Opinnäytetyö (AMK)

Tekniikan koulutusohjelma

2018

Ossi Nyman

YRITYKSEN TIETOTURVAN KEHITTÄMINEN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tekniikan koulutusohjelma

2018 | 34

Ossi Nyman

YRITYKSEN TIETOTURVAN KEHITTÄMINEN

Opinnäytetyön tavoitteena oli kehittää erään pienyrityksen tietoturvaa. Työ aloitettiin nykytilanteen kartoituksella, jossa tietoturvan nykytila havaittiin puutteelliseksi. Havaituista puutteista päätettiin keskittyä tietoliikenne- ja laitteistoturvallisuuden kehittämiseen, sekä haittaohjelmilta suojautumiseen. Yrityksellä on kaksi liiketilaa kahdella paikkakunnalla. Tämän työn käytännön toteutukset suoritettiin vain toisessa toimipisteessä.

Yrityksen rajallisten taloudellisten resurssien vuoksi muihin tietoturvan osa-alueisiin ei oteta kantaa tässä työssä ja varsinaiset laitehankinnat rajoittuivat vain tietoturvareitittimen hankintaan.

Työn tuloksena syntyi kuitenkin myös jatkosuunnitelma tulevaisuuden varalle, kun yrityksen toiminta laajentuu ja investoinneille on osoittaa enemmän resursseja. Suunnitelmassa huomioitiin yrityksen molemmat toimipisteet.

Opinnäytetyön tuloksena yrityksen tietoturvalle rakennettiin perusta ja yritys sai tietoa tietoturvasta. Työn tuloksena yrityksen toisen toimipisteen lähiverkko on nopeampi, luotettavampi ja turvallisempi haittaohjelmia ja internetin tuomia uhkia vastaan.

ASIASANAT:

tietotekniikka, tietoturva, tietosuoja, kyberturvallisuus, turvallisuus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Technology

2018 | 34

Ossi Nyman

IMPROVING DATA SECURITY OF A SME

The aim of the thesis was to improve data security for small business. The company is a new small business that intends to expand its operations in the near future. The work was initiated by evaluating the current situation. The current state of data security was found to be inadequate and out of date. The company operates out of two separate locations. The technical works outlined in this thesis were only implemented in one of the premises.

Because of the limited financial resources of the business, other aspects of data security were not considered in this work. Hardware acquisitions were also limited to a single secure router.

This thesis also resulted in a follow-up plan for future business expansion, when more resources become available. The follow-up plan was made for both locations.

As a result of this thesis, the foundations of data security were built, and the company gained information about data security. Also, this thesis provided the company with a faster, more reliable and safer network against malware and threats brought by internet.

KEYWORDS:

information technology, data security, security, confidentiality, integrity, availability

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET TAI SANASTO

802.11	IEEE:n standardi langattomille lähiverkoille.
802.11i	IEEE:n standardi langattomien lähiverkkojen salaukselle, joka tunnetaan paremmin nimellä WPA2.
Active Directory	Microsoftin kehittämä Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu.
ADSL	Asymmetric Digital Subscriber Line. Verkkokytkintekniikka, jonka ominaispiirre on tiedonsiirron epäsymmetrisyys. Tiedonsiirron nopeus on erilainen laskevaan (Download) ja nousevaan (Upload) suuntaan.
Hyper-V	Windows Server palvelinkäyttöjärjestelmiin sisältyvä virtualisointialusta virtuaaliresurssien luontiin ja hallinnointiin.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö, joka muun muassa määrittelee keskeisiä tekniikan alan standardeja.
IPsec	IPsec on joukko tietoliikenneprotokollia, jotka todentavat ja salaavat tietoliikenteen.
L2L	Lan-to-Lan. VPN-tekniikkaan liittyvä termi, jossa kahden yksityisverkon välille luodaan internetin yli virtuaalinen erillisverkko.
Mac	Macintosh. Applen valmistama tietokone.
MAC-osoite	Media Access Control – Jokaisella verkkosovittimella on valmistajan yksilöimä uniikki osoite.
OSPF	Open Shortest Path First on reititysprotokolla TCP/IP-verkkoihin.
PSK	Pre Shared Key. Langattomien verkkojen salauksen yhteydessä tarkoitetaan ennalta jaettua salausavainta. Radiotekniikassa PSK on lyhenne sanoista Phase Shift Keying, joka tarkoittaa signaalin vaihemodulointia.
Reititin	Verkon aktiivilaite, joka reitittää tietoliikennettä eri verkkojen välillä.
SSID	Service Set IDentifier. Langattoman verkon nimi.
Valetukiasema	Rogue Access Point. Nimitys, jota käytetään valetukiasemasta, jonka avulla langattomaan lähiverkkoon pyrkivä hyökkääjä yrittää anastaa verkossa liikkuvaa tietoa. Valetukiasema mainostaa itseään samalla SSID nimellä ja yrittää saada verkon käyttäjät liikennöimään sen kautta. Tämä on

	eräs niin kutsutuista Mies välissä -hyökkäyksistä (engl. Man-In-The-Middle attack).
VPN	Virtual Private Network. Virtuaalinen erillisverkko. Virtuaalisia erillisverkkoja käytetään kahden verkon yhdistämiseksi julkisen internetin yli. VPN luo näennäisesti yksityisen verkon esimerkiksi yrityksen kahden toimipisteen välille, jotka sijaitsevat eri paikkakunnilla. Kahden reitittimen tai kahden palomuurin välinen yhteys tunneloidaan ja salataan sopivalla menetelmällä.
WEP	Ensimmäinen langattomien 802.11 verkkojen suojausmenetelmä. WEP käyttää RC4-salausalgoritmiä. WEP-salaus on erittäin helposti murrettavissa ja sitä ei enää suositella käytettäväksi. (Tech-FAQ, 2018b)
Windows Server	Microsoftin luoma palvelinkäyttöjärjestelmä.
WPA	Wi-Fi Protected Access. WiFi Alliance:n kehittämä suojausmenetelmä langattomille 802.11 verkoille. WPA kehitettiin alun perin siirtymävaiheen protokollaksi ennen WPA2 julkaisua. WPA käyttää TKIP-salausta. (Wikipedia, 2018.)
WPA2	IEEE:n standardisoima suojausmenelmä 802.11i. WPA2 myötä käyttäjän valittavana on TKIP:n lisäksi AES-salaus. (Radio-electronics, 2018.)

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena oli parantaa erään pienyrityksen tietoturvaa. Yrityksen nimi ja toimiala pidettiin salassa yrityksen toiveesta. Yrityksen liiketilojen tietoverkot oli rakennettu työntekijöiden toimesta ilman asiantuntija apua. Työasemat olivat yhtä Mac-tietokonetta lukuun ottamatta Windows-pohjaisella käyttöjärjestelmällä varustettuja. Osalla työntekijöistä oli viruksentorjuntaohjelmistona ilmainen Avast, Mac-käyttäjällä ei ollut viruksentorjuntaohjelmistoa lainkaan.

Liiketilan internetyhteys oli paikallisen operaattorin tarjoama ADSL-yhteys. Reititin-modeemina toimi Zyxelin valmistama laite. Reititin-modeemiin oli kytketty lähiverkkokaapelilla TP-Linkin valmistama langaton reititin langattoman verkkoyhteyden kantaman ja nopeuden lisäämiseksi. Kummallakin laitteella oli oma verkkonsa, josta oli pääsy internetiin, sekä yrityksen verkkoon.

Molemmat reitittimien verkot olivat salasanalla suojattuja. Alkukartoituksessa havaittiin, sekä Zyxelin, että TP-Linkin graafisten hallintasovellusten käyttäjätunnukset ja salasanat laitevalmistajan oletuksiksi. Molempien langattomien verkkojen salasanojen suojaustaso oli luokkaa kohtalainen tai heikko.

Haavoittuvuuksiksi määritettiin puutteellinen viruksentorjuntaohjelmisto, langattomien verkkojen suojaus, sekä liian heikot salasanat.

Välittöminä toimenpiteinä langattomien verkkojen suojaukset asetettiin hyväksyttävälle tasolle ja salasanat vaihdettiin asianmukaisiksi.

Kun käytössä olevat resurssit selvitettiin, toiseen toimipisteeseen päädyttiin hankkimaan F-Securen Sense reititin. Tavoitteeksi muodostui tietoturvan perusasioiden parantaminen yrityksessä ilman suurta taloudellista panostusta. Tietoturvan kaikkien osa-alueiden laajuuden vuoksi tässä työssä päätettiin keskittyä haittaohjelmilta suojautumisen lisäksi vain tietoliikenne- ja laitteistoturvallisuuden kehittämiseen.

2 TIETOTURVA KÄSITTEENÄ

Tietoturva tai tietoturvallisuus koostuu kahdeksasta osa-alueesta.

