

Työasemien tietoturva organisaatioissa

LAB-ammattikorkeakoulu
Tradenomi (AMK), Tietojenkäsittely
2021
Ville Pekkola

Tiivistelmä

Tekijä(t) Pekkola Ville	Julkaisun laji Opinnäytetyö, AMK	Valmistumisaika 2021
	Sivumäärä 39	
Työn nimi Työasemien tietoturva organisaatioissa		
Tutkinto Tradenomi, Tietojenkäsittely (AMK)		
<p>Tiivistelmä</p> <p>Opinnäytetyön tarkoituksena oli tutkia työasemien tietoturvaa yritysten ja organisaatioiden työasemaympäristöjen osalta. Työ tutki tietoturvaa konseptina, sekä työasemille tarpeellisia ja käyttöönotettavia suojauskeinoja. Työ rajattiin koskemaan työasemia kuten pöytäkoneita ja kannettavia tietokoneita, jotka on yhdistetty yrityksen toimialueverkkoon Windows-käyttöympäristössä. Opinnäytetyö oli tyypiltään konstrukttiivinen tutkimus, jossa konstrukttiivisella tutkimusotteella etsittiin tietoturvaratkaisujen todennukseen ratkaisumallia. Tutkimustietoa saatiin viiteympäristöistä, joissa työssä käsiteltäviä suojakeinoja oli käytössä työasemilla.</p> <p>Työasemien pitäminen suojattuna on aiheuttanut organisaatioille haasteita etätyön lisääntyessä. Yrityksen sisäverkon ulkopuolella laitteiden hallinta on vaikeutunut, kun laitteet ovat saatavilla lähinnä vain julkisen internetin tai VPN-yhteyden avulla. Laitteiden pitäminen ajan tasalla ja hallinnan piirissä on elintärkeää turvallisen IT-ympäristön kannalta. Raportit, hälytykset ja korjaavat toimet hallintamalleihin perustuen mahdollistavat IT-järjestelmänvalvojalle mahdollisuuden reagoida ongelmatilanteissa työasemien osalta.</p>		
Asiasanat Tietoturva, Työasematurvallisuus, Työasemanhallinta		

Abstract

Author(s) Pekkola, Ville	Type of Publication Bachelor's Thesis, UAS	Published 2021
	Number of Pages 39	
Title of Publication Workstation security in organizations		
Name of Degree Bachelor of Information Technology (UAS)		
<p>Abstract</p> <p>Thesis focused to investigate workstation security on organizations domain networks and workstation environments. Research was based on conceptual theory of securing workstations with necessary protection methods. Scope of research was on workstation framework such as personal computers and laptop computers in Windows environment.</p> <p>Thesis was done based on constructive research methods which allowed researcher to find solutions to relevant problems regarding workstation security and compliance. Key idea was to find methods to obtain reports and alerts from workstations about security measures and how did they operate with organisation's devices.</p> <p>Popularity of remote work has caused challenges on workstation managing and keeping company devices secured. In some environment's workstations are only available through public internet or VPN connection. Keeping devices up to date is increasingly necessary and important these days for continuative business operations. Reports, alerts, and corrective controls based on security management models provide IT system administrator sufficient tools to act when problematic situation is occurred in environment.</p>		
<p>Keywords</p> <p>Information Security, Workstation Security, Workstation Management</p>		

Sisällysluettelo

1	Johdanto.....	1
1.1	Työn taustaa.....	1
1.2	Tutkimusongelma ja tavoitteet	1
1.3	Rajaukset	2
1.4	Tutkimusmenetelmä	3
2	Tietoturvan teoria.....	5
2.1	Yleinen määritelmä	5
2.2	CIA-malli	6
2.3	Tietoturvan jaottelu	7
2.4	Tietoturvallisuuden hallinta	8
3	Tietoturva organisaatioissa	9
3.1	Tietoturvan vastuut	9
3.2	Käytännöt yrityksissä	9
3.3	Konsepti	10
4	Työasemat organisaatioissa	11
4.1	Työasemien tietoturvallisuus.....	11
4.2	Erilaiset työasemat	11
4.3	Kirjautuminen ja pääsynhallinta	12
4.4	Verkkoyhteydet.....	14
5	Tietoturvauhat.....	17
5.1	Työasemiin kohdistuvat riskit	17
5.2	Ohjelmistoturvallisuus	19
5.3	Selain	20
5.4	Sähköposti.....	21
6	Työasemien suojaaminen	23
6.1	Suojauksen periaatteet	23
6.2	Käynnistys	23
6.3	Työaseman salaus.....	25
6.4	Virustorjunta	26
6.5	Keskitetty hallinta.....	28
7	Suojauksen varmistaminen	29
7.1	Konstruktivisen mallin toteutus.....	29
7.2	Mallin testaaminen.....	34
7.3	Mallin soveltaminen ja kehittäminen	36
8	Yhteenveto	38

Käsitteet

AD – Active Directory on Microsoft Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista.

AV – Virustorjunta. Ohjelmistot, joilla etsitään ja tuhotaan paikallisesta järjestelmästä tai etäpisteestä haitallisia prosesseja, niiden tarvitsemia tiedostoja tai ajettaviin ohjelmätiedostoihin tarttunutta haittakoodia.

BIOS – Tietokoneohjelma, joka etsii ja lataa käyttöjärjestelmän tietokoneelta keskusmuistiin, sekä käynnistää sen tietokoneen käynnistyessä

Boot Sector – Käynnistyssektori on pysyvän tietojen tallennuslaitteen sektori, joka sisältää konekoodin, joka ladataan hajasaantimuistiin ja suoritetaan sitten tietokonejärjestelmän sisäänrakennetun laiteohjelmiston avulla.

BYOD – (engl. Bring Your Own Device) viittaa konseptiin, jossa omien laitteiden käyttö tietyn verkon sisällä on sallittua, sen sijasta, että käyttäjälle tarjotaan laite käyttöön.

DNS – (engl. Domain Name System) Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.

EDR – Endpoint Detection and Response, jolla seurataan ja turvataan päätelaite kyberuhilta ja haavoittuvuuksilta reaaliaikaisesti

FIDO2 – FIDO Alliancen ja World Wide Web Consortiumin (W3C) luoma protokolla, vahvan autentikoinnin mahdollistamiseksi verkossa

HTTP / HTTPS – (engl. Hypertext Transfer Protocol Secure) ovat protokollia, joita selaimet ja www-palvelimet käyttävät tiedonsiirtoon. HTTPS on suojattu versio protokollista.

IEEE – Institute of Electrical and Electronics Engineers on kansainvälinen tekniikan alan järjestö, joka määrittelee monille teknologianaloille käytettäviä standardeja

IPSec – Joukko TCP/IP-perheeseen kuuluvia tietoliikenneprotokollia, joilla turvataan internet-yhteyksiä- Protokoliin sisältyy myös avaintenvaihtoprotokollat

ISO – Kansainvälinen standardisimisjärjestö, joka tuottaa kansainvälisiä standardeja.

LAN – Lähiverkko (engl. Local Area Network) on rajoitetulla alueella toimiva tietoliikenneverkko, jonka muodostaa esimerkiksi yrityksen yhden toimipisteen sisäverkko

Malware – Haittaohjelma, haitallinen ohjelmisto, joka on suunniteltu aiheuttamaan vahinkoa käyttäjälle tai laitteelle.

MFA – Multifactor Authentication eli Monivaiheinen tunnistautuminen tarkoittaa palveluun kirjautuvan käyttäjän tunnistamista useammalla keinolla, jonka avulla estetään tietojenka-lasteluhyökkäykset.

MITM – Man-in-the-middle attack, suomennettuna mies välissä -hyökkäys. MITM on tietoturvahyökkäys, jossa kahden viestijän väliseen liikenteeseen tunkeutuu hyökkääjä, joka esittää kummallekin osapuolelle olevansa toinen viestijä.

PXE – (engl. Preboot Execution Environment) kuvaa standardisoitua asiakas-palvelin ympäristöä, jossa asiakas käynnistää itsensä ohjelmistopohjaiseen ympäristöön verkon yli.

Ransomware - kiristysvirus tai kiristyshaittaohjelma, joka pyrkii salaamaan tietokoneen tiedostot laitteen muistista ja lukitsemaan laitteen kiristystä varten.

SCCM – Microsoft System Center Configuration Manager, joka on järjestelmänhallintaohjelmistotuote, jonka Microsoft on kehittänyt suurten Windows ympäristöjen hallinnoimisen työkaluksi

SSL – salausmenetelmä, joka muodostuu sanoista Secure Sockets Layer ja on käytännössä sama asia kuin TLS-salaus. Kyseessä on protokolla, jolla salataan verkon yli tapahtuvaa liikennettä kahden sovelluksen välillä.

TPM – Platform Module, joka on siru tietokoneen emolevyllä. TPM toimii mm. Bitlocker salauksessa pitämällä osan salausavaimesta itsellään tietokoneen muistin sijasta levyllä.

UEFI – Unified Extensible Firmware Interface on standardi, joka määrittelee rajapinnan laitteiston firmwaren ja käyttöjärjestelmän välillä

VPN – Virtual Private Network, tarkoittaa virtuaalista erillisverkkoa, jolla kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon

WLAN – langaton lähiverkko (engl. Wireless Local Area Network) on paikallinen tietoliikenneverkko, jossa internetiin kytketty reititin muodostaa langattoman internet-yhteyden, toimivan samalla langattomana tukiasemana laitteille. WLAN kaupallinen nimitys on Wi-Fi.

1 Johdanto

1.1 Työn taustaa

Opinnäytetyössä tutkitaan yritysten työasemien tietoturvaa. Kasvavissa ja ison kokoluokan organisaatioissa päätelaitteiden määrä asettaa vaatimuksia niiden hallittavuuteen. Tämä korostuu nykypäivänä, kun laitteiden fyysinen sijainti voi vaihdella esimerkiksi etätyön lisääntymisen myötä. Kaikissa tilanteissa laitteet eivät ole sidoksissa yrityksen toimitiloihin tai verkkoon. Myös omien laitteiden käyttö on yleistymässä myös yrityksissä oppilaitoksien tavoin. Tietoturva on itsessään kiinnostusta herättävä ja vakavasti otettava aihe alkaneella vuosikymmenellä. Viimeisen vuosikymmenen aikana on nähty kansainvälisesti, kuin myös kansainvälisesti suuria kyberuhkia ja hyökkäyksiä isoja organisaatioita vastaan. Kyberuhilta suojautuminen on keskiössä moderneissa suurissa organisaatioissa. Altistuminen tietoturvaloukkauksille ja tietomurroille voivat aiheuttaa yrityksille mittavaa taloudellista vahinkoa, sekä myös horjuttaa yleisestä luotettavuutta yritysmaailman ja ihmisten keskuudessa.

2020-luvulle tultaessa nykyiset tietokoneet, joiden parissa työskentelemme päivittäin ovat kehittyneet nopeasti lyhyellä aikavälillä. Kehityskaari aina 1990-luvulta asti on ollut kasvavaa. Vielä kymmenen vuotta sitten oletettiin kehityksen taittuvan lopulta. Kuitenkin tietokoneiden laskentateho on noussut kaksinkertaiseksi aina puolentoista vuoden ajanjaksoilla vieläkin, joka aiheuttaa erilaisia haasteita yrityksille suojata niitä. (Paukku, 2013) Laskentatehon kasvun osalta lähteet arvioivat tietokoneiden syrjäyttävän ihmisälyn 2020-luvulla. Moderni teknologia onkin myös kulttuurin osalta vastannut nykypäivän tarpeisiin. Laaja kehitys tietoverkkoyhteyksissä ja ajasta tai paikasta riippumaton käytettävyys on tuonut myös eri järjestelmille paljon vaatimuksia mukanaan.

Työ pyrkii selvittämään eri keinoja suojata ja turvata yrityksen työasemia eri käyttötilanteissa. Monet suojamekanismit yhdistettyinä toimiviin prosesseihin takaavat laiteympäristön turvallisen käytön. Työssä tutkitaan käsiteltävää asiaa IT-järjestelmänvalvojan toimenkuvan kannalta. Tutkimuksessa havaitut toimivat keinot prosessien ja toimintatapojen kehittämiseksi pyritään liittämään olemassa olevaan teoriaan tuomaan lisäarvoa alan työskuvassa hyödynnettäväksi.

1.2 Tutkimusongelma ja tavoitteet

Yrityksissä on useita tietoteknisiä laitteita mahdollistamassa henkilöstön työskentely ja liiketoiminnan eri toiminnot. Tietoturvan merkitys kasvaa modernissa organisaatiossa. Enevässä määrin riskit monen organisaation liiketoiminnassa kohdistuvat tietoturvaan.

Keskeisin ongelma on perehtyä keinoihin suojata työasemia yrityksen verkossa ja sen ulkopuolella potentiaalisilta uhilta. Työssä tutkitaan lisäksi, miten tarvittavien suojausmekanismien toimivuus laitteilla voidaan varmentaa. Tähän ei oletettavasti löydy selkeää ja yksimieleistä vastausta, jonka takia täytyy rakentaa toimiva prosessi ja toimintamalli.

Työn tavoite on selvittää, minkälaisia työasemia yrityksissä käytetään eri tilanteissa. Tämän myötä selvitetään keinot suojata työasemia ja varmistua, että suojaukset toimivat halutusti. Tavoitteena on muodostaa konstruktio, jota hyödyntämällä eri suojausratkaisuja saadaan todennettua käytännössä. Yrityksen työasemilla voi olla käytössä useita tietoturvaratkaisuja, mutta on mahdollista, ettei kaikilla työasemilla yhteensopivuusongelmien myötä ole ratkaisut täysin toiminnassa. Lisäksi suuri määrä työasemia aiheuttaa hallittavuuteen haasteita. Suurten työasemaympäristöjen hallinnointi tulisi hoitaa keskitetysti, jolloin mahdollistetaan myös niiden yhdenmukaisuus. Työaseympäristön tulisi vastata yrityksen tarpeita olemalla samaan aikaan tietoturvallisesti toteutettu ja suurimmat riskit ennalta huomioitu. Suurin osa työasemien riskeistäkin kohdistuu niiden käyttäjiin, joka aiheuttaa haasteita niiden suojaamisille.

Yrityksen IT-osastolle on elintärkeää saada reaaliaikaista dataa ja статистиikkaa siitä, miten ympäristön laitteet käyttäytyvät. Työn tavoite on etsiä keinoja tuottaa tätä tietoa ja raportteja ongelmatilanteiden varalle, jolloin järjestelmänvalvoja voi puutteisiin vaikuttaa. Päämääränä tulee olla automatisoidut valvontaratkaisut yrityksen tietoteknisessä ympäristössä. Tämä voidaan mahdollistaa muun muassa ajastettujen raporttien, hälytysten, sekä ilmoituksien myötä.

Työn tulee voida osoittaa teknisen tietoturvan eri kategorioista relevantteja teknisiä ratkaisuja, joilla voidaan suojata työasemia organisaatioissa. Työn tavoitteena on palvella ensisijaisesti IT-alalla toimivia tukihenkilöitä ja järjestelmänvalvoja, jotka ratkaisujen parissa toimivat yritysmaailmassa. Tutkimukseen tai työhön käytettävää materiaalia haetaan laajasti ja objektiivisesti eri lähteistä.

1.3 Rajaukset

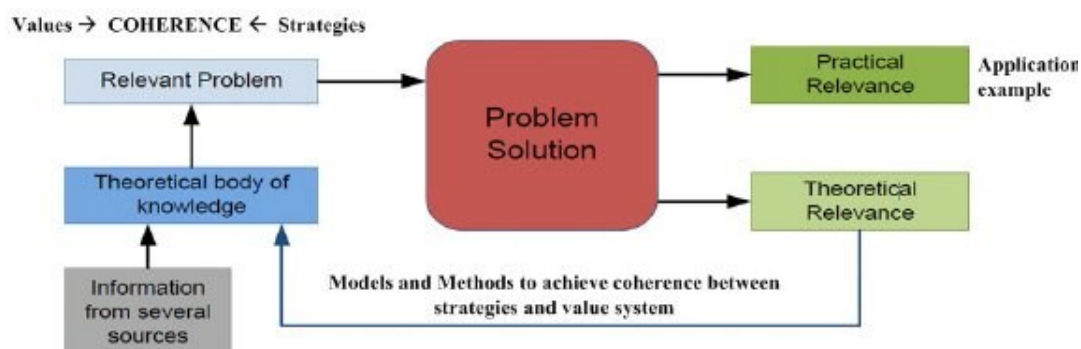
Opinnäytetyössä tutkitaan työasemien tietoturvaa organisaatioissa. Työasemiksi luetaan tässä työssä tietokoneet, kuten pöytäkoneet ja kannettavat työasemat. Työssä keskitytään myös pääosilta Windows-ympäristön normeihin, mutta suuri osa konsepteista pätee myös muihin käyttöjärjestelmäympäristöihin, kuten Linuxiin. Rajausta on perusteltu Windows-ympäristöjen yleisyyden ja markkinaosuuden takia, sillä harvoissa yrityksissä on muita käyttöjärjestelmäympäristöjä käytössä työasemien osilta. Rajauksen ulkopuolelle jää myös mobiililaitteet, kuten puhelimet tai tabletit, sekä myös IoT-laitteet. Työssä sivutaan

kuitenkin virtuaalisia ratkaisuja mm. kevyiden työasemien osalta (thin clients), koska virtualisointi on yleistynyt viimeisen 10 vuoden aikana runsaasti. Työn rajausta on toimialasta riippumaton. Työn teoriaosuudessa käsitellään yleisimpiä periaatteita ja standardisoituja menetelmiä.

Työssä tutkitaan ensisijaisesti isoja ja suuren kokoluokan organisaatioiden IT-ympäristöjä. Työssä esitetty teoria ja tutkimustieto pätee moneen käyttöympäristöön ja on sovellettavissa yleisesti erilaisia työasema kokonaisuuksia suunnitellessa. Työssä selvitetään uhkien ja haavoittuvuuksien pohjalta tarvittavia suojauskeinoja työasemille, jotka ennaltaehkäisevät riskejä. Tekninen tietoturva rajaa pois hallinnollisen ja fyysisen tietoturvallisuuden käsiteltävästä viitekehyksestä. Käsiteltävä osuus mahdollistaa tietoturvan toteutuksen teknisillä keinoin tilasta, käyttäjästä tai organisaation omaksumista normeista riippumatta. Kuitenkin suurella osalla tietoturvaratkaisuja suojellaan laitteiden ja järjestelmien lisäksi myös käyttäjää. (Svidergol, 2021)

1.4 Tutkimusmenetelmä

Opinnäytetyön toteutan konstruktiiivisena tutkimuksena, jonka tavoitteena on tuottaa konstruktiiivinen malli työasemien tietoturvan hallintakeinoja myötäillen. Tutkimusta varten on mahdollista hyödyntää yhden tai useamman yrityksen viiteympäristöä työasemien tietoturvan osalta, mutta varsinaista toimeksiantajaa tutkimuksella ei ole. Konstruktiiivinen tutkimus takaa työlle käytännönläheisen menetelmän toimia ja tutkia teoriaa teknologioiden takana. Työssä on relevantti ongelma, jolle haetaan loogisia ratkaisuja eri keinoja hyödyntämällä. Menetelmien pohjalta on mahdollista kehittää konstruktiiivinen malli, joka kuvaa tässä kontekstissa prosessia ongelmatilanteiden varalle. Ratkaisuja ei tule olemaan yhtä oikeata, vaan useita eri keinoja ja tapoja täyttää asetetut tavoitteet tai tarpeet. Tutkimusmenetelmässä teoreettista tietoa sovelletaan käytäntöön, jonka perusteella voidaan pohdita, toimiiko teoria oletetusti eri skenaarioissa. Suurin tavoite tutkimusmenetelmässä on jalostaa olemassa olevaa tietoa käytännön toteutuksissa, joiden pohjalta syntyy uutta mielenkiintoista soveltamista, sekä pohdintaa. Syntyvät johtopäätökset pitää kuitenkin olla perusteltavissa teoriaan pohjautuen, muuten ne eivät ole luotettavia.



