvassa kuin fyysistä passia tai henkilökorttia. Mikäli passi tai henkilökortti katoaa, voi heti todeta henkilöllisyyden suojan olevan vaarannettu, mutta verkossa tapahtuvat identiteetti varkaudet huomataan yleensä vasta kun se on jo tapahtunut. Jotkin tietoturvapalveluita tarjoavat yritykset ovat lisänneet palveluihinsa myös identiteettimonitorointia. Tämä palvelu ilmoittaa mahdollisista tietovuodoista ja varkauksista. Suomi.fi-verkkopalvelusta löytyy muistilista, miten toimia tilanteessa, jossa henkilötietoja on päätynyt luvattomasti ulkopuolisille tietomurron tai tietovuodon seurauksena.

3 TYÖKALUT JA OHJEET

Internetissä on laaja valikoima selainpohjaisia tai ladattavia sovelluksia tietoturvan tarkistamiseen tai parantamiseen. Osa näistä on vilpittömiä ja toiset saattavat aiheuttaa enemmän tuhoa kuin turvaa. Internetissä useat ilmaiset skannaus tai tarkistussovellukset tulisi tarkastella perin pohjin. Internetissä ilmainen yleensä tulee käyttäjän tietojen keräämisen hinnalla. Ilmaiset internetselaimet ovat ilmaisia kerätyn markkinointi datan ansiosta, eivätkä siis loppujen lopuksi ole ilmaisia. Mikäli ilmainen skannaus tai tarkistustyökalu on tarjolla nettisivulla, tulisi siitä tarkistaa sitä tarjoavan yrityksen muu tarjonta. Onko yrityksellä esillä todisteita heidän tarjoaman suojan toimivuudesta? Vaikuttaako heidän sivustonsa luotettavalta ja aidolta? Tällaiset kysymykset tulisi tulla vastatuksi heti yrityksen etusivulla. Suomenkielinen etusivu antaa yleensä viitteitä siitä, että silloin myös mahdollinen tekninen tuki on saatavilla suomenkielisenä sekä myös käytettävät ohjelmat. Tunnettuja ja arvostettuja tietoturvapalvelujen tarjoajia ovat esimerkiksi: F-Secure, Kaspersky, Norton ja Avast. Palvelujen yksityiskohdat ja saatavuus selviävät yritysten sivuilta. Näistä F-Secure suomalaisena yrityksenä tarjoaa monta hyödyllistä selainpohjaista ilmaista työkalua tietoturvallisuuteen.

Kyberturvallisuuskeskuksen sivuilla on useita erilaisia oppaita ja neuvoja tietoturvallisuuteen. Heidän sivuiltaan näkee myös ilmoituksia löydetyistä tietoturvarikkeistä sekä tietovuodoista. Suomi.fi-verkkopalvelusta löytyy digituen palvelupaikat. Digitukea tarjoavat muun muassa kirjastot ja yhdistykset. Kunnan, kirjastojen ja viranomaisten digineuvonta on maksutonta. Digituen sivuilla on myös opastusta ja vastauksia sähköiseen asioimiseen liittyvissä kysymyksissä. Suomi.fi- verkkopalvelusta löytyy myös yrityksille ohjeita ja neuvoja eri tilanteisiin. Apua verkkopalvelun käyttöön saa kansalaisneuvonnasta. Kansalaisneuvonnan verkkosivuja ylläpitää Väestörekisterikeskus. Kansalaisneuvonnan verkkosivuilla on linkit useiden virastojen nettisivuille, sekä kanavat yhteydenottoon.

4 YHTEENVETO

Opinnäytetyön tarkoitus oli luoda opastava työ tietokoneen ja tietotekniikan kanssa toimimiseen arjessa tietoturvallisuuden näkökulmasta. Käyttäjien laaja taitotason kirjo, vaikeuttaa suuresti rajan luomista perustiedolle tietoturvan kannalta. Vaikka tietoturva itsessään on mahdollista kiteyttää toimien ja välineiden kokonaisuudeksi, kattaa se käytännössä laaja-alaisesti tietotekniikan eri osa-alueita. Myös toisistaan poikkeavat sovellukset ja käyttöliittymät vaikeuttavat yleispätevän ohjeistuksen luomista.

Tietoturvan laaja-alaisuuden vuoksi työ keskittyy avaamaan niitä osasia, jotka luovat tietoturvaa. Esimerkkien myötä käyttäjä pystyy soveltamaan tietoaan erilaisiin tilanteisiin itsenäisesti. Työn antaman pohjatiedon ymmärryksen perusteella, käyttäjän on helpompi siirtyä isompiin ja teknisempiin kokonaisuuksiin, mikäli sille on tarvetta. Näin ollen uudetkin sovellutukset ovat helpommin lähestyttäviä, sillä ymmärrys niiden perustoiminnasta on jo tiedossa.

Työtä voisi jatkokehittää luomalla kuva- tai videomateriaalia, missä läpikäytäisiin erilaisilla laitteilla ja sovelluksilla arjen tyypillisimpiä tilanteita. Sen lisäksi voisi laaja-alaisella kyselyllä mahdollisesti kartoittaa eri ikäryhmien avuntarpeita tietotekniikan ongelmissa paremmin.

LÄHTEET

Digivinkit.2019. Windows 10 paikallinen käyttäjätili ja käyttäjän lisääminen. https://www.digivinkit.fi/windows-10-paikallinen-kayttajatili. Viitattu 14.12.2022

Digi- ja väestövirasto. https://dvv.fi/kansalaisvarmenne-ja-sahkoinen-henkilollisyys. Viitattu 1.12.2022

European Parliament.2022. USB-type C to become EU's common charger by end of 2024. https://www.europarl.europa.eu/news/en/headlines/society/20220413STO27211/usb-type-c-to-become-eu-s-common-charger-by-end-of-2024. Viitattu 4.12.2022

IEEE802.11. https://grouper.ieee.org/groups/802/11/. Viitattu 16.12.2022

ISO/IEC 17799:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Suomen Standardisopimusliitto SFS

Järvinen, P. 2003. Salausmenetelmät. Jyväskylä: Docendo

Kodinturvaopas. Sammutusvälineet ja alkusammutus. https://www.kodinturvaopas.fi/paloturvallisuus/sammutusvalineet-ja-alkusammutus/#Sammutuspeite. Viitattu 6.12.2022

Traficom. Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/. Viitattu 5.12.2022

Traficom. Kyberturvallisuuskeskus. 4.2.2019. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/773-miljoonan-kayttajatunnuksen-vuoto-korostaa-salasanojen-kierratyksen Viitattu 4.12.2022

Rikoslaki 19.12.1889/39