-Hallinnollisesta turvallisuudesta

-Henkilöstöturvallisuudesta

-Fyysisestä turvallisuudesta

-Tietoliikenneturvallisuudesta

-Laitteistoturvallisuudesta

-Ohjelmistoturvallisuudesta

-Tietoaineistoturvallisuudesta, sekä

-Käyttöturvallisuudesta. (Rousku, 2003.)

Tietoturva on osa organisaation toimintaa ja laatua. Tietoturvan rakentamisella pyritään varmistamaan tietoaineistojen, tietojärjestelmien ja palveluiden suojaus. Tavoitteena on luottamuksellisuuden, eheyden ja saatavuuden varmistaminen. (Pietikäinen, 2018.)

Tietoturvan kahdeksan osa-aluetta muodostavat laajan kokonaisuuden. Tässä työssä kehittämisen osa-alueet rajattiin haittaohjelmilta suojautumisen lisäksi tietoliikenne- ja laitteistoturvallisuuteen. Kaikkien osa-alueiden kehittäminen vaatii yritykseltä enemmän resursseja, joita ei ollut saatavilla tämän työn aikana.

2.1 Hallinnollinen turvallisuus

Hallinnollinen turvallisuus on organisaation johdon vastuualue. Johto määrittää organisaation tietoturvapolitiikan, jakaa vastuut ja tehtävät sekä ottaa käytännön vastuun tietoturvallisuudesta. Johdon on huolehdittava työntekijöiden tarvittavasta tietoturvakoulutuksesta, ohjeistuksesta sekä tietoturvan toteutumisen valvonnasta.

2.2 Henkilöstöturvallisuus

Henkilöstöturvallisuudella pyritään minimoimaan työntekijöistä muodostuva tietoturvariski. Riskejä voidaan vähentää tietoaineistojen ja käyttöjärjestelmien käyttöoikeuksia rajaamalla. Tarvittaessa työntekijöistä voidaan pyytää rekrytointivaiheessa turvallisuusselvitys.

2.3 Fyysinen turvallisuus

Fyysinen turvallisuus kattaa muun muassa aineistot, laitteet, henkilöt, tilat ja varastot. Riskitekijöinä ovat ihmiset, sekä luonnonilmiöt. Kulunvalvonnalla, vartioinnilla sekä tulipalojen, sähkö- ja vesivahinkojen torjuntaan tähtäävillä toimenpiteillä ja teknisillä toteutuksilla voidaan lisätä turvallisuutta. Myös tietojärjestelmien ja aineistojen varmuuskopiointi on osa fyysistä turvallisuutta.

2.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuutta pidetään internetin tuoman uhan vuoksi yhtenä merkittävimpänä tietoturvan osa-alueena. Tietoliikenneturvallisuudella pyritään estämään tietomurrot ja tietoturvaloukkaukset. Käytön- ja pääsyn valvonta, seuranta, salaus, laitteiston kokoonpano ja verkon hallinta kuuluvat tietoliikenneturvallisuuteen.

2.5 Laitteistoturvallisuus

Tietojenkäsittely- ja tietoliikennelaitteiden käytettävyys, toiminta, kokoonpano, kunnossapito ja laadunvarmistus kuuluvat laitteistoturvallisuuteen. Laitteistoturvallisuuden saavuttaminen edellyttää hyvää järjestelmien suunnittelua ja laitteistoarkkitehtuuria. Vikasietoisuutta voidaan parantaa muun muassa tietoliikenteen varayhteyksillä ja varapalvelimilla.

2.6 Ohjelmistoturvallisuus

Organisaation käytössä olevien ohjelmien ylläpitoon, päivitykseen ja laadunvarmistukseen liittyvät toimenpiteet kuuluvat ohjelmistoturvallisuuteen. Ohjelmistoturvallisuuden kannalta on hyvä, jos ohjelman lähdekoodi on saatavilla. Vaikka kaupalliset ja tunnetut ohjelmat saattavat tuntua turvallisilta niiden laajan levikin vuoksi, piilee niissä kuitenkin riski niiden piilotetun ohjelmakoodin takia.

2.7 Tietoaineistoturvallisuus

Tietoaineiston, asiakirjojen ja kaikenlaisten tiedostojen käytettävyys, eheys ja luottamuksellisuus kuuluvat tietoaineistoturvallisuuteen. Asianmukaisella hallinnalla, säilytyksellä, käsittelyllä ja hävittämisellä taataan tietoaineistoturvallisuuden toteutuminen. Tietoaineistoturvallisuus on usein julkisuudessa tietovuototapauksissa, joissa henkilötietoja varastetaan. Euroopan Unionin GDPR tietosuoja-asetus koskettaa kaikkia Euroopan Unionin jäsenmaita 25.5.2018 alkaen. Asetus koskettaa kaikkia organisaatioita ja yrityksiä, jotka käsittelevät henkilötietoja. (EUR-Lex, 2018.)

2.8 Käyttöturvallisuus

Tietotekniikan käyttö, käyttöympäristö, ATK-tuki, ylläpito, huoltotoimenpiteet ja tietojenkäsittely kuuluvat käyttöturvallisuuteen. Käyttöturvallisuutta lisää uusien järjestelmien varmistaminen testiympäristössä ennen varsinaista käyttöönottoa. Huoltotoimenpiteiden hyvällä ja järjestelmällisellä suunnittelulla taataan myös käytön jatkuvuuden varmistaminen.

2.9 Tietoturvapolitiikka

Tietoturvapolitiikan tarkoituksena on määritellä yrityksen tai organisaation periaatteet, vastuut, sekä toimintatavat tietoturvan toteuttamiseen ja kehittämiseen liittyen. Myös tietoturvan seuranta ja valvonta määritellään tietoturvapolitiikassa. Tietoturvasuunnitelma, sekä erilliset ohjeet ja määräykset täydentävät tietoturvapolitiikkaa.

Tämän opinnäytetyön kohteena olevalla yrityksellä ei ollut omaa tietoturvapolitiikkaa. Yritys noudatti kattojärjestön ohjeita ja oppaita tietoturvan osalta. Ohjeistus oli selkeä, mutta ei kovin yksityiskohtainen. Ohjeistuksessa oli kymmenen kohtaa, joissa asiat oli lueteltu lyhyesti ja selkeästi. Kattojärjestön opas käsitteli samat kymmenen asiaa laajemmin, mutta yksityiskohtaisiin teknisiin tai ohjelmallisiin seikkoihin ei oteta kantaa myöskään oppaassa. Ohjeistuksen mukaan vähintään seuraavista asioista on huolehdittava:

-Toimitilojen riittävä lukitus ja suojaus.

-Sähköisessä muodossa olevien tietojen suojaus salausjärjestelmällä.

-Langattomien verkkojen suojaus.

-Riittävän vahvat salasanat ja käyttäjätunnukset.

-Viruksentorjunnan, palomuurin ja tietokoneiden päivitykset on oltava ajan tasalla.

-Säännöllinen varmuuskopiointi.

-Ulkoisten It-palveluiden tietoturvavaatimusten täyttyminen.

-Sähköistä viestintää käytettäessä pitää olla asiakkaan hyväksyntä.

-Asiakirjojen ja muun aineiston tietoturvallinen säilytys, arkistointi, tallennus ja hävitys.

-Kaikkien tietoa sisältävien laitteiden hävitys tietoturvallisella tavalla.

3 UHAT

Tässä luvussa on käsitelty ne uhat, joille tässä opinnäytetyössä käsitelty yritys altistuu kaikkein eniten. Yrityksen työntekijöiden henkilökohtaiset kannettavat tietokoneet ovat kaikkein alttiimpia haittaohjelmille, koska ne toimivat työn lisäksi kotona henkilökohtaisessa käytössä.

Heikko salasana on uhka erityisesti yrityksen toimitilan langattomassa verkossa. Langattoman verkon kantama ulottuu myös yrityksen tilojen ulkopuolelle, jolloin mahdollinen hyökkääjä voi toimia liiketilan ulkopuolella työntekijöiden tietämättä. Vanhentuneen WPA-suojauksen käyttö uusimman WPA2 sijaan helpottaa mahdollisen hyökkääjään murtautumista verkkoon entisestään.

3.1 Työasemat ja muut päätelaitteet

Tietokone tai muu päätelaite, jossa on puutteellinen tai ei ole lainkaan viruksentorjuntaohjelmistoa on altis monenlaisille uhille. Windows-pohjaiset käyttöjärjestelmät ovat suosionsa ansiosta kaikkein alttiimpia haittaohjelmille, mutta haittaohjelmia löytyy myös muille käyttöjärjestelmille. Haittaohjelmat voivat pahimmillaan keskeyttää yrityksen toiminnan. Puhdistustoimenpiteet joudutaan leviämisvaaran vuoksi suorittamaan kaikille laitteille, joilla on pääsy kyseiseen lähiverkkoon. Tapauksesta riippuen toimenpiteet saattavat tarvita ulkopuolista asiantuntemusta, jolloin prosessiin kuluva aika kasvaa entisestään.