Kuvio 1 Konstruktiivinen tutkimusmenetelmä (Camarinha-Matos, 2014)

Yllä olevassa mallissa on kuvattuna konstruktiivisen tutkimusotteen prosessi. Relevanttiin ongelmaan etsitään ratkaisua tutkimalla teoriaa ja sovelletaan käytännön osaamista. Ratkaisun löytyessä pohditaan teoreettista yhtenäisyyttä aiempaan pohjatietoon. Tällöin testataan ratkaisun ja mallin toimivuutta käytännön lisäksi myös teoriassa. Jos uusi kehitetty konstruktio voidaan todeta toimivaksi, tuottaa se lisätietoa olemassa olevan teorian päälle. Testattu konstruktio tulee analysoida, jonka jälkeen sen toimivuus voidaan validoida ja pohtia, miten konstruktioita voidaan soveltaa tai kehittää. Konstruktioita ei ole kuitenkaan mahdollista tieteellisesti todistaa hyväksi tai huonoksi, oikeaksi tai vääräksi. (Lukka, 2001)

2 Tietoturvan teoria

2.1 Yleinen määritelmä

Tietoturva itsessään on todella laaja kokonaisuus. Tietoturva ulottuu yrityksen toimialueesta riippumatta erittäin vahvasti päivittäiseen tekemiseen. Toisilla aloilla aiheen vakavuus ja tärkeys korostuu kuitenkin selvästi toisia enemmän. Toimialat, joilla käsitellään arkaluontoisia tietoja, korostuvat eniten tietoturvan piirissä. Tietoturvan merkitys on kasvussa modernissa organisaatiossa. Enenevässä määrin riskit organisaatiossa kohdistuvat tietoturvaan sen eri osa-alueissa. Tietoturvassa tekninen osa-alue käsittää vain osan. Tietoturvallisuus on erityisen tärkeää, koska sen avulla turvataan organisaatioiden arkaluontoinen tieto. Tämän yksi mahdollistaja ovat tekniset ratkaisut ja toimet. (Tunggal, 2020)

Organisaatioissa on eri vastuualueita, jotka vastaavat tietoturvan toteuttamisesta. Tietoturva itsessään on vain yksittäinen osa yrityksen sisäisiä IT-toimintoja. Tietoturvasta vastataan myös hierarkkisesti yrityksissä monella eri tasolla. Teknisen tietoturvan toteutuksesta kuitenkin lähtökohtaisesti aina on vastuussa yrityksen johdon lisäksi sisäinen IT-osasto.

Tietoturvalla tarkoitetaan hallinnollisia, fyysisiä ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus. Tällä tarkoitetaan sitä, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Eheydellä taas varmistetaan, etteivät tietoja voi muuttaa muut kuin siihen oikeutetut tahot ja järjestelmät. Saatavuus taas tarkoittaa, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Tietoturva on tietojen, järjestelmien ja palveluiden suojaamista erilaisissa tilanteissa. Nykyään tietoja voidaan menettää eri tavoilla tai tiedot voivat joutua asiaan kuulumattoman käsiin. Tietoja on turvattava ja niitä voidaan tehdä monin eri tavoin. Heikon tietoturvan seurauksia ovat mm. virukset, ulkopuolisten tahojen tunkeutuminen järjestelmään, ilkivalta, tietomurrot ja tietosuojaloukkaukset. (Goodrich & Tamassia, 2011)

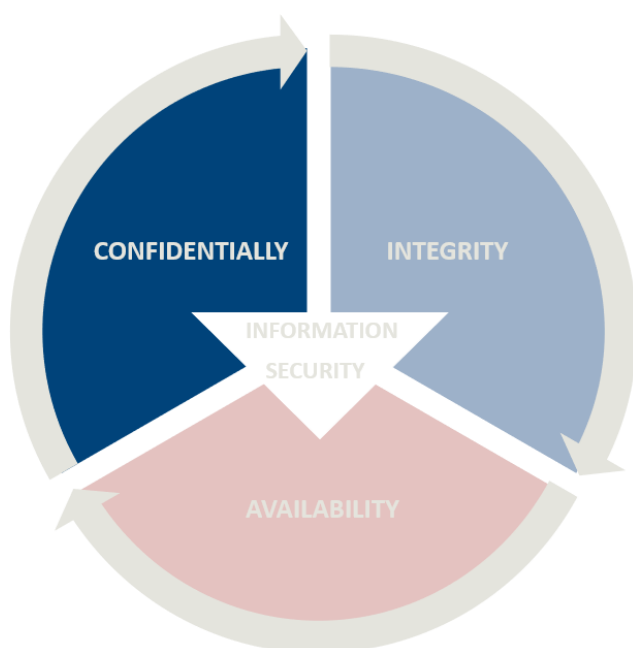
Tietoturvalla tarkoitetaan hallinnollisia, fyysisiä ja teknisiä toimia, joilla varmistetaan tiedon tuottamuksellisuus (confidentially), eheys (integrity), sekä saatavuus (availability). Näitä kuvataan tietoturvan periaatteiksi. Tietoturvan periaatteita tarkastellessa voidaan niitä kuvata alla olevalla mallilla. Malli tunnetaan englanniksi nimellä CIA-triadi. Yhdessä nämä periaatteet muodostavat kulmakiven jokaisen organisaation tietoturvan toteuttamisessa. Tietoturvaa toteutettaessa arvioidaan mahdollisten uhkien ja haavoittuvuuksien vaikutukset organisaation toiminnan ja sen omaisuuksien kannalta. (Forcepoint, 2019)

2.2 CIA-malli

Luottamuksellisuus (confidentially) käsittää sen, että käsiteltävät tiedot ovat vain niiden käyttöön oikeutettujen tahojen saatavilla, joilla on oikeudet käyttää niitä. Tämä sisältää organisaatioiden toimenpiteet, joilla se pitää tietonsa yksityisenä tai salaisena. Luottamuksellisuuden toteutuessa ne, jotka ovat oikeutettuja pääsemään yrityksen resursseihin käsi, pääsevät. Vastaavasti luvaton pääsy on ennaltaehkäisty ja estetty.

Eheydellä (integrity) taas määritellään tietojen oikeudellinen muutoksellisuus, joka koostaa luotettavan ja paikkansapitävän, eheän tiedon. Tiedon eheys mahdollistetaan käyttöi-
keuksien eli luottamuksellisuuden lisäksi tiedon suojaamisella. Tämä on mahdollistettu eri suojausmenetelmiä hyödyntämällä, kuten käsiteltävien tietojen salauksien, tiivisteiden, digitaalisten allekirjoitusten ja klassifioinnin avulla. Eheydellä varmistetaan tiedon muuttumattomuus hallitsemattomasti ja sen pysyminen ajan tasalla ja tallessa.

Saatavuus (availability) pitää sisällään eniten selvästi teknisen ympäristön ylläpitoon liittyviä toimia. Tiedon saatavuus toteutuu silloin, kun tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä ja käytettävissä. Tiedon saatavuus käsittää käytännössä verkkojen, järjestelmien, ohjelmistojen ja laitteiden toimivuuden, sekä niihin pääsyn oikeutetuilta käyttäjiltä oikeutettuina aikoina. Täydellinen saatavuus on arvokasta, joskin hankalasti toteutettavissa. Saatavuutta voidaan mitata pääsyn luotettavuudella sekä nopeudella. (Walkowski, 2019)



Kuva 1 Tietoturvan "CIA-triadi"

2.3 Tietoturvan jaottelu

Tietoturva voidaan jaotella kolmeen eri kokonaisuuteen. Yrityksen toimitilojen sekä niissä sijaitsevien laitteiden suojaamista kutsutaan yleisesti nimellä fyysinen turvallisuus. Tietoturvan osa-alueena fyysinen turvallisuus on myös mukana, koska osa riskeistä esiintyy fyysisien tilojen puitteissa. Esimerkiksi tärkeitä tietoja sisältävän palvelimen eheyttä, luotamuksellisuutta ja saatavuutta ei voida varmistaa, mikäli se ei ole fyysisesti turvattu. Fyysinen uhka, kuten tulipalo, saattaa tuhota tietokoneita tai varmuuskopioita. Fyysiseen turvallisuuteen liittyvät olennaisesti kulunvalvontajärjestelmät, kameravalvonta, liiketunnistimet, vartiointi ja sekä tilojen suojaus. Osa näistä fyysisen turvallisuuteen liittyvistä käsitteistä mahdollistetaan jollain teknisellä toteutuksella, mutta niitä ei kuitenkaan lueta osaksi varsinaista teknistä tietoturvaa. Myös kiinteistöjen palo-, vesi- tai sähkövahingoilta suojauminen on osa kokonaisvaltaista turvallisuuden toteutusta. (Tirronen, 2003)

On oleellista huomioida näiden lisäksi myös inhimilliset ja ihmisistä riippuvat uhat, kuten varkaudet, ilkivalta, sekä luvaton pääsy. Eri kiinteistöissä tai organisaatioissa ilmenee tarpeita vierailijoille, joiden pääsyä on syytä hallita ja rajoittaa oikeissa mittasuhteissa. Tämä voidaan mahdollistaa vierailijakäytänteillä, kuten kirjaus järjestelmään ja turvallisuuden parantaminen vierailijakortilla tai saattajalla. (Koivisto & Andreasson, 2013, s. 63-64)

Hallinnollinen tietoturva on osa yrityksen tietoturvakokonaisuutta, ja sen avulla hallitaan tietoturvaa kokonaisuutena. Tekniset ratkaisut, kuten palomuurit, kulkukortit, tiedon salaaminen tai virustentorjunta eivät modernissa yrityksessä enää riitä tietoturvan hallintaan, jolloin hallinnollisen tietoturvan tärkeys korostuu. Hallinnollisella tietoturvalla nimensä mukaisesti hallitaan tietoturvaa kokonaisuutena, luodaan tietoturvapolitiikka sekä käytännöt ja prosessit tietoturvalle toimintatapaan, varmistetaan henkilöstön tietoturvaosaaminen ja luodaan prosessit sekä käytänteet tietoturvapoikkeamista ja -hyökkäyksistä selviämiseen. Hallinnollinen tietoturva vastaa moniin tarpeisiin organisaation tietoturvassa niin käytänteistä lainsäädännöllisiin vaatimuksiin. Hallinnollisen tietoturvan toteuttajana organisaatioissa on usein yrityksen johto ja päätösvallassa olevat tahot.

Tekninen tietoturva mahdollista yritykselle sen teknisten järjestelmien ja ratkaisujen, kuten ohjelmistojen, palomuurien, sekä verkkojen tietoturvalle toimintaympäristön. Sillä pyritään varmistamaan, että käytetyissä laitteistoissa ja ohjelmistoissa ei ole tietoturvapuutteita. Tekninen tietoturvan tavoitteena on myös estää yrityksen tai organisaation järjestelmiin pääsy ei-auktorisoiduilta tahoilta ja suojautua tietomurroilta. Myös tiedon muuttuminen hallitsemattomasti, järjestelmien saatavuus, sekä käytettävyyks on tärkeää varmistaa teknisellä tietoturvalla.

Kyseinen osa-alue pitää sisällään yleisesti myös laajan terminologian ja paljon eri käsitteitä. Teknistä tietoturvaa voidaan testata esimerkiksi tietoturva-auditoinneilla, kypsyyden ja kyvykkyyden määrittelyllä, penetraatiotestauksella, sekä tutkimalla sovitun teorian pätevyyttä käytännössä. Olemassa olevien palveluiden tekninen tietoturva voidaan varmentaa tai tietoturvatoteutuksia voidaan suunnitella rakenteilla oleviin ratkaisuihin.

2.4 Tietoturvallisuuden hallinta

Tietoturvaa voidaan hallita mallien ja järjestelmien pohjalta, jotka on mahdollista jaotella niihin liittyvän toiminnon mukaisesti. Mallien päätarkoitus on suunnitella, toteuttaa, noudattaa, seurata, arvioida, ylläpitää ja kehittää tietoturvallisuutta. Hallintajärjestelmällä voidaan toteuttaa organisaation tietoturvastrategiaa. Hallinnan myötä vastuut, prosessit ja resurssit ovat otettu huomioon yksityiskohtaisesti. Toimivan järjestelmän myötä organisaatiolla on valmiudet parannella sekä kehittää systemaattisesti tietoturvamenetelmiään. Hallinnan toteuttamisessa voidaan käyttää apuna erilaisia kypsyyden mittareita ja standardeja, kuten ISO-standardit. Esimerkiksi laatustandardi ISO/IEC 20000 keskittyy pääsääntöisesti IT-palvelutuotannon palveluihin ja toimii sertifioituna laatukehikkona. Kyseinen laatustandardi käsittää samoja prosesseja kuin ITIL. Toimiva hallintamalli mahdollistaa muun muassa ennaltaehkäisevät, valvovat ja käsittelevät toimet ongelmatilanteiden varalta työasemaympäristössä. (Koivisto & Andreasson, 41-43, 2013)

Ennaltaehkäisevät toimet estävät uhkien ja haavoittavuuksien etenemisen organisaation ympäristöön asti. Suurin osa toiminnoista tulisi toteuttaa jo tämän toiminnon avulla. Tietoteknisen ympäristön osalta ennaltaehkäiseviä järjestelmiä ja laitteisto on esim. virustorjunta, palomuuuri, sekä pääsynhallinta ja todennusjärjestelmät.

Valvovat toimet pitävät ympäristöä yllä sekä todentavat ennaltaehkäisevien toimien toteutumisen ympäristössä. Valvova toiminto kuvaa mitä tahansa turvatoimea, jonka avulla muodostuu hälytys tai ilmoitus ei-toivotusta tai epäilyttävästä toiminnasta, joka ympäristössä on havaittu eri järjestelmillä. Hälytykset voidaan huomata esim. lokitiedoissa tai laitteiden valvonta- ja monitorointipalvelun avulla.

Käsittelevät toimet reagoivat uhkista ja haavoittavuuksista johtuneisiin tietoturvariskeihin, jotka toimivat niiden vakavuuden vaatimalla tavalla, korjaten ympäristön toimintaa. Käsiteltävästä toimesta voidaan puhua myös korjaavana tai palauttavana toimena. Jokaiselle muodostuneelle riskille asettuu myös sen tila. Tila eli status kertoo järjestelmänvalvojalle siitä, onko riski aktiivinen, poistunut vai ratkaistu. Käsiteltävä toiminto korjaa vahingon, palauttaa resurssin riskiä edeltävälle ajalle, tai suorittaa poistavan toimenpiteen muodostuneelle riskille.

3 Tietoturva organisaatioissa

3.1 Tietoturvan vastuut

Toimijoille, kuten yrityksille ja organisaatioille, on säädetty velvollisuus huolehtia tarjoamiensa verkkojen ja palvelujen tietoturvasta ja sen toteuttamisesta. Lisäksi on myös vaadittu niiden toteuttamisesta huolellisesti ja mitoitukselta suhteessa torjuttavan uhan vakavuuteen. Velvollisuudet ja vaatimukset käsittävät myös sananvapauden, luottamuksellisen viestin tai yksityisen suojan osalta tietoturvan toteutusta. Tietoturvan toteuttaminen ei saa rajoittaa edellä mainittuja enempää kuin mikä katsotaan välttämättömäksi. Lisäksi laki säättää tietoturvan toteutuksen edellytyksiä eri maissa. Tietoturvaa on velvoitteiden ja lakien lisäksi mahdollistettu myös suositusten ja ohjeistusten muodossa. (Kyberturvallisuuskeskus, 2021)

Kansallisella tasolla eri ilmiöt, kuten etätyö, ovat yleistyneet viimeisten 10 vuoden aikana merkittävästi Suomessa. Viimeisen kolmen vuoden aikana etätyötä tehneiden osuus palkansaajista on kasvanut 5 prosenttiyksikköä (tilanne vuoden 2019 lopussa) nostaen etätyötä tehneiden osuuden 37 % väestön työikäisistä palkansaajista. (TEM, 2020) Etätyö lisää tietoturvan merkittävyyttä ja asettaa haasteita tietoturvallisen käyttöympäristön toteutukselle organisaatioissa. Työololabometrin perusteella voidaan tehdä johtopäätöksiä siitä, että ainakaan kyseinen trendi ei ole laskemaan päin. Kuitenkin käytännön tasolla etätyö on ollut mahdollista vain pienelle osalle palkansaajia vieläkin. (Melin, 2020) Tietoturvan merkitys on kasvanut laajasti myös organisaatiotasolla vallitsevan teknologisen kehitystahdin sekä maailmantilanteen myötä.

Tietoturvan kehittäminen organisaatioissa asettaa haasteita modernin toimintaympäristön takia, kun käyttäjät ja heidän käyttämänsä laitteet eivät usein enää ole niin helposti saatavilla, eikä näin ollen samassa fyysisessä sijainnissa. Tämä asettaa haasteiden lisäksi myös rajoitteita ja vaatimuksia tietoverkkoihin ja hallintaratkaisuihin. Valtiollisella tasolla on myös todettu, että etätyöskentely voi nostaa esiin kysymyksiä organisaatioiden tietoturvasta. Huomattavaksi jää, miten toimivat ohjeistukset ovat ihmisillä saatavilla tai kuka niiden julkaisusta vastaa. (Kyberturvallisuuskeskus, 2021)

3.2 Käytänteet yrityksissä

Käytännön tasolla suuri osuus ison kokoluokan organisaatioista toteuttaa tietoturvaa olemassa olevien vaatimusten ja käytänteiden mukaisesti. Tutkimuksessani määritellyt organisaatioiden kokoluokat perustuvat Tilastokeskuksen määrittelemään yritysten kokoluokitteluun, jossa Suomessa suuryritykseksi luetaan henkilöstömäärän mukaan yli 250

työntekijää työllistävät yritykset. Suuryritysten osalta on oletettava, että nämä ovat asettaneet tietoturvan osalta tarkasti määritetyt tietoturvakäytänteet ja menettelytavat.

