Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2019

Miika Wallenius

SÄHKÖPOSTIN TIETOTURVAN PARANTAMINEN – CISCO EMAIL SECURITY -TUOTTEEN KÄYTTÖÖNOTTO

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

Joulukuu 2019 | 52 sivua

Miika Wallenius

SÄHKÖPOSTIN TIETOTURVAN PARANTAMINEN – CISCO EMAIL SECURITY TUOTTEEN KÄYTTÖÖNOTTO

Sähköpostiviestintä on vuosien aikana integroitunut vahvasti osaksi yleistä Internet kokemusta. Vuosien suosiosta johtuen sähköpostista on tullut rikollisille suosittu työkalu. Tästä syystä kaiken kokoisten yritysten on parannettava omia sähköpostiliikenteeseen liittyviä tietoturvaratkaisuja. Opinnäytetyön tavoitteena oli parantaa asiakasyrityksen sähköpostiliikenteen tietoturvaa Cisco Email Security -tuotteella. Lisäksi tutkittiin, kuinka sähköpostiviestintä teknisesti toimii, mitä uhkia siihen kohdistuu ja miten uhkia voidaan torjua. Opinnäytetyö suoritettiin Wisdomic Solutions Oy:n toimeksiannosta.

Cisco Email Security -tuote on sähköpostisuodatusjärjestelmä, jonka tarkoituksena on parantaa yritysten sähköpostiviestinnän tietoturvatasoa. Järjestelmä otettiin käyttöön kahdelle käytössä olevalle ESAV-palvelimelle. Järjestelmän käyttöönoton yhteydessä tarkistettiin, oliko yrityksellä myös nykyaikaiset DNS-tietueisiin perustuvat puolustusmekanismit SPF, DKIM ja DMARC käytössä.

Järjestelmän käyttöönotto suoritettiin projektina. Suunnittelussa otettiin huomioon asiakasyrityksen sähköpostiympäristö. Asiakas käytti sähköpostiviestintään O365 -palvelua. Tämän lisäksi varmistettiin pääsy DNS-hallintaan, sekä tarvittavien testitunnusten toimivuus. Käyttöönotto aloitettiin valmistelemalla saapuva sähköpostiliikenne yliheitolle. Valmistelussa asetettiin asiakkaan O365-järjestelmä hyväksymään viestit ESA:ta ja ESA hyväksymään viestit O365:tä. Tämän jälkeen yliheitto suoritettiin ohjaamalla asiakkaalle saapuva sähköpostiliikenne ESA:n kautta. Seuraavaksi valmisteltiin lähtevän liikenteen yliheitto luomalla O365:een yhdistin, joka ohjasi liikenteen ESA:n. Lisäksi DNS-tietueet otettiin käyttöön. Lähtevän liikenteen yliheitto suoritettiin määrittelemällä asiakkaan O365:een määrityksiä, joilla liikenne ohjattiin ESA:n.

Opinnäytetyön tavoitteet saavutettiin onnistuneella käyttöönotolla. Sähköpostiliikenteeseen liittyvää taustatutkimusta voidaan tulevaisuudessa hyödyntää muissa vastaavanlaisissa kehityksissä. Yhteenvetona voidaan päätellä sähköpostiliikenteen kasvun jatkuvan, ja yritysten on jatkuvasti panostettava sähköpostiturvallisuuden ylläpitoon ja kehitykseen.

ASIASANAT:

Cisco ESA, sähköposti, tietoturva

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Engineering, Information and Communications Technology

December 2019 | 52 pages

Miika Wallenius

IMPROVING EMAIL SECURITY – DEPLOYING CISCO EMAIL SECURITY PRODUCT

Over the years email has integrated itself as a strong part of the Internet experience. Due to the popularity of email lasting for years it has become a popular tool for criminals. Regardless of size, companies must improve their email traffic's security. The goal of the thesis was to improve the customer's email traffic with the Cisco Email Security system. The thesis also investigates how email technically works, what threats it is vulnerable to and how to prevent them. The thesis was commissioned by Wisdomic Solutions ltd.

Cisco Email Security is an email filter create to improve the security level of the companies email traffic. The system was deployed on two existing ESAV servers. When the system was deployed, it was checked whether the customer had advanced DNS based defense mechanisms, namely SPF, DKIM and DMARC.

The deployment of the system was carried out as a project. The commissioner's customer's email environment was taken in to account in the planning. The customer used O365 service for email messaging. Access to the DNS control and functionality of the test account were ensured. The deployment was started by preparing the incoming email traffic for migration. In the preparation the customer's O365 system was set to accept messages from ESA and ESA was set to accept messages from O365. After this, the migration was carried out by directing the incoming email traffic through ESA. The migration of the outgoing traffic was prepared next by creating a connector to the O365 which redirected the traffic to ESA. DNS records were enabled as well. The migration of the outgoing traffic was carried out by defining the O365 settings, which were used to redirect the traffic to ESA

The thesis goals were achieved by a successful deployment. The results and methodology of this thesis can be used in similar developments in the future. In summary, it can be concluded that email traffic will continue to grow, and companies must keep investing in the maintenance and development of email security.

KEYWORDS:

Cisco ESA, email, information security

SISÄLTÖ

KUVAT

TAULUKOT

KÄYTETYT LYHENTEET TAI SANASTO

BEC	Yrityksiin kohdistuva tietoverkkorikollisuuden muoto (Business Email Compromise)
DKIM	Digitaalinen allekirjoitusmekanismi (DomainKeys Identified Mail)
DMARC	Määrittelee SPF ja DKIM autentikointeihin sovellettavia käytäntöjä (Domain-based Message Authentication, Reporting & Conformance)
DNS	Internetin nimipalvelujärjestelmä, joka muuttaa verkkotunnukset IP-osoitteiksi. Lisäksi nimipalvelun tehtävänä on sähköpostin reititys (Domain Name System)
DNS-tietue	Nimipalvelun sisältötieto
Domain	Verkkotunnus koostuu kirjaimista ja numeroista, jonka avulla verkossa oleviin laitteisiin voidaan viitata helpommin muistettavalla nimellä kuin IP-osoitteilla.
EOP	Microsoftin pilvipohjainen sähköpostin suodatuspalvelu (Exchange Online Protection)
ESA	Ciscon tuottama sähköpostinsuodatusjärjestelmä (Email Security Appliance)
FTP	TCP-protokollaa käyttävä tiedonsiirtomenetelmä kahden laitteen väliseen tiedonsiirtoon (File Transfer Protocol)
HTTPS	Yhdistelmäprotokolla, jota selaimet ja www-palvelimet käyttävät suojattuun tiedonsiirtoon (Hypertext Protocol Secure)
IMAP	Sähköpostin vastaanottamiseen käytettävä protokolla (Internet Message Access Protocol)
MD5	Algoritmi, jota käytetään salaustekniikoissa (Message Digest)

MX-tietue	Kertoo sähköpostia vastaanottavan palvelimen (Mail Exchanger)
O365	Microsoftin valmistama toimisto-ohjelmistopaketti (Office 365)
POP	Sähköpostin vastaanottamiseen käytettävä protokolla (Post Office Protocol)
SMTP	Sähköpostin lähettämiseen käytettävä protokolla (Simple Mail Transfer Protocol)
SPF	Kertoo domainista oikeutetut sähköpostia lähettävät tahot (Sender Policy Framework)
SSH	Salattuun tietoliikenteeseen tarkoitettu protokolla, jolla voidaan ottaa salattuja yhteyksiä järjestelmästä toiseen (Secure Shell)
SSL/TLS	Protokolla jolla suojataan tietoliikennettä IP-verkkojen yli. SSL (Secure Sockets Layer) toimi aiemmin teknisenä protokollana, nykyään tekniikkana on TLS (Transport Layer Security), mutta terminä käytetään edelleen SSL-salausta.
Telnet	SSH:n tavoin tieteliikenneprotokolla, jolla otetaan yhteys järjestelmästä toiseen. Toisin kuin SSH, Telnet ei salaa liikennettä.
TXT-tietue	Käytetään tekstin lisäämiseksi DNS-tietueeseen
URI	URI on merkkijono, jolla viitataan esimerkiksi jonkin tietyn tiedon paikka tai nimi (Uniform Resource Identifier)
URL	URI:n alakäsitettä URL käytetään osoittamaan WWW-sivuja. (Uniform Resource Locator)
XML	Merkintäkielien standardi (Extensible Markup Language)

1 JOHDANTO

1.1 Toimeksianto ja tavoitteet

Opinnäytetyön aihe on Cisco Email Securityn käyttöönotto asiakasyrityksessä. Sähköposti on maailmanlaajuisesti yleisin viestintämuoto, ja sen käyttäjämäärät kasvavat tasaisesti. Yli puolet väestöstä käyttänee sähköpostia viestintävälineenä. Koska yritysten toiminta on erittäin riippuvaista sähköpostiviestinnästä, ne ovat suuressa riskissä joutua erilaisten hyökkäysten ja petosten kohteeksi. Tästä syystä kaiken kokoisten yritysten on jatkuvasti kehitettävä omia sähköpostiin liittyviä puolustusmekanismeja [1].

Opinnäytetyön tavoitteena on muodostaa käsitys sähköpostiviestinnän nykyisestä asemasta, siihen kohdistuvista tietoturvauhista ja siitä, kuinka uhkia voidaan torjua. Lisäksi tavoitteena on Cisco Email Security -tuotteen avulla tutustua sähköpostiturvallisuuden parantamiseen käytännössä. Yleisesti sähköpostiviestintään ja siihen liittyviin lukuihin lähdemateriaalina on käytetty verkossa saatavilla olevia artikkeleita, raportteja ja julkaisuja. Näitä lähteitä on täydennetty aiheeseen liittyvillä kirjoilla. Cisco Email Securityn liittyvissä luvuissa lähdemateriaalina on käytetty Ciscon omia materiaaleja. Aihetta on jo aikaisemmin tutkittu Juuso Leppäsen opinnäytetyössä [2]. Tässä työssä tavoitteena on selvittää syvemmin sähköpostin nykyinen tila, siihen liittyvät uhkakuvat ja miten näitä uhkakuvia voitaisiin torjua yleisellä tasolla. Myös Cisco ESA -järjestelmän esittelyssä selvitetään eri toteutuksien eroja ja käydään läpi ominaisuuksia, joita Leppäsen työssä ei vielä ole avattu.

Käyttöönotossa asiakasyrityksen sähköpostiliikenne suojataan kahdella olemassa olevalla Cisco ESAV-palvelimella. Projektin toimeksiantajana toimii Wisdomic Solutions Oy. Järjestelmän käyttöönoton yhteydessä yrityksen sähköpostiliikenteen tietoturvaa parannetaan myös erilaisilla DNS-tietueisiin perustuvilla mekanismeilla, mikäli näitä ei ole vielä otettu käyttöön.

Opinnäytetyön alussa käydään läpi sähköpostin nykytilaa, historiaa ja sen toimintaperiaatetta. Tämän jälkeen tutustutaan sähköpostiin liittyviä tietoturvauhkia, ja kuinka tietoturvauhkia voidaan torjua. Sen jälkeen tutustutaan Cisco ESA -palveluun. Käytännön osuudessa kerrotaan, kuinka Cisco ESA -palvelun käyttöönotto asiakkaalle tapahtuu.

2 SÄHKÖPOSTI

Sosiaalisen median, pikaviestintäpalveluiden ja muiden alustojen ottaessa oman aseman, sähköposti on edelleen yleisin viestintämuoto. Sähköposti on vuosien aikana vahvasti integroitunut osaksi yleistä Internet kokemusta, kun suurin osa verkossa tehtävistä aktiviteeteista kuten sosiaalinen media, verkkosivustot, pikaviestintäpalvelut tai mikä tahansa muu käyttäjätunnus internetissä vaatii sähköpostitiliä [1].

Vuonna 2018 koko maailmassa lähetettiin ja vastaanotettiin yhden päivän aikana yli 281 miljardia sähköpostiviestiä. Päivittäisen sähköpostiviestinnän on ennustettu kasvavan vuosittain yli neljä prosenttia. Vuonna 2022 tuon luvun ennustetaan kasvavan yli 333 miljardin sähköpostin lähettämiseen ja vastaanottamiseen päivässä [1].

Sähköpostitilien määrä kasvaa nopeammin kuin sen käyttäjämäärät. Kasvulle löytyy muutama eri syy. Yksi syy on se, että monella käyttäjällä on sekä henkilökohtainen sähköpostitili, sekä työpaikan sähköpostitili. Toinen syy voi olla se, että jokin tietty palvelu vaatii sähköpostitilin luomista, jotta kyseistä palvelua on mahdollista käyttää. Esimerkkinä tilanne, jossa henkilöllä on jo valmiiksi Microsoftin Outlook -sähköpostitili, mutta hän käyttää Android -käyttöjärjestelmällä varustettua puhelinta. Jotta puhelimen kaikki ominaisuudet toimisivat, käyttäjän tarvitsee tehdä Googlen Gmail -sähköpostitili. Keskimäärin yhdellä henkilöllä on 1,75 käyttäjätiliä, ja luvun odotetaan olevan 1,86 käyttäjätiliä vuonna 2022. Maapallon väestöstä yli puolet käytti sähköpostia vuonna 2018, sähköpostikäyttäjiä oli yli 3,8 miljardia. Käyttäjämäärän uskotaan kasvavan joka vuosi kolme prosenttia, eli vuonna 2022 sähköpostia käyttää yli 4,2 miljardia ihmistä [1].

2.1 Historia

Moni ei uskoisi, kuinka pitkä historia sähköpostilla on. Ensimmäinen esimerkki sähköpostin käytöstä ajoittuu vuoteen 1965. Yhdysvaltain yliopiston MIT (Massachusetts Institute of Technology) tietokoneilla oli käytössä ohjelmisto ”MAILBOX”, jolla käyttäjät pystyivät jättämään viestin ohjelmaan. Kun toinen käyttäjä kirjautui tietokoneelle, hän pystyi lukemaan jätetyn viestin ohjelmasta. Järjestelmä oli varsin tehokas, mutta käyttäjien oli käytettävä samaa tietokonetta [3].