3.1.1 Virukset ja madot

Tietokonevirukset ja madot ovat ohjelmia, joiden tarkoitus on häiritä tietokoneen toimintaa. Virukset ja madot pyrkivät usein myös leviämään tietokoneesta toiseen. Leviäminen tapahtuu tyypillisesti sähköpostiviestien liitetiedostojen avulla ja ylipäätään sähköpostin välityksellä.

3.1.2 Troijan hevonen

Troijan hevonen tai troijalainen on haittaohjelmiin liitettynä termi, jossa haittaohjelma on piilotettu tai naamioitu esimerkiksi tiedostoja sisältävän massamuistitikun sisään. Troijalaiset pyrkivät tyypillisesti toimimaan jälkiä jättämättä. Troijalaiset voivat avata haavoittuvuuksia tai käynnistää madon tai viruksen tietokoneessa.

3.1.3 Vakoiluohjelmat ja muut kyseenalaiset ohjelmat

Vakoiluohjelmat asentuvat kohdekäyttäjän tietokoneelle tyypillisesti huomaamatta. Ne eivät tee välttämättä tietokoneen suorituskykyyn vaikuttavaa haittaa, mutta niiden tarkoitus on kerätä henkilötietoja, selaushistoriaa ja muuta tietoja erityisesti kohdennettua mainontaa varten.

Tyypillinen esimerkki epäilyttävästä kyseenalaisesta ohjelmasta on internet sivustoilla ponnahdusikkunoina ilmestyvä kehotus käynnistää sivuston tarjoama ilmainen viruksentarkistusohjelma. Käyttäjä voi tietämättään antaa ohjelmalle luvan muuttaa käyttöjärjestelmän asetuksia ja määrityksiä, jotka johtavat moniin ongelmiin. (Microsoft, 2018.)

Selkeästi tietokoneen suorituskykyä haittaavia ohjelmia on muun muassa kryptovaluutta bitcoinin louhintaan liittyvät ohjelmat. Ne käynnistyvät käyttäjän huomaamatta, kun vieraillaan saastuneella internetsivustolla. Myös Android-käyttöjärjestelmällä varustetut matkapuhelimet ovat alttiita louhintaohjelmille. (Meshkov, 2018.)

3.1.4 Ilmaiset viruksentorjuntaohjelmistot

Parhaimmillaan ilmaiset viruksentorjuntaohjelmistot havaitsevat haittaohjelmat yhtä tehokkaasti kuin maksulliset vaihtoehdot. Tyypillisesti ilmaisversiot eivät kuitenkaan tuo turvaa kaikille uhille, vaan käyttäjän on maksettava saadakseen tuotteen kaikki suojausominaisuudet käyttöön. Tuotteesta riippuen maksulliset ohjelmistot sisältävät haittaohjelmien torjunnan lisäksi muitakin tärkeitä ominaisuuksia, kuten palomuurin, roskapostisuodatuksen, verkkopankkisuojan ja tärkeimpänä tuotetuen. On myös erittäin oleellista, kuinka usein virustunnisteet päivitetään ohjelmistossa. Useimmat ilmaiset ohjelmistot päivittyvät automaattisesti vain kerran vuorokaudessa. (Vänninen, 2013.)

3.2 Salasanat

Salasanasuositukset päivittyvät vuosittain. Tällä hetkellä termiä salasana voidaankin pitää vanhentuneena ja uusin termi voisi yhtä hyvin olla salalause. Toisin sanoen, salasanaa miettiessä pitäisi panostaa erityisesti merkkien lukumäärään. Viestintäviraston Kyberturvallisuuskeskus pitää hyvänä lähtökohtana 15 merkin mittaista salasanaa. Ilman vaikeasti muistettavia erikoismerkkejäkin pystyy luomaan vahvan salasanan esimerkiksi keksimällä jokin pitkä epälooginen lause. Ä ja Ö-kirjainten käyttö lisää suojaa niiden harvinaisuuden vuoksi, joten niitä kannattaa suosia.

Saman salasanan käyttöä eri palveluissa tulisi aina välttää mahdollisten sanakirjahyökkäysten varalta. Pahin tilanne on esimerkiksi tietomurron kohteeksi joutunut sosiaalisen median palvelu, jossa käyttäjien salasanoja varastetaan. Joukosta löytyy aina salasanoja, jotka ovat samoja kyseisen henkilön muissa salasanaa vaativissa paikoissa.

Salasanoja eri palveluihin on tyypillisesti kymmeniä. Kun kaikissa palveluissa olisi oltava eri salasana, tulee niiden kaikkien ulkoa muistamisesta hankalaa. Tällöin olisikin hyvä ottaa käyttöön salasanojen hallintaan ja säilöntään suunniteltu apuohjelma, kuten esimerkiksi Keepass, F-Secure Key tai Password Safe. (Viestintävirasto, 2018a.)

3.3 Langattomat verkot

Tietoturvatutkijat löysivät haavoittuvuuden WPA2:sta lokakuussa 2017. Haavoittuvuutta on mahdollisuus hyödyntää niin kutsutulla man-in-the-middle -hyökkäyksellä. Hyökkäys kohdistuu protokollan kättelyn toteutukseen ja siihen ei ole varsinaista korjausta. Ongelmaa voidaan lievittää rajoittamalla langatonta verkkoliikennettä. Hyökkääjän on oltava langattoman verkon kantaman sisällä ja hyökkääjän on saatava langaton liikenne kulkemaan niin kutsutun valetukiaseman kautta. Hyökkääjä näkee tällä metodilla vain kaiken suojaamattoman liikenteen langattomassa verkossa. WPA/WPA2-protokollat ovat haavoittuvia, mikäli verkossa käytetään TKIP tai AES-GCMP salaustekniikoita. AES-CCMP salaustekniikka, sekä verkkoliikenteen ylemmillä protokollakerroksilla toimivat salausmenetelmät rajoittavat haittaa. Muita yleisesti tiedossa olevia keinoja ovat verkkokaapelin käyttäminen langattoman tukiaseman sijaan, sekä laitteiden pitäminen ajan tasalla päivitysten suhteen. (Viestintävirasto, 2018b.)

WiFi Alliance julkaisi CES 2018 messuilla julkaisevansa uuden WPA3 salauksen vuoden 2018 aikana. WPA3 mahdollistaa laitekohtaisen suojauksen, sekä henkilökohtaisen salausavaimen luomisen verkossa. WPA3:ssa on myös suoja niin kutsuttuja Brute Force -hyökkäyksiä vastaan. WPA3:n käyttöönotto vaatii yhteensopivan reitittimen, sekä tuen päätelaitteisiin. (Wi-Fi Alliance, 2018.)

Yrityksen langattomissa verkoissa oli käytössä jo vanhentunut WPA-suojaus. Kun ottaa huomioon, että jopa WPA2 on jo osittain murrettu, WPA-suojausta ei voi suositella käytettäväksi.

3.4 Kyberrikollisuus

Kyberrikollisuus jaetaan yleisesti tietotekniikkarikoksiin ja tietokoneavusteisiin rikoksiin. Yritykset ovat alttiita tyypillisesti tietotekniikkarikoksille.

Yleisimpiä tietotekniikkarikoksia ovat tietomurrot ja tietoliikenteen häirintään liittyvät rikokset. Tietomurron motiivina on yleensä teollisuusvakoilu, taloudellisen hyödyn tavoittelu tai erilaisten tietojen anastus rikollisten päämäärien tavoitteluun. Tyypillinen esimerkki tietoliikenteen häirinnästä on palvelunestohyökkäys. (Viestintävirasto, 2018c.)

3.4.1 Sosiaalinen hakkerointi

Yritykset ovat alttiita myös sosiaaliselle hakkeroinnille, joka on yleistynyt teollisuusvakoilun välineenä. Sosiaalinen hakkerointi on käsitteenä laaja. Tyypillisin esimerkki on yrityksen työntekijän harhautus tai taivuttelu luovuttamaan tietoja ulkopuoliselle taholle, jonka tavoite on päästä sisälle yrityksen järjestelmiin tai tietoihin. Urkintaa voi tapahtua puhelimitse tai sähköpostin välityksellä. Urkkija voi esiintyä esimerkiksi yrityksen työntekijänä, joka on kadottanut salasanansa.

Pienyrityksissä henkilöstön vähäinen lukumäärä toimii hyvin ehkäisevänä seikkana. Suuryrityksissä kaikki työntekijät eivät välttämättä tunne esimerkiksi it-tukihenkilöitä henkilökohtaisesti, jolloin kohdehenkilön harhauttaminen on helpompaa.

Tässä opinnäytetyössä käsitelty yritys on liiketoimintansa vuoksi altis sosiaaliselle hakkeroinnille. Uhkaa on lievitetty tietoisuuden lisäämisellä, sekä keskitetyillä verkon ja käyttöoikeuksien ylläpitotoiminnoilla.