Näiden lisäksi suuryrityksellä tai isolla organisaatiolla tulisi olla myös merkittävät turvallisuusinfrastruktuurit, jotka toimiessaan mahdollistavat reagoinnin sisäisiin tai ulkoisiin uhiin niiden vaatimalla vakavuudella. Yrityksen johto on velvollinen asettamaan ja päättämään tietoturvan prioriteeteista, sekä sen hallinnollisten ja organisaatiollisten toimien määrittelystä. Johdon vastuulla on myös tietoturvan toteutuminen sen asettamien tavoitteiden ja vaatimusten mukaisella tasolla. (SANS Institute, 2001)

3.3 Konsepti

Tietoturvan prioriteettia ja käytänteitä ohjaavat vahvasti organisaation sisäinen strategia, toimiala sekä resurssit, joilla sitä toteutetaan käytännössä. Eri toimialoilla CIA-mallin mukainen teoria vaihtelee ydinliiketoiminnan prioriteettien mukaisesti. Tämä hyvin pitkälti on keskiössä määrittelemään turvallisuusratkaisuiden pääkohdat, millä ohjataan organisaation johtoa keskittymään kriittisimpiin riskeihin. Riskejä analysoidaan toimialaan kohdistuvien uhkien ja haavoittuvuuksien osilta. Osa näistä kuitenkin pätee jokaiseen toimintakehykseen yhtenevästi. Tavoitteellisten tietoturvan periaatteiden merkitys organisaatiossa määräytyy yrityksen liiketoiminnan periaatteiden mukaisesti. Periaatteiden tärkeys määräytyy käytännössä yrityksen toimialan mukaan. (Walkowski, 2019)

Konseptia rakentaessa on ensisijaisena tarve määrittää tietoturvapoliittikka. Tietoturvapoliittikka on organisaation sisäinen määräys, joka annetaan yrityksen henkilöstölle helposti saataville ja tietoisuuteen. Yleensä tietoturvapoliittikka on yrityksillä julkista tietoa ainakin osittain. Yleismääräisesti julkisesta politiikasta voidaan jakaa yrityksen tietoturvakäytänteet muun muassa asiakkaiden tiedoksi, mutta usein näissä asiat ilmaistaan vain konseptitasolla. Tietoturvapoliittikkaan sisällytetään tietoturvaan ja tietosuojaan liittyvät muut määräykset ja ohjeet. Tietoturvapoliittikan ensisijaisena tavoitteena on liiketoiminnan palvelujen jatkuvuuden turvaaminen kaikissa olosuhteissa. Teknisen tietoturvan näkökulmasta tämä sisältää IT-ympäristön mahdollistamien ratkaisujen saatavuuden, eheyden ja luottamuksellisuuden. (2NS, 2019)

4 Työasemat organisaatioissa

4.1 Työasemien tietoturvallisuus

Yrityksissä työasemat ovat pääsääntöisesti yleisimmät päätelaitteet, joita eri toimintojen mahdollistamiseksi käytetään. Työasemien lisäksi nykyään voi myös olla käytössä erilaisia mobiililaitteita, joiden yleistymisen on osittain syrjäyttämässä perinteisiä työasemaympäristöjä. Tässä luvussa kuitenkin perehdytään perinteisempiin ja laajoissa käyttökoh-teissa oleviin laitteisiin, jolloin mobiililaitteet jäävät rajauksen ulkopuolelle.

Työasemiksi määritellään pääsääntöisesti tehokäyttöön tarkoitettujen ammattimaisten toimintojen hoitoon tarkoitetut laitteet. Niistä puhuttaessa kyseiset tietokoneet on valjastettu usein todella tarkoin määritettyihin toimintoihin soveltuviksi, kuten mallintamiseen tai suunnitteluun. Tämä asettaa työasemien komponenteille vaatimuksia, jotta työasemien suorituskyky kattaa halutut tarpeet. Työasemakomponentit poikkeavat usein perinteisistä kuluttajamarkkinoiden tietokoneista ominaisuuksiltaan. (O'Donnell, 2019) Lisäksi pitää tunnistaa erilaiset riskit, jotka kohdeorganisaatioon kohdistuvat. Erilaisia riskejä voidaan torjua eri teknisin keinoin. Riskit muodostuvat uhista ja haavoittuvuuksista. (Harrell, 2020)

4.2 Erilaiset työasemat

Työasemat hankitaan yrityksiin erilaisia käyttötarpeita varten. Eri käyttötarve voi tarkoittaa eri yrityksessä täysin erilaista päätelaitetta. Erilaisia käyttötarpeita voi yrityksen toimialasta riippuen olla monia. Kun työasemalta vaaditaan tehoa, kuten esimerkiksi suunnitteluohjelmia tai laskentatehoon perustavia toimintoja varten, valitaan usein pöytäkone kyseiseen tarkoitukseen. Kaikissa yritysten toiminnoissa ei välttämättä tarvita samanlaista laskentatehoa, vaan käyttötarkoitus on kevyempää tai toiminto hyvin rajattu. Tällöin soveltavaksi voi tulla yrityskäyttöön tarkoitettu kannettava tietokone, joiden käyttö on yleistynyt huomattavasti 2000-luvulla.

Työasemia onkin tarpeellista tutkia käyttötarkoitusten pohjalta. Tämä auttaa myös selvittämään, kuinka laajalti perinteiset käsitykset tietokoneista ovat laaja-alaisempia ja tulevat koko ajan muuttumaan. Eri lähteiden perusteella työasemat voidaan jaotella perinteisiin pöytätietokoneisiin, jotka ovat teholtaan edellä mainitun vaatimusten mukaisia, sekä tehokäyttöön tarkoitetut kannettavat työasemat. (Ward, 2020) Nämä ovat yleisimmät yrityksissä käytettävät työasematyypit, jonka lisäksi on olemassa myös virtuaaliset työasemat, jotka eroavat perinteisestä työasemakäsityksestä vahvasti. (Decker, 2012) Virtualisointi on yleistynyt paljon 2010-luvulla, joka on mahdollistanut kustannustehokkaita ratkaisuja varsinkin yrityksille eri tarkoituksiin. Nykypäivänä ei välttämättä ole kustannustehokasta

ostaa yritykselle kalliita laitteita, jos kevyeen käyttötarkoitukseen soveltuu tehoiltaan edullinen keskusyksikkö, jonka avulla vain virtuaalisesti tuodaan tarvittavat resurssit näkyviin käyttäjälle. Yksi esimerkki virtuaalisesta työasemasta on niin sanonut thin clientit.

(Spiceworks, 2020)

Useissa yrityksissä liiketoiminta perustuu tuotteisiin, jolloin sisäistä tuotanto- tai valmistusprosessia suoritetaan resurssilla kuten tietokoneella. Tässä kontekstissa voidaan puhua tuotantotyöasemasta, jolla on hyvin tarkkaan määritelty toimintaperiaate ja yksinkertainen tarve toiminnoilta. Tuotannossa ei usein tarvinta työasemalta paljon laskentatehoa, koska toimenpiteet, joita työasemalla halutaan suorittaa, ovat yksinkertaisia ja kevyitä. Myös työasema tulisi silloin pitää mahdollisimman helppokäyttöisenä ja yksinkertaisena.

Myös tuotannon työasemia voi olla lukuisia erilaisia, mutta perusperiaate on yleensä sama. Työaseman tarkoituksena on suorittaa sille määritetty yksinkertainen toiminto joko automaattisesti tai käyttäjän toimesta. Näitä tarpeita voi olla perinteisellä tuotantolaitoksissa esimerkiksi liukuhihnalla / linjastolla, jolloin työasemalla ohjataan tuotantoprosessin eri vaiheita tietyssä kohtaa. Tämän mahdollistaa yrityksen toiminnanohjausjärjestelmä tai tuotantolinjaan sidottu muu ohjelmisto. Myös kassapäätteet, kulunvalvonta, testerit, robottien ohjauspäätteet tai muut vastaavat työasemat voidaan lukea samaan kategoriaan.

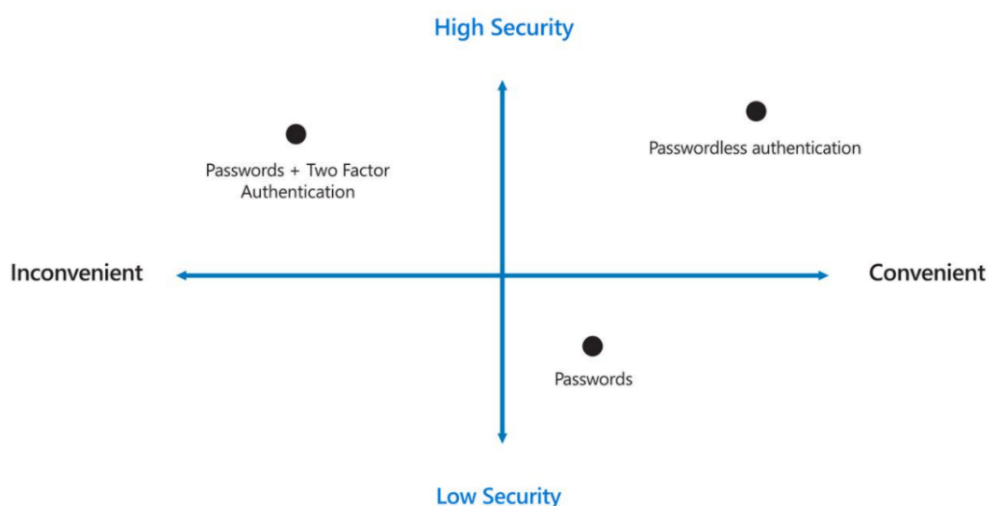
Tuotannon työasemien tietoturvaa mietittäessä onkin parhain lähestymistapa toiminto ja tarve edellä. Yksinkertaisen toiminnon suorittamiseen työasemalta harvoin tarvitaan pääsyä julkiseen internetiin. Tämän pohjalta työasemat onkin mahdollista pitää yhdistettynä ainoastaan yrityksen toimialueen sisäverkkoon, joka on lisäksi eriytetty muusta verkosta omaksi segmentiksi. Tämä periaate mahdollistaa työasemilta pääsyn vain tarvittaviin resursseihin, jolloin vain tarpeellinen verkkoliikenne on sallittu työaseman ja tarvittavien järjestelmien välillä.

4.3 Kirjautuminen ja pääsynhallinta

Yrityslaitteille ja työasemille on saatavilla lukuisia ratkaisuja tietoturvallisen autentikoinnin ja pääsyn varmistamiseksi. Kriittisiin ympäristöihin kuten yrityksen toimialueen palveluihin on perinteisesti käytetty käyttäjätunnusta sekä salasanaa, mutta nykypäivänä muita vaihtoehtoja tietoturvallisempaan autentikointiin on tarjolla sen lisäksi. Useat tietoturvatoinnit panostavat pääsynhallinta- sekä identiteetinhallintamenetelmiin ja -järjestelmiin. Tarkoitukskohteet, joissa järjestelmänvalvojan tulisi hallita käyttäjätunnuksia, salasanoja, pääsyjä ja oikeuksia ovat vähentymässä radikaalisti moderneissa työasemaympäristöissä. (Harris, 2021)

Salasanapolitiikka käytetyissä järjestelmissä tulisi olla toteutettu ainakin parhaan käytännön mukaisesti. Ainakin yli 10 merkkiä pitkä salasana, joka sisältää isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä, tulisi olla jokaisessa käyttökohteessa ehdoton minimi. Tämä ennaltaehkäisee riskejä runsaasti, sillä edellä mainitun politiikan mukaisen salasanan murtamiseen menisi laskentatehollisesti vuosia. (Viestintävirasto, 2021) Salasanoja tulee myös suojata. Erilaiset salasanaholvit ja pääsynhallintajärjestelmät mahdollistavat salasanojen turvallisen säilytyksen työasemien käyttäjille, tai mahdollistavat salasananatoman pääsyn tarvittaviin resursseihin. Pääsynhallinnassa keskitytään käyttäjän tunnusten sijaan nimensä mukaisesti pääsyyn, joka määritellään ennalta tehtävänimikkeen ja tarpeiden mukaisesti halutulle käyttäjälle.

Monimenetelmäinen todentaminen ja muut vastaavat toiminnot voivat suojata organisaatiota, mutta käyttäjät turhautuvat usein lisäsuojauskerrokseen salasanojen muistamisen lisäksi. Salasanattomat todentamistavat ovat kätevämpiä, koska salasanoja ei tarvitse muistaa ja koska ne ovat yhteensopivia useimpien laitteiden ja järjestelmien kanssa. Lisäksi ne ovat käytännössä immuuneja tietojen kalastelulle. Nykypäivän salasanattomuus on yleistynyt 2020-luvulle tultaessa. Salasanattomuuskäytänteet ovat tuoneet mukanaan monia uusia standardeja, kuten Web Authentication API:n ja Fast Identity Online (FIDO2). FIDO2 mukainen autentikointimenetelmä pohjautuu monimenetelmäiseen tunnistautumiseen, jossa autentikointi tapahtuu FIDO2 avainten avulla sekä turvalaitteen avulla. Turvalaitteesta yksi esimerkki on muun muassa Yubico-valmistajan tuote Yubikey. (Yubico, 2021)



Kuva 2 Salasanattomuuden hyödyt (Microsoft, 2021)

4.4 Verkkoyhteydet

Kaikkialla yrityksen tiloissa ollaan yhteydessä verkkoon tavalla tai toisella. Verkkoliikenteen hallinta työasemien osalta korostuu, kun työaseman tarvitsee olla yhteydessä ulko-verkkoon. Organisaation tietoverkot tulee olla suunniteltu ja toteutettu mahdollisimman turvallisesti ja helposti ylläpidettäväksi. Jos työasemaa ei tarvitse käyttötarkoituksensa takia yhdistää muihin kuin paikallisiin resursseihin ja palvelimiin, tulisi sen pääsyä ulko-verkkoon rajoittaa. (IBM, 2021) Verkkoja voi myös suojata sertifikaateilla. Ilman sertifikaattia laite ei yhdistä lähiverkkoon tai langattomaan verkkoon. Lähiverkon RJ-45 Ethernet -portit yrityksen toimitiloissa pitäisi myös suunnitella kytkettävän siten, ettei mikä tahansa laite pääse yhdistämään lähiverkkoon pelkästään olemalla yrityksen tiloissa.

Lähiverkko

Lähiverkon eli englanniksi lyhennettynä LAN osalta mikään ei ole muuttunut moniin vuosiin. Kannettavien ja mobiililaitteiden yleistyessä 2010-luvulla on siirrytty käyttämään enemmän WLANin eli langattoman lähiverkon menetelmiä, jolloin verkko on laajemmin työasemien saatavilla. (Mogul, 1990) Vaikka nykypäivänä etäkäyttömahdollisuudet ja langattomat yhteydet ovat syrjäyttäneen lähiverkon suosion, on silti välttämätöntä pitää yrityksen toimialueen verkko suojattuna ja turvallisena. Lähiverkon tulisi yrityksen sisällä olla suunniteltu niin, että se on jaettu mahdollisuuksien mukaan loogisiin osiin käyttökohteen tai tilan mukaisesti. Tällöin verkkosuunnittelussa on mahdollista estää eri verkon osien keskustelu keskenään ja eriyttää laitekohtaisesti verkot. Suuressa tuotantolaitoksessa esimerkiksi on järkevää eriyttää toimistotilat, tuotantoalue ja tulostimet tai muut laitteet toisistaan erilleen. Tämä on mahdollista virtuaalisten LAN-verkkojen (VLAN) ja kytkimien avulla. Loogisesti eroteltuja verkkoja voidaan hallinnoida tietoliikenneporttien kautta. (Quick, 2017)

Vaikka yrityksen tiloissa on fyysistä suojausta käytössä, on silti täysin mahdollista, että ulkopuolinen henkilö pääsee käyttämään yrityksen lähiverkkoa esimerkiksi neuvotteluhuoneiden verkkoliitännöjen kautta. Moniin tiloihin voi päästä sisään röyhkeästi ja varmasti sisään kävelemällä tai sopivasti huijaamalla. Myös tiloissa olemassa olevan laitteen kautta on helppo kytkeä oma laite yrityksen verkkoon käyttämällä työasemaan tai tulostimeen tarkoitettua kaapelia. (Koivisto & Andreasson, 75-76, 2013) Tätä voidaan hallinnoida porttikohtaisella autentikoinnilla, jota kutsutaan 802.1X tai DOT1X -tekniikaksi. Kyseessä on IEEE:n kansainvälinen standardi, jota hyödynnetään lähiverkon lisäksi myös langattomissa verkoissa. Porttikohtaisen autentikoinnin käytännön tarkoitus on estää luvattoman laitteen pääsy ja kommunikointi yrityksen sisäverkossa. Tunnistetut laitteet eli yrityksen omat työasemat voidaan ohjata kytkinporttien kautta omaan VLANiin. Tunnistautuminen

luotettavaksi laitteeksi voidaan tehdä usealla tavalla, joista yksi on hyödyntämällä konekohtaisia varmenteita eli sertifikaatteja. Sertifikaatteja ja autentikointia voidaan hallita Microsoftin Active Directory keskitetystä toimialueverkon tietokannasta, tai RADIUS-palvelimen avulla. Teknisesti 802.1X-menetelmässä yhdistäjä hakee tunnuksilla tai konekohtaisella sertifikaatilla salausmenetelmän, kuten EAP avulla autentikointipalvelimen kautta tunnistuksen itselleen. Tunnistautumisessa verrataan tunnistautujan laitteen MAC-osoitetta tietokannassa olevaan. Menetelmän myötä on helpompi hallita vieraskäyttäjiä verkossa määrittämällä neuvotteluhuoneeseen tai muuhun yhteiseen tilaan kaikkien ei-tunnistettavien laitteiden yhdistämään vierasverkkoon. (OmniSecu, 2021)

Langaton lähiverkko

Langaton lähiverkko eli WLAN on yleistynyt 2000-luvulla pääsääntöisesti käytettäväksi verkoksi päätelaitteiden keskitettyä enemmän kannettaviin ja mobiililaitteisiin. Langattomasta lähiverkon lyhenteestä WLAN käytetään myös kaupallista nimeä Wi-Fi, joka viittaa langattoman verkon standardeihin. WLAN on myös kansainvälinen standardi, jossa langattomat laitteet operoivat 2,4GHz- ja 5GHz- radiotaajuuksilla. (Kyberturvallisuuskeskus, 2016) Langaton verkko muodostuu, kun langatonta verkkokorttia käytettävä laite yhdistää langattomaan tukiasemaan tilassa, jossa ainoastaan langaton tukiasema on yhdistetty langattomaan reitittimeen tai kytkimeen. Langattomia verkkoja voi luoda melko vapaasti, sillä vastuu langattoman verkon turvallisuudesta on sen luojalla. Verkon ylläpitäjä vastaa riittävästä salauksesta verkossaan. Kirjoitushetkellä käytettävien salausprotokolla langattomissa lähiverkoissa on WPA2-PSK. Salauksen myötä yhteys on suojattu ja salaus varmistettu salausavaimen avulla. Tämän myötä verkkoon ei voi yhdistää ilman salausavainta. (Hoelscher, 2021)

Työasemien tietoturvan osalta langattomuus tuo mukanaan erilaisia riskejä verrattuna lähiverkkoon. Verkkoympäristöt mahdollistavat laitteiden ja niiden käyttäjien olevan yhteydessä internetiin. Kun laitemäärät kasvavat ja kaikki ovat yhteydessä langattomasti, tuo se tietoturva-asteita yrityksille pitää ne turvallisina. Yrityksen langaton verkko näkyy myös taajuuksilla tilojen läheisyydessä. Varsinkin langattoman verkon kohdalla sertifikaatin käyttö olisi suotavaa omien päätelaitteiden osalta. Myös sisäinen ja vierasverkko tulisi erottaa. (Vanover, 2009) Yleisesti yritysten tietoturvapoliitikoissa määritetään säännöt ja ohjeistukset langattomien verkkojen osalta. Yleisesti käyttäjiä ohjeistetaan olemaan käyttämättä julkisia ja ei-tunnettuja verkkoja, joiden ylläpitäjästä ei ole varmuutta. Myös salauksittomien verkkojen käyttöä tulisi välttää. (Microsoft, 2021)

Virtual Private Network

Etätyö pätee myös uhiin ja haavoittavuuksiin, sillä kotiverkossa ollessa on laite myös riskin alainen. Mikäli kodin verkko ei ole suojattu tarpeen vaatimilla menetelmillä, voi päätelaite johtua hyökkäyksen kohteeksi. (Whitney, 2021) Verkkotason suojauksena organisatioissa voidaan hyödyntää virtuaalisen erillisverkon toimintatapoja. VPN eli Virtual Private Network käsitteenä on hyvin uusi ja tullut vasta viime vuosina yleiseen tietoisuuteen. Virtuaalinen erillisverkko luo suojatun yhteyden haluttuun palvelimeen, joka VPN-asetuksissa on määritetty, jonka kautta laitteen verkkoliikenne menee ulospäin julkiseen internetiin. Yritykset käyttävät VPN-yhteyksiä pääsääntöisesti, kun yrityksen verkon ulkopuolella työskentelevä työntekijä haluaa päästä tarvittaviin resursseihin käsiksi. Käyttäjän ollessa esimerkiksi kotona omassa verkossaan voi virtuaalisen verkon avulla yhdistää yrityksen palvelimeen, joka ohjaa kotiverkon liikenteen yrityksen resursseihin.