Vuonna 1969 Yhdysvaltain puolustusministeriö perusti ARPANET:in (Advanced Research Projects Agency Network), joka on nykyisin käyttämämme Internetin edeltäjä. ARPANET:in avulla tietokoneiden välillä voitaisiin lähettää viestejä. Lokakuun 29.päivä ARPANET:in avulla lähetettiin ensimmäinen viesti tietokoneelta toiselle tietokoneelle. Vuonna 1971 Ray Tomlinson kehitti sähköisen postin, kuten me sen tänä päivänä tunnemme, luomalla ARPANET:iin sähköpostijärjestelmän. Konsepti lähes välittömästä kommunikoinnista laitteiden välillä osoittautui niin hyödylliseksi ja käytännölliseksi, että se alkoi pian levitä. Sisäisten verkkojen myötä lähetysprotokollat tulivat monimutkaisemmiksi. Tarvittiin tapa, jolla lähettäjän olisi mahdollista ilmaista viestin vastaanottava tietokone. Ray Tomlinsonilla kehitti ratkaisun, joka näkyy vielä tänäkin päivänä sähköpostiviestinnässä: ”@” -symboli. Viestin haluttu kohde ilmoitettiin muodossa ”käyttäjätunnus@tietokoneennimi”. Tämä osoitemuoto on säilynyt vielä tähän päivään saakka. Vuoteen 1976 mennessä kaikesta ARPANET:n verkkoliikenteestä 75 % koostui sähköisen postin liikenteestä. Sähköistä viestintää pidettiin niin hyödyllisenä, että alettiin pohtia, miten postin lähetys onnistuisi sisäisen verkon ulkopuolelle. Viestintää organisaatiosta toiselle sähköisen postin avulla pidetään sysäyksenä Internetin synnylle. Koska organisaatioiden välinen viestintä yleistyi, syntyi tarve ohjelmistolle, joka käsittelee ja tallentaa viestejä. Tämän myötä nykyaikaisten sähköpostilaatikoiden esiasteet kehitettiin nopeasti [3].

80-luvulla Internetin palvelutarjoajat (engl. Internet Service Providers) olivat alkaneet yhdistämään ihmisiä ympäri maailmaa. Tämän myötä myös sähköposti isännöinti (engl. hosting) sivustot alkoivat nousta esiin. Monelle Internetin uudelle käyttäjälle sähköposti oli ensimmäinen sitä hyödyntävä sovellus. Vuonna 1993 sana ”sähköinen posti (engl. electronic mail)” oli korvattu sanalla ”sähköposti (engl. email)” ja Internetin käyttö oli tullut yleisemmäksi. Seuraavien vuosien aikana yrityksen, kuten America Online, Echomail, Hotmail ja Yahoo muovasivat ja kehittivät sekä Internettiä, että sähköpostia. Yritykset laittoivat suuria summia rahaa markkinointiin, jotta mahdollisimman monella olisi esteetön pääsy Internettiin hyötymään sen eduista. 90-luvun loppupuolella Internetin käyttö räjähti, kasvaen 55 miljoonasta käyttäjästä 400 miljoonaan käyttäjään vuosien 1997 ja 1999 välillä. Koska markkinointi oli tullut laajalti ilmaiseksi, roskapostin määrä kasvoi eksponentiaalisesti. Tuli tarve ohjelmistolle, joka lajittelisi sähköposteja. Myöhemmin sähköpostitilin omistaminen on muuttunut ylellisyydestä itsestäänselvyydeksi. Jokaiselta ihmiseltä oletetaan nykyään löytyvän sähköpostitili siinä missä puhelinnumero [3].

2.2 Sähköpostiviestinnän toimintaperiaate

Kun ihminen vastaanottaa sähköpostin, harvoin hän ajattelee, että miten sähköposti on saapunut perille, tai minkälaisen matkan se on kulkenut ennen kuin on saavuttanut määränpään. Jotta posti saavuttaa määränpään, on siihen käytetty useampaa protokollaa, ja se on käynyt useamman palvelimen kautta. Näistä tärkein protokolla on SMTP (Simple Mail Transfer Protocol), jonka tehtävä on sähköpostiviestin lähetys järjestelmästä toiseen. Kun vastaanottaja vastaanottaa viestin, SMTP -protokollaa ei käytetä, vaan tähän on erikseen erilaisia protokollia kuten POP (Post Office Protocol) ja IMAP (Internet Message Protocol). Jotkut valmistajat ovat kehittäneet Internetin standardien lisäksi omia protokolliaan sähköpostiviestien vastaanottamiseen, esimerkiksi Microsoft Exchangen MAPI (Messaging Application Programming Interface) ja Lotus Notesin käyttämä NRPC (Notes Remote Procedure Call) [4].

2.2.1 SMTP-protokolla

SMTP (Simple Mail Transfer Protocol) on sähköpostin lähettämiseen käytettävä protokolla. SMTP:tä käytetään, kun posti kulkee lähettäjältä ensin lähettäjän sähköpostipalvelimelle, ja sieltä vastaanottajan sähköpostipalvelimelle. SMTP-protokollaa ohjaa MTA (Mail Transfer Agent). Protokolla käyttää salaamattomaan liikenteeseen porttia 25. SSL/TLS suojattuun liikenteeseen, jota kutsutaan myös SMTPS protokollaksi, käytetään porttia 465 [5].

2.2.2 POP3-protokolla

POP3 (Post Office Protocol version 3) on viimeisin versio POP:ista ja sitä käytetään sähköpostin vastaanottamiseen. Protokollaa käyttäessä vastaanottaja lataa sähköpostiviestin sähköpostipalvelimelta päätelaitteelle, esimerkiksi tietokoneelle. Kun viesti on ladattu laitteelle, se poistuu palvelimelta. POP3:ssa on myös ominaisuutena optio, jolla voidaan säilyttää sähköpostiviesti palvelimella jokin tietty aika. Protokolla on yhdensuuntainen tietoliikennepolku, eli tieto kulkee ainoastaan palvelimelta päätelaitteelle [5]. POP3:n suurin heikkous on se, että se ei tarjoa sähköpostiviesteille pysyvää tallennuspaikka, vaan viestit säilötään laitteelle, jolla käyttäjä avaa sähköpostinsa. Koska viestit siirretään kokonaisuudessaan palvelimelta päätelaitteelle, viestit näkyvät ainoastaan sillä laitteella,

jolle ne on ladattu. Lisäksi sähköpostien varmuuskopiointi on haastavampaa viestien ollessa käyttäjien laitteilla palvelimen sijaan [4]. Etuna POP3 ei vaadi verkkoyhteyttä toimiakseen, koska sähköpostit ovat kokonaisuudessaan ladattu päätelaitteelle, eli käyttäjällä on pääsy sähköpostilaatikon koko sisältöön ilman verkkoyhteyttä. POP3 käyttää salaamattomaan liikennöintiin porttia 110. SSL/TLS suojattua liikennöintiä kutsutaan POP3S protokollaksi ja se käyttää porttia 995 [3].

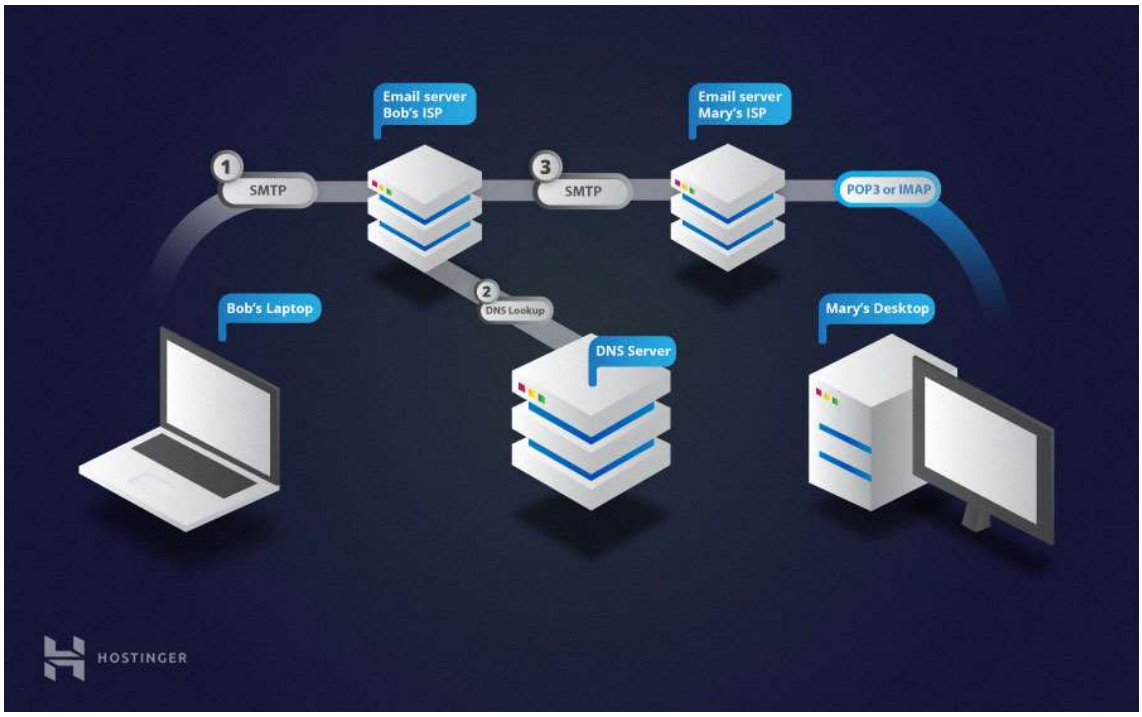
2.2.3 IMAP-protokolla

IMAP (Internet Message Access Protocol) on myös sähköpostin vastaanottamiseen tarkoitettu protokolla ja se käyttää porttia 143 salaamattomaan liikenteeseen, sekä porttia 993 SSL/TLS suojattuun liikenteeseen, jota kutsutaan myös IMAPS portiksi. Toisin kuin POP3, IMAP lataa ainoastaan sähköpostien otsikot päätelaitteelle, ja koko muu sisältö jää on palvelimelle. Toinen suuri ero on se, että IMAP on kahdensuuntainen tietoliikennepolku, eli tieto kulkee sekä palvelimelta päätelaitteelle, että päätelaitteelta palvelimelle. IMAP etuna on sen synkronointi, jonka ansiosta sähköpostia voidaan käyttää usealla eri laitteella ja viestit ovat varmuuskopioituna palvelimella [4]. Kun käyttäjä tekee muutoksen ilman verkkoyhteyttä, muutokset synkronoituvat heti kun laite yhdistetään verkkoon. Lisäksi sähköpostilaatikon avaaminen on nopeampaa, kun IMAP ei päivitä koko sähköpostilaatikkoa päätelaitteelle. Huonona puolena voidaan pitää sitä, että offline-tilassa käyttäjällä ei ole koko sähköpostilaatikon sisältöön, koska ne ovat palvelimella [5]. IMAP myös edellyttää, että palvelimella on tallennuskapasiteettia sähköpostiviestien säilömiseen.

2.2.4 Sähköpostin kulku

Sähköpostiviestin matka alkaa, kun lähettäjä klikkaa ”lähetä” painiketta, jolloin lähettäjän sähköpostiohjelma yhdistää lähettäjän SMTP-palvelimelle, käyttäen SMTP protokollaa. Esimerkiksi Gmailia käytettäessä, sähköpostiohjelma yhdistää Gmailin SMTP-palvelimelle. Lähettäjän SMTP-palvelin tarkistaa lähetetyn sähköpostin vastaanottajan. Otetaan esimerkiksi, että vastaanottaja on ”vastaanottaja@esimerkki.fi”, lähettäjän SMTP-palvelin lähettää ”DNS Lookup” kyselyn DNS-palvelimelle, jossa se pyytää @esimerkki.fi:n MX (mail exchange) tietuetta. MX-tietue on DNS-tietue, joka määrittää palvelimen, joka vastaanottaa domainin sähköpostiliikenteen. Tässä tapauksessa lähettäjän

SMTP-palvelin haluaa tietää @esimerkki.fi domainin MX-tietueen, josta selviää, mikä palvelin vastaanottaa kyseiselle domainin tulevat sähköpostit vastaan. Kun lähettäjän SMTP-palvelin on saanut @esimerkki.fi:n MX-tietueen, se lähettää lähetetyn sähköpostiviestin vastaanottajan sähköposteja käsittelevälle palvelimelle. Tämän jälkeen sähköpostiviesti välitetään @esimerkki.fi:n SMTP-palvelimelle, joka tarkistaa, löytyykö ”vastaanottaja” kyseiseltä palvelimelta. Jos tili löytyy palvelimelta, sähköpostiviesti välitetään palvelimelta vastaanottajan päätelaitteelle jotain sähköpostiviestejä vastaanottamiseen tarkoitettua protokollaa käyttäen [5] (Kuva 1).



Kuva 1. Sähköpostiviestin matka lähettäjältä vastaanottajalle [5]

3 SÄHKÖPOSTIN UHAT

Sähköpostin ollessa ihmisten ensisijainen viestinnän väline työelämässä, sekä yksityiselämässä vahvasti integroitu kaikkiin käyttämiimme palveluihin, on siitä tullut myös tehokas työkalu verkkorikollisille [6]. Itse asiassa tällä hetkellä on lähes kaksi kertaa todennäköisempää saada haittaohjelma sähköpostin kautta, kuin esimerkiksi saastuneelta verkkosivulta painetusta mainoksesta [7]. Hyökkäystapoja on monia ja ne ovat osoittautuneet tehokkaiksi, koska pienelläkin resurssimäärällä niillä voi saada paljon vahinkoa aikaan. Koska haittaohjelmista ja huijausmekanismeista tulee jatkuvasti kehittyneempiä, sähköpostiliikenteen tietoturvan ylläpito on keskeinen konsepti kaiken kokoisille yrityksille [2]. Jos sähköpostin sisältö muutettaisiin normaaliksi postiksi, kymmenestä postista seitsemän olisi mainoksia, kaksi laskua ja yksi kirjeistä sisältäisi myrkkyä [6]. Mainosten ja tarpeellisten postien osuudella ei välttämättä ole huomattavaa eroa sähköpostin ja normaalin postin välillä, suurin ero on todellisen vaaran aiheuttava ”myrkyllinen posti”, joka voidaan rinnastaa haittaohjelman sisältävään sähköpostiin.