4 GDPR

GDPR eli General Data Protection Regulation on Euroopan Unionin tietosuoja-asetukseen liittyvä termi. 25.5.2018 kaikissa Euroopan Unionin jäsenvaltioissa voimaan astuva uusi asetus yhtenäistää ja korvaa eri maiden väliset käytännöt henkilötietojen käsittelyyn liittyen. Asetus määrittelee, miten henkilötietoja käsitellään Euroopan Unionissa.

4.1 Tärkeimmät muutokset edelliseen lainsäädäntöön

Yritysten ja organisaatioiden, jotka käsittelevät henkilötietoja, on nimettävä tietosuojavastaava. Tietosuojavastaava toimii yhteistyössä valvontaviranomaisten kanssa ja varmistaa, että yritys tai organisaatio noudattaa asetusta.

Asetuksessa ei määritellä mikä luetaan henkilötiedoksi ja mikä ei, vaan henkilötiedot kuvataan kaikeksi tiedoksi joka yksilöi henkilön. Nämä tiedot ovat esimerkiksi nimen ja kotiosoitteen lisäksi ip- ja MAC-osoitteet, luottokortti- ja puhelinnumerot. Tallennustapaan ei oteta kantaa. Sekä sähköisessä muodossa, että fyysisessä muodossa oleva tieto kuuluu asetuksen piiriin.

Henkilötietojen keräämiseen on pyydettävä erikseen lupa, ellei kyse ole lakisääteisestä velvoitteesta. Lupa on tarvittaessa kyettävä todistamaan. Oikeus tietojen keräämiseen on oltava mahdollisuus peruuttaa.

Tietoturvaloukkauksista on ilmoitettava viipymättä 72 tunnin kuluessa. Mikäli ilmoitus viivästyy yli 72 tuntia, on annettava perusteltu selitys valvontaviranomaiselle.

Henkilötietorekisteriä pitävän on pyynnöstä annettava henkilöstä kerätyt tiedot selkeässä ja jäsennellyssä muodossa. Tiedot on pyynnöstä siirrettävä rekisterinpitäjältä toiselle esteettömästi. Henkilöstä kerätyt väärät tiedot on kyettävä oikaisemaan ilman aiheetonta viivytystä.

Henkilötiedot on kyettävä pyynnöstä tuhoamaan ilman aiheetonta viivytystä, mikäli suostumus henkilötietojen keräämiseen perutaan. Tekniset valmiudet on oltava sellaiset, että voidaan varmistua siitä ettei mitään tietoja jää lokitiedostoihin, varmuuskopioihin tai tulosteisiin. (EUR-Lex, 2018.)

4.2 Haasteet ja uhat

Tässä opinnäytetyössä käsitelty yritys käsittelee henkilötietoja. Haasteena on ennen asetuksen voimaantuloa kerätyt tiedot. Mikäli lupaa tietojen keräämiseen ei ole kysytty, on kyseiset tiedot poistettava. Yrityksessä ei ole erikseen it-tukihenkilöä tai tietosuojavastaavaa, joten tietosuojavastaava on valittava. Tietosuojavastaavan on huolehdittava, että hän omaa tarvittavat tiedot ja taidot prosessin hallintaan, sekä tarvittaessa yhteistyöhön valvontaviranomaisten kanssa. Asetuksen toimeenpano vaatii taloudellisia resursseja.

Selkeänä uhkana voidaan pitää liiketoiminnan jatkumista tietomurron sattuessa. Ulkopuolisten käsiin joutuneiden henkilötietojen arvoa on vaikea määritellä rahallisesti. Asetuksessa on kuitenkin mainittu sakko, joka määrätään yrityksille, jotka eivät noudata direktiiviä. Sakko on yrityksille 4% maailmanlaajuisesta kokonaisliikevaihdosta, joten summa on merkittävä. Taloudellisten tappioiden lisäksi yrityksen julkisuuskuva kärsii, mikäli direktiiviä ei noudateta. Vaikka yritys välttäisi sakot tietomurron sattuessa, voi maineen menetys pahimmassa tapauksessa uhata yrityksen tulevaisuutta. (Findwise, 2018.)

5 NYKYTILANTEEN KARTOITUS

5.1 Työasemat ja muut päätelaitteet

Toimipisteessä oli kartoitushetkellä yksi Mac-tietokone, muut Windows-pohjaisella käyttöjärjestelmällä. Käyttöjärjestelmäpäivitykset olivat ajan tasalla ja ne olivat asetettu asentumaan automaattisesti.

Työntekijöillä oli sekä Applen valmistamia matkapuhelimia, että Android-käyttöjärjestelmällä varustettuja matkapuhelimia, jotka oli kytketty yrityksen langattomaan verkkoon. Työntekijät käyttivät yrityksen langatonta verkkoa matkapuhelimilla internetyhteyden vuoksi.

5.1.1 Viruksentorjuntaohjelmistot

Mac-tietokoneessa ei ollut viruksentorjuntaohjelmistoa lainkaan, Windows-tietokoneissa oli ilmainen Avast Antivirus. Windows-tietokoneiden virustietokannat olivat ajan tasalla ja Avast päivitti tietokannan noin kerran päivässä.

Avastin ilmaisversiossa oli suoja vain viruksia ja vakoiluohjelmia vastaan.

5.2 Langattomat verkot

Liiketilassa oli kaksi erillistä verkkoa, joista kummastakin oli pääsy sekä yrityksen verkkoon, että internetiin. Kumpaankin verkkoon oli lisäksi mahdollisuus liittyä sekä 2.4Ghz, että 5Ghz taajuuskaistaa käyttäen. Salausmuotoina kummassakin langattomassa verkossa oli WPA-PSK.

5.2.1 Langattoman verkon salasanat

Verkon kaikki salasanat koostuivat pelkästään numeroista ja ne olivat kahdeksan merkin mittaisia.

5.3 Verkon aktiivilaitteet

ADSL-modeemina toimi Zyxel VMG3926-B10A, joka jakoi verkkoa myös langattomasti ja toimi verkon DHCP-palvelimena. Toisena langattomana reitittimenä toimi TP-Link Archer C1200.

Zyxelin, sekä TP-linkin asetuksia tarkasteltaessa huomattiin verkon kaistanleveydeksi 20Mhz 2.4Ghz verkoille ja 40Mhz 5Ghz verkoille.

6 TOIMENPITEET

6.1 Haavoittuvuuksien poistaminen

Välittöminä toimenpiteinä suoritettiin langattomien verkkojen suojauksen parantaminen, sekä viruksentorjunnan parantaminen. Langattomien verkkojen salasanat muutettiin monimutkaisemmiksi ja merkkimäärältään pidemmiksi. Langattomien verkkojen suojausversioksi muutettiin WPA-PSK sijaan uudempi WPA2-PSK, sekä salausmuodoksi TKIP sijaan AES. Radioiden lähetystehot pidettiin nykyisellä tasolla, mutta mahdollisuudet niiden pienentämiseksi tarkastettiin. Lähetystehoja pienentämällä kaikki työasemat eivät enää kyenneet yhdistämään verkkoon, joten lähetystehoja ei lopulta pienennetty.

Kaikki toimipisteen työasemat olivat 802.11n/ac yhteensopivia, jolloin langattomien verkojen taajuuksien kaistanleveydet voitiin nostaa 2.4Ghz osalta 40Mhz ja 5Ghz osalta 80Mhz. Tällä muutoksella langattomien verkkojen nopeus teoriassa tuplaantui.

6.1.1 F-Secure Sense-reititin

Toimipisteeseen oli hankittu aikoinaan toinen langaton reititin laajentamaan verkkoa, jotta kaikilta työasemilta oli pääsy riittävän nopeaan langattomaan verkkoon. Alkutoimenpiteiden jälkeen ei kuitenkaan pidetty enää tarpeellisena käyttää kahta langatonta verkkoa. Harkinnan jälkeen päädyttiin hankkimaan kustannustehokas F-Securen Sense reititin, joka korvasi molemmat langattomat verkot. Zyxelin langaton verkko kytkettiin pois päältä ja Sense-reititin toimi jatkossa ainoana langattomana yhdyskäytävänä toimipisteen verkkoon. Myös kaikki ethernet laitteet kytkettiin Sense-reitittimeen, jotta kaikki tuleva ja lähtevä liikenne kulkevat Sensen kautta. Sense reitittimessä ei ollut sisäänrakennettua DHCP-palvelinta, eikä internetmodeemia, joten Zyxel oli jätettävä jakamaan verkon osoitteita ja yhdyskäytäväksi internetiin. Zyxelissä on lisäksi palomuuri ja suojaus palvelunestohyökkäyksiä vastaan, jotka jätettiin luonnollisesti päälle tuomaan lisäturvaa.

F-Securen Sense on pääasiassa kuluttajille suunnattu kodin tietoturvareititin, mutta toimiva ratkaisu myös pienyritysten tarpeisiin. Sensen käyttöönotto on tehty kuluttajaystävälliseksi ja se ei vaadi varsinaista alaan perehtyneisyyttä.