VPN-toteutuksia on useita. Yleisimmät käytössä olevat VPN-protokollat ovat nimeltään IP-Sec ja SSL-VPN. Suurin ero näissä on kahden protokollan operointi eri tietoliikenteen standardisoidun OSI-mallin kerroksilla. IPSec VPN katsotaan osana TCP/IP mallia, jossa se operoi OSI-mallin verkkokerroksissa, kun taas ohjelmistopohjaiset VPN yhteydet toteutetaan 4–7 kerroksissa, kuten sovellus ja esitystapakerroksissa. (Athow, 2020)

Useimmiten, kun halutaan suojata yhteys ja toteuttaa se mahdollisimman turvallisesti, voidaan kaikki päätelaitteen verkkoliikenne ohjata kulkemaan yrityksen verkon kautta. Tällöin puhutaan tietoliikenteen ohjaamisesta VPN-tunneliin. VPN-tunneleissakin on eroja. Kun halutaan ohjata kaikki liikenne yrityksen verkon kautta laitteelle, puhutaan full-tunnel VPN-käytännöstä. Jos VPN-tunneliin halutaan suodattaa vain tarvittavat tietoliikenneprotokollat ja portit, on vaihtoehtona split-tunnel tekniikka. Tässä menetelmässä käytettävän verkkoyhteyden nopeus ei hidastu työasemalla, kun taas kaiken liikenteen osuessa tunneliin hidastumista tapahtuu. (Hiley, 2021)

5 Tietoturvaumat

5.1 Työasemiin kohdistuvat riskit

Työasemiin kohdistuvat uhat ja haavoittuvuudet tulevat pääsääntöisesti aina julkisen internetin kautta. Pääsääntöisesti aina, kun mikä tahansa päätelaite on yhdistetty verkkoon, tekee se laitteen haavoittuvaiseksi ympäristössä. Edellisessä luvussa ilmi tullut mahdollisuus kytkeä laitteet vain yrityksen sisäverkkoon ratkaisee yksinkertaisimpien työasemien osilta riskien muodostumisen, mutta harvassa käyttötarkoituksessa se on mahdollista. Etätöiden yleistymisen kannalta kotiverkot ja etätöskentely tuottavat haasteita työaseman tietoturvaan liittyen. Tässä luvussa tutustutaan yleisimpiin työasemiin kohdistuviin uhkiin ja haavoittavuuksiin.

Suurin osa käytettävistä palveluista tai ohjelmista on internet yhteyden päässä. Yleisimmät työkalut työasemien käyttäjillä ovat internetselain ja sähköposti. On myös tutkittu, että 95 % muodostuneista tietoturvariskeistä johtuu inhimillisistä virheistä, eli käyttäjien toimista. Melkein puolet uhista kohdistuu pääsääntöisesti pieniin yrityksiin, joilla ei välttämättä ole tarvittavia resursseja suojautua yleisimmiltäkään hyökkäyksiltä. Suurin osa uhista kohdistetaan myös tietoisesti yritysten heikompiin käyttäjiin, joihin harvemmin lukeutuvat yrityksen IT-henkilöt. (Milkovich, 2020)

Tietojenkalastelu

Tietojenkalastelu on taloudellista hyötyä tavoittelevaa rikollista toimintaa, jolla pääosin tavoitellaan henkilö- ja kirjautumistietoja. Käyttäjätietojen myötä rikolliset pyrkivät huijaamalla saamaan uhrilta rahaa. Tietojenkalastelu (phishing) kohdistuu käyttäjään useimmiten sähköpostien tai mainosten kautta, joissa viestin sisältö on luotu kiinnostavaksi tai todellisia mainoksia vastaavaksi. Tietojenkalastelua tapahtuu massamaisena jakeluna laajasti sähköpostin kautta. Tietojenkalastelussa hyödynnetään erilaisia keinoja päämäärän saavuttamiseksi. Usein tietojenkalasteluissa hyökkääjä esiintyy virallisena tahona ja viestin sisältöä naamioidaan usein tarkastikin muistuttamaan tunnettuja palveluita tai palveluntarjoajia, kuten pankkeja tai laitevalmistajia. Näissä yleensä koitetaan johtaa uhria halutulle verkkosivustolle, johon uhri syöttäisi arkaluontoisia tietojaan. (Fruhlinger, 2020)

Yleisimmin esiintyviä huijauksia ja tietojenkalasteluyrityksiä ovat yrityksiin kohdistuvat toimitusjohtajapetokset, jotka tunnetaan englanniksi nimellä CEO Fraud. Kyseinen huijausmetodi perustuu vahvasti tietojenkalastelun lisäksi myös sosiaaliseen hakkerointiin. Ominaispiirteitä niin tälle kuin myös vastaaville petoksille on niiden esiintyminen mahdollisimman autenttisena. (Clifford, 2021)

Yrityksen johdon sähköpostit ovat haluttua valuuttaa, sillä niissä liikkuu päivittäin suuret määrät viestejä. Tekaistu aidon näköinen viesti työaikana voi mennä monella käyttäjällä nopeastikin ohi henkilökohtaisen filterin, jos viesti tavoittaa saapuneet-kansion. On tutkittu, että melkein puolet (46 %) tietojenkalastelu- ja huijausviesteistä on lähtöisin Nigerian tietoverkoista. Päivittäin huijarit kohdistavat viestejään jopa yli 400 yrityksen sähköpostipalvelimiin tietoturvayhtiö Symantecin mukaan.

Haittaohjelmat

Haittaohjelmat eli Malware ovat tietokoneelle asentuvia ohjelmistoja, jotka voi olla piilotettu sovellukseen tai tiedostoon. Niiden tarkoitus on aiheuttaa vahinkoa asennettuun tietokoneeseen tai sen käyttäjälle. Haittaohjelmilla on lukuisia eri tarkoituksia, joiden mukaan ne toimivat. Pääsääntöisesti puhutaan koneelle asentuvista ohjelmista, jotka tulevat epäluotettavien lähteiden kautta työasemille. Haittaohjelman asentuessa koneeseen voi sitä olla vaikea aluksi huomata etenkin sen naamioituessa taustaprosessiksi. Usein haittaohjelman käynnistyessä koneella voi huomata hidastumista tai jotain mikä viittaa epänormaalin oloiseen käytökseen.

Usein haittaohjelmien kohdalla puhutaan vain viruksista. Tämä on kuitenkin virheellinen käsitys, sillä virukset käsittävät nykyään vain 10 % esiintyvistä haittaohjelmista. Yleisimpiä haittaohjelmia ovat virusten lisäksi tietokonemadot (worms), mainosohjelmat (adware), vaikoiluohjelmat (spyware), kiristysohjelmat, sekä troijalaiset. (Sowells, 2018)

Kiristysohjelmat

Haittaohjelmien jälkeen seuraavaksi merkittävin uhka työasemille on niiden kohdistuvat kiristysohjelmat tai virukset, jotka pyrkivät salaamaan levyosiossa olevat tiedostot ja tekemään niistä käyttökelvottomia. (CISA, 2021) Kiristystyökalut leviävät laitteille lukuisten eri tilanteiden kautta. Otollisin paikka altistua kiristysviruksille on vierailta epäluotettavilla ja salaamattomilla verkkosivuilla, joissa on haitallista sisältöä. Myös sähköpostien liitteinä tai mainoksissa voi laite saada altistuksen. Kiristysviruksen tekijä haluaa yleensä uhrilta lunnaita salauksen purkamiseksi. Kiristyskeinona käytetään arkaluontoisten tietojen levittämistä, mikäli käyttäjä ei maksa lunnaita. Lunnaiden maksussa on alettu hyödyntämään digitaalisia maksuvälineitä ja valuuttaa, kuten kryptovaluutta Bitcoinia, jolloin maksutapahtumaa on miltei mahdoton jäljittää viranomaisien toimesta. (Trendmicro, 2021)

Trojalaiset

Trojalainen tai troijalainen hevonen juontuu Troijan sodassa käytetystä puuhevosesta, jolla kreikkalaiset huijasivat troijalaisia sotilaita. Troijalaiset esiintyvät haitallisen koodin muodossa tai ohjelmistona, joka vaikuttaa ulospäin täysin luotettavalta. Kyseessä on

haittaluontoinen ohjelmisto, joka ladattuna käyttäjän koneelle pyrkii asentumaan taustalle suoritettavaksi prosessiksi vakoillakseen laitetta ja sen käyttäjää. (Johanssen, 2020)

Päästyään koneelle ohjelma pyrkii leviämään eteenpäin ja aiheuttamaan mahdollisimman paljon vahinkoa. Troijalaiset ovat viruksista yleisimpiä. Suurin osa moderneista antivirusohjelmistoista ennaltaehkäisee troijalaisten pääsyn tietokoneelle. Monissa yhteyksissä troijalainen-nimitys on käsitys kopioimattomista ohjelmista, jotka ovat haitallisia. Tämän myötä erottelu onko troijalainen haittaohjelma vai virus selkeytyy. Monet virukset kuitenkin käyttävät samoja menetelmiä tartunnan levittämiseen kuin troijalaiset, vaikka varsinaisesti troijalaiset eivät viruksia ole. (McAfee, 2021)

MITM hyökkäykset

MITM eli man-in-the-middle hyökkäys on suomennettuna mies välissä -hyökkäys, jossa hyökkääjä tunkeutuu kahden viestijän liikenteen väliin. Hyökkääjä kaappaa tai kuuntelee kahden laitteen, kuten työaseman ja palvelimen välistä liikennettä varastaakseen tunnukset, salasanoja tai muuta henkilökohtaista tietoa. Myös käyttäjän vakoilu ja datan korruptointi on man-in-the-middle hyökkäyksissä yleistä. Hyökkäyksinä ne edustavat vanhinta tyyliä työasemien kyberuhista. Liikenteen salakuuntelu ja manipulointi on lähtöisin 1980-luvulta, jolloin hyökkäyksen suorittaminen oli paljon helpompaa kuin nykyään. (Swinhoe, 2019)

Hyökkääjä voi hyödyntää erilaisia tekniikoita päästääkseen salatun liikenteen väliin riippuen tavoitteista. Esimerkiksi verkkosivujen DNS-huijaukset ovat yksi yleinen muoto, joita kohdistetaan Suomessa verkkopankkisivustoihin. Hyökkäyksissä luotettua sivustoa käytetään samalla nimipalvelimella, jonka taakse on naamioitu haitallinen sivusto, jolla kerätään käyttäjästä arkaluontoiset tiedot, kuten pankkitunnukset tai luottokortin numerot.

5.2 Ohjelmistoturvallisuus

Organisaatioissa työasemilla käytetään lukuisia erilaisia ohjelmistoja liiketoiminnan tarpeiden mukaan. Yleisimmät organisaation sisällä tarvittavat ohjelmistot ovat muun muassa toiminnanohjausjärjestelmät eli ERP-järjestelmät. Toiminnanohjausjärjestelmät vaihtelevan yrityksen toimialan mukaan ja niitä on monia erilaisia kansainvälisesti ja myös Suomessa kansallisilta yrityksiltä saatavilla. (eCraft, 2021) Nykyään toiminnanohjausjärjestelmiä käytetään kokonaisvaltaisesti ohjaamaan koko liiketoimintaa keskitetyn alustan tavoin. ERP-järjestelmällä voidaan ohjata yrityksen keskeisiä toimintoja, kuten taloutta ja tuotantoa. Sitä käytetään myös eri sidosryhmien välillä, esimerkiksi työntekijät, asiakkaat ja kumppanit. Toiminnanohjausjärjestelmän lisäksi yrityksillä on suunnittelu-, markkinointi-, tuotetieto- tai asiakkuudenhallintaohjelmia. (Labarre, 2021)

Perinteinen tapa käyttää organisaation sisällä ohjelmistoja on asentaa ohjelma tietokoneille, jolloin se käyttää yrityksen verkossa olevia sovelluspalvelimia hyödykseen toimiakseen. Tämä on ollut toimiva tapa ympäristöissä, jossa on kattavat henkilöresurssit palvelimien, järjestelmien, sekä päätelaitteiden ylläpidon varalle. Myös tarvittavat päivitykset ja tietoturvallinen toimintaympäristö on ollut mahdollista toteuttaa. Nykypäivänä yritykset pyrkivät joustaviin ja kustannustehokkaampiin ratkaisuihin. Etätyön yleistyttyä halutaan myös ohjelmistojen ja resurssien olevan riippumattomia laitteesta, verkosta, ajasta tai paikasta. Perinteinen on premise - ratkaisumalli on kuitenkin väistymässä yhä enemmän pilvipalvelujen myötä. (Munk, 2019)

SaaS-ohjelmistototeutukset ovat nousseet viime vuosien aikana kovaan suosioon, etenkin 2020-luvulla. Software as a Service -ohjelmistomalli on kasvanut yleisesti käytettäväksi tavaksi mahdollistaa ohjelmien joustava käyttäminen paikasta ja ajasta riippumatta. SaaS on tapa julkaista sovellus saataville verkkoyhteyden ja verkkoprotokollien yli käytettävälle laitteelle. Pilvipohjaisessa tavassa ohjelmiston tarjoaja vastaa sovelluksen ylläpidosta ja saatavuudesta. Sovelluksen vaatimat tietokannat, lisenssit ja palvelimet ovat ohjelmistotoimittajan vastuulla, jolloin asiakas maksaa vain ohjelmistosta palveluna, jota tilataan toimittajalta. Usein SaaS tuotteet ovat silti täysin kustomoitavissa asiakkaan toiveiden mukaisesti. Vaikka tietoturvamielessä pilvipalveluna tuotetut ohjelmat eivät välttämättä kuulosta datan sijainnin osalta turvallisimmalta vaihtoehdolta, sen soveltamisalat ja hyödyt ovat silti kiistämättömät. Turvallisuutta voidaan kasvattaa käyttämällä julkipilven sijaan myös hybridimallia, jossa toiminnallisuudet tulevat julkiverkosta mutta tieto varastoidaan yrityksen sisäverkossa. Myös VPN-toteutukset mahdollistavat tietoturvallisen liikennöinnin ohjelmistoihin. (Butt, 2021)

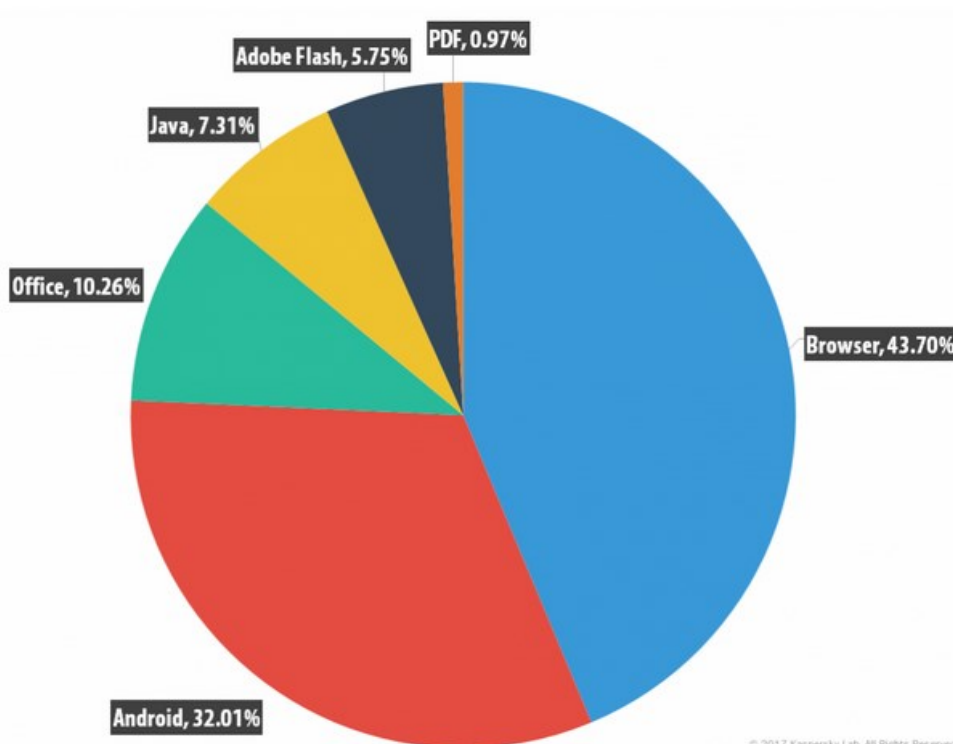
5.3 Selain

Käytettävien ohjelmisto työasemilla on sähköpostin lisäksi verkkoselaimet. Verkkoselaimen ja siinä käytettävien lisäosien kautta tulee merkittävä määrä uhkia ja riskejä työasemille. Suurimmassa osassa itse käyttäjä on heikoimmillaan käyttäessään selainta. Selain tulisi aina pitää mahdollisimman rajoitettuna ja sallia vain työnteon kannalta välttämättömät toimet yrityksen verkossa. Ilman tarvittavia toimia voi selaimen käyttö olla haitallista yrityksen verkossa. (Dascalescu, 2017)

Organisaation ryhmäkäytänteissä on lukuisia tapoja estää ja hallita selaimilla suoritettavia toimintoja. Selaimet itsessään pitävät sisällään monia turvallisuusmekanismeja, jotka ennaltaehkäisevät tapahtuvia uhkia käyttäjän työasemalla. Yleisimpiä on muun muassa pääsyn estäminen sivuille, joissa ei ole käytössä TLS/SSL protokollan mukaista salausta, eli sivut, jotka eivät käytä suojattua versiota HTTP-protokollasta. Myös 3. osapuolten

evästeet, ponnahdusikkunat ja virheellistä sertifiointia käyttävät verkkosivut tulisi oletuksena olla estettyjen listalla. Käytyjen sivujen ei pitäisi olla mahdollista seurata käyttäjän historiaa tai toimia verkossa, eikä myöskään nähdä geolokaatiota. Suurin osa selaimen turvallisesta käyttöympäristöstä on yleisesti hyväksyttyä toimintatapaa, eli niin sanottua parhaan käytännön mukaista (Best Practise) tapaa toteuttaa tietoturva.