3.1 Haittaohjelmat

Kuten aikaisemmin todettu, sähköposti muodostaa suurimman uhan joutua haittaohjelman kohteeksi. Yleisesti ottaen haittaohjelmia levitetään kahdella eri tavalla, joko liitetiedostolla tai URL-linkillä. Liitetiedosto on ollut pitkään näistä yleisempi levitystapa, mutta tietoturvayhtiö Proofpointin vuoden 2019 raportissa käy ilmi, että tämä asetelma on muuttunut, ja URL-linkillä levitetyt haittaohjelmat olisivat tänä päivänä huomattavasti yleisempiä [8]. Mahdollisia muutoksen syitä ovat ihmisten lisääntynyt tietoisuus siitä, että sähköpostissa olevia liitetiedostoja ei tulisi avata. Lisäksi pilvipalveluiden yleistyessä tiedoston jakaminen tapahtuu usein sähköpostiin saapuvien linkkien välityksellä, jolloin linkkien avaaminen sähköpostin kautta on yleistynyt [8]. Liitetiedoston ja URL-linkkien vertailu osoittaa hyvin sen, kuinka rikolliset seuraavat jatkuvasti niin yksittäisten ihmisten kuin yritysten toimintatapoja, ja hyökkäysmenetelmät sovelletaan toimintatapoja hyödyntäen.

Liitetiedosto ei itsessään välttämättä ole haittaohjelma, jonka rikollinen haluaa uhrin laitteelle, vaan se voi olla jonkinlainen latausohjelma. Latausohjelmat ovat yleensä skriptejä tai makroja, jotka käynnistyessään lataavat muita ohjelmia. Skripti saattaa esimerkiksi

avata PowerShellin, joka alkaa lataamaan itse haittaohjelmaa. Makrot ovat usein Office-tiedostojen sisällä, ja ne käynnistyvät, kun kyseinen Office-tiedosto avataan. Verrattuna haittaohjelman liittämisen suoraan sähköpostiviestiin, latausohjelmilla on muutama etu, jonka takia niitä käytetään. Jos uhri suorittaa liitetiedostona olevan skriptin, itse haittaohjelmalla on suora pääsy kohteeseen, ilman että sen tarvitsee päästä sähköpostisuojausten läpi. Toinen etu on se, että hyökkääjä voi tarkistaa kohteen, kun skripti on ajettu. Riippuen siitä täyttääkö kohde hyökkääjän kriteerit, hyökkääjä voi päättää haittaohjelman lähettämisestä. Kolmantena etuna voidaan mainita vielä, että mikäli haittaohjelma havaitaan ja poistetaan uhrin toimesta, voidaan siihen tehdä nopeasti muutoksia hyökkääjän toimesta. Näin käyttäjät, jotka ovat altistuneet skriptille, saavat uudemman version haittaohjelmasta [7].

Toinen tapa levittää haittaohjelmia on viestin tekstiosiossa oleva URL-linkki, joka ohjaa uhrin haitalliselle verkkosivustolle. Sähköpostiviesti voi sisältää esimerkiksi Dropboxiin viittaavan linkin ja tämän linkin kautta uhri lataa koneelle tiedoston, joka sisältää haittaohjelman.

3.2 Roskaposti

Yli puolet sähköpostiliikenteestä koostuu roskapostista. Vuonna 2011 roskapostin osuus oli jopa 75 % koko sähköpostiliikenteestä. Vuoden 2017 alkupuolella osuus oli noin 54 % ja määrä on ollut pienessä nousussa vuoden 2015 loppuvuodesta [7].

Roskaposteissa käytetään useita eri teemoja, mutta niissä on monesti yksi yhdistävä tekijä: Ne ovat liian hyvää ollakseen totta. Niissä saatetaan mainostaa erittäin edullisia lääkkeitä, tehokkaita painonpudotusohjelmia tai uhkapelejä. Toisinaan roskapostia käytetään myös vakavampiin rikoksiin. Joissakin tapauksissa rikollinen yrittää rekrytoida pahaa ajattelemattomia ihmisiä, joille hän lupaa pienellä vaivalla paljon rahaa. Näissä on yleensä kysymyksessä esimerkiksi rahanpesu, jossa virtuaalivaluuttoja muutetaan toiseen valuuttaan ja päinvastoin. Tällainen toiminta on kuitenkin laitonta, ja myös käyttäjä saattaa syyllistyä oikeaan rikokseen, vaikka hän ei sitä välttämättä heti itse ymmärrä. Roskapostit voivat toimia myös tietojenkalastelutyökaluna, jolloin se houkuttelee mainoksen avulla kirjautumaan verkkosivustolle, jonka jälkeen rikollinen voi saada uhrista arkaluonteista tietoa. Tietojenkalastelusta tarkemmin alaluvussa 3.4.

Suurimmasta roskapostin levityksestä on vastuussa spambotit. Spambotit keräävät sähköpostiosoitteita Internetistä ja luo niistä postituslistoja lähettääkseen roskapostia. Ne eivät kuitenkaan ole ainoa syypää roskapostin levitykselle. On paljon yrityksiä, jotka mainostavat tuotteitaan sähköpostin avulla, ja tässä ei itsessään ole mitään väärää. Ongelmia alkaa syntyä silloin, kun yritys ei tarjoa tapaa, jolla voit peruuttaa mainosviestin saapumisen. Välillä nämä yritykset saattavat myös jakaa sähköpostiosoitettasi muiden mainostajien kanssa, joka kasvattaa ei-toivotun kaupallisen mainonnan määrää käyttäjän sähköpostissa.

Roskapostia on sähköpostiliikenteessä niin paljon, että pelkästään sen siivoamiselle voidaan antaa jo hintalappu. Mikäli yrityksellä ei ole minkäänlaista roskapostia suodattavaa järjestelmää, yhdeltä käyttäjältä kuluu työpäivästä aikaa päivittäin viidestä kymmeneen minuuttiin. Yksistään tämä ei vielä kuulosta paljolta, mutta koko yrityksen mittakaavassa tämä tarkoittaa, että jokaista sataa ihmistä kohden menisi kahden ihmisen työpanos sähköpostilaatikon siivoamiseen roskapostista, mikäli yrityksellä ei ole suodatinta tätä varten [7].

3.3 Business Email Compromise (BEC) -huijaukset

BEC -huijauksilla tarkoitetaan yrityksiin kohdistettuja huijauksia, ja ne koskevat kaiken kokoisia yrityksiä. BEC -huijauksia tapahtuu monessa eri muodossa. Yleensä rikolliset yrittävät huijata yritykseltä rahaa, mutta joskus motiivina toimii jokin muu arkaluonteinen tieto yrityksestä, jota voidaan hyödyntää suuremmassa hyökkäyksessä, tai työtekijöiden henkilötietoja kalastellaan identiteettivarkauksia varten.

Usein huijauksen kohteena ovat yrityksen rahaliikenteestä vastaavat henkilöt. Yleinen rikollisten huijauskeino on esittäytyä yrityksen korkeassa asemassa olevaa henkilöä joka ilmoittaa, että sähköpostissa on maksamaton lasku, ja maksu tulisi suorittaa välittömästi. Viestin lähettäjän sähköpostitili on saatettu kaapata, mutta yleensä sähköpostit ovat väärennettyjä sähköpostitilejä. Viesteissä yleensä ilmoitetaan, että asialla on erittäin kova kiire, ja mikäli maksua ei suoriteta, siitä voi olla suuret vahingot yritykselle. Viestit saattavat sisältää huomattavan määrän kirjoitusvirheitä, ja ulkoasussa saattaa muitakin puutteita, jotka normaalisti herättäisivät epäilystä. Kuitenkin kun yhdistetään muut tekijät, kuten kiire, suuret taloudelliset vahingot yritykselle ja se että viesti on saapunut korkeassa asemassa olevalta henkilöltä, uhri ei välttämättä ota viestin puutteita huomioon.

3.4 Tietojenkalastelu

Tietojenkalastelulla tarkoitetaan huijausta, jossa rikollinen lähettää sähköpostin, joka näyttää saapuneen joltain oikealta, usein myös tunnetulta ja luotettavalta yritykseltä, esimerkiksi pankilta. Sähköpostissa saatetaan pyytää pankkitunnuksia tai luottokorttitietoja. Mikäli uhri vastaa postiin lähettämällä pankkitunnukset, hänen pankkitili pystytään kaappaamaan. Toinen yleinen tietojenkalastelun avulla tehtävä rikos on käyttäjätunnusten kaappaaminen. Uhrille saapuu viesti Gmailiin, jonka lähettäjänä näyttää olevan Googlen järjestelmävalvoja. Viestissä ilmoitetaan, että Google-tilin salasana on vaihdettava välittömästi viestissä olevan linkin kautta. Todellisuudessa viesti ei ole tullut Googlelta, eikä linkki ohjaa käyttäjää Google-tilin salasanan vaihtoon, vaan linkki ohjaa käyttäjän huijaussivustolle, jonka kautta rikollinen saa hänen Google-tilin käyttäjätunnuksen ja salasanan, kun uhri on ne sinne syöttänyt.

3.5 Arkaluonteisen sisällön lähetys

Usein sähköpostiin liittyvät tietoturvariskit yhdistetään ainoastaan saapuvaan sähköpostiliikenteeseen. Myös lähtevän sähköpostiliikenteen riskit on otettava huomioon. Käyttäjä, joka tahattomasti jakaa arkaluonteista tietoa suurelle jakelulistalle, saattaa aiheuttaa suuren tietovuodon. Arkaluonteisiin tietoihin voidaan lukea esimerkiksi potilastiedot, henkilötiedot sekä luottokorttitiedot. Joskus myös arkaluonteista tietoa halutaan lähettää sähköpostilla, koska tiedot saadaan nopeasti henkilöltä toiselle, välimatkasta riippumatta. Yrityksellä tulisi olla selkeät käytännöt ja määritykset arkaluonteiden tiedon lähettämiselle. Arkaluonteista tietoa sisältävä sähköposti tulisi aina lähettää suojattuna.

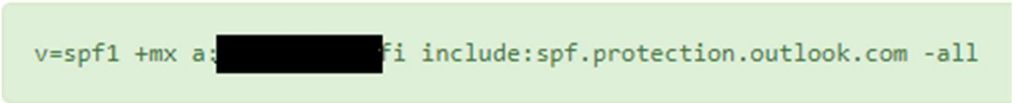
4 TIETOTURVAN PARANTAMINEN

4.1 DNS-tietueet

Sähköpostia voidaan lähettää kenen tahansa sähköpostiosoitteen nimissä, ja tästä syystä on tärkeää, että viestin lähettäjä pystytään varmistamaan ja todentamaan [9]. Tätä todentamista varten on kehitetty DNS-tietueisiin perustuvia mekanismeja, joiden tehtävä on todentaa viestin lähettäjä. Näitä ovat SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) ja DMARC (Domain-based Message Authentication, Reporting and Conformance).

4.1.1 SPF-tietue

SPF on TXT-tietue. Tietueen avulla määritellään, mitkä sähköpostipalvelimet ja IP-osoitteet saavat lähettää sähköpostia kyseisen domainin nimissä. Mikäli sähköpostiviesti lähetetään määritettyjen palvelimien tai osoitteiden ulkopuolelta, SPF ehdot eivät täyty eli kyseisellä palvelimella tai osoitteella ei ole ollut lupaa lähettää sähköpostia. Tästä syystä posti menee todennäköisesti vastaanottajan roskapostiin, tai mikäli yrityksellä on roskapostisuodatin käytössä, posti ei välttämättä saavu edes vastaanottajan roskapostikansioon. [9] Kuva 2 on esimerkki SPF-tietueesta.



Kuva 2. Esimerkki SPF-tietueesta

Tietueesta nähdään suoraan mitä SPF versiota käytetään, mistä kyseisellä domainilla on lupa lähettää postia, sekä mitä tapahtuu, kun SPF ehdot eivät täyty. Seuraavaksi luettelossa on Kuva 2 SPF-tietueen tunnisteet.

- v=spf1; Kertoo käytetyn SPF version. Tällä hetkellä on suositeltavaa käyttää spf1 versiota, koska se on yleisin versio, jota sähköpostipalvelimet osaavat hyödyntää.

- +mx; Hyväksyy MX-tietueessa määritetyistä IP-osoitteista lähettää sähköpostia. Etuliitteenä oleva ”+” -merkki ilmaisee ”PASS”, eli SPF menee läpi. ”PASS” on myös oletuksena, joten tässä tapauksessa +mx olisi sama kuin pelkkä mx.
- a:(sensuroitu).fi; Hyväksytään esimerkiksi jonkin tietyn palvelimen tai monitoimilaitteen lähettää sähköpostia domainista.
- include:spf:protection.outlook.com; Sallitaan sähköpostin lähettäminen O365 palvelusta kyseisen domainin nimissä.
- -all; Tämä arvo pätee kaikkiin lähettäjiin. Se lisätään yleensä viimeisenä tietueeseen, ja sillä määritetään, miten käsitellään posteja, jotka eivät täytä mitään aikaisempaa arvoa. Testivaiheessa voidaan käyttää etuliitettä ”~”, joka on ”SOFTFAIL”, eli viestit merkataan, mutta ne ovat hyväksyttyjä. Muutoin tulisi aina etuliitteenä olla ”-”, joka tarkoittaa, että viesti ei läpäise SPF ehtoja.