Sensen turvaominaisuuksien keskeisin osa on F-Securen suojauspilviratkaisu, jossa Sense-reititin tutkii aktiivisesti verkkoon liitettyjä laitteita ja verkossa liikkuvia tiedostoja. Reitittimen hankintaan sisältyi myös Sense-sovellus, joka asennettiin kaikkiin toimipisteen työasemiin ja työntekijöiden matkapuhelimiin. Ratkaisu on kustannustehokas ja kevyt, jolla saatiin katettua sekä toimipisteen verkko, työasemat ja työntekijöiden omat päätelaitteet. Ratkaisu sisältää perinteisen viruksentorjunnan lisäksi tulevaisuuden kannalta oleellisen Iot-laitteiden suojauksen, selainsuojauksen, seurannan eston ja automaattiset päivitykset reitittimeen. Sense toimii täysin itsenäisesti ja haittaohjelmien tietokantapäivitykset ja itse laitteen päivitykset tapahtuvat automaattisesti F-Securen pilviratkaisun kautta.

Sense-reititin osoittautui tarjousten jälkeen kustannustehokkaimmaksi ratkaisuksi lähiverkon turvallisuuden ja haittaohjelmilta suojautumisen parantamiseen pienellä budjetilla. Sensen hinta yrityksille oli 159€, joka sisälsi myös yhden vuoden turvan haittaohjelmilta suojautumiseen yrityksen kaikkiin päätelaitteisiin. Sense sovellus asennettiin kaikkiin työasemiin ja työntekijöiden matkapuhelimiin. Kilpailijan tuote, WatchGuard AP120, yhden vuoden lisenssillä olisi kustantanut 392€ ja tällöin päätelaitteisiin olisi pitänyt hankkia erikseen asianmukainen turva haittaohjelmia vastaan. F-Securen yrityskäyttöön myytävät viruksentorjuntaohjelmistot olisi tullut kustantamaan 46,20€ per työasema ja matkapuhelimiin 30,45€ per laite. (F-Secure, 2018.)

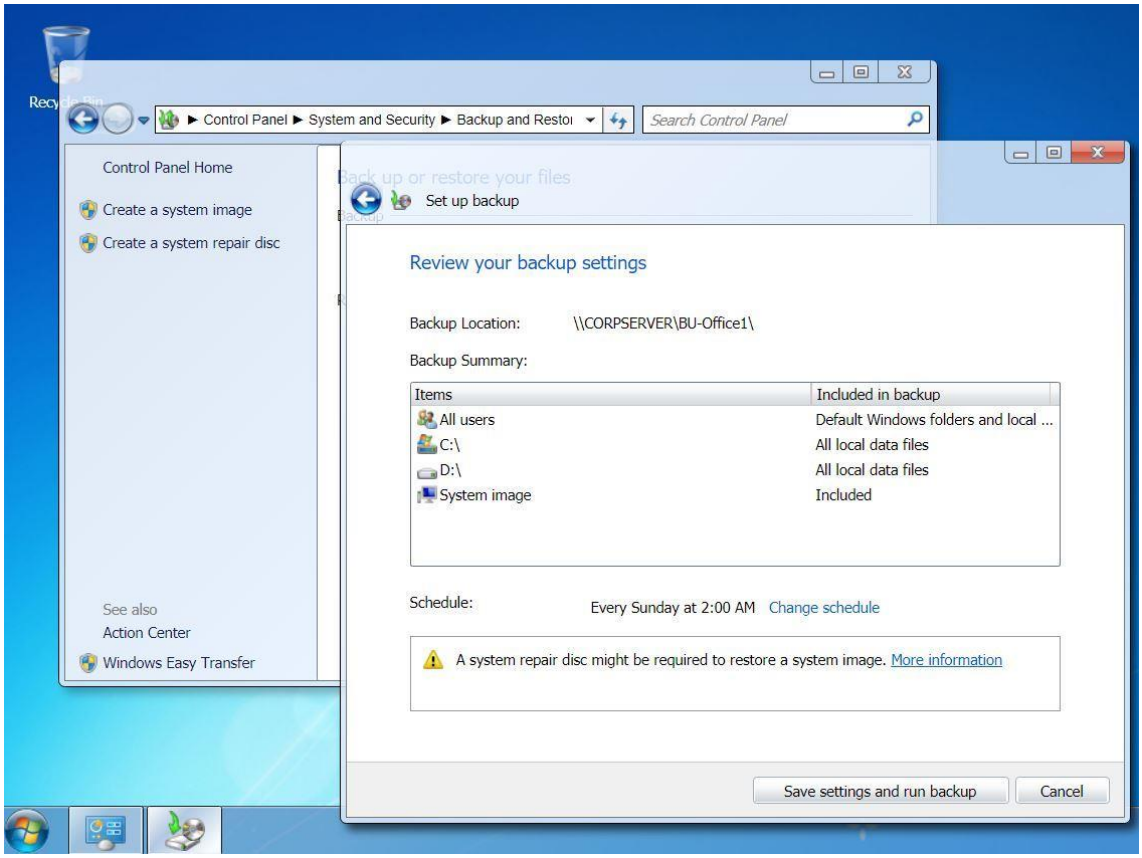
7 TULEVAISUUDEN SUUNNITELMA

7.1 Windows Server

Yrityksen laajentuessa, Windows Server ympäristö toisi mahdollisuuden muun muassa keskitettyyn käyttäjätilien, käyttöoikeuksien, palvelimien, varmuuskopioiden ja päivitysten hallintaan. Windows Serverin Hyper-V virtuaalikoneympäristöllä voidaan korvata nykyinen yrityksen käytössä oleva verkkolevy ja poistaa työasemat nykyisestä roolistaan. Tavoitetila olisi, että työasemat olisivat vain päätelaitteita, jolloin työaseman rikkoutuessa tai anastettaessa työasema voitaisiin korvata uudella ilman, että tietoja menetetään. Tämänkaltainen ympäristö loisi jo itsessään tietoturvaa yrityksen tietojärjestelmiin.

7.1.1 Automatisoidut varmuuskopiot

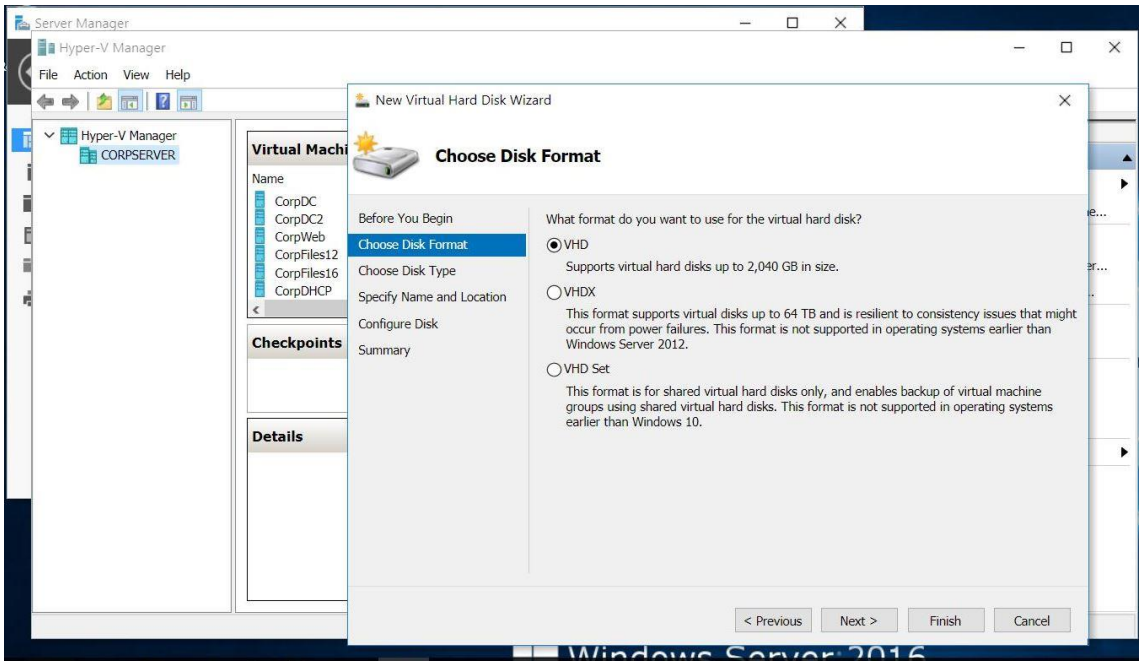
Hyper-V ympäristöön voidaan luoda virtuaalinen kone, joka toimii levynkuvien ja käyttäjien omien tiedostojen varmuuskopio sijaintina.



Kuva 1. Työaseman varmuuskopiointi verkkosijaintiin Windows XP -käyttöjärjestelmällä (TestOut simulaattori, 2018).