Yleisesti käytettävien selaimien osuus hyökätyistä palveluista laitteiden osalta oli 44 % vuoden 2017 ensimmäisellä neljänneksellä tapahtuneista uhista. Vertailukohtana olivat mm. yleisimmin käytössä olevat selainlisäosat tai ohjelmistot, kuten Java ja Adobe Flash Player, joita selaimella käytetään graafisen sisällön esittämiseen.



Kuvio 2 2017/Q1 ohjelmistoihin kohdistuneet riskit (Unuchek, 2017)

5.4 Sähköposti

Sähköposti on yleisin viestintäväline, jota organisaatioiden sisällä ja välillä käytetään. Siinä missä verkkoselainta käytetään melkein kaikkeen tietokoneella, on sähköposti vielä kriittisempi kohde tietoturvan kannalta. Sähköpostin turvallisuus on konsepti tai toimi, jolla mahdollistetaan toimialueelle ja käyttäjille turvattu ympäristö henkilötietojen, identiteetin, käyttäjätunnusten ja salasanojen osalta. Kaikki tietoturvatimet selaimet osalta tulee tähdätä ennaltaehkäisemään luvaton pääsy sähköpostitilille tai työasemalle. Yhdysvaltalainen verkko-operaattori Verizon on todennut, että 90 % kyberuhista kohdistuu

sähköpostitileihin ja sovelluksiin. Sähköpostin viestien ja liitteiden kautta hyökkääjät pyrkivät saamaan pääsyn käyttäjän laitteelle, joka on kriittisintä yrityksen IT-ympäristön kannalta. (Day, 2019)

Sähköpostia voidaan suojata lukuisin keinoin. Antivirusohjelmisto suojaa työaseman tiedostojen ja prosessien lisäksi myös saapuvien sähköpostien osalta. Tärkeässä roolissa toimii myös käytetty roskapostisuodatin. Suodatuksen periaate on siirtää käyttäjän sijasta ei-toivotut viestit ja haitallinen sisältö suoraan roskapostikansion alle, tai estää viestien saapuminen sähköpostipalvelimen kautta sähköpostitilille. Viestejä voi myös käsitellä säännöillä, jolloin haitalliset lähettäjät ja verkko-osoitteet voi estää sähköpostin hallintaneelistä kokonaan kaikilta käyttäjiltä. On myös parhaiden käytäntöjen mukaista olla lataamatta automaattisesti toiminnollista sisältöä tai liitteitä viesteistä automaattisesti. Arkaluontoisen tiedon välittämisessä tulisi välttää sähköpostin käyttöä ja monissa käyttötarkoituksissa se onkin kielletty yritysten tietoturvasäilytyksessä. Tarpeiden tullen tulisi arkaluontoiset viestit kryptata eli käyttää turvattua sähköpostiprotokollaa viestin lähetyksessä. (Durga, 2021)

6 Työasemien suojaaminen

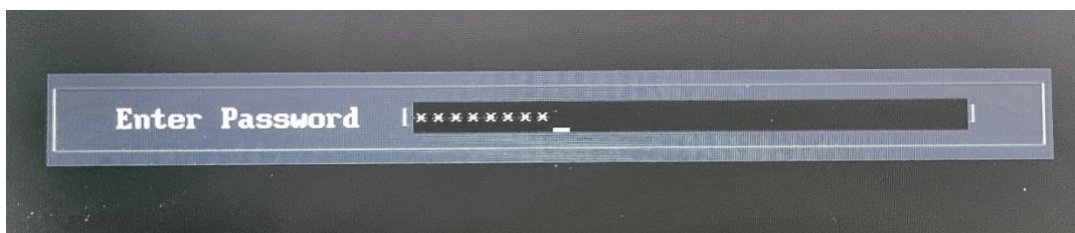
6.1 Suojauksen periaatteet

Kuten kaiken muunkin tietotekniikan osa-alueen kategorioissa, myös työasemien eli laitteiden tietoturva tulee suunnitella ja niiden suojaaminen varmistaa. Tietoturva on parasta toteuttaa ennaltaehkäisevillä periaatteilla, sillä puutteiden korjaaminen jälkikäteen on usein hankalampaa ja enemmän resursseja kuluttavaa. Lisäksi laitteita tulisi olla mahdollista valvoa ja hallita tilanteessa kuin tilanteessa. Laitteiden tulee siis olla yrityksen hallinnassa saatavilla, jotta ne voidaan pitää ajan tasalla ja turvattuina. (Koivisto & Andreasson, 65-66, 2013)

Tässä luvussa tulen etenemään työaseman suojauksen periaatteisiin siinä järjestyksessä, kuin kone käynnistetään ja sillä työskennellään. Työasemia tulee yrityksissä suojata usein monilla eri tasoilla. Näistä tasoista voidaan tutkia ensin komponenttien ja käynnistysjärjestelmän lisäksi myös enemmän perinteisempää käyttöjärjestelmässä tapahtuvaa suojausta.

6.2 Käynnistys

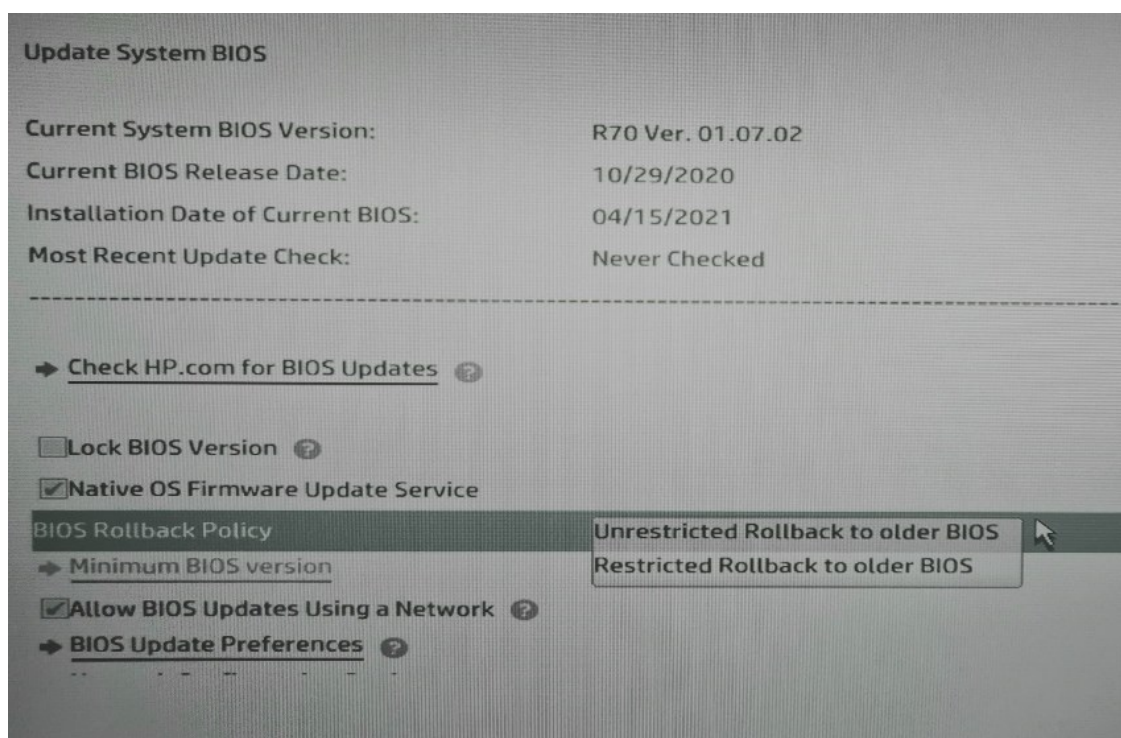
BIOS on lyhenne sanoista Basic Input-Output System ja se on tietokoneen emolevyllä sijaitseva ohjelmisto, jonka pääasiallinen tarkoitus on ladata tietokoneen käyttöjärjestelmä välimuistiin ja käynnistää se. BIOS lataa käynnistysvaiheessa myös komponenttien tai lisälaitteisiin tarvittavan tuen, jotta ne toimivat jo ennen käyttöjärjestelmän asennustakin. Tämän myötä BIOS myös testaa laitteiston toimivuuden virheiden varalta ennen käyttöjärjestelmän lataamista. Työasemissa usein turvaudutaan käyttöjärjestelmä- tai verkkotasolla tapahtuvaan tietoturvaan, muttei kuitenkaan sovi unohtaa tietokoneen käynnistystasolla tapahtuvaa tekniikkaa. BIOS on mahdollista suojata eri keinoin, kuten salasanalla ja suojatulla käynnistyksellä. Nykyään laitevalmistajat ovat emolevyjen osalta tehneetkin etenkin BIOSin kohdalla tarvittavia suojaratkaisuja uhkien varalle. Tässä luvussa käsitellään nykyaikaisen BIOS ohjelman suojausta ja sitä, mitkä ovat relevantteja uhkia ennen käyttöjärjestelmä tasoa. (Mazerik, 2013)



Kuva 3 BIOS-salasanalla estetään luvaton pääsy käynnistysasetuksiin

UEFI BIOS

Kaikista haitallisimmiksi ja vaikeimmiksi osoittautuvat virukset kohdistuvat tietokoneiden BIOSin flash-muistiin. Perinteisen BIOS-ohjelmiston korvaajaksi onkin kehitetty uusiin työasemiin standardisoitu UEFI-ohjelmisto, johon sisäänrakennettu Secure Boot – toiminto. Kyseinen toiminto mahdollistaa käynnistyksen käyttöjärjestelmän ytimeen (kernel), jonka laiteohjelmisto (firmware) on digitaalisesti allekirjoitettu. Tämä myös estää haittaohjelmien ja ei-toivottujen työkalujen tunkeutumisen tietokoneen BIOSiin. Nykyaikaisissa koneissa on lähtökohtaisesti UEFI BIOS aina perinteisen Legacy BIOSin sijasta.



Kuva 4 Kannettavan työaseman UEFI BIOS käyttöliittymä

Työasemilla BIOS-viruksiin on usein hankala reagoida jälkikäteen, sillä usein ainut keino palautua työasemakohtaisesti on BIOS-version päivitys laitteelle. Tässä riskinä kuitenkin voi mahdollisesti olla viruksen puolustusmekanismi, jolloin koko laiteohjelmisto päivitystä yrittäessään tuhoaa itsensä, jolloin koneen emolevy on entinen. Paras onkin suojata se eri keinoin ennaltaehkäisevästi.

Boot sector virus

Työaseman BIOSiin kohdistuvien uhkien lisäksi on myös merkittävämpiä tapoja, joilla laite voi saastua. Jokaisella työasemalla on käynnistysosio, jossa sijaitsee myös käyttöjärjestelmän käynnistyksestä vastaava Master Boot Record (MBR). Näihin kohdistuvat virukset ovat yleensä kaikista vaikeimpia neutralisoida. Käynnistysvirukset ovat tunnettuja 90-

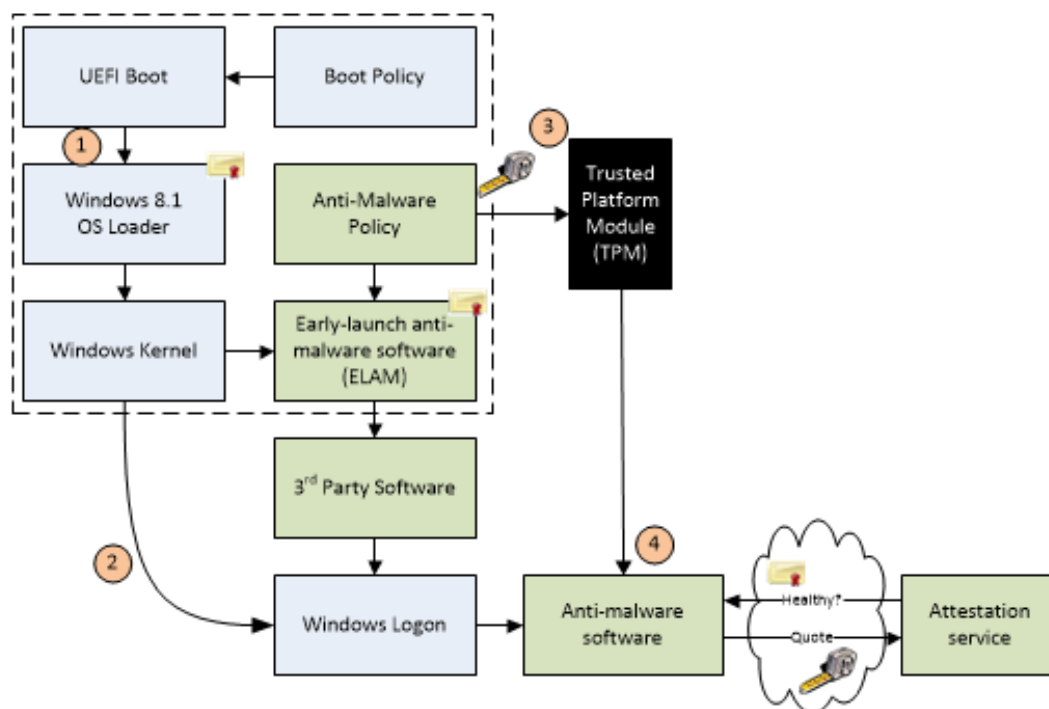
luvulta, jolloin lopulta emolevyvalmistajat yksinkertaisesti alkoivat suojautumaan niiltä es-täen pääsyn MBR osioon. (F-Secure, 2021)

Tietokoneen kiintolevy jaetaan aina osioihin, jolloin levynhallinnassa eri osiot näkyvät ikään kuin eri levyinä. Jokaisella osiolla voi olla oma tehtävänsä ja oma tiedostojärjestel-mänsä. Vaikka osioita olisi vain yksi, sisältää se silti Master Boot Recordin. Käynnistysosi-oon kohdistuvat virukset pääsevät työasemille usein fyysisen median kautta, kuten usb-tallennuslaitteiden. (Kaspersky, 2021)

Haittaohjelma pääsee käsiksi käynnistysosioon usein sillä hetkellä, kun sitä muokataan. Sen tavoitteena on kirjoittaa osioon vaikuttavaa koodia, joka käynnistyessä kryptaa eli sa-laa levyn sisällön. Kun levy on salattu, on miltei mahdotonta palautua tapahtuneesta. Täl-löin virus pääsee leviämään myös muihin laitteen tiedostoihin ja osioihin, jolloin ainut keino on alustaa levy. Helpoin tapa saada käynnistysosioon kohdistuva virus on, kun saastunut usb-tallennusväline on työaseman käynnistysvaiheessa käytössä ja käynnistys-luettelossa vaihtoehtona. (Landesman, 2021)

6.3 Työaseman salaus

Työaseman salauksesta puhuttaessa ei voi olla törmäämättä Windowsin sisäänrakennet-tuun Bitlocker-ominaisuuteen. BIOS-suojauksen jälkeen seuraavin kriittisin asia on tieto-koneen kiintolevyn tai ulkoisen muistilaitteen salaus. Bitlocker on salausmenetelmä, joka on sisäänrakennettu ominaisuus Windowsin yritysversioihin. Ominaisuus pohjautuu XTS-AES 128- ja 256-bittisiin kryptausmenetelmiin, jotka Microsoft on tuotteistanut osaksi omaa käyttöjärjestelmäänsä. Ominaisuus on laajalti käytössä varsinkin yrityskannetta-vissa. Ominaisuuden hallinta onnistuu Windows-tuotteiden ryhmäkäytäntö (Group Policy)-työkalujen avulla. Salaus turvaa muistiin tallennetut tiedostot ja tiedot tilanteissa, joissa laite katoaa tai se varastetaan. Tietojen palautus tai niihin käsiksi pääsy edellyttää suo-jaus- tai palautusavaimella tehtävää palautusta muistilaitteelle. Työaseman salausta voi-daan pitää fyysisenä toimenpiteenä, jolloin ei toivotussa tilanteessa estetään asiaton pääsy laitteelle, vaikka se olisi fyysisesti menetetty hallinnasta. Myös kiintolevyn käyttö ky-seisen työaseman ulkopuolella ei ole mahdollista ilman salauksen purkamista tai levyn tyhjennystä. (Bott, 2020)



Kuva 5 Windowsin suojatun käynnistyksen arkkitehtuuri kuvattuna

Monissa moderneissa yrityslaitteissa on erillinen TPM-piiri (Trusted Platform Module) lisäämässä levynsalauksen tehokkuutta. Uusissa yrityskannettavissa TPM on yleensä integroituna emolevyyn ja oletuksena määritetty BIOSiin. Tällöin salausavaimet tallennetaan kyseiseen piiriin, jotta suojausavainta ei tarvitse erikseen syöttää työaseman levyosiot käynnistäessä, esim. päästäkseen käyttöjärjestelmään. Yksinkertaisuudessaan TPM kerää yhteen tiedot työaseman luotetuista komponenteista ja käyttöjärjestelmän laiteohjaimista. Tämä suojaa järjestelmää hyökkäyksiltä, jotka kohdistuvat alttiimpiin laiteohjaimiin tai komponentteihin. Nykyinen TPM 1.2 generaatio hyödyntää SHA-1 hash algoritmia. (Bond & Landrock, 2011)

6.4 Virustorjunta

Virustorjuntaohjelma on yleisin ratkaisu työaseman suojaamiseen. Virustorjunta tarkoittaa ohjelmistoa, joka asennetaan tietokoneen käyttöjärjestelmään. Päätargetoitu virustorjunnalla on havaita ja estää haitallisen ohjelmiston eli haittaohjelman pääsy suojattuun laitteeseen. Kun haittaohjelma jää virustorjunnan haaviin heti, ei se ehdi aktivoitua eli suorittaa itseään kyseisellä laitteella. Havaintojen jälkeen virustorjunta puhdistaa työaseman saastuneista tiedostoista ja haittaohjelmista, jotka voivat sisältää viruksia tai matoja (computer worms), troijalaisia, kiristysohjelmia sekä mahdollisesti ohjelmia, joilla vakoilla käyttäjän toimintaa tietokoneella. (Johansen, 2019)

Virustorjuntaohjelmat on yleisesti valtavirrassa parhaiten omaksuttu keino suojata tietokoneita. Tänä päivänä ei usein törmää tietokoneeseen, jota ei suojattaisi virustorjunta- eli antivirusohjelmistolla. Virustorjunta toimii skannaamalla koneella olevia tiedostoja ja prosesseja verraten niitä tietokantaansa. Virustorjuntajärjestelmien tietokannat sisältävät dataa digitaalisesti allekirjoitetuista tiedostoista ja koodista, joihin se vertaa löydöksiään. Tällöin virustorjunta pelkän tietokantansa perustella pystyy estämään jopa 98 % tunnetuista haittaohjelmista. Vaikkei ole täysin kestävä tapaa estää käyttäjien työasemia saastumasta haittaohjelmilta, virustorjuntaa tarjoavat yritykset panostavat jatkuvasti uusiin keinoihin kuten algoritmeihin ja tekoälyyn tuotteissaan. Kuten aiemmissa luvuissa on todettu, ei myöskään antivirusohjelmisto voi estää käyttäjien tekemiä inhimillisiäkin virheitä työasemilla, huolimatta käyttäjän kyvykkyydestä toimia turvallisesti laitteellaan. (Maimon, 2019)

Skannaamisperiaatteen lisäksi on otettava huomioon myös uudet haittaohjelmat ja virukset. Edistyneimmät antivirusohjelmistot oppivat tunnistamaan nykyään koneilla epäilyttävää käytöstä. Epäilyttävät toimet voivat ilmetä tiedostoissa koodina, järjestelmän äkillisenä muutoksena tai komponenttien epänormaalina toimintana. Usein haittaohjelmat voivat ohittaa virustorjunnan kokonaan, mutta silti säilyä tietokoneella passiivisena pitkiäkin aikoja.