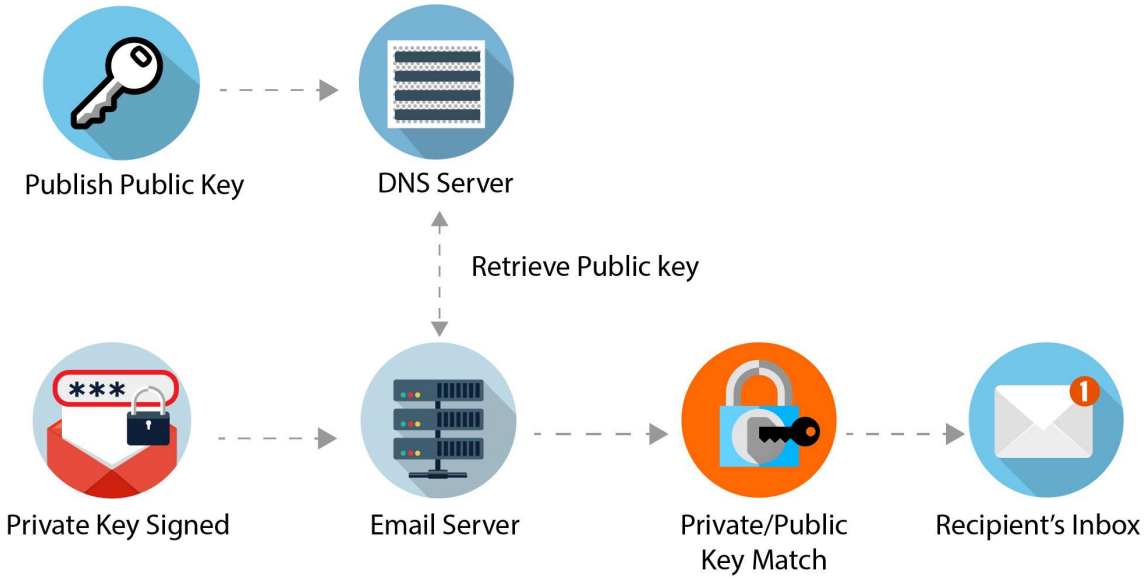
4.1.2 DKIM-tietue

DKIM avulla voidaan todentaa sähköpostin lähettäjä ja varmistaa, että sähköpostiviestiä ei ole muokattu lähettämisen jälkeen. Kun lähettäjä lähettää sähköpostin, viesti allekirjoitetaan domainin yksityisellä avaimella (engl. private domain key). Yksityinen avain on suojattu salauksella, jonka vastaanottajan sähköpostipalvelin purkaa julkisella avaimella. Julkinen avain on DNS:ssä lähettäjän määrittelemässä DKIM TXT-tietueessa (Kuva 4). Mikäli julkinen avain täsmää yksityiseen avaimeen, DKIM menee läpi ja lähettäjä voidaan vahvistaa. [10] Kuva 3 on esimerkki DKIM-tietueesta.

Kuva 3. Esimerkki DKIM-tietueesta

DKIM-tietueessa on jonkin verran vähemmän tunnisteita kuin SPF-tietueessa. Seuraavassa luettelossa on DKIM-tietueen tunnisteet.

- v=DKIM1; Tällä hetkellä DKIM:stä on olemassa ainoastaan yksi versio, DKIM1.
- p=(sensuroitu); Julkinen avain, jonka vastaanottajan sähköpostipalvelin hakee, ja vertaa yksityiseen avaimeen. Vaikka kuvassa oleva avain on julkinen, tietoturvasyistä se on sensuroitu.



Kuva 4. DKIM toimintaperiaate

4.1.3 DMARC-tietue

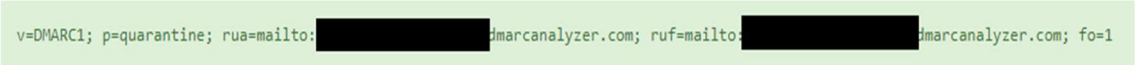
Edellä mainittujen SPF:n ja DKIM:n ongelmana on se, että ei ole olemassa yhteistä käytäntöä, jolla todentamattomia sähköpostiviestejä tulisi käsitellä. DMARC pääasiallinen tehtävä on helpottaa osapuolten välistä yhteistyötä, jonka avulla lähettäjä pystyy parantamaan lähtevän sähköpostivirran autentikoinnin parantamista. DMARC:n avulla saadaan raportti viesteistä, joiden autentikointi ei ole mennyt läpi, ja sen perusteella järjestelmänvalvoja voi tehdä korjauksia järjestelmään. Vastaavasti DMARC kertoo vastaanottajalle, kuinka kyseisestä domainista saapuvia autentikoimattomia sähköposteja tulisi käsitellä. Ilman tätä järjestelmää, lähettäjän on hyvin vaikea analysoida, kuinka paljon oikeita sähköposteja on lähetetty autentikoimatta. Lisäksi vastaanottaja joutuu itse tulkitsemaan, että voiko postia ottaa vastaan, vai tuleeko sen pääsy estää [11]. Kuva 5 esimerkki käytössä olevasta DMARC-tietueesta.

Domainin ylläpitäjällä voi julkaista kolmea eri menettelytapaa, joita vastaanottajaa opastetaan soveltamaan, kun hän vastaanottaa domainista saapuvan sähköpostiviestin, joka ei täytä DMARC ehtoja: ei mitään (engl. none), karanteeni (engl. quarantine) ja hylätä (engl. reject)

”None” vaihtoehtoa käytetään silloin, kun halutaan kerätä dataa. Esimerkiksi DMARC:n käyttöönotossa on tärkeää, että ennen kuin menettelytavaksi valitaan ”quarantine” tai ”reject”, on kerätty tarvittava data, jota analysoimalla voidaan korjata oikeutetut sähköpostiviestit, jotka eivät ole täyttäneet DMARC:in ehtoja.

Järjestelmän käyttöönoton viimeisessä vaiheessa päätetään, kuinka autentikoimattomia sähköpostiviestejä tulisi käsitellä. ”Quarantine”, eli karanteeni vaihtoehtoa soveltaessa vastaanottajaa ohjataan käsittelemään sähköpostiviestiä tarkistuksella. Karanteenia vaihtoehtoa käyttäessä vastaanottaja voi soveltaa erilaisia vaihtoehtoja, kuten esimerkiksi ohjata sähköpostin kohdehenkilön roskapostikansioon tai ohjata sähköpostiviestin väliaikaiseen karanteeniin, josta kohdehenkilö voi vapauttaa sähköpostiviestin. Mikäli vastaavanlaisia sähköpostiviestejä ei tulevaisuudessa haluta läpi, voi vastaanottaja kiristää omaa roskapostisuodatinta, jonka avulla viestit eivät jatkossa siirry palvelimelta kohdehenkilölle. Mikäli autentikoimaton sähköpostiviesti ohjautuu kohdehenkilön roskapostilaatikkoon, tai väliaikaiseen karanteeniin, on tärkeää selvittää syy, koska kohdehenkilö saattaa avata haitallisen sähköpostiviestin, tai tarpeellinen viesti saattaa jäädä kohdehenkilöltä huomaamatta, mikäli viesti ei tule käyttäjän normaaliin sähköpostilaatikkoon [12].

Toinen menettelytapa autentikoimattomalle sähköpostiviestille on ”reject” eli hylkäys. Yleisesti ottaen viestin hylkäämistä sovelletaan kahdella eri toteutuksella. Suositeltavammassa ja laajimmin käytetyssä toteutuksessa vastaanottajan sähköpostijärjestelmä hylkää vastaanottamasta viestin kokonaan. Tämä on suositeltava tapa, koska lähtevä viesti ei poistu lähettäjän palvelimelta, jonka ansiosta lähettäjän sähköpostijärjestelmään tulee heti tieto, että mistä syystä sähköposti viesti ei ole mennyt läpi. Toisessa toteutuksessa vastaanottajan sähköpostijärjestelmä vastaanottaa sähköpostiviestin, mutta ei välitä sitä enää kohteeseen. Sähköpostiviestistä saattaa generoitua ”Delivery Status Notification” viesti lähettäjälle, tai viesti saattaa kadota ilman, että siitä välittyy ilmoitusta kohdehenkilölle tai lähettäjälle. Mikäli ”reject” toimintatapaa sovelletaan, lähettäjän on oltava varma, että kaikki domainia käyttävät sähköpostiviestit, jotka halutaan välittää eteenpäin, täyttävät DMARC:n ehdot [12].



Kuva 5. Esimerkki DMARC-tietueesta

DMARC tietueessa käytetään myös tunnisteita, joista saadaan selville seuraavia tietoja.

- v=DMARC1; Kertoo että DMARC:sta käytetään versiota DMARC1
- p=quarantine; Menettelytapa jota käytetään, kun sähköpostiviesti ei täytä DMARC ehtoja
- rua=mailto:(sensuroitu)dmarcanalyzer.com; URI, johon XML-raportti lähetetään
- ruf=mailto:(sensuroitu)dmarcanalyzer.com; URI, johon ”Forensic” raportti lähetetään
- fo=1; Määritellään että mitä tietoja ”Forensic” raporttiin kerätään. Esimerkin arvolla ”1” tuotetaan raportti, jos SPF tai DKIM epäonnistuu. Jos arvo on ”0”, raporttiin tuotetaan tulokset, joissa sekä SPF että DKIM ovat epäonnistuneet. Arvolla ”d” saadaan ainoastaan DKIM epäonnistuneet tulokset, ja ”s” arvolla ainoastaan SPF epäonnistuneet.

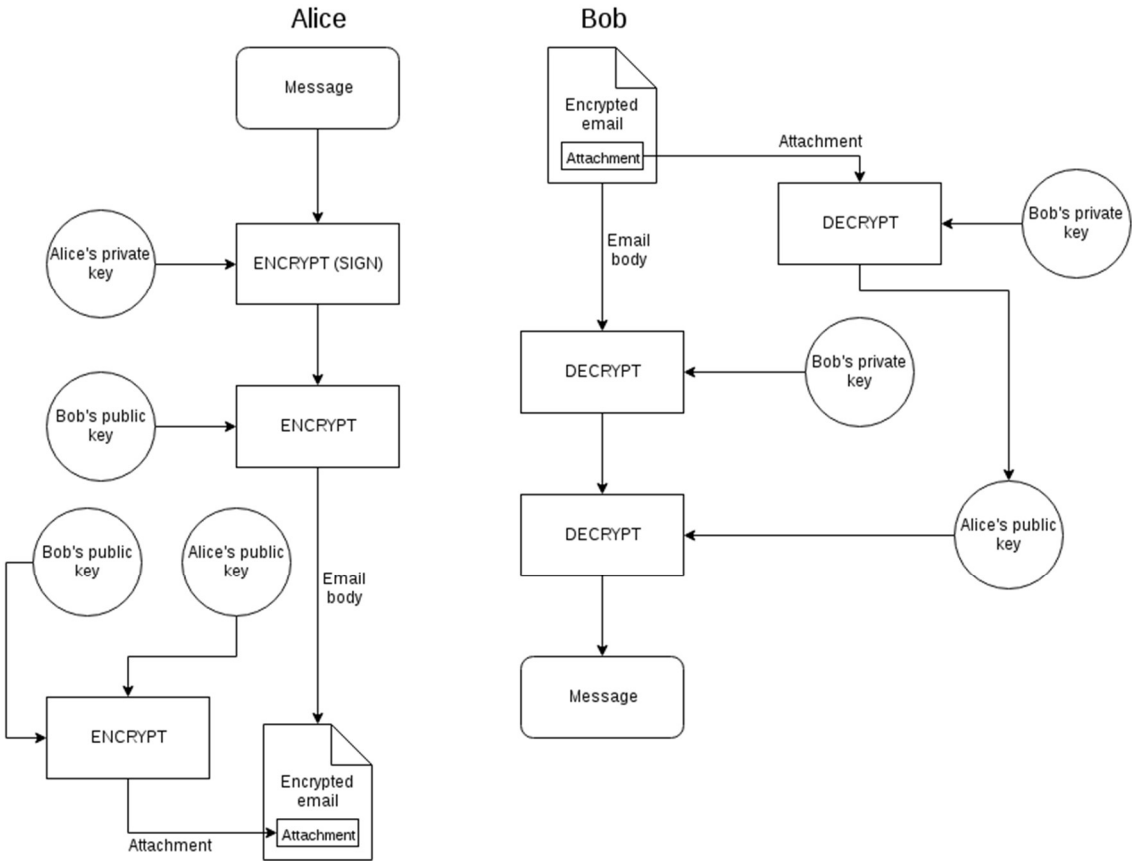
4.2 Sähköpostiviestin salaus

Kun sähköpostiviesti salataan, tavoitteena on varmistaa, etteivät ulkopuoliset pääse käsiksi viestin sisältöön. Salatun ja salaamattoman sähköpostiviestin eroa voidaan verrata postikortin ja kirjekuoren eroihin. Postikortissa kaikki sisältö on näkyvissä vastaanottajatietojen vieressä, kun taas kirjekuoressa vastaanottajatiedot ovat kaikille näkyvissä, mutta itse sisältö on piilossa kuoren sisällä. Sähköpostiviestien salaus perustuu salausavainten riittävään pituuteen. Salausavaimen ollessa riittävän pitkä, sen murtaminen järkevässä ajassa ei ole mahdollista.

Syitä viestinnän salaamiselle on monia. Erilaiset lait ja sopimukset kuten GDPR velvoittavat organisaatioita suojaamaan tietynlaisia sähköpostiviestejä. Tällaisia sähköpostiviestejä ovat esimerkiksi viestit, jotka sisältävät käyttäjien tietoja. Mikäli yritys syyllistyy tietovuotoon, eikä se ole toiminut lakien määrittämällä tavalla, voi sakkojen summa olla hyvinkin suuri. Sakkojen lisäksi myös yrityksen maine, sekä liiketoiminta voivat kärsiä tietovuodoista.