7.1.2 Tallennustila

Windows Serverin Hyper-V ympäristö mahdollistaa virtuaalisten kiintolevyjen luonnin. Levyn kokoa voidaan kasvattaa tarpeen mukaan ja sen fyysinen tallennusmedia voidaan varmuuskopioida kuten työasematkin.

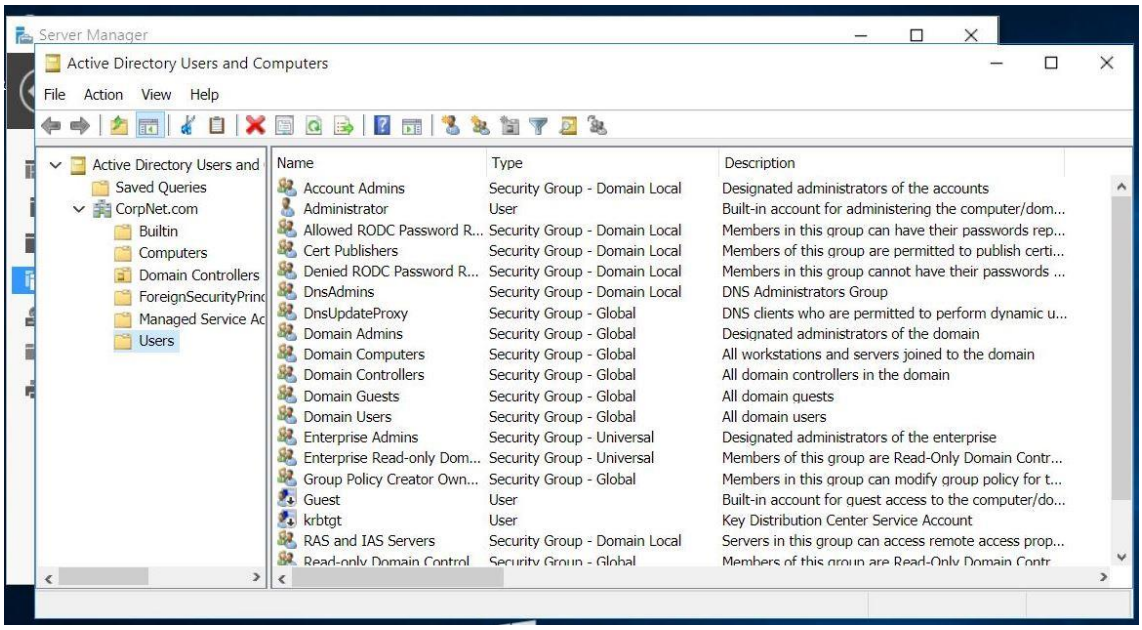


Kuva 2. Virtuaalikiintolevyn luominen Hyper-V ympäristössä Windows Server 2016:lla (TestOut simulaattori, 2018)

7.2 Active Directory

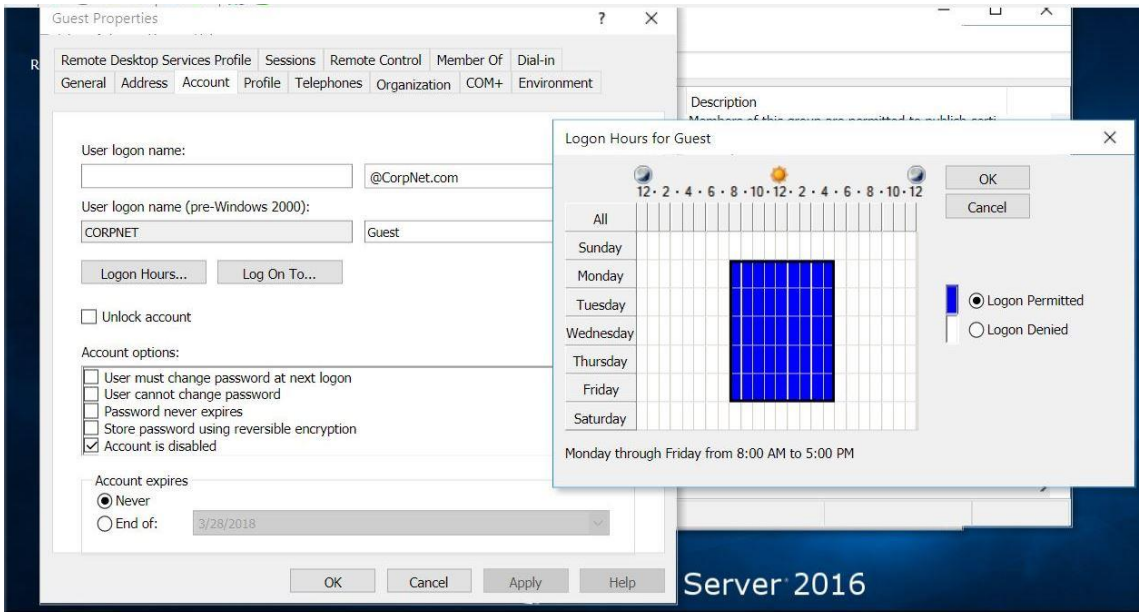
Active Directorylla hallitaan verkon resursseja ja se sisältää käyttäjätietokannan, sekä hakemistopalvelun. Active Directory on sisällytetty Windows Server -käyttöjärjestelmiin.

7.2.1 Käyttäjien ja tietokoneiden hallinta



Kuva 3. Käyttäjien ja tietokoneiden luonti Active Directoryn tietokantaan Windows Server 2016:lla (TestOut simulaattori, 2018).

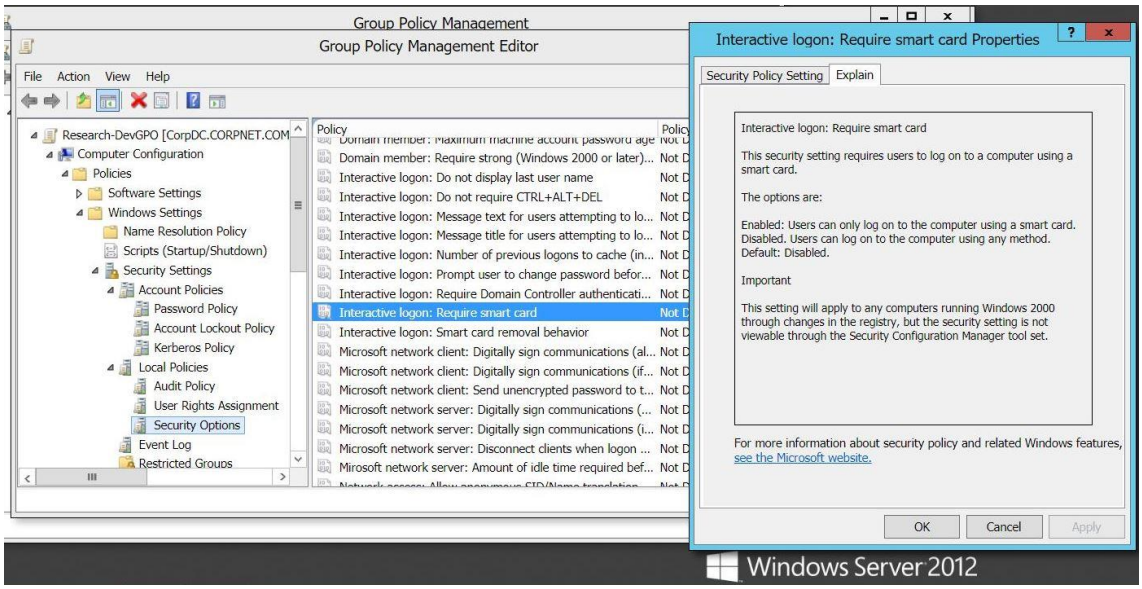
Active Directory mahdollistaa käyttäjätunnusten ja tietokoneiden keskitetyn luomisen ja hallinnoinnin. Ylläpitäjä voi asettaa rajoituksia muun muassa käyttöoikeuksiin ja kirjautumisaikoihin. Käyttörajoitukset voidaan asettaa käyttäjätunnukseen, ryhmään tai tietokoneobjektiin.



Kuva 4. Käyttäjän kirjautumisoikeuksien muuttaminen Active Directoryssä Windows Server 2016:lla (TestOut simulaattori, 2018).

7.2.2 Autentikointi toimikortilla

Mikäli yritys kokee salasanojen käytön liian turvattomaksi, voidaan Active Directoryn Group Policy Management -työkalulla ottaa toimikorttikirjautuminen käyttöön työasemissa.



Kuva 5. Toimikorttikirjautumisen käyttöönotto Active Directoryn Group Policy Management -työkalulla Windows Server 2012:lla (TestOut simulaattori, 2018).