Yksi merkittävä seikka ovat myös käyttöjärjestelmien tuomat ominaisuudet. Melkein kaikki virukset ja haittaohjelmat kohdistuvat Windows-järjestelmiin. Linux-pohjaisiin käyttöjärjestelmädistribuutioihin ei edes käytetä virustorjuntaohjelmistoa. Suurin syy tähän teknisesti ovat ohjelmakirjasto ja asennukset, joita Linux-käyttöjärjestelmiin tehdään. Windows työasemilla suoritettavat ohjelmat pitää hakea itse luotetuista lähteistä, jolloin ohjelman arvioiminen jää käyttäjän tai järjestelmänvalvojan vastuulle. Linux-ympäristöissä paketit on mahdollista ladata ja asentaa luotetun ja keskitetyn ohjelmakirjaston tai latauspalvelun kautta, jossa yksinkertaisesti ei ole ei-luotettuja paketteja. Merkittävin yksittäinen syy on myös käyttöjärjestelmä markkinan osuudet, sillä Windowsia käytetään 87 % kaikissa työasemalaitteissa käyttöjärjestelmänä. (Stevanovic, 2020)

Virustorjunnan lisäksi tietoturvayhtiöillä on olemassa erityisesti suurille ympäristöille suunniteltu EDR ratkaisu eli Endpoint Detection and Response järjestelmä. Kyseinen termi on tuoreehko ja sillä kuvataan automaatioihin perustuvia turvatoimia, joita voidaan suorittaa yrityksen päätelaitteille havaitsemaan epäilyttäviä toimia tai suoritettavia prosesseja. EDR-tuotteiden pääpaino on kerätä yrityksen laitteista reaaliaikaista dataa ja valvoa jatkuvasti hallinnassa olevia laitteita. Termin on kehittänyt Gartnerin entinen tietoturva-analyytikko Anton Chuvakin vuonna 2013. (Sore, 2020)

6.5 Keskitetty hallinta

Kun yrityksessä on työasemia ympäristössään runsaasti ja useissa sijainneissa, niiden hallittavuus laitekohtaisesti vaikeutuu. Suuret määrät työasemia vaatii yrityksen IT-osastolta paljon resursseja pitääkseen laitteet ajan tasalla ja hallittuina. Keskitetyn hallinnan periaatteena tulee olla laitteen elinkaaren hallinta, päivittäminen sekä palautumisen mahdollistaminen ongelmatilanteissa. Yksittäisten työasemien asennukset käyttöjärjestelmän, sovellusten ja asetusten osalta lasketaan tunneissa, joten asennus kannattaa hoitaa organisaatioiden työasemaympäristöissä keskitetysti työasemahallintaratkaisua ja esiasennusta hyödyntäen. Myös monen sadan laitteen hallinta ja ylläpito vievät todella paljon resursseja henkilöiltä. Toimialueen hallintaa varten Active Directory ja ryhmäkäytännöt ovat pääasiallinen väline, mutta ne eivät kuitenkaan sovellu kaikkeen, kuten laitteiden elinkaaren hallintaan. Tunnetuimmat järjestelmät pohjautuvat Windows-töasemaympäristöihin, mutta periaatteellisesti pätevät myös Linux-pohjaiseen laitteiden hallintaan.

System Center Configuration Manager, eli paremmin tunnettu lyhenteellä SCCM, on Microsoftin maksullinen elinkaaren ja keskitetty työasemahallintaratkaisu Windows-pohjaisille työasemaympäristöille. Kyseessä on keskitetty ja automatisoitu hallintatyökalu, joka mahdollistaa yrityksen työasemaympäristön hallinnan ja elinkaaren ylläpidon. Ratkaisu pitää sisällään tietoturvaratkaisun, päivitykset, varmuuskopioinnin sekä etähallintamenetelmät järjestelmänvalvojalle. SCCM on pääasiassa on-premise ja standalone -tyylinen toteutus ympäristöön, kun SCCM:n edeltäjä Microsoft Intune on pilvipohjainen hallintaratkaisu, joka soveltuu myös hybridiympäristöihin. Lisääntynyt tarve varsinkin BYOD-laitteiden osalta on asettanut organisaatioille haasteita hallita laitteitaan. (Martinez, Daalmans, & Bennett, 2017, s. 40)

Keskitetyn työasemahallinnan kautta on mahdollista määrittää myös päivitysten asentuminen koneille. Päivitysten osalta voidaan hyödyntää myös Windowsin WSUS-palvelua toimialueen laitteille. Kriittisten päivitysten jakelu päätelaitteille on elintärkeää turvallisen ja toimivan käyttöjärjestelmän kannalta. Myös käyttöjärjestelmän versiopäivitysten tulisi asentua kaikille päätelaitteille keskitetysti ja hallitusti. Myös työasemajakelussa olevat asennettavat ohjelmistot tulisi kaikki sisällyttää keskitetyn ratkaisun piiriin, jottei laitteille asenneta ei-tunnettuja ja tuen ulkopuolisia ohjelmistoja. Tämän tarkoitus on lisätä tietoisuutta käytössä olevista ohjelmista, niiden versioista ja päivittämisestä. Keskitetty hallintatyökalu kerää myös lokitietoja laitteista, josta voidaan parsia virheitä muodostumaan hälytyksiksi.

7 Suojauksen varmistaminen

7.1 Konstruktiivisen mallin toteutus

Tässä luvussa hyödynnetään olemassa olevaa teoriaa ja käytänteitä, joiden pohjalta rakennetaan konstruktiivisella tutkimusotteella käytännön työnkulkuihin operoivaa mallia. Mallin tarkoituksena on havainnollistaa työasemien suojauksen varmistaminen ongelmatilanteissa. Mallia rakentaessa tuli ottaa huomioon viiteorganisaation soveltavuus mallin testaamista varten. Konstruktiota toteuttaessa oli myös tärkeää keskittyä ongelmaan, johon etsitään ratkaisua. Myös innovatiiviset työskentelymetodit tuli hyödyksi tässä luvussa, kuten suoraviivainen ja looginen päättelykyky sen pohjalta, mikä on rajattu pois tutkimuksesta, sekä mikä varmuudella tuottaa tuloksia. Konstruktiivisen tutkimusotteelle ominainen loputon määrä mahdollisia toteutumia tuli myös ottaa huomioon tutkimustuloksia kerätessä. Yksi esitetty ydinpiirre tutkimustavasta oli vahvasti keskiössä tutkimusta tehtäessä. Tutkimuksessa keskityin tosielämän ongelmaan työnkuvan pohjalta, jolle on käytännössä tarpeellista etsiä ratkaisuja.

Konstruktion toteuttamista varten piti hyödyntää käytössä olevaa viiteympäristöä laajasti, jotta tutkimuksessa tarvittavaa dataa oli laajasti saatavilla. Tutkimuksessa hyödynnetty työaseympäristön koko oli n. 1000 hallittua työasemaa monissa eri aliverkoissa keskiteysti hallittuina. Jokainen laite oli kannettava työasema, joilla kaikilla oli pääasiallinen käyttäjä. Viiteorganisaatio koostui useista kymmenistä toimipisteistä, jotka olivat omissa aliverkoissaan. Laitteilla ei myöskään tietoturvapoliittisesti ollut yhteyksiä eri tai samoissa aliverkoissa sijaitseviin työasemiin, vaan liikenne kahden client tietokoneen välillä oli estetty. Tutkimushetkellä merkittävästi laajin verkkosegmentti oli ssl-vpn aliverkko, jossa suurin osa etätyöskentelijöistä operoi. Viiteympäristön verkossa käsiteltiin keskivertoa enemmän myös arkaluontoista materiaali, joka asetti lisäpainoa tietoturvan toteuttamiselle ja sen organisoinnille. Ympäristössä ei ollut vanhoja käyttöjärjestelmiä versioita käytössä laisinkaan, eikä myöskään pöytätietokoneita. Myös virtuaaliset työasemat ja tuotantotyöasemat eivät sisältyneet tutkittavaan organisaatioon. Tämä vaikutti osittain tutkimuksen laajuuteen, mutta samalla rajasi sitä yksinkertaisemmaksi toteuttaa.

Laitteita varten käytössä oli monia suojausratkaisuja, joista sai käytettävää tietoa päätelaitteista. Myös käyttäjien turvallisuutta oli otettu ratkaisuissa huomioon. Tunnuksen ja sähköpostin suojauskeinoja oli myös käytössä ja toiminnassa päivittäisessä viestimisessä, kuten toimialueen ulkopuolisten tahojen kanssa viestiessä arkaluontoisia tietoja. Myös selaimien turvallisuutta ja asetuksia oli laajasti suunniteltu ja pantu täytäntöön. Konstruktion tavoitteena oli luoda looginen työnkulku, jonka mukaan reagointi virheisiin

ongelmatilanteissa olisi luontevaa ja järkevää. Työnkulkua toteutettaessa ja testatessa voidaan reagoida puutteellisiin prosesseihin, virheellisesti määritettyihin sääntöihin ja politiikoihin, sekä korjata ongelmia suojausratkaisuissa. Toimivuutta ratkaisujen osalta peilataan yhteensopivuuteen (engl. compliance) työasemilla. Työasema täyttää yhteensopivuusvaatimukset vain, mikäli se toimii, päivittyy, reagoi ja keskustelee hallinnan kanssa sovitusti. Jos suuri osa yhteensopivuusvaatimuksista ei laitteen kohdalla täyty, on tarpeen tehdä korjaavia toimenpiteitä kyseisen laitteen osalta.

Osassa ratkaisuissa oli käytössä hallintapaneeli, josta oli mahdollista saada reaaliaikaista dataa käyttöön analysoitavaksi. Mallin luomisen jälkeen tuli myös varata seuranta-aikaa, jotta malli oli mahdollista validoida toiminnallisuuksien ja työnkulun osilta. Seuranta-aika tulee olla riittävän pitkä, ainakin noin 1–2 kuukautta. Seuranta-aikana saadaan myös viitteitä toistuvuudesta ja yleisimmistä haasteista. Seuranta tulisi tehdä sekä reaaliaikaisesti että koostena esimerkiksi viikoittain, jolloin tehdään löydöksiä viiteympäristöstä. Seuranta-aikana kerätty dataa on käsitelty viiteympäristössä välittömästi, eikä sitä ole koostettu koko ajalta yhdeksi kokonaisuudeksi pelkästään. Tämä siksi, koska ei olisi järkevää virheiden osalta odottaa seuranta-ajan päättymistä, jos niihin kannattaa vakavuuden tai riskiin pohjautuen puuttua välittömästi. Suuri osa laitteista oli täysin yrityksen toimitilojen ja sisäverkon ulkopuolella. Kytkös hallintaan oli tapahtunut seuranta-aikana yhdistämällä VPN-määrytykset yrityksen verkon ja päätelaitteen välillä. Verkkoympäristöstä oli mahdollista päätellä, että n. 55 % laitteista ei ollut pitkän aikavälin aikana ollut toimipisteen verkoihin kytkeytyneenä.

Yrityksen järjestelmänvalvojalla tai ylläpitäjällä tulee olla mahdollisuus seurata työasemien tietoturvaluottuutta. Tämän työn teoriaosuudessa on sivuttu lukuisia ratkaisuja, joilla työasemia suojataan. Yksikään suojausmekanismi ei kuitenkaan ole riittävä, jollei se toteudu koko ympäristössä yhtenäisesti. Tämän takia on tärkeää varmistua, että käytössä olevat suojauskeinot ovat toiminnassa halutusti. Suuri määrä työasemia yrityksen verkossa vaatii suunniteltua hallintaa sekä toimiva prosesseja. Kokonaisuutta toteuttavat joko IT-osaston jäsenet, tai vaihtoehtoisesti edistykselliset järjestelmät, joihin on mahdollista määrittää automatiikkaa.

Kun työasemaympäristössä on käytössä keskitetty hallintatyökalu tai ohjelmisto, voidaan sen tuottamaa dataa hyödyntää laajastikin edellä mainittujen tietojen saamiseksi. Myös monet keskitetyt antivirusohjelmistokokonaisuudet tarjoavat vastaavia tietoja, jos kaikki laitteet ovat listautuneet sen hallintaan. Usein keskitetyissä hallintaratkaisuissa on käytössä graafinen käyttöliittymä, kuten hallintapaneeli. Paneelista on mahdollista jaotella kohteita haluttuihin ryhmiin tai kategorioihin ja luoda sääntöjä eri tarpeiden mukaisesti.

Työasemahallintaohjelmisto käy ympäristöä ja sen laitteita läpi ajastetusti ja tekee ympäristöstä haun työasemien tilasta. Tiedoista saadaan kerättyä kollektiivisesti raportit nykytilasta. Raporteista voidaan tarkastella muun muassa käyttöjärjestelmäversiot laitteilta, päivitysten läpi meno, aktiivisten päätelaitteiden määrät ja nykyiset käyttäjät, sekä lukuista muuta dataa. Hallinnan lisäksi myös antivirusohjelmistoissa on mukana oma hallintansa. Sillä, ovatko järjestelmien palvelinympäristöt saatavilla sisäverkossa vai julkipilvessä, on suuri merkitys. Sisäverkon osalta laitteen tulee olla yhdistynyt toimialueen verkkoon, kun taas julkipilvessä riittää toimiva internetyhteys. Kummassakin skenaariossa on puolensa yleisen tietoturvallisuuden kannalta. Kuitenkin pelkästään sisäverkossa toimivat resurssit ovat hankalasti tavoitettavissa, kun päätelaitteella työskennellään etänä.

Työn teoriaosuudessa saadut pohjatiedot toimivat apuna, kun etsittiin käytännön kannalta suojaustoimia, joiden toimivuutta pystyttiin todentamaan päätelaitteilta. Hallintamalleja ja standardisoituja tapoja ratkoa ongelmatilanteita pystyi konstruktiivisen mallin toteuttamisessa käyttämään apuna. Teoriaosuudessa löydetty monialaiset menetelmät hallita tietoturvaa laitteilla hyödyntäen edistyneitä järjestelmiä antoivat valmiudet käytännön tietotaidon osalta. Teorian pohjalta toimivuuksia oli mahdollista tutkia käytännön ja toteutuneen osilta. Järjestelmänvalvojan toimenkuva on hyvin pitkälti vianselvitystä ongelmatilanteissa, jossa käytetään paljon loogista päättelykykyä oman tietotaidon lisäksi. Kuitenkin, jos kaikki toiminnot tulisi hoitaa manuaalisesti ilman mitään automaatioita tai järjestelmiä, olisi toimenkuvassa resurssipulaa yksittäisellä järjestelmänvalvojalla. Merkittävä osuus teoriasta ei kuitenkaan päde suoraan moniin ympäristöihin, koska käytäntö voi usein merkittävästikin erota teoriasta tai määritellyistä prosesseista.

Oleellista on myös päätelaitteen yhteys hallintaan aina sen ollessa päällä ja verkkoyhteydessä. Jos työasema on jostain syystä kykenemätön keskustelemaan tarvittavan isännän kanssa, tulee järjestelmänvalvojan saada siitä tarpeenmukainen ilmoitus. Tämä mahdollistaa reagoinnin ja selvitystyöt ongelmatilanteissa. Katoamisen tai ei-toivotun skenaarion esiintyessä laite tulee olla mahdollista eriyttää (isolate) verkosta kokonaan tai tyhjentää verkon yli käyttökelvottomaksi. Myös kriittisissä uhissa edellä mainittu toiminto on tarpeellinen. Laite on suotavaa eristää verkosta hälytyksen analysoimisen ajaksi, jos varmuutta sen vakavuudesta ei ole.

Kun edellytykset suojaustoimintojen toimivuudelle ovat kunnossa kaikilla laitteilla, voidaan puhua teoriassa keskitetysti hallitusta tietoturvasta työasemien osalta. Kaiken toimiessa halutusti, on oleellista huomioida riittävät resurssit ylläpidon ja hallintatoimien varalle. Virheet järjestelmissä tulee huomioida riittävin keinoin ylläpidon toteutumiseksi. Muissa tapauksissa pettää ympäristön teoreettinen turvallisuus, jolloin ollaan enemmän alttiita uhille

ja haavoittavuuksille, joista muodostuu riskejä ympäristölle. Mikäli suojaustoiminnot ovat puutteellisia tai ne eivät toimi halutusti, on niiden lisähyöty olematon, eikä niitä tulisi ylläpitää tai käyttää turvatoimina. Vastaavassa tilanteessa lisäresursointi paikallisiin tai manuaalisiin ratkaisuihin olisi järkevämpää. Kuitenkin suojaustoiminnot eivät käyttöönottovaiheissa ole ikinä täysin valmiita tuotantoon, vaan niitä tulee testata ja kehittää systemaattisesti. Pitkällä aikavälillä saavutettu hyötysuhde on paljon järkevämpää resurssien osilta, kuin eri ratkaisujen vaihtaminen toisiin lyhyissä sykleissä.