Tunnetuin salausjärjestelmä on PGP (Pretty Good Privacy), joka perustuu julkisen ja yksityisen avainparin käyttöön. Tämä tarkoittaa sitä, että lähettäjällä ja vastaanottajalla on sekä julkinen ja yksityinen avain. Oikeaoppisesti PGP:tä käyttäen lähettäjä salaa sähköpostiviestin omalla yksityisellä avaimella, jolla myös allekirjoitetaan viesti, sekä vastaanottajan julkisella avaimella. Viestissä oleva liitetiedosto salataan erikseen, salauksessa

käytetään lähettäjän ja vastaanottajan julkista avainta. Vastaanottaja purkaa salauksen oman yksityisen avaimen ja lähettäjän julkisen avaimen avulla [13] (Kuva 6).



Kuva 6. Salatun viestin lähettäminen PGP-salauksella [13]

PGP-salauksen suurin heikkous sen käytettävyys. Jotta salausta voidaan käyttää, lähettäjä tarvitsee vastaanottajan julkisen avaimen, ennen kuin lähetys voidaan tehdä. Avainten hankkimisessa ja yläpidossa on monelle liikaa vaivaa, suhteessa salaamattoman viestin helppouteen [14].

Toinen yleinen salaukseen käytettävä järjestelmä on S/MIME, joka on tarkoitettu pelkästään sähköpostiviestin salaamiseen ja digitaaliseen allekirjoittamiseen toisin kuin PGP, joka on yleiskäyttöinen salausjärjestelmä. S/MIME perustuu julkisen avaimen salaukseen ja ennen kuin sitä voidaan hyödyntää, tulee sekä lähettäjän että vastaanottajan sähköpostivarmenteet olla kunnossa. S/MIME:n ongelmana on sähköpostivarmenteiden hallinta. Kuitenkin nykyisin useat sähköpostijärjestelmät, kuten Gmail ja Outlook tukevat S/MIME:ä, joka helpottaa sen hyödyntämistä.

Lisäksi suosittu menetelmä viestien salaamiseen on salata ainoastaan sähköpostiviestissä oleva liitetiedosto jollakin salausohjelmalla. Menetelmän käytössä haasteena on se, että osapuolten on keksittävä toimintatapa koko prosessille. Tämä tarkoittaa, että salaustekniikka sekä salauksen purkamiseen tarkoitetun avaimen toimitus on erikseen sovittava osapuolten välillä. Ongelmia voi tulla, mikäli suojauksen avaamiseen tarvitaan jokin tietty ohjelmisto, jota vastaanottajalla ei ole. Toisessa tapauksessa lähettäjä saattaa toimittaa salausavaimen huolimattomasti, esimerkiksi samassa sähköpostiviestissä, jossa salattu liitetiedosto on, jolloin salauksesta ei ole mitään hyötyä, jos viesti kaapataan [14].

Vaikka sähköpostiviestinnän salaaminen on erittäin tärkeää, ja joissakin tapauksissa jopa laki sitä määrää, on se osoittautunut pelkkien avoimien standardien avulla olevan liian vaivalloista suhteessa salaamattoman viestin lähettämiseen. Avoimien standardien rinnalle on tullut runsaasti erilaisia tuotteita. Bruce Scheierin tiimin raportin mukaan vuonna 2016 sähköpostin salaustuotteita oli noin 90 ja muun viestinnän salaustuotteita noin 200 [14].

5 CISCO ESA

Cisco ESA on Ciscon sähköpostinsuodatusjärjestelmä ja se toimii yhdyskäytävänä yrityksen sähköpostipalvelimen ja Internetin välillä. ESA on suunniteltu tunnistamaan ja estämään monenlaisia sähköpostin välittämiä uhkia, kuten haittaohjelmia, roskapostia ja tietojenkalastelua. Lisäksi järjestelmän avulla voidaan varmistaa lähtevän sähköpostiliikenteen eheys, esimerkiksi digitaalisella allekirjoituksella tai sähköpostiviestin salaamisella. Kuten on jo aikaisemmin mainittu, nykyään suurimmassa osassa verkossa tehtävistä hyökkäyksistä työkaluna käytetään sähköpostia, joten Cisco ESA:n tapaisista tuotteista on tullut lähes välttämättömiä kaiken kokoisille yrityksille.

5.1 ESA -tuotteet

ESA on saatavilla neljällä eri toteutuksella: paikallisesti, virtuaalisesti, pilvipalveluna sekä hybridinä. Kaikilla vaihtoehdoilla on yksinkertainen lähestymistapa toteutukseen, ja jokaisella toteutuksella järjestelmä voidaan ottaa käyttöön myös monimutkaisemmissa ympäristöissä.

Jokaisessa toteutuksessa ohjelmistoa ajetaan vähintään kahdella palvelimella, jotka ovat klusteroitu. Klusteroinnilla tavoitellaan kahta asiaa, toinen on vikasietoisuus, jonka ansiosta järjestelmä on käytettävissä, vaikka yhteen palvelimista tulisi vika. Lisäksi klusteroinnilla voidaan säätää palvelimien kuormitusta.

5.1.1 Paikallinen toteutus (On-premises)

Paikallisessa toteutuksessa on käytössä fyysinen ESA-palvelin, joka tyypillisesti asennetaan yrityksen palomuurin ulkopuolelle eli ns. demilitarisoidulle alueelle. Saapuva SMTP-liikenne ohjataan ESA-palvelimelle MX-tietueiden avulla. Laite suodattaa saapuvat sähköpostiviestit, ja välittää hyväksytyt viestit uudelleen ohjattuina yrityksen sähköpostipalvelimelle. ESA ohjaa myös ulospäin kulkevan sähköpostiliikenteen, jossa se käsittelee viestit sille määriteltyjen käytäntöjen mukaisesti. Tällainen määritys voisi olla esimerkiksi sähköpostiviestin digitaalinen allekirjoitus. [15] Palvelimista on saatavilla useampaa eri versiota, jotka ovat listattuna **Virhe. Viitteen lähdettä ei löytynyt.**

Taulukko 1. Saatavilla olevat ESA-palvelimet

	Model	Disk Space	Raid Mirroring	Memory	CPUs
Large enterprise	ESA C695	4.8 TB (600 x 8)	Yes (RAID 10)	32 GB DDR4	1 x 2.6 GHz, 12 core
Large enterprise	ESA C690	2.4 TB (600 x 4)	Yes (RAID 10)	32 GB DDR4	2 x 2.4 GHz, 12 core
Medium-sized enterprise	ESA C395	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB DDR4	1 x 2.1 GHz, 12 core
Medium-sized enterprise	ESA C390	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB DDR4	1 x 2.4 GHz, 6 core
Small to midsize businesses or branch offices	ESA C195	1.2 TB (600 x 2)	Yes (RAID 1)	16 GB DDR4	1 x 2.1 GHz, 8 core
Small to midsize businesses or branch offices	ESA C190	1.2 TB (600 x 2)	Yes (RAID 1)	8 GB DDR4	1 x 1.9 GHz, 6 core

Kaikilla palvelimilla on käytössä sama ohjelmisto, sekä niihin on saatavilla kaikki ominaisuudet. Mallien erot tulevat fyysisestä laitteistosta, kuten suorittimen laskentatehosta, muistin määrässä, levytilan koosta ja sen raid-modista, sekä verkkokorttien määrästä. [16]

5.1.2 Virtualisointi

Virtuaalisessa toteutuksessa ESA-palvelimia kutsutaan ESAV-palvelimiksi. Palvelua voidaan ajaa esimerkiksi virtuaalisella VMware ympäristössä, jota ajetaan fyysisellä Cisco UCS-palvelimella. Palvelu ei kuitenkaan ole riippuvainen ainoastaan Ciscon palvelimista, vaan sitä voidaan ajaa myös muiden valmistajien laitteilla. Myös virtuaalisia palvelimia on useampaa eri versiota, ja ne ovat listattuna.

Taulukko 2. Saatavilla olevat ESAV-palvelimet

	Model	Disk	Memory	Cores
Evaluations only	ESAV C000v	200 GB (10K RPM SAS)	4 GB	1 (2.7 GHz)
Small enterprise (up to 1000 employees)	ESAV C100v	200 GB (10K RPM SAS)	6 GB	2 (2.7 GHz)
Medium-sized enterprise (up to 5000 employees)	ESAV C300v	500 GB (10K RPM SAS)	8 GB	4 (2.7 GHz)
Large enterprise or service provider	ESAV C600v	500 GB (10K RPM SAS)	8 GB	8 (2.7 GHz)
Servers				
Cisco UCS Cisco UCS	VMware ESXi 6.0 and 6.5 Hypervisor			

Myös virtualisoituna kaikki palvelut ja ominaisuudet ovat käytössä mallista riippumatta ja erot mallien välillä ovat ainoastaan suorittimen laskentatehossa, muistin määrästä ja levytilan koosta.

5.1.3 Pilvipalvelut

Pilvipalvelussa käytetään samaa ohjelmistoa kuin paikallisessa ja virtuaalisessa toteutuksessa, mutta palvelimet tarjoaa Cisco, ja ne eivät sijaitse yrityksen omassa infrastruktuurissa vaan Ciscon datakeskuksessa. Tämä auttaa yritystä vähentämään kustannuksia, koska paikallista sähköpostiturvallisuusinfrastruktuuria ei tarvita. Palvelun käyttöönotto on yksinkertaista, koska se on kaikenkattava sisältäen ohjelmiston, laskentatehon sekä tuen [15].

5.1.4 Hybridi

Järjestelmän toteutuksessa voidaan hyödyntää myös useampaa eri mallia, kuten esimerkiksi paikallista ja pilvi toteutusta. Tätä kutsutaan hybridiksi, ja se on kaikkein joustavin ratkaisu. Yritys voi esimerkiksi käyttää ESA:n pilviominaisuutta suojatakseen saapuvan sähköpostiliikenteen, ja samalla hallita lähtevän sähköpostivirran eheyttä paikallisella toteutuksella. Yritys vois myös käyttää samaan aikaan sekä paikallista, että virtuaalista toteutusta. Tätä voidaan hyödyntää tilanteissa, jossa esimerkiksi yrityksellä on pääkonttorin lisäksi pienempiä toimistoja. Näin saadaan samat suojaukset myös pienempiin toimistoihin ilman fyysisiä laitteita tai asennuksia [15].

5.2 Ominaisuudet

Cisco ESA käyttää useampaa eri kerrosta tarjotakseen parhaan mahdollisen sähköpostiturvan, joka sisältää ennaltaehkäiseviä ja reaktiivisia toimenpiteitä, joilla pyritään vahvistamaan puolustautumista.

Globaali uhkatiedustelu (engl. Global threat intelligence) tarjoaa kattavan sähköpostisuojauksen, jota tukee Ciscon Talos ryhmä. Talos on yksi maailman suurimpia uhkia tiedusteleva ryhmä. Se tarjoaa 24 tunnin näkymän globaaliin sähköpostiliikenteeseen. Talos analysoi poikkeavuuksia, paljastaa uusia uhkia ja seuraa sähköpostiliikenteen kehitystä. Talos myös auttaa estämään ns. nolla-tunti (engl. zero hour) uhkia luomalla jatkuvasti sääntöjä, joita jaetaan päivityksinä asiakkaiden sähköpostiratkaisuihin. Päivityksiä saadaan noin kolmen minuutin välein.[15] Nolla-tunti uhilla tarkoitetaan uhkia, joissa hyväksikäytetään haavoittuvuuksia, joista kehittäjät eivät ole tietoisia, ja näin ollen uhkiin ei ole olemassa tietoturvakorjauksia. Termi saa nimensä siitä, että haavoittuvuutta käytetään ennen ensimmäistä tuntia, kun kehittäjät ovat tietoisia uhasta.

Maineen suodatin (engl. reputation filtering) estää ei-toivottuja sähköpostiviestejä huonomaineisista lähteistä, joka perustuu Taloksen uhkatietoihin. Jokaiselle upotetulle hyperlinkille suoritetaan tarkistus. Huonomaineiset verkkosivustot estetään automaattisesti. Maineen suodatus pysäyttää noin 90 % roskapostista, ennen kuin se saavuttaa yrityksen verkon [15].

Roskaposti suojauksen (engl. spam protection) avulla Cisco estää roskapostia, hyödyntäen monikerroksista skannaus arkkitehtuuria, jonka ansiosta yli 99 % roskapostista onnistutaan estämään, kuitenkin false-positiven ollessa vähemmän kuin yksi miljoonasta. ESA:n roskapostitoiminnot käyttävät Cisco Context Adaptive Scanning Engine (CASE) -sovellusta. CASE tutkii koko viestin kontekstin, mukaan lukien mitä sisältöä viestissä on, kuinka viesti on rakennettu, kuka on viestin lähettänyt ja mitä toimia viesti pyytää vastaanottajaa tekemään [15].

Väärennetyn sähköpostin havaitseminen (engl. forged email detection) pyrkii antamaan suojaa BEC-hyökkäyksiltä, jotka kohdistuvat yrityksen avainhenkilöihin, kuten johtoon tai hallintoon. Se auttaa estämään räätälöidyt hyökkäykset ja tarjoaa yksityiskohtaiset lokit kaikista yrityksistä ja suoritetuista toimista [15].

Cisco tietojenkalastelun edistyksellinen suojaus (engl. Cisco Advanced Phising Protection) estää identiteettipetoksiin perustuvia hyökkäyksiä, kuten käyttäjän manipulointiin, toiseksi tekeytymiseen ja BEC -huijaukset, yhdistämällä Talos ryhmän keräämät uhkatiedot, paikalliset sähköpostitiedustelut ja edistyneitä koneoppimistekniikoita. Tällä pyritään mallintamaan luotettavaa sähköpostikäyttäytymistä Internetissä sekä organisaatioiden, että henkilöiden välillä [15].

Cisco verkkoalue suojaus (engl. Cisco Domain Protection) estää huijareita lähettämästä yrityksen domainilla kalasteluviestejä. CDP automatisoi DMARC -sähköpostitunnistusstandardin käyttöönottoprosessin, jonka ansiosta työntekijät, asiakkaat ja toimittajat voidaan suojata paremmin. Tämä suojaa yritysten brändiä, ja lisää sähköpostimarkkinoinnin tehokkuutta vähentämällä tietojenkalasteluviestin perille pääsyä [15].