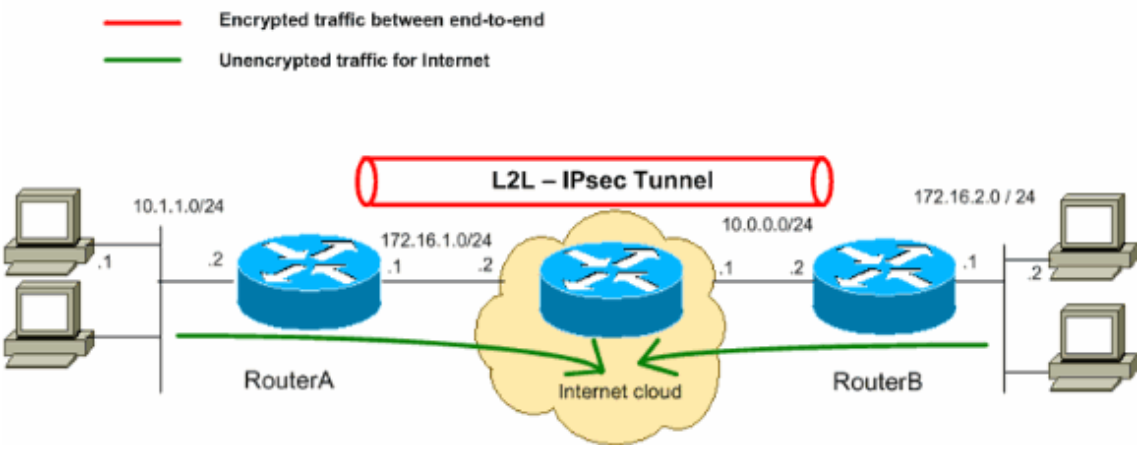
Toimikorttia pidetään luotettavampana tunnistautumismenetelmänä kuin käyttäjätunnuksen ja salasanan yhdistelmää. Jotta salasana on riittävän vahva, sen on oltava melko pitkä ja monimutkainen. Tällöin salasanan ulkoa muistaminen hankaloituu ja käyttäjät usein kirjoittavat salasanan muistiin paperille, jolloin myös salasanan joutuminen ulkopuolisten käsiin lisääntyy merkittävästi. (Koivunen, 2018.)

7.3 VPN

Yrityksellä on tarve yhdistää tulevaisuudessa kahden eri paikkakunnalla sijaitsevan toimipisteen yksityiset verkot. Turvallinen yhteys voidaan rakentaa tunneloimalla yhteys esimerkiksi kahden reitittimen tai kahden palomuurin välille, jotka toimivat VPN-

yhdyskäytävinä. VPN:n muodostustapoja on monia, mutta yrityksen käyttötarkoitukseen sopisi L2L IPSec, jossa kaksi lähiverkkoa yhdistetään salaamalla liikenne IPSec-protokollalla. Tässä tunnelointimallissa vain liikenne, joka kulkee sisäverkkojen välillä, reitite-tään VPN-tunneliin. Kun kahden verkon väliseen reititykseen käytetään lisäksi OSPF-protokollaa salatulla autentikoinnilla, saadaan lisää tietoturvaa.

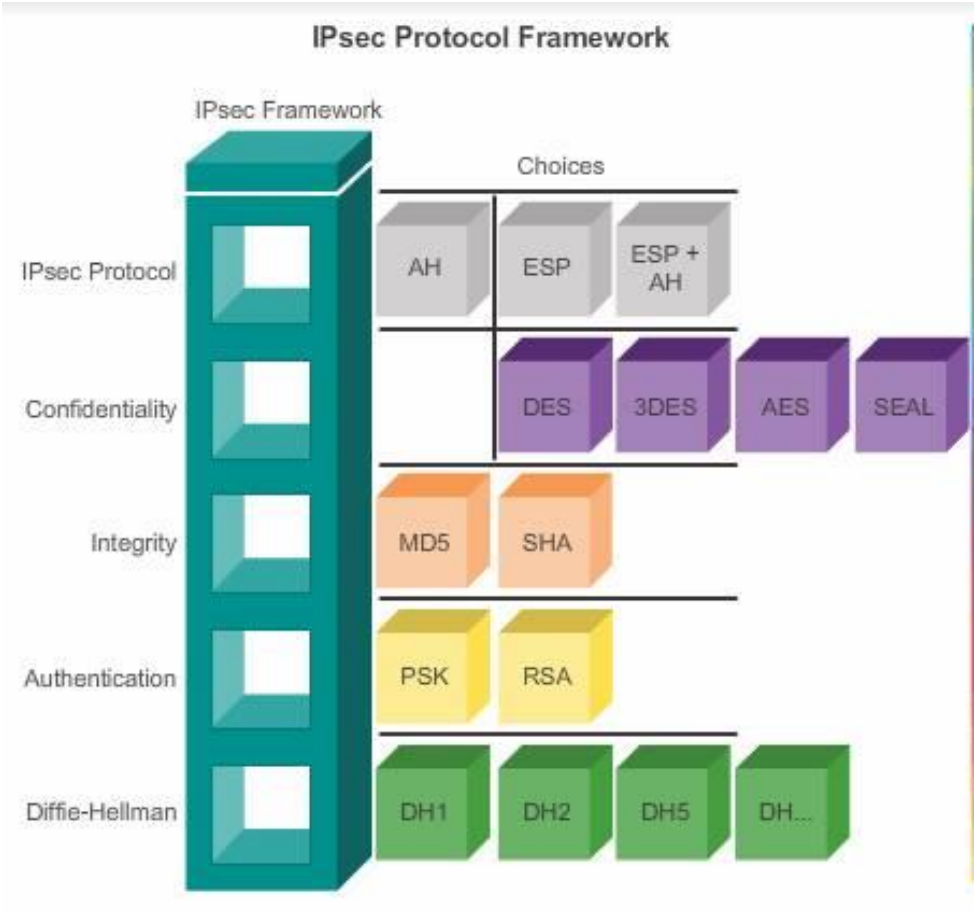
Pyysimme tätä työtä varten tarjouksen valmiista ratkaisusta. Halvin tarjous oli kumpaan-kin toimipisteeseen WatchGuard Firebox T10-D reititin-palomuurit yhden vuoden tieto-turvapaketilla, joka kustantaisi yritykselle 578€/kpl.



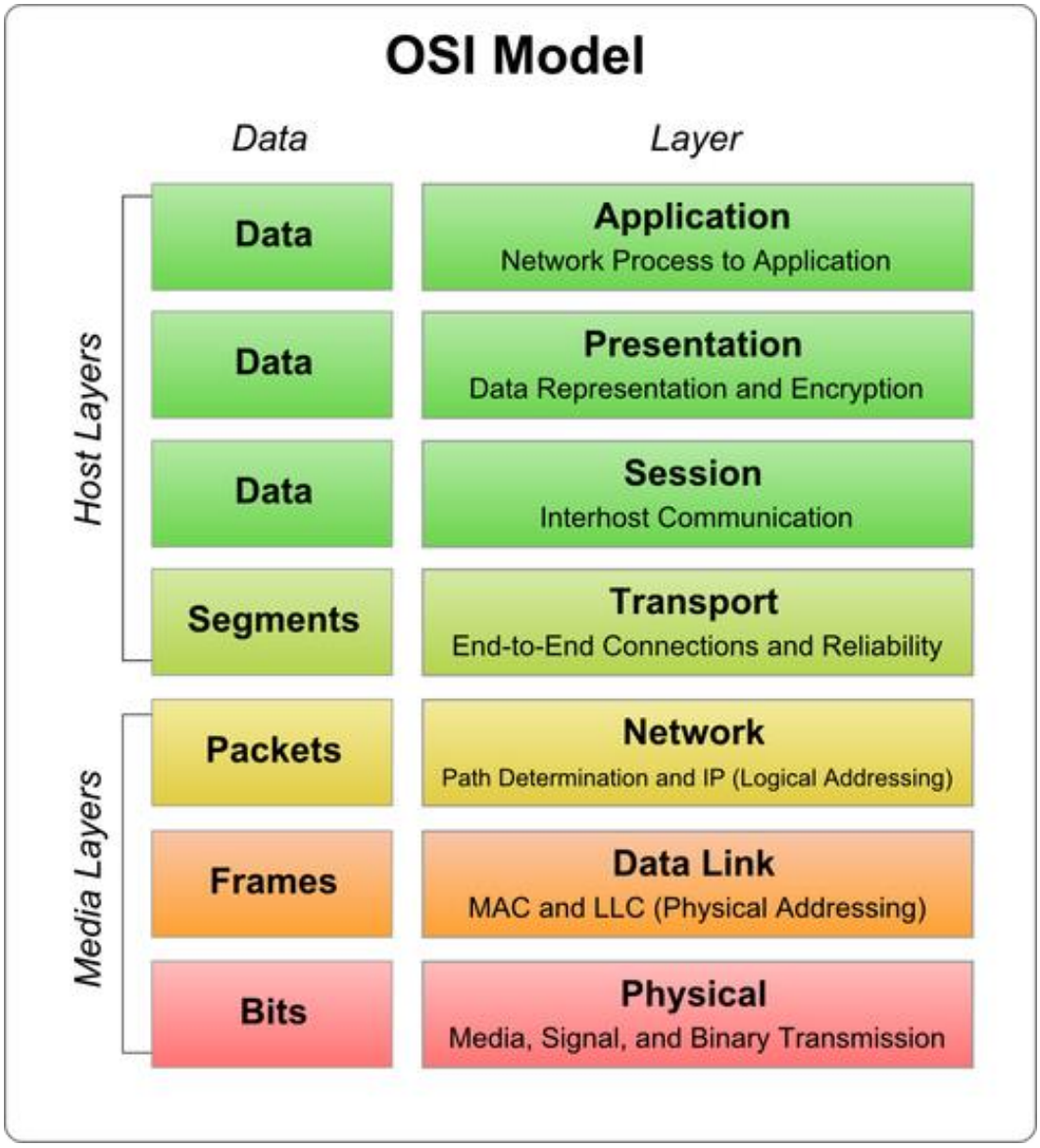
Kuva 6. VPN-tunnelointi kahden toimipisteen välillä julkisen internetin yli (Cisco Systems, 2018a).