Mallin käytäntö lähti rakentumaan ongelmatilanteen ja sen ratkaisemisen pohjalta. Ongelmatilanteet työkaluissa ja järjestelmissä ovat yleisiä. Suurella todennäköisyydellä jatkuvalla seurannalla kaikki ei toimi 100 % tarkkuudella ja halutusti. Ongelman syntyessä järjestelmänvalvojan tulee olla tietoinen tapahtuneesta, joka voidaan taata hälytyksen avulla. Hälytys voi olla ilmoitus, sähköposti tai rivi järjestelmän lokeissa. Näistä kaksi ensiksi mainittua ovat reaaliaikaisia yleisesti, sillä lokitietoja on työlästä pitää silmällä, vaikkakin tarpeellista pitkässä juoksussa. Muodostunut hälytys pitää analysoida ja käsitellä. Käsitellessä pitää tutkia tarkemmin, mikä mekanismi tai attribuutti kyseisen ilmoituksen on muodostanut. Hälytyksiä voi olla useanlaisia. Osa hälytyksistä voi perustua ennalta määritettyihin sääntöihin tai työnkulkuun. Hälytykset voivat myös olla virheellisiä, jota kutsutaan englanniksi termillä false positive. Hälytyksiä voi myös ennaltaehkäistä. Ennaltaehkäiseviä toimia voidaan työasemaympäristöjen tietoturvan osalta toteuttaa ennakkoinnilla, politiikoilla, säännöillä, sekä toimivalla hallinnalla.

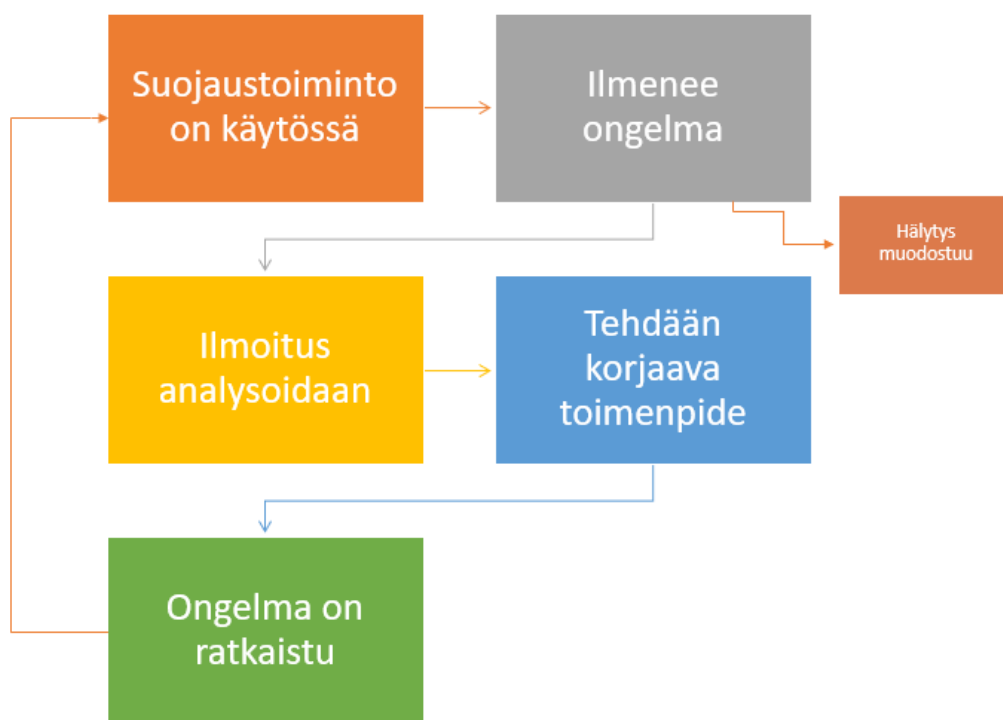
	Null hypothesis is TRUE	Null hypothesis is FALSE
Reject null hypothesis	Type I Error (False positive)	Correct outcome! (True positive)
Fail to reject null hypothesis	Correct outcome! (True negative)	Type II Error (False negative)

Kuva 5 Graafisesti esitetyt tyypin 1 ja 2 virheet (false positives) (Anderegg, 2014)

Ilmoituksen analysoinnin jälkeen päätetään hälytyksen paikkansapitävyydestä ja mahdollista jatkotoimista. Tähän asti hallintamallin mukaiset valvovat ja ennaltaehkäisevät toimet

ovat käytetty, jolloin ongelmatilanteen muodostanut tila ympäristössä tulee käsitellä korjaavin tai palauttavin toimin. Korjaavat toimenpiteet määrityksensä mukaisesti pyrkivät ratkaisemaan hälytyksen aiheuttaneen juurisyyn. Korjaavan toimenpiteen suorittaminen vaatii harkintaa ja pohdintaa järjestelmänvalvojalta. Pääsääntöisesti esiintyviin arkisiin ongelmiin tulisi löytyä prosessien mukainen ratkaisumenetelmä tai keino. Toimenpiteitä on mahdollista suorittaa keskitetysti kaikille laitteille, jos ongelma koskee tai tulisi mahdollisesti koskemaan myös muita laitteita. Jos virhe koskee vain yhtä työasemaa, voi parempi ja nopeampi toimintatapa suorittaa korjaus toteuttaa se paikallisesti eli konekohtaisesti.

Keskitetyt korjaukset tulee suorittaa valvovista järjestelmistä, kuten virustorjunnan hallinnasta tai työasemahallintatyökalun kautta. Myös Active Directory -toimialuepalveluiden kautta voi tehdä ryhmäkäytänteitä, johon kaikki autentikoidut laitteet valikoituvat. Etenkin laajoissa ja suurissa työasemaympäristöissä lukumäärällisesti laitteiden osalta kaikki isommat korjaukset ja määritykset tulisi suorittaa yhtenäisesti, jotta työmäärä ja ylläpidolliset toimet pysyvät hallinnassa. Korjaavan toimenpiteen jälkeen asia ratkeaa tai vaatii lisäselvitystä. Ratkettuaan tilanne palautuu haluttuun eli toimivaan ympäristöön, jonka ylläpitäminen ja valvonta jatkuu aktiivisesti.



Kuva 6 Konstruktio malli työasemien hallinnoimisessa

7.2 Mallin testaaminen

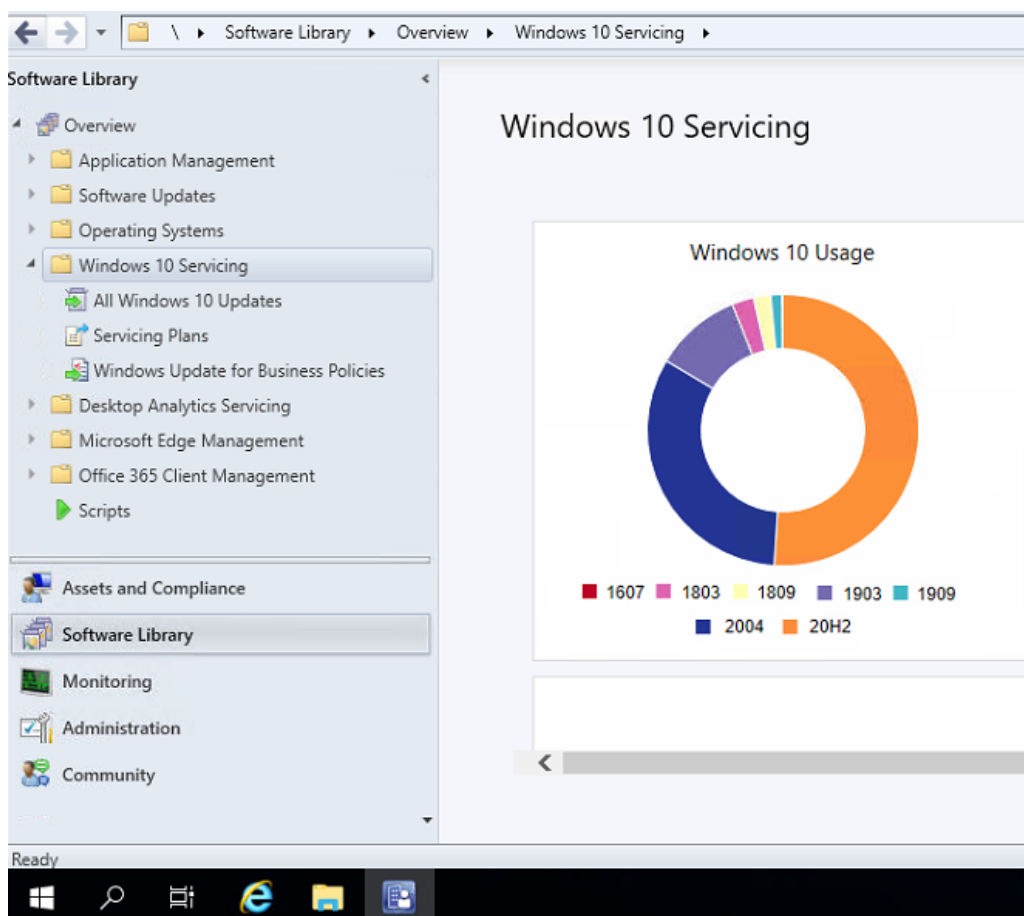
Konstruktivisen mallin testauksessa hyödynnettiin viiteympäristöön tehtyjä raportointimenetelmiä ja hälytyksiä, joita automaattiset skriptit lähettivät järjestelmänvalvojalle. Kaikki raportit tai hälytykset kaikki eivät tulleet takautuvasti tai reaaliaikaisesti työasemista, vaan ainoastaan kun käyttöönoton jälkeen ympäristössä tapahtui löydös tai ongelmatilanne, jota haluttiin ennaltaehkäistä. Tieto monivaiheisen todentamisen osalta saatiin Windows PowerShell komennolla haettua viiteorganisaation käyttäjänhallinnasta. Bitlocker ratkaisun käytöstä saatiin SCCM:n ja Asset Manager (laittehallinta) työkalun kautta Query-tyypisellä kyselyllä päätelaitteista. Moni muu hälytys tai raportti sähköpostitse tai järjestelmään oli mahdollista toteuttaa suoraan keskitetyn antivirusratkaisun hallintapaneelin kautta, käyttämällä haluttuja attribuutteja.

Raporteista ja hälytyksistä ilmeni mm. End of Life (EOL) -kierrätykseen menneiden koneiden takaisin käyttöönotot käyttäjien toimesta ohjeistuksien vastaisesti, sekä myös kierrätykseen tarkoitettujen hajonneiden koneiden yhdistäminen verkkoon. Näistä löytyi raportoinnissa kirjautuneen käyttäjän tieto, jolloin korjaava toimenpide oli mahdollista suorittaa. Hälytyksen antoivat myös suoraan viestissä tiedon, jos kyseessä oli Windows 7 -käyttöjärjestelmällinen laite, joita yrityksen verkoissa ei ole enää sallittu käytettävän. Tiedot oli mahdollista suodattaa raportiksi, joka koostuu toistuvasti viikoittain antivirusohjelmiston hallintapaneelissa. Myös ei-käytössä olevat laitteet pystyivät suodattamaan viimeisen ajankohdan mukaan, kun laite on ollut yhteydessä verkkoon. Kyseisten laitteiden poistaminen rekisteristä selvensi todellisen määrän sen hetkisestä laitemäärästä. Kun uusi laite ilmestyy verkkoon ja antivirusohjelmisto asentuu onnistuneesti tietokoneelle, liittyy se automaattisesti ensisijaiseen ryhmään. Raporteista pystyi myös tarkastella asennetut tai suoritettut ohjelmistot päätelaitteilla. Yksi hälytys kriteeri oli mm. olla antivirus ohjelmiston agentin toimimattomuus työasemalla, jolloin asiaan pitää tehdä mahdollisesti korjaava toimenpide (reagointi) hälytyksen tultua (ennaltaehkäisy tai tunnistus). Ennen reagoivaa toimenpidettä kuitenkin piti varmistaa ovatko hälytykset aiheellisia (analysointi), eli mistä hälytys johtuu. Jos kaikista kriittisin suojaustoimi julkista internetiä käytettäessä ei toimi, ei koneella tulisi olla pääsyä verkkoon hetkellisesti, ennen kuin korjaava toimenpide on suoritettu. Yksi selitys voi olla ohjelmiston korruptointi tai yksinkertaisesti lisenssin puuttuminen ohjelmistoa varten.

Myös Bitlocker-haku tuotti tulosta konstruktion osalta, sillä ilmeni virhetilanteen takia suuren määrän laitteista olevan käynnissä ilman Bitlocker-salauksen toimivuutta. Kyseessä oli ongelma esiasennuksessa, jossa salausavaimen tallennus emolevyn TPM-piiriin ei ollut toiminut uusilla laitteilla. Tämän myötä oli mahdollista käydä PXE käynnistyksessä oleva

esiasennus määrittelyt, sekä myös vialliset työasemat läpi, jottei kyseistä pääse tapahtumaan jatkossa. Virhetilanne oli kaikin puolin riskialtis. Laitteiden kadotessa tai joutuessa ei-halutulle tielle olisi voinut asettaa organisaation ympäristön alttiiksi riskeille.

Monivaiheinen todentaminen oli oletuksena käytössä kaikilla toimialueen henkilökäyttäjillä pakotettu tilassa. Ilman todennuksen määrittystä ei tilillä ole kirjautumisoikeutta toimialueen palveluihin ja resursseihin. Kootusti otettavasta raportista tehtiin ajastus, joka toistui viikoittain ympäristöstä. Raportista, joka muodostui järjestelmänvalvojalle, pystyi seuraamaan virheelliset tilit. Seuranta-ajan puitteissa ilmeni, ettei uusien tunnuksien osalta monivaiheinen todentaminen ollut aktivoitunut käyttöön. Syynä tälle oli muuttuneet ohjeistukset tunnustenluonti vaiheen prosesseissa, jolloin luontivaiheessa asettamista pakotettuun tilaan ei enää toteutettu kuten aiemmin. Tämä oli yksinkertainen ohjeistaa jatkoon.



Kuva 7 Viiteympäristön raportointi Windows-Build versioiden osalta. Kuvakaappaus SCCM - työasemahallinta työkalun käyttöliittymästä

Käytettävän ympäristön osalta myös Microsoftin keskitetty työasemahallintatyökalu SCCM antoi kattavaa tietoa tutkimusta varten. Raporteista pystyi jaottelemaan muun muassa ympäristössä käytössä olevat Windows 10 Pro versioiden Build-versiot. Raportista näki osuudet prosentteina ja lukumäärällisesti työasemista, jotka eivät olleet päivittyneet

ajantasaisiksi versiopäivityksien osalta. Myös laiteohjaimissa ja BIOS laiteohjelmiston versioissa oli huomattavaa vaihtelua ajantasaisuudessa. Tutkimusvaiheen löydösten perusteella organisaatiossa päätettiin lähteä projektiluontoisesti ottamaan käyttöön keskitettyä päivitystyökalua, joka operoisi enemmän tarpeidenmukaisesti ja ei vaatisi VPN yhteyksiä toimiakseen. Tämä olisi mahdollista toteuttaa täysin irrallisena nykyisistä ratkaisuista, tai vaihtoehtoisesti integroida olemassa oleviin järjestelmiin. Myös hybridi pilvipohjaiseen infrastruktuuriin tulisi jatkossa lisätä enemmän kehitysresursseja viiteympäristössä. Suunnitelmat hybridi- ja cloud-first-pohjautuviin ratkaisujen osalta oli huomioitu kehitystoimenpiteissä ja tulevilla projekteilla myös monella muulla osa-alueella.

Suurin haaste viiteorganisaatiolla on ollut toteuttaa keskitetysti päivitysjakelut onnistuneesti. Hallintatyökalujen raporteista ilmeni huomattavaa hajontaa kuukausittaisissa läpimenoprosenteissa. Suurin syy, joka oli loogisesti pääteltävissä viittasi päätelaitteiden ongelmiin viestiessään hallinnan kanssa. Osa päätelaitteista ei ollut aktiivisesti yhteydessä hallintaan erinäisten syiden johdosta. Merkittävin syy oli n. 5 % laitteista, jotka olivat pudonneet inaktiivisiksi client-järjestelmiksi. Tämä oli pääteltävissä siten, että kyseinen osuus työasemista ei ollut yhteydessä toimialueen verkkoon, jossa myös hallintatyökalu viesti laitteille. Tähän vaikutti vahvasti etätyöskentely kuluvan vuoden aikana, jolloin yrityksen sisäverkon VPN yhteyksiä ei ollut laitteella kytketty päälle kertaakaan, tai toimialueen toimipisteen verkossa ei ollut tehty aktiivisia istuntoja, jotka olisivat palauttaneet tilan aktiiviseksi. Tämän johdosta oli loogista päätellä, etteivät VPN-yhteydet olleet toimivimmasta päästä yrityksen verkkoympäristön osalta, jolloin niitä tulisi pitkällä tähtäimellä kehittää palvelemaan tarpeita.

7.3 Mallin soveltaminen ja kehittäminen

Malli voitiin tutkimuksessa todeta niin käytännön kuin teoriankin pohjalta toimivaksi. Tämä ei kuitenkaan tarkoita, että mallia ei olisi mahdollista jatkokehittää tai se olisi täysin valmis sellaisenaan. Suunniteltu malli vaatii myös edellytyksiä organisaatioille. Organisaation tulisi sisältää laajan työasemaympäristön. Laaja on subjektiivinen käsite mutta tämän tutkimuksen pohjalta olisi loogista käsitellä satoja työasemia sisältäviä kokonaisuuksia, joita hallitaan keskitetysti ja suunnitellusti.

Malli oli toimiva ympäristössä, jossa laitekanta oli hyvin standardisoitu, eikä isoja eroja laitekannassa ilmennyt. Mallin soveltuvuus kuitenkin perusperiaatteiden myötä soveltuu myös käytettäväksi prosessien ohelle lukuisilla eri toimialoilla, joissa työasemaympäristö koostuu työasemista. Työasemien tyypeillä ei ole suoranaista vaikutusta mallin toimivuuteen. Samat normit ja käytettävät metodit toimivat käyttöjärjestelmästä tai konemallista

riippumatta. On myös paikkansapitävää, ettei mallissa esitettyjä prosessia tai työnkulkua ole mahdollista laiminlyödä, sillä se aiheuttaisi kriittisiä riskejä koko yrityksen verkkoon.