Harmaanpostin havaitseminen ja turvallinen tilauksen peruuttaminen (engl. Graymail detection and safe unsubscribe) tunnistaa, luokittelee ja valvoo yritykseen saapuvaa harmaatapostia. Harmaaposti koostuu markkinoinnista, sosiaalisesta verkosta ja joukkoviesteistä. Kun viesti on tunnistettu ja luokiteltu, järjestelmävalvoja voi ryhtyä asianmukaisiin toimenpiteisiin koskien jokaista kategoriaa. Usein viesti on uutiskirje, josta löytyy linkki uutiskirjeen tilauksen peruutukseen. Tilausmekanismin jäljitteleminen on suosittu tietojenkalastelumekanismi, ja tästä syystä käyttäjien tulee olla varovaisia, kun he klikkaavat linkkejä. Turvallisen tilauksen peruutus -ominaisuus tarjoaa suojaa uhilta, jotka naamioidaan tilausten peruutus linkeiksi [15].

Ciscon edistynyt haittaohjelma suojaus (engl. Cisco Advanced Malware Protection) ja Cisco uhkaverkko (Cisco Threat Grid) on erillinen palvelu, joka voidaan integroida ESA:an. Se yhdistää staattisen ja dynaamisen haittaohjelma-analysoinnin yhdeksi yhtenäiseksi ratkaisuksi. Nykyisillä tietoturvatekniikoilla se yhdistää reaaliaikaisen käyttäytymisanalysoinnin ja modernin uhkatiedustelun, joka antaa yritykselle suojaa sekä tunnetuista, että tuntemattomilta hyökkäyksiltä. [15]

URL-osoitteisiin liittyvä suojaus ja hallinta suojaa käyttäjiä haitallisilta URL-osoitteilta URL-suojauksella, liitteiden skannauksella ja hallinnoiduilla, eli lyhennetyillä URL-osoitteilla. Viesteihin sovelletaan käytäntöjä, joita on määritelty URL-osoitteiden maineen tai luokan perusteella. [15]

Cisco ESA:an on mahdollista integroida kahta eri virustorjuntaohjelmaa: Sophos ja McAfee. Yleiset määritykset ovat samankaltaiset molemmilla vaihtoehdoilla.[14] Integroimalla

virustorjunta oletusyhdyskäytävään, ESA:n avulla yritys voi toteuttaa monikerroksisen virussuojauksen [15].

Uhkasuodatus auttaa puolustautumaan kasvavia uhkia, sekä sekoitettuja hyökkäyksiä vastaan. Erilaisia sääntöjä voidaan luoda yhdistelemällä parametreja, kuten tiedoston tyyppi, nimi, koko ja URL-osoite. Suodattimet voivat kirjoittaa epäilyttäviin viesteihin linkitetyt URL-osoitteet uudelleen, ja kun käyttäjä klikkaa osoitetta, linkki ohjaa käyttäjän verkkosivustolle Cisco Web Security -palvelimen kautta. Verkkosivuston sisältö tarkistetaan ja suodatin näyttää käyttäjälle estoikkunan, mikäli sivusto sisältää haittaohjelman [15].

Web-vuorovaikutuksen seuranta on kokonaisuudessaan integroitu ominaisuus, jonka avulla järjestelmänvalvojat voivat seurata loppukäyttäjiä, jotka ovat klikanneet URL -linkkiä, jonka ESA on uudelleenkirjoittanut. Raportti ilmoittaa käyttäjät, jotka klikkaavat eniten haitallisia URL-linkkejä, sekä suosituimmat URL-linkit joita käyttäjät ovat klikanneet. Lisäksi järjestelmävalvoja saa tietää ajankohdan, syyn ja toimenpiteet, joita URL -linkille on tehty [15].

Lähtevien sähköpostiviestien suojaus onnistuu Cisco Email Security DLP:llä. Sen ansiosta yrityksen on helppo noudattaa maailmanlaajuisia määräyksiä, ja estää luottamuksellisen tiedon vuotamista. Valittavissa on yli sata määritystä, jotka kattavat valtion, yksityisen sektorin ja yrityskohtaiset määräykset. Ennalta määritetyt DLP käytännöt sisältyvät ESA:an, joka helpottaa niiden soveltamista [15].

Cisco ESA mahdollistaa lähettäjän hallita viestin sisältöä jopa viestin lähettämisen jälkeen. Sähköpostin salauksella lähettäjän ei tarvitse pelätä väärin kirjoitettua vastaanottajan osoitetta tai virheitä viestin sisällössä, koska he voivat lukita viestin koska tahansa. Salatun viestin lähettäjä saa vahvistuksen heti, kun vastaanottaja on avannut viestin. Mikäli vastaanottaja lähettää viestin eteenpäin, viesti salataan automaattisesti. Turvallisuuden parantamiseksi viestin sisältö kulkee suoraan ESA järjestelmästä vastaanottajalle ja vain salausavain tallennetaan pilveen. ESA:n salaus täyttää salausvaatimukset säädöksille kuten Payment Card Indutry Data Security Standard (PCI DSS), Health Insurance Portability And Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX) sekä eurooppalaisen direktiivin [15].

5.3 Hallinta

Kaikissa ESA laitteistoissa pyörii sama AsyncOS, joka on koottu ohjelmistokokonaisuus. Se sisältää käyttöjärjestelmän, laiteajurit, muistin hallinnan, prosessien aikataulut ja kaikki sovellukset. ESA:n hallinta tapahtuu pääasiallisesti web-pohjaisella graafisella käyttöliittymällä ja yhteyden muodostaminen tapahtuu HTTPS-protokolalla. AsyncOS sisältää myös komentorivipohjaisen käyttöliittymän, johon yhdistäminen tapahtuu SSH-yhteydellä. Komentorivipohjaisella käyttöliittymällä voidaan suorittaa melkein kaikki samat toiminnot, kuin graafisella käyttöliittymällä.[16] Lisäksi ainoastaan SSH:lla voidaan luoda ja muokata viesti suodattimia. Kolmas yhteys on FTP-yhteys, jolla voidaan hakea lokitiedostoja ja päivittää lisenssejä.

6 CISCO ESA -KÄYTTÖÖNOTTOPROJEKTI

Tässä luvussa asiakasyritykselle otetaan käyttöön Cisco ESA järjestelmä. Asiakkaalla oli tarve siirtyä kehittyneempään sähköpostisuodatusjärjestelmään, ja tähän Cisco ESA oli hyvä ratkaisu. Järjestelmä otetaan käyttöön kahdella jo olemassa olevalla Cisco ESAV C300 -palvelimella, joissa on myös muita asiakkaita. Työ suoritettiin projektina ja projektiin kuului lisäksi ohjaajani ja asiakasyrityksen yhteyshenkilö. Lisäksi yrityksen ESA pääkäyttäjä avusti teknisissä ongelmissa. Roolini oli suorittaa käyttöönotto, informoida asiakasyrityksen yhteyshenkilöä muutoksista, sekä projektin etenemisestä ohjaajani tukemana. Lisäksi projektin aikana päivitettiin yrityksemme nykyisiä ESA ohjeita.

6.1 Valmistelut

Ensimmäisenä tehtiin toimintasuunnitelman projektille. Etukäteen oli tiedossa, että asiakas käyttää Microsoft Office 365 -palvelua sähköpostiviestinnässä. Valmisteluissa tuli huomioida myös pääsy DNS-hallintaan, selvittää kaikki sähköpostia lähettävät järjestelmät, jotka lähettävät sähköpostia O365 ulkopuolelta, ottaa talteen kaikki sähköpostiin liittyvät DNS-tietueet sekä hankkia tiedotuskanava, jota pitkin asiakkaille voitaisiin lähettää tiedotteita. DNS-hallintaan oli valmiiksi pääsy, ja muihin kysymyksiin saataisiin vastaus aloituspalaverissa joka, käydään asiakkaan kanssa.

Toimintasuunnitelmassa oli jokaiselle viikolle merkattu, että mitä toimenpiteitä kyseisellä viikolla tehdään. Aikatauluksi projektille tuli 4–5 viikkoa ja työtunteja kahden työpäivän verran. Tämä suunnitelma käydään läpi asiakkaan yhteyshenkilön kanssa aloituspalaverissa. Tiedettiin että asiakkaan yhteyshenkilö ei puhu suomea, joten projektin kielenä oli englanti. Tämä oli hyvä huomioida, koska kumpikaan osapuolista ei puhunut omalla äidinkielellä, joten kommunikaatio ongelmia saattaisi tulla. Lisäksi kaikki tapaamiset järjestettiin etänä.

6.2 Aloituspalaveri asiakkaan kanssa

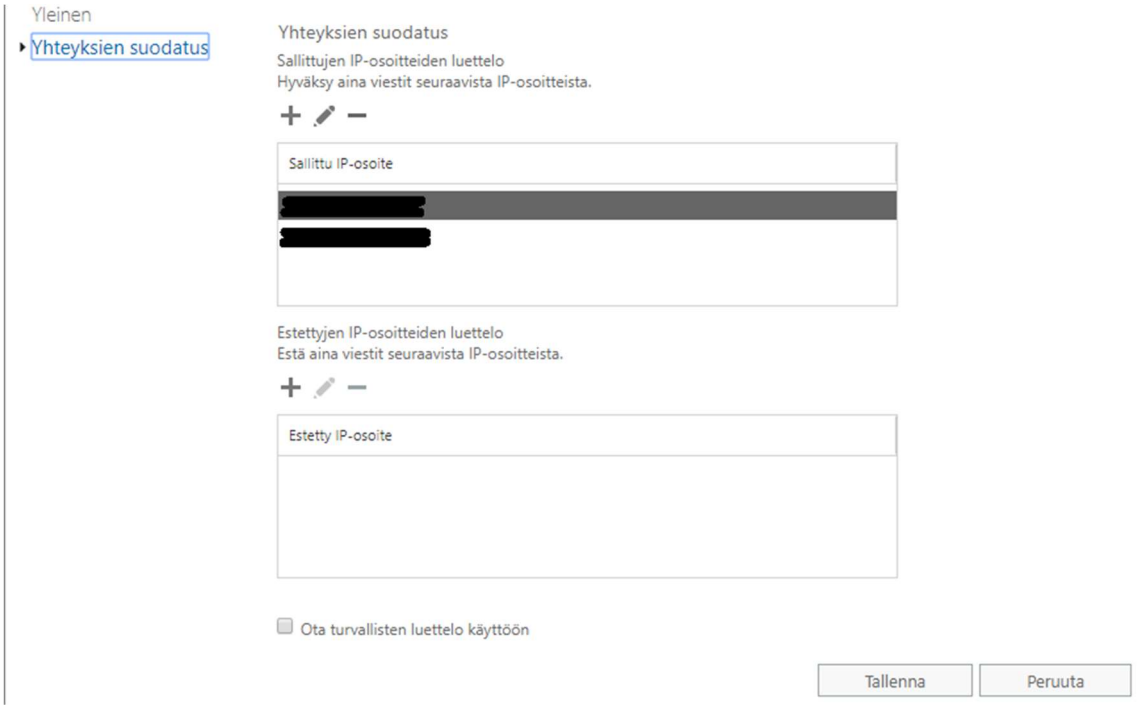
Aloituspalaverin asialistalla oli kertoa asiakkaalle projektin kaikki työvaiheet ja aikataulu. Lisäksi heiltä tarvittiin testaamista varten käyttäjätunnusta heidän O365-järjestelmään. Palaverissa kävi ilmi, että heidän verkkotunnuksella ei lähetetä sähköpostia O365:n

ulkopuolelta, eli käyttöönotossa ei tarvitsisi huomioida muita järjestelmiä. Lisäksi saatiin testitunnuksen, jolla voidaan testata jokaisen muutoksen jälkeen järjestelmän toimivuutta. Asiakkaan kanssa sovittiin, että heille ilmoitettaisiin muutoksien ajankohdasta, ja kun ne olivat tulleet voimaan. Lisäksi heille ilmoitettiin, että loppukäyttäjien ei pitäisi huomata muutoksia, eikä käyttökatkoja olisi tiedossa.

6.3 Cisco ESA:n käyttöönotto

6.3.1 Valmistelut

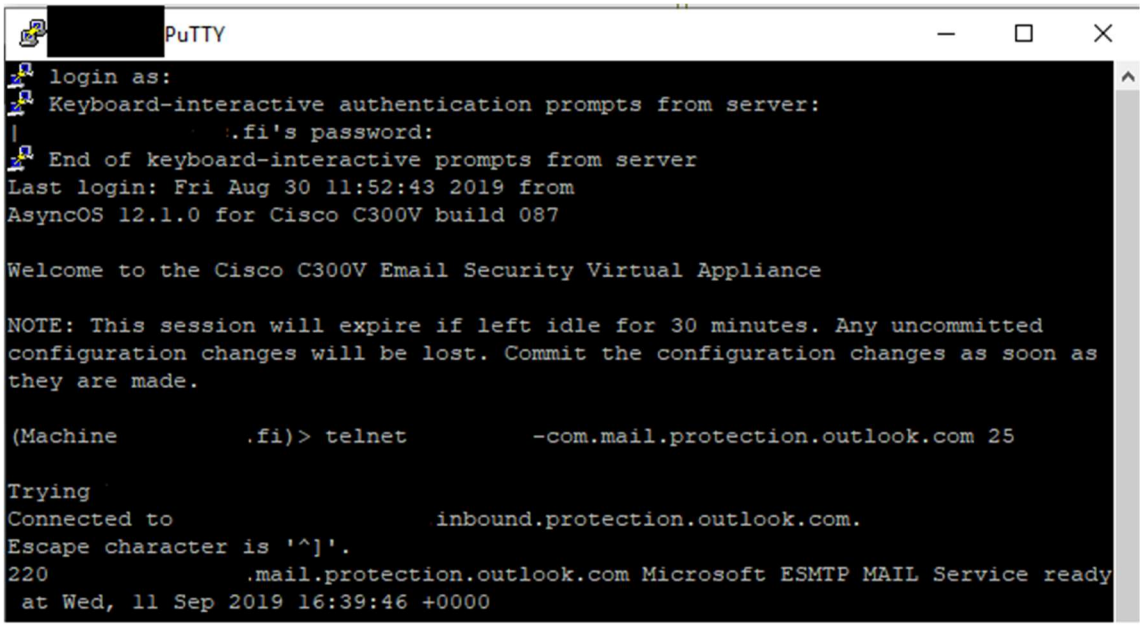
Ensimmäisenä valmisteltiin ESA välittämään asiakkaalle saapuva sähköpostiliikenne asiakkaan O365-järjestelmään. Tämä tapahtui hyväksymällä asiakkaan O365-järjestelmän vastaanottamaan ESA-palvelimilta sähköpostia. Asetukset tehtiin O365 Exchange Online Protection (EOP) Admin Centerissä (Kuva).



Kuva 7. Sallitaan O365 vastaanottamaan sähköpostia ESA:sta

Kun suodattimen sääntö oli tehty, testattiin ESA:n ja O365:n välinen SMTP-yhteys. Tämä tapahtui kirjautumalla ESA-palvelimeen SSH-yhteydellä. Kun ESA -palvelimeen oltiin

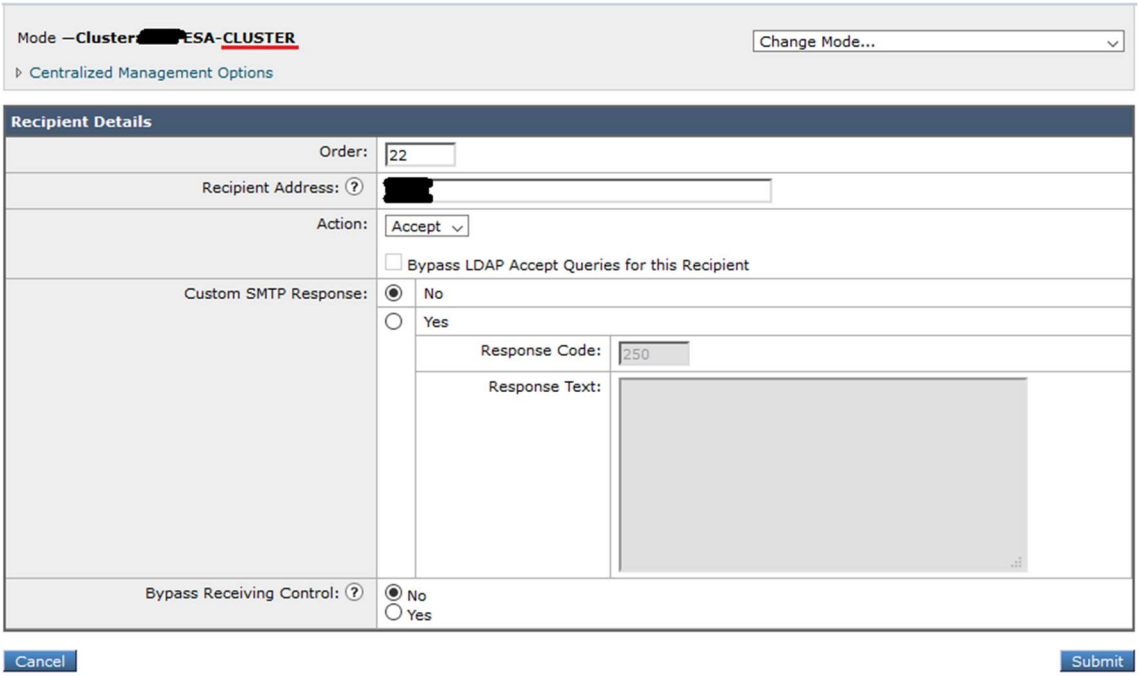
kirjauduttu, sillä otettiin yhteys O365-palvelimelle käyttäen telnet-yhteyttä. Portiksi valittiin portti 25, jota käytetään oletuksena sähköpostiliikenteessä (Kuva)



Kuva 8. ESA:n ja O365:n välisen yhteyden testaus.

Valmisteluiden jälkeen asetettiin ESA välittämään asiakkaalle saapuva sähköpostiliikenne asiakkaan sähköpostipalvelimelle. ESA -järjestelmään kirjauduttiin tällä kertaa graafiseen web-käyttöliittymään käyttäen HTTPS -protokollaa. Kirjautumisen jälkeen oli varmistettava, että muutokset tehdään klusteri tasolla, eli tehdyt muutokset tulisivat voimaan molemmilla ESA-palvelimilla.

Ensimmäisenä asiakkaan domain lisätään RAT-listaan, joka kertoo, miltä sähköpostidomaineilta ESA ottaa sähköposteja vastaan (Kuva 7).



Kuva 7. Määritetyt RAT asetukset

RAT asetuksessa määritellään seuraavia asioita.

- Order: Järjestysnumero joka kertoo, että missä kohtaa RAT listaa kyseinen domain on. Esimerkissä oleva domain on listalla 22:na
- Recipient Addresses: Domain, jolta ESA ottaa vastaan sähköpostia
- Action: Toimenpide joka suoritetaan kyseiseltä domainilta saapuvalle sähköpostille. Esimerkissä ESA hyväksyy sähköpostiviestit domainilta
- Custom SMTP Response: Voidaan määritellä kyseiselle domainille mukautettu SMTP vastaus
- Bypass Receiving Control: Haluttaessa voidaan ohittaa mekanismit, jotka saattavat kuristaa sähköpostiliikennettä

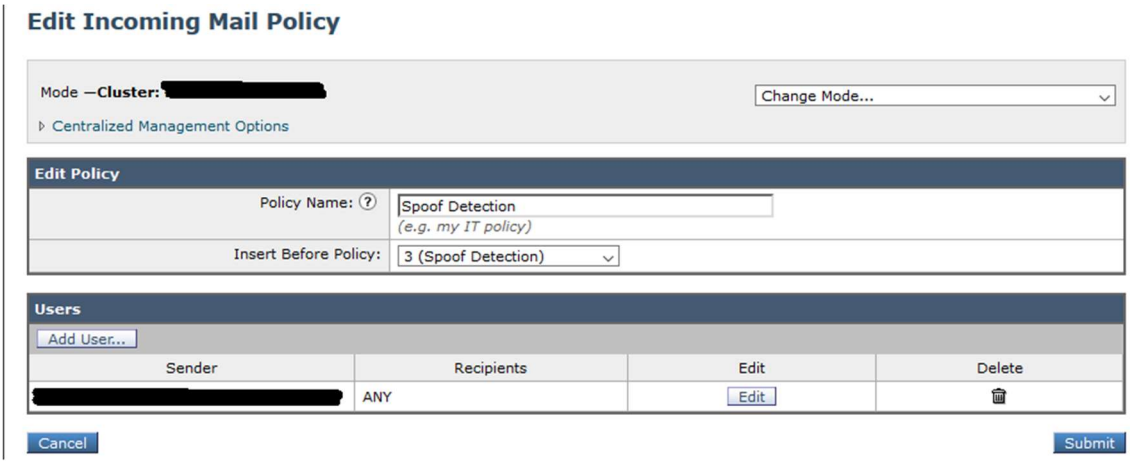
Seuraavaksi lisätään SMTP-reitti, jonka tehtävänä on kertoa, että mihin hyväksytyt viestit välitetään, kun ESA on käsitellyt ne (Kuva 8)

Kuva 8. SMTP-reititys määritykset

SMTP reitityksessä huomattiin seuraavat asiat.

- Receiving domain: Domain joka vastaanottaa viestit ESA:lta
- Destination Hosts: Kohde johon domainille osoitetut sähköpostit ohjataan.
    - Priority: Mikäli kohteita on useampi, tällä arvolla niitä voidaan priorisoida
    - Destination: Viestien vastaanottavan sähköpostijärjestelmän osoite
    - Port: Portti jota viestin kuljettamiseen käytetään

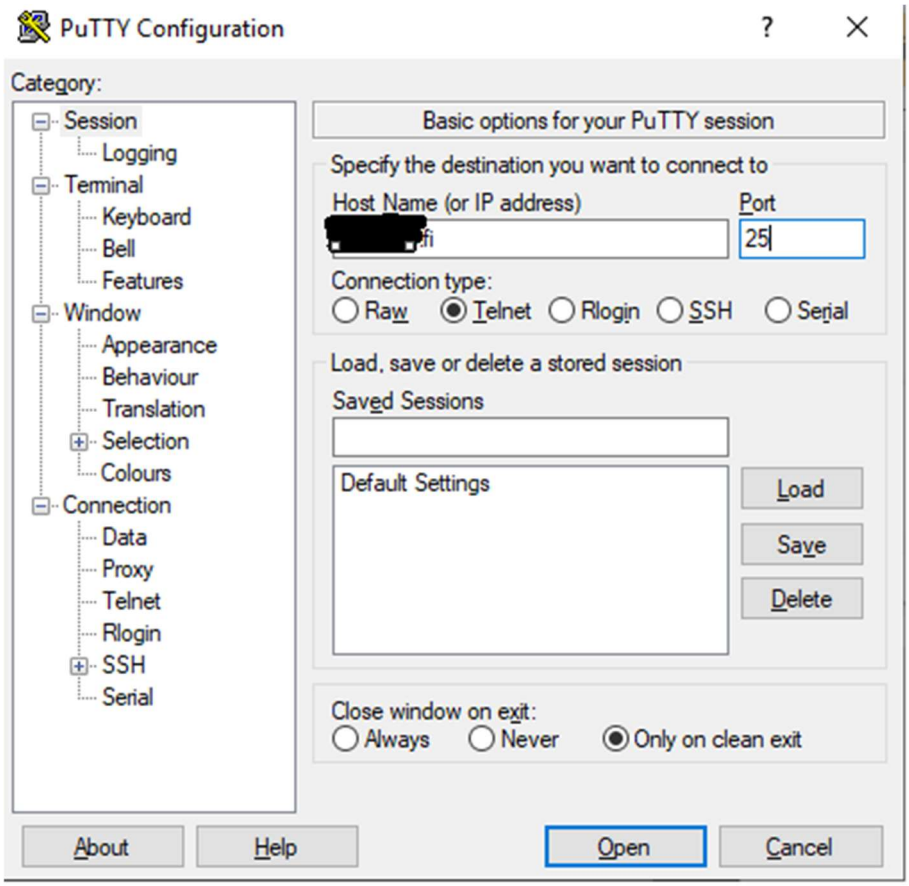
Lisäksi asiakkaan domain lisätään Spoof Detection -listaan, joka toimii tiukennettuna sisältösuodattimena. Erona oletussuodattimeen on se, että ne käsittelevät SPF-käytännöt eri tavalla. Spoof Detection ohjaa kaikki sähköpostit karanteeniin, jotka eivät täytä SPF-määrityksiä, kun taas normaali suodatin siirtää SOFTFAIL-sähköpostit karanteenin lisäksi myös suoraan loppukäyttäjän sähköpostilaatikkoon (Kuva 9).



Kuva 9. Asiakkaan domain lisättiin Spoof Detection -listaan

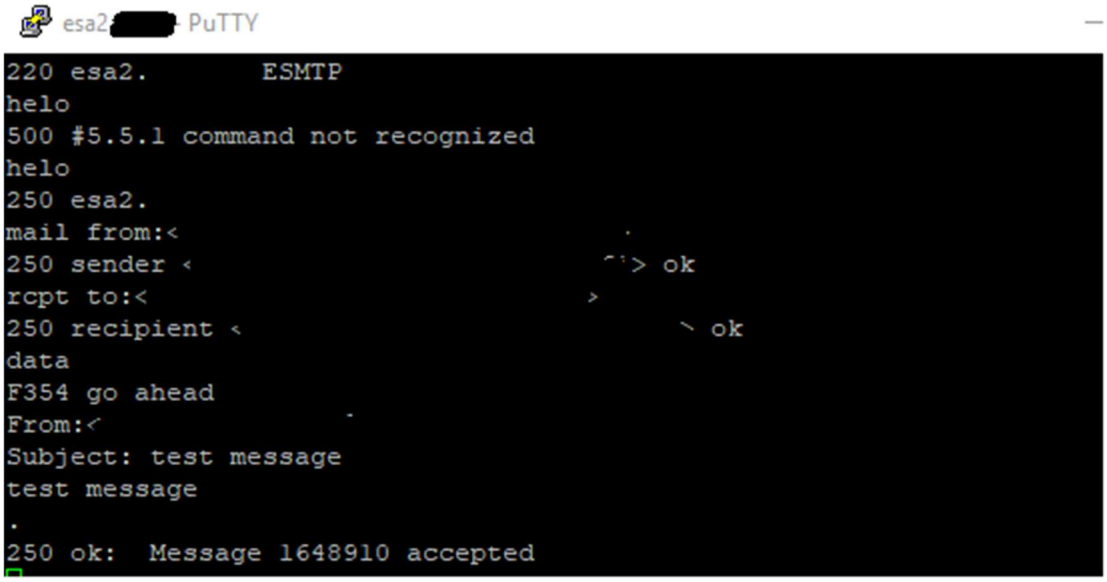
Tämän jälkeen molemmilla ESA-palvelimille suoritettiin testi, jonka tarkoituksena oli varmistaa, että ESA onnistuu välittämään sähköpostia asiakkaan sähköpostijärjestelmään.

Testi toteutettiin ottamalla telnet-yhteys ESA-palvelimeen käyttämällä porttia 25 (Kuva 10).



Kuva 10. ESA-palvelimen telnet-yhteys suoritettiin Puttyn avulla

Testissä lähetettiin sähköpostiviesti domainin ulkopuolisesta sähköpostiosoitteesta asiakkaan testitunnuksen sähköpostilaatikkoon (Kuva 11).



Kuva 11. Saapuvan sähköpostiliikenteen testaus

6.3.2 Saapuvan sähköpostiliikenteen yliheitto

Kun varmistui, että ESA:n kautta sähköpostin lähettäminen asiakkaan ympäristöön onnistuu, ja asiakkaan O365-järjestelmä vastaanottaa ESA:lta tulevat sähköpostiviestit, oli vuorossa saapuvan sähköpostin yliheitto. Yliheitosta ilmoitettiin etukäteen koko asiakasyrityksen henkilökunnalle, jotta mahdollisiin häiriöihin osattaisiin varautua. Kuitenkin oletuksena oli, että käyttökatkoja loppukäyttäjille ei olisi tulossa. Yliheitossa DNS-hallinnassa muokattiin yrityksen sähköpostiliikenteeseen viittaavat DNS-tietueet siten, että kaikki yritykseen saapuva sähköpostiliikenne ohjataan ESA:an, joka välittää viestit yrityksen sähköpostipalvelimelle.

Ennen yliheittoa oli varmistettava, että asiakkaan kaikkien DNS-tietueiden TTL-arvot olivat asetettu mahdollisimman matalaksi, jotta niihin tehtävät muutokset tulevat voimaan mahdollisimman nopeasti. Suositeltavat TTL-arvot ovat välillä 60 sekunnista 3600 sekuntiin. Lisäksi vanhat DNS-tietueet otettiin talteen siltä varalta, että ongelmatilanteessa muutokset voitaisiin perua. Yliheitossa asiakkaan MX-tietueet muutettiin siten, että ne viittasivat ESA -palvelimiin (Kuva 12). Tässä vaiheessa myös SPF-tietue tarkistettiin, että se on samaa muotoa kuin Kuva 2. Muutosten jälkeen odotettiin, että uudet DNS-tietueet päivittyivät julkiseen DNS-palvelimeen. Kun tietueet olivat päivittyneet julkiseen DNS-

palvelimeen, varmistettiin saapuvan sähköpostiliikenteen toimivuus, lähettämällä sähköpostiviestejä yrityksen testitunnuksen sähköpostiin. Testitunnuksen sähköpostilaatikon tarkistuksen lisäksi saapuvan sähköpostiliikenteen toimivuus varmistettiin käyttämällä Cisco ESA:n viestin seuranta (engl. Message Tracking) työkalua, josta voidaan seurata ESA:an kautta kulkevia sähköposteja.

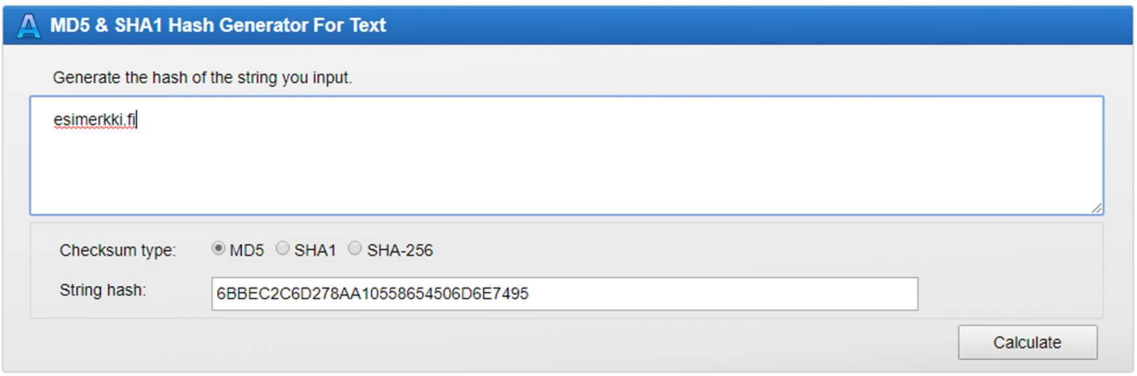
Aluksi yliheiton jälkeen vaikutti siltä, että kaikki saapuvaan sähköpostiliikenteeseen viittaavat asiat olisivat kunnossa. Kuitenkin seuraavana päivänä asiakas ilmoitti, että heidän käyttäjät eivät saa sähköposteja eräältä palvelimelta, joka lähettää automaattisesti sähköpostia yrityksen omille käyttäjille. Selvisi että kyseessä on O365-järjestelmästä irrallaan oleva palvelin, joka lähettää sähköpostia. Käyttäjät eivät saaneet sähköpostiviestejä palvelimelta, koska se ei täyttänyt nykyisen SPF-tietueen määrityksiä. Tämä korjattiin lisäämällä SPF-tietueeseen tunniste, joka viittaa palvelimeen. Muutoksen jälkeen yhteyshenkilö ilmoitti, että vika oli korjaantunut.

Pref	Hostname	IP Address	TTL
10	esa1[redacted]	[redacted]	60 min
20	esa2[redacted]	[redacted]	60 min

Kuva 12. MX-tietueet muutosten jälkeen

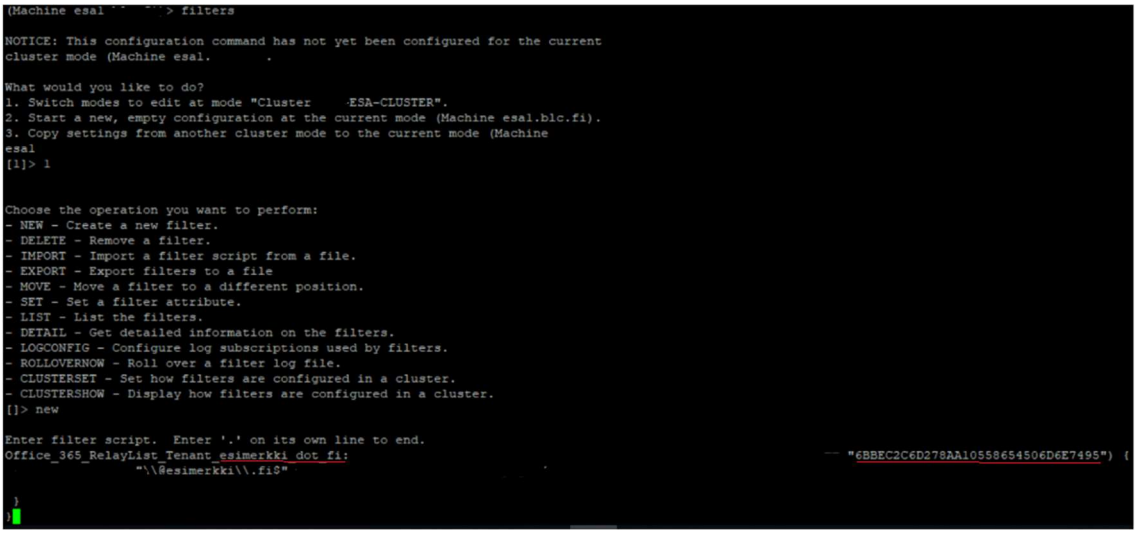
6.3.3 Lähtevän sähköpostiliikenteen valmistelut

Seuraavaksi aloitettiin lähtevän sähköpostiliikenteen suojauksen valmisteluja. Ensimmäisenä ESA-järjestelmään lisätiin suodatin, jolla ESA hyväksyy vastaanottamaan asiakasyrityksen O365-järjestelmästä sähköpostiviestejä. Suodatinta varten tarvitsi tehdä MD5-tarkistussumma. Kuva 13 MD5-tarkistussumman tehtiin http://onlinemd5.com sivuston avulla.



Kuva 13. Esimerkki MD5-tarkistussumman luonnista esimerkki.fi -domainille

Tämän jälkeen luotiin suodatin ESA-järjestelmään. Koska ESA:n graafisella käyttöliittymällä ei voi luoda tai hallita suodattimia, tarvitsi ottaa SSH-yhteys ESA -palvelimeen ja luoda suodatin komentorivipohjaisella käyttöliittymällä. Tämäkin toimenpide tehtiin klusteritasolla, joten seuraavat muutokset tulivat molempiin ESA-palvelimiin (Kuva 14).

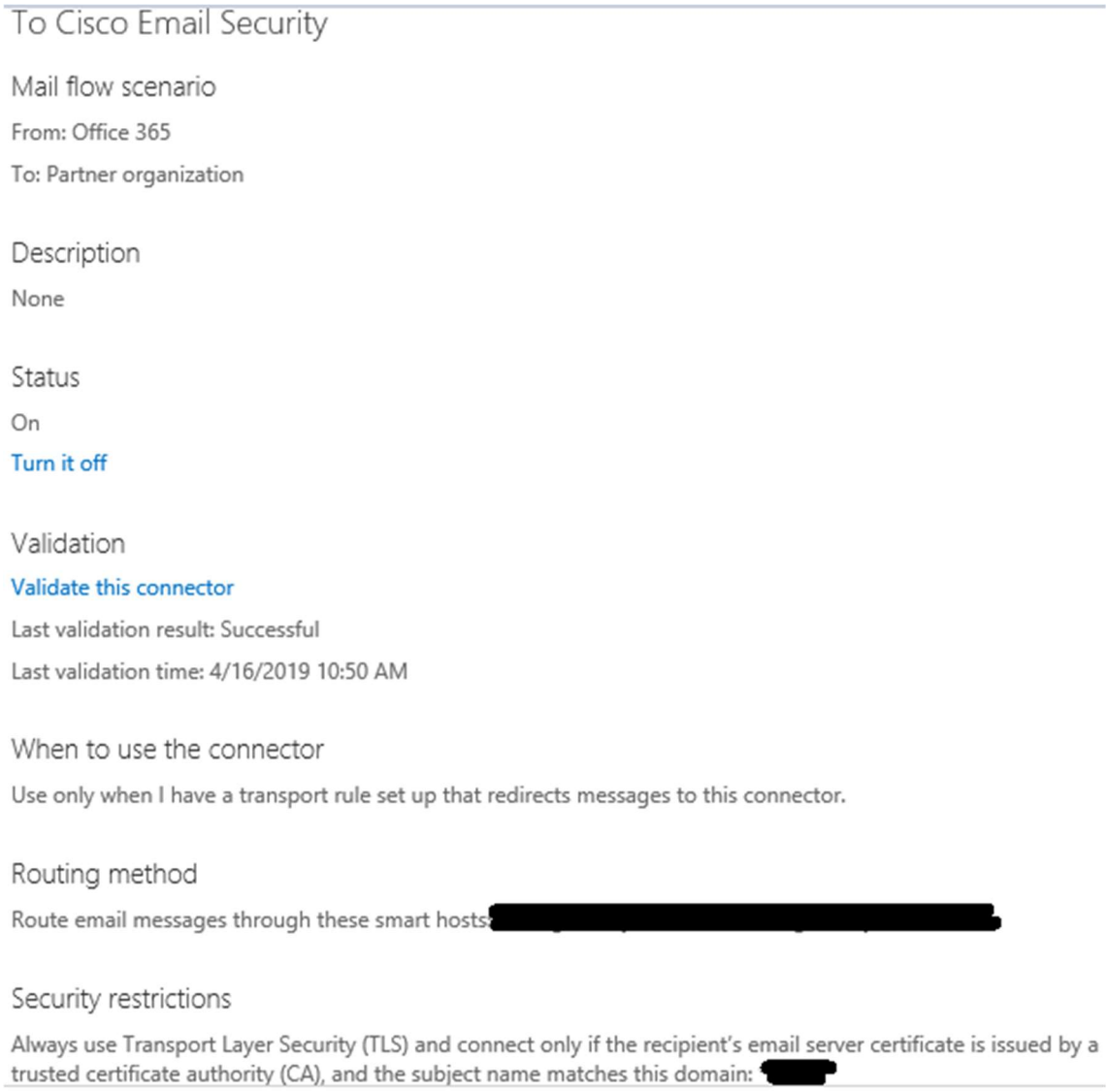


Kuva 14. Esimerkki suodattimen luonnista esimerkki.fi -domainille

Kun suodatin oli luotu, lähetettiin sähköpostiviesti asiakkaan sähköpostista ulkoiseen sähköpostiin, jolla varmistettiin, että ESA vastaanottaa viestejä O365-järjestelmästä.

Testin läpäistyä seuraavaksi oli vuorossa valmistella asiakkaan O365-ympäristö ohjaamaan lähtevä sähköpostiliikenne ESA:n kautta. Tämä tapahtui luomalla yhdistin osoittamaan lähtevä sähköpostiliikenne ESA:een. Yhdistin luotiin O365 EOP Admin

Center:issä, josta avattiin ”mail flow” eli sähköpostivirta ja sieltä ”connectors” eli yhdistimet. Yhdistin luotiin määrityksillä, jotka näkyvät Kuva 15.



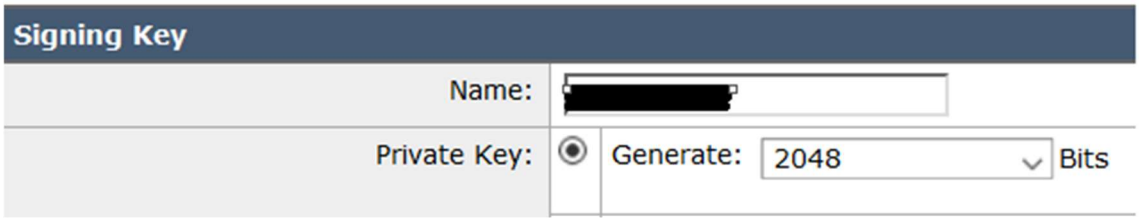
Kuva 15. Lähtevän postin yhdistimen asetukset

Yhdistimessä on määritelty, että viestit lähtevät O365-järjestelmästä kumppaniorganisaatiolle. Yhdistintä käytetään ainoastaan silloin, kun on määritelty kuljetus sääntö, joka ohjaa viestit yhdistimelle. Lisäksi turvallisuus asetuksiin määritetään yhdistin käyttämään aina TLS-salausta, se muodostaa yhteyden ainoastaan, kun vastaanottajan sähköpostipalvelimen varmenteen on myöntänyt luotettu varmenteen myöntäjä ja hakijan nimi vastaa määriteltyä domainia. Lopuksi yhdistimen määrityksen viimeisessä vaiheessa asennus pyysi sähköpostiosoitetta, johon tarvittaisiin pääsy, jotta voidaan varmistaa yhdistimen toiminta.

6.3.4 DNS-tietueiden valmistelu