7.3.1 IPsec

IPsec toimii OSI-mallin kolmannella kerroksella, joten ylemmän tason protokollat eivät tarvitse toimiakseen erillistä tukea.



Kuva 7. IPsec protokollan rakennekuva (Cisco Systems, 2018b).



Kuva 8. OSI-malli (Tech-FAQ, 2018c).

7.3.2 OSPF

Open Shortest Path First -protokolla käyttää Dijkstra nimistä algoritmiä parhaimman reitin löytämiseen. OSPF reititysprotokollaa käytetään yleensä suurissa monen reitittimen verkoissa verkon käytettävyyden ja viansiedon parantamiseksi, mutta koska OSPF mahdollistaa myös salatun autentikoinnin reitittimien välillä, voidaan sillä tuoda lisää turvaa pienempäänkin verkkoon. Käytännössä MD5 autentikoinnin käyttäminen vaikeuttaa huomattavasti hyökkääjän mahdollisuutta valereitittimen käytölle.

7.3.3 Etäkäyttö

Mikäli yritys hankkisi toimipisteisiin esimerkiksi WatchGuard Firebox T10-D reititin-palomuurit, toimisi WatchGuard VPN-yhdyskäytävänä. Turvallinen etätyö voidaan toteuttaa asentamalla työasemaan VPN-client sovellus, jolla muodostetaan yhteys VPN-yhdyskäytävään internetin yli.

7.4 MAC-suodatus

MAC eli Media Access Control on langattoman tai Ethernet-verkkosovittimen yksilöivä osoitekoodi. MAC-suodatuksella voidaan lisätä tietoturvaa, mikäli se tehdään ethernet verkoissa. MAC-suodatuksella reititin tai kytkin sallii liikennöinnin vain erikseen sallituille MAC-osoitteille. Esimerkiksi Ciscon valmistamilla Catalyst-sarjan kytkimillä saadaan tehokas turva, kun MAC-suodatuksen yhteydessä käytetään niin kutsuttua Port Security ominaisuutta. Tällöin suodatus toimii porttikohtaisesti ja suojatoiminto voidaan asettaa toimimaan siten, että kyseinen portti menee ’shutdown’ -tilaan, mikäli siihen liitetään jokin muu kuin sallitun MAC-osoitteen omaava laite. MAC-osoitteet voidaan lisätä staattisesti käsin tai voidaan käyttää dynaamista toimintoa, jossa vain erikseen asetetun MAC-osoitelistan liikenne sallitaan. Lisäksi portin toimintaa voidaan muuttaa, kun siihen liitetään ei-sallittu MAC-laite. Portti voidaan sulkea tai se voidaan asettaa tilaan, jossa se alkaa ylläpitämään lokia portin läpi menevästä liikenteestä.

MAC-suodatusta ei kuitenkaan pidetä hyvänä turvatoimintona langattomissa verkoissa. Verkkoanalysaattorit, kuten Wireshark, mahdollistavat sallittujen MAC-osoitteiden urkinnan langattoman verkon liikenteestä, jolloin suodatuksesta ei ole hyötyä.

8 LOPUKSI

Työn lopputuloksena yritykselle luotiin perusta tietoturvalle tietoliikenne- ja laitteistoturvallisuuden osalta, sekä päätelaitteet suojattiin tehokkaammin haittaohjelmilta. Taloudellisten resurssien ollessa rajalliset, laite- ja ohjelmistohankinnat rajoittuivat toistaiseksi F-Securen Sense-reitittimen hankintaan. Työn tuloksena yritys sai kuitenkin paljon tietoa tietoturvasta ja alustavan suunnitelman yrityksen tietoverkkojen ja tietoliikenteen parantamiseen, kun taloudelliset resurssit mahdollistavat hankinnat.

Seuraava askel yrityksen tietoturvan kehittämisessä on ehdottomasti uuden Euroopan Unionin tietosuoja-asetuksen läpivienti yrityksessä. Asetuksen tuomat oikeudet ja velvollisuudet ovat merkittäviä niin kuluttajille, kuin yrityksille. Asetuksesta tekee merkittävän myös se, että vaihtoehtoa ei ole. Kaikkien henkilötietoja käsittelevien yritysten on pakko tehdä tarvittavat toimet. Toivottavasti viimeistään tämä herättää yritykset kehittämään tietoturvan muitakin osa-alueita nyt ja tulevaisuudessa.

LÄHTEET

Cisco Systems, 2018a. L2L IPsec tunnel. Viitattu 18.5.2018. https://www.cisco.com/c/dam/en/us/support/docs/routers/1700-series-modular-access-routers/71462-rtr-l2l-ipsec-split-00.gif

Cisco Systems, 2018b. IPsec protocol Framework. Viitattu 18.5.2018. https://frankfu.click/wp-content/uploads/2016/02/IPSeC_Protocol_framework2.jpg

EUR-Lex, 2018. EUR-Lex tietokanta. Viitattu 18.5.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN

Findwise, 2018. Mitä jokaisen kuuluu tietää EU:n uudesta tietosuoja-asetuksesta GDPR? Viitattu 18.5.2018. https://findwise.com/en/gdpr-fi

F-Secure, 2018. F-Secure Sense. Viitattu 18.5.2018. https://www.f-secure.com/fi_FI/web/home_fi/sense/technology

Koivunen, E. 2018. Tunnistautuminen. Viitattu 18.5.2018. https://www.vahtiohje.fi/web/guest/tunnistautuminen

Meshkov, A. 2018. Cryptocurrency mining affects over 500 million people. Viitattu 18.5.2018. https://adguard.com/en/blog/crypto-mining-fever/

Microsoft, 2018. Virusten ja muiden haittaohjelmien estäminen ja poistaminen. Viitattu 18.5.2018. https://support.microsoft.com/fi-fi/help/129972/how-to-prevent-and-remove-viruses-and-other-malware

Pietikäinen, S. 2018. Tietoturvallisuus. Viitattu 18.5.2018. https://www.vahtiohje.fi/web/guest/691

Radio-electronics, 2018. IEEE 802.11i Wi-Fi Security: WEP & WPA / WPA2. Viitattu 18.5.2018. http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11i-security-wpa2-wep.php

Rousku, K. 2003. Tietoturvapolitiikka. MikroPC-lehden artikkeli 04/2003.

Tech-FAQ, 2018a. SSID. Viitattu 18.5.2018. http://www.tech-faq.com/ssid.html

Tech-FAQ, 2018b. WEP. Viitattu 18.5.2018. http://www.tech-faq.com/wep-wired-equivalent-privacy.html

Tech-FAQ, 2018c. OSI-malli. Viitattu 18.5.2018. http://www.tech-faq.com/osi-model.html

TestOut simulaattori, 2018. Kuvat simulaattorista. Viitattu 18.5.2018. http://www.testout.com/

Viestintävirasto, 2018a. Salasanalla on väliä. Viitattu 18.5.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/12/ttn201412031257.html

Viestintävirasto, 2018b. WPA2-protokollan haavoittuvuudet mahdollistavat WiFi-verkkojen salauksen murtamisen. Viitattu 18.5.2018. https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2017/haavoittuvuus-2017-033.html

Viestintävirasto, 2018c. Tietoverkkorikollisuus - rikoksia verkossa tai verkon avulla. Viitattu 18.5.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/05/ttn201506031327.html

Wi-Fi Alliance, 2018. New Wi-Fi security features available in 2018. Viitattu 18.5.2018. https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements

Wikipedia, 2018. WPA. Viitattu 18.5.2018. https://fi.wikipedia.org/wiki/WPA_(salausprotokolla)

Vänninen, T. 2013. Ilmaistorjunnat rivissä. MikroPC-lehden artikkeli 1/2013.