Mallia olisi järkevä soveltaa isoon organisaatioon, jossa työasemien määrä ylittäisi 500 hallittua laitetta. Laitteita voi olla kannettavien työasemien lisäksi myös toimistotilojen lisäksi tuotannossa eri toimintoja mahdollistamassa. Työasemista osa kannattaa olla virtualisoituja työasemia, joissa laskentatehoa ei tuoteta itse työaseman raudalla vaan palvelinympäristössä. Myös erilaiset tarpeet organisaation ja sen käyttäjäkunnan toisi lisääarvoa mallin soveltamiseen. Monimutkaiset ympäristöt ja suuri määrä erilaisia ohjelmistoteutuksia haastaisi mallin puitteissa toimivuutta tietoturvan ylläpitämisessä.

Sekä mallia, että järjestelmiä on mahdollista kehittää suuntaan, jossa huomattavat määrät korjaavia toimenpiteitä on mahdollista käsitellä automatiikan avulla. Tämä edellyttäisi suuressa osassa organisaatioista resurssien siirtämistä keskitettyihin järjestelmiin, johon sääntöjen implementointi ja istutus onnistuisi ylläpidollisesti ajatellen helpoiten. Mitä enemmän laitemäärät kasvavat, vaatii niiden ylläpito enemmän resursseja. Jos resursseja ei ole henkilöstössä varattu tarpeeksi, tulee vaje täyttää edistyneiden järjestelmien avulla. Myös budjetissa tulee olla tilaa skaalautuvuudelle. Joissain tilanteissa ongelmatilanne vaatii keskivertoa enemmän reagointia korjaavan toimenpiteen suorittamiseen. Kun järkevästi varattu resurssimäärä yhtä laitetta kohti kasvaa kannattamattomaksi, on järkevää korjaavien toimenpiteiden sijaan uusia viallinen laite suoraan. Tämä onnistuu, kun laitteita on saatavilla nopeasti esimerkiksi esiasennusympäristön myötä luotu puskuri laitteita valmiiksi toimitettavaksi.

Luvussa 4.2 tässä työssä esitetty tietoturvan hallintamalli toimii perustana mielestäni jatkokokehityskohteissa myös tutkimuksessa luodun mallin osalta. Kaikki toimenpiteet pitäisi pohjautua loogiseen ajatteluun tai teoriaan, kuten ennalta määritettyihin normeihin. Kyseisessä hallintamallissa ilmenneet toiminnot mahdollistavat työasemille kollektiivisesti turvallisen käyttöympäristön.

8 Yhteenveto

Työ löysi ratkaisuja esitettyyn tutkimusongelmaan sekä tutkimuskysymyksiin saatiin vastauksia ja ratkaisuvaihtoehtoja. Teoriaosuudesta koostui kattava pohjatieto tutkimuksen perustaksi, jossa käsiteltiin tietoturvaa tekniseltä aspektilta, tietoturvan hallintakeinoja, erilaisia työasemia, työasemiin kohdistuvia uhkia, sekä suojausmenetelmiä sovellettavaksi työasemille. Työn rajaus onnistui myös hyvin, eikä työstä tullut liian laaja ja teoreettinen. Konstruktiivinen tutkimusmetodi antoi toimivan tutkimusotteen toteuttaa työ valituilla rajauksilla ja hyödynnettävyyks kohteilla.

Työn myötä tuli selvitettyä nykyiset ongelmat työasemien tietoturvassa etätyön yleistymisen kannalta sekä pilvipohjaisten ohjelmistojen ja tietoteknisten ympäristöjen kannalta. Yrityksen IT-ympäristöä suunniteltaessa on otettava huomioon nykyiset vaatimukset ja mahdolliset ongelmatilanteet, kun laitteet eivät välttämättä ole rajatussa tilassa tai samassa verkossa yhdistettyinä. Suunniteltu ja testattu konstruktio soveltuu osaksi järjestelmänvalvoja käyttäjien toimenkuvaa, jossa hallintamallin mukaisia toimintoja toteutetaan päivittäisissä ylläpitotehtävissä. Etätyö ja pilvipohjaiset järjestelmät, sekä ohjelmistototeutukset on yleistyneet viimeisen viiden vuoden aikana laaja-alaisesti. Hallitseva kehityskaari viittaa vahvasti resurssien keskittämistä pilveen. Etätyön yleistyessä on tärkeää tehdä suunniteltuja ja ennakoitavia päätöksiä organisaation verkkojen, sekä suojausratkaisujen osalta.

Modernit järjestelmät ovat erittäin isoja kokonaisuuksia, jolloin tulee organisaatioissa ottaa huomioon monta asiaa uusien järjestelmien käyttöönotossa ja niiden elinkaarten hallinnassa. Tämä pätee myös tietoturvaratkaisuihin yrityksen verkossa ja laitteilla. Myös järjestelmien ylläpitoa pitää suunnitella tarkasti. Uutta tietoturvajärjestelmää tai suojausmenetelmää käyttöönottaessa pitää punnita riskit ja käyttötarpeet jo suunnitteluvaiheissa. Käyttöönotto kannattaa tehdä projektina, jossa on projektihenkilöiden lisäksi ohjausryhmä haastamassa projektissa käytettyä teoriaa, metodeja ja käytännön ratkaisuja, sekä antamassa eri näkökulmia asioihin. Etenkin jos käyttöönotettava järjestelmä kuten pääsyn- tai identiteettihallinnan järjestelmät, on kyseessä erittäin laajoja kokonaisuuksia, jotka vaativat perinpohjaista suunnittelua ja testausta organisaation moninaisten käyttötarkoitusten varalta. Tietoturvaratkaisun käyttöönotossa kannattaa pohtia käytetäänkö ratkaisua keskitetysti vai onko ratkaisu käytössä jokaisella käyttäjällä erikseen.

Turvaratkaisun tai suojatoimen ei tulisi myöskään vaikeuttaa henkilöstön eli työasemien käyttäjien työskentelyä, vaan mahdollistaa turvallinen käyttö itselleen ja laitteelle. Ratkaisujen keskiössä tulee laitteiden lisäksi olla myös vahvasti käyttäjä esillä. Työasemaympäristössä tulisi olla keskitettyjä hallintamenetelmiä ja järjestelmiä, jotta mallia on mahdollista

toteuttaa halutulla työnkululla. Suojaustoiminnon virhetilanteesta tulisi aina muodostua hälytys järjestelmänvalvoja tason käyttäjälle. Hallintaan tulisi pyrkiä automatisoimaan toimenpiteitä sääntöjen pohjautuen. Tämä säästää yrityksen resursseja IT-henkilöstön osalta ja keskittää niitä sekä oleellisimpiin, että edistyksellisimpiin toimenkuviin organisaation sisällä. Ratkaisujen automaatioihin tulisi panostaa ja järjestelmiä tulisi opettaa käsittelemään virhe- ja ongelmatilanteita reaaliaikaisesti, johon ihminen ei pysty reagoimaan yhtä nopeasti ja suoraviivaisesti. Tämä on mahdollista tilanteissa, joissa tulkinnanvaraa ei ole, vaan työnkulku on selvä ja looginen.

Kokonaisuudessaan toteutettu konstruktio ei ole täysin uusi, mutta se pohjautuu vahvasti olemassa olevaan teoriaan ja aikaisemmin tehtyihin malleihin. Sen lisäksi malli tuo lisäarvoa yrityksille, joiden IT-järjestelmien kehityskaari on nopeutuvassa ja kasvavassa vauhdissa. Mallia rakentaessa pyrin välttämään, ettei teoreettinen kontribuutio ole vain aikaisempien teorian havainnollistamista. Tämä ei toteutunut täysin, mutta toi uutta mielenkiintoista soveltamista alla käytettävien periaatteiden lisäksi.

Lähteet

Anderegg, W. R. L. 2014. Awareness of Both Type 1 and 2 Errors in Climate Science and Assessment. Viitattu 30.4.2021 Saatavissa https://www.researchgate.net/publication/268035363_Awareness_of_Both_Type_1_and_2_Errors_in_Climate_Science_and_Assessment/figures?lo=1

Athow, D. 2020. VPN Tunnels explained, what are they and how can they keep your internet data secure. Viitattu 11.2.2021. Saatavissa <https://www.techradar.com/vpn/vpn-tunnels-explained-how-to-keep-your-internet-data-secure>

Bond, M. & Landrock, P. 2011. The Trusted Platform Module Explained. Cryptomathic. Viitattu 19.1.2021. Saatavissa <https://www.cryptomathic.com/news-events/blog/the-trusted-platform-module-explained>

Bott, E. 2020. ZDNet. Everything you need to know about BitLocker Viitattu 12.1.2021. Saatavissa <https://www.zdnet.com/article/windows-10-experts-guide-everything-you-need-to-know-about-bitlocker/>

Butt, A. 2021. What To Expect From The Rapidly Growing And Evolving Software As A Service Market In 2021. Forbes. Viitattu 12.3.2021. Saatavissa <https://www.forbes.com/sites/theyec/2021/01/19/what-to-expect-from-the-rapidly-growing-and-evolving-software-as-a-service-market-in-2021/?sh=1fdc17ac7300>

Camarinha-Matos, L. 2014. Constructive Research method. Viitattu 12.3.2021. Saatavissa https://www.researchgate.net/publication/267332010_Achieving_Coherence_between_Strategies_and_Value_Systems_in_Collaborative_Networks/figures

CISA. 2021. Ransomware guidance and recourses. Viitattu 12.3.2021. Saatavissa <https://www.cisa.gov/ransomware>

Clifford, J. 2021. How to Detect and Protect Against CEO Fraud. TCS Blog. <https://blogs.tcsusa.com/how-to-detect-and-protect-against-ceo-fraud>

Dascalescu, A. 2017. Here's How To Get Solid Browser Security. Heimdal Security. Viitattu 2.3.2021. Saatavissa <https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/>

Day, B. 2019. Complete Guide on Email Security & Threats Faced by Organizations-Guardian Digital. Viitattu 29.2.2021. Saatavissa <https://guardiandigital.com/blog/email-security>

Decker, F. 2012. Three Different Types of Computers for Use in Business. Chron. Viitattu 9.1.2021. Saatavissa <https://smallbusiness.chron.com/three-different-types-computers-use-business-48842.html>

Durga, P. A. 2021. Security Solutions to Protect from Spam and Phishing Attacks. Geekflare. Viitattu 2.2.2021. Saatavissa <https://geekflare.com/email-security-solution/>

eCraft. 2021. Mikä on toiminnanohjausjärjestelmä eli "erppi"? Viitattu 9.4.2021. Saatavissa <https://www.ecraft.com/fin/blog/2021/3/30/mika-on-toiminnanohjausjarjestelma-eli-erppi>

Fruhlinger, J. 2020. What is phishing? How this cyber attack works and how to prevent it. CS Online. Viitattu 15.4.2021. Saatavissa <https://www.csoononline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>

F-Secure. 2021. Boot virus. F-Secure Labs. Viitattu 22.3.2021. Saatavissa <https://www.f-secure.com/v-descs/boovirus.shtml>

Harrell, J. 2020. Endpoint Management and Security In a Work-From-Home World. DZone. Viitattu 14.1.2021. Saatavissa <https://dzone.com/articles/endpoint-management-and-security-in-a-work-from-ho>

Harris, A. 2021. Are Privileged Access Management PAM and Identity Access Management IAM the same? Osirium. Viitattu 29.4.2021. Saatavissa <https://www.osirium.com/blog/privileged-access-management-and-identity-access-management>

Hiley, C. 2021. What is VPN split tunneling? Viitattu 26.4.2021. Saatavissa Cybernews <https://cybernews.com/what-is-vpn/split-tunneling/>

Hoelscher, P. 2021. What is the best WPA2 security mode AES, TKIP, or both? Viitattu 12.4.2021. Saatavissa Comparitech <https://www.comparitech.com/blog/information-security/wpa2-aes-tkip/>

IBM. 2021. What is a computer network? Viitattu 16.2.2021. Saatavissa <https://www.ibm.com/cloud/learn/networking-a-complete-guide>

Johansen, A. G. 2019. Norton Security Center. Viitattu 18.3.2021. Saatavissa What is antivirus software? Antivirus definition <https://us.norton.com/internetsecurity-malware-what-is-antivirus.html>

Johanssen, A. G. 2020. What is a Trojan? Is it a virus or is it malware? Norton. Viitattu 15.4.2021. Saatavissa <https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>

Kaspersky. 2021. What is a Boot Sector Virus? Viitattu 9.1.2021. Saatavissa <https://usa.kaspersky.com/resource-center/definitions/boot-sector-virus>

Koivisto, J. & Andreasson, 2013. Tietoturvaa toteuttamassa. Helsinki Tietosanoma. Viitattu 22.1.2021

Kyberturvallisuuskeskus. 2016. Langattomasti, mutta turvallisesti. Viestintävirasto. Viitattu 9.1.2021. Saatavissa https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Labarre, O. 2021. Enterprise Resource Planning ERP. Investopedia. Viitattu 17.4.2021. Saatavissa <https://www.investopedia.com/terms/e/erp.asp>

Landesman, M. 2021. How to Deal With Boot Sector Viruses. Lifewire. Viitattu 15.4.2021. Saatavissa <https://www.lifewire.com/boot-sector-virus-repair-153282>

Lukka, K. 2001. Konstruktiivinen tutkimusote. Viitattu 15.4.2021. Saatavissa Metodix <https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/>

Maimon, D. 2019. Existing Evidence for the Effectiveness of Antivirus in Preventing Cyber Crime Incidents. Georgia State University. Viitattu 15.4.2021. Saatavissa https://scholarworks.gsu.edu/cgi/viewcontent.cgi?article=1000&context=ebsc_tools

Martinez, S.Daalmans, P.& Bennett, B. 2017. Mastering System Center Configuration Manager s. 1091. John Wiley & Sons, Incorporated.

Mazerik, R. 2013. Anatomy of BIOS Security. Infosec Institute. Viitattu 15.4.2021. Saatavissa <https://resources.infosecinstitute.com/topic/anatomy-of-bios-security/>

McAfee. 2021. Differences between viruses, ransomware, worms, and trojans. McAfee Knowledge Center. Viitattu 15.4.2021. Saatavissa https://service.mcafee.com/webcenter/portal/cp/home/articleview?locale=fi_FI&articleId=TS100872

Microsoft. 2021. Langattomien verkkojen turvallisempi käyttö. Viitattu 21.3.2021. Saatavissa <https://support.microsoft.com/fi-fi/office/langattomien-verkkojen-turvallisempi-k%C3%A4ytt%C3%B6-2614313a-7330-4d18-b619-0abec460fcb>

Microsoft. 2021. Miksi salasananattomuus on hyvä vaihtoehto? Viitattu 21.3.2021. Saatavissa <https://www.microsoft.com/fi-fi/security/business/identity-access-management/passwordless-authentication>

Milkovich, D. 2020. Cybint. Viitattu 15.4.2021. Saatavissa 15 Alarming Cyber Security Facts and Stats <https://www.cybintsolutions.com/cyber-security-facts-stats/>

Mogul, J. 1990. Efficient use of workstations for passive monitoring of local area networks. ACM SIGCOMM Computer Communication Review, 1–8. Viitattu 15.4.2021. Saatavissa https://www.researchgate.net/publication/234784560_Efficient_use_of_workstations_for_passive_monitoring_of_local_area_networks

Munk, D. 2019. Cloud-Based Vs. On-Premise Servers. Forbes Tech Council. Viitattu 15.4.2021. Saatavissa <https://www.forbes.com/sites/forbestechcouncil/2019/03/22/cloud-based-vs-on-premise-servers/?sh=663cd66279e2>

NIST Special Publication 800–53. 2013. SP 800-53 Rev. 4. National Institute of Standards and Technology. Viitattu 15.4.2021. Saatavissa <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02192014.pdf>

O'Donnell, C. 2019. What is a workstation computer? Velocity Micro. Viitattu 15.4.2021. Saatavissa <https://www.velocitymicro.com/blog/what-is-a-workstation-computer/>

OmniSecu. 2021. How IEEE 802.1X dot1x Port Based Authentication works. Viitattu 15.4.2021. Saatavissa <https://www.omniseclu.com/tcpip/how-ieee-802.1x-port-based-authentication-works.php>

Paukku, T. 2013. Nykytietokone tulee tiensä päähän 2020-luvulla. Helsingin Sanomat, Teknologia. Viitattu 15.4.2021. Saatavissa <https://www.hs.fi/teknologia/art-2000002644085.html>

Quick, B. 2017. How Do VLANs Work? Inteltech. Viitattu 15.4.2021. Saatavissa <https://www.inteltech.com/blog/how-do-vlans-work/>

Sore, B. 2020. What Is EDR and Why Is It Important? Heimdal Security. Viitattu 15.4.2021. Saatavissa <https://heimdalsecurity.com/blog/what-is-edr/>

Sowells, J. 2018. Understanding the Threat 8 Different Types of Malware. US Cyber Security Magazine. Viitattu 15.4.2021. Saatavissa <https://www.uscybersecurity.net/malware/>

Spiceworks. 2020. The 2020 State of Virtualization Technology. Viitattu 15.4.2021. Saatavissa <https://www.spiceworks.com/marketing/reports/state-of-virtualization/>

Stevanovic, I. 2020. Operating System Market Share. Viitattu 15.4.2021. Saatavissa Kommando Tech <https://kommandotech.com/statistics/operating-system-market-share/>

Swinhoe, D. 2019. What is a man-in-the-middle attack? How MitM attacks work and how to prevent them. Viitattu 15.4.2021. Saatavissa CSOnline <https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html>

Trendmicro. 2021. What is Ransomware? Viitattu 15.4.2021. Saatavissa <https://www.trendmicro.com/vinfo/us/security/definition/Ransomware>

Unuchek, R. 2017. IT threat evolution Q1 2017, Statistics. Securelist. Viitattu 15.4.2021. Saatavissa <https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/>

Vanover, R. 2009. When does it make sense to use a certificate authority on an internal network? Viitattu 15.4.2021. Saatavissa <https://www.techrepublic.com/blog/data-center/when-does-it-make-sense-to-use-a-certificate-authority-on-an-internal-network/>

Viestintävirasto. 2021. Salasanat haltuun, Neuvoja salasanojen käyttöön ja hallintaan. Kyberturvallisuuskeskus. Viitattu 15.4.2021. Saatavissa https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf

Walkowski, D. 2019. What Is the CIA Triad? F5 Labs. Viitattu 15.4.2021. Saatavissa <https://www.f5.com/labs/articles/education/what-is-the-cia-triad>

Ward, S. 2020. What Is the Difference Between Laptop and Notebook Computers? The Balance Small Business. Viitattu 15.4.2021. Saatavissa <https://www.thebalancesmb.com/before-you-buy-a-laptop-or-notebook-computer-2946956>

Whitney, L. 2021. How to protect your organization's remote endpoints against ransomware. TechRepublic. Viitattu 15.4.2021. Saatavissa <https://www.techrepublic.com/article/how-to-protect-your-organizations-remote-endpoints-against-ransomware/>

Yubico. 2021. FIDO2 passwordless authentication. Viitattu 15.4.2021. Saatavissa <https://www.yubico.com/authentication-standards/fido2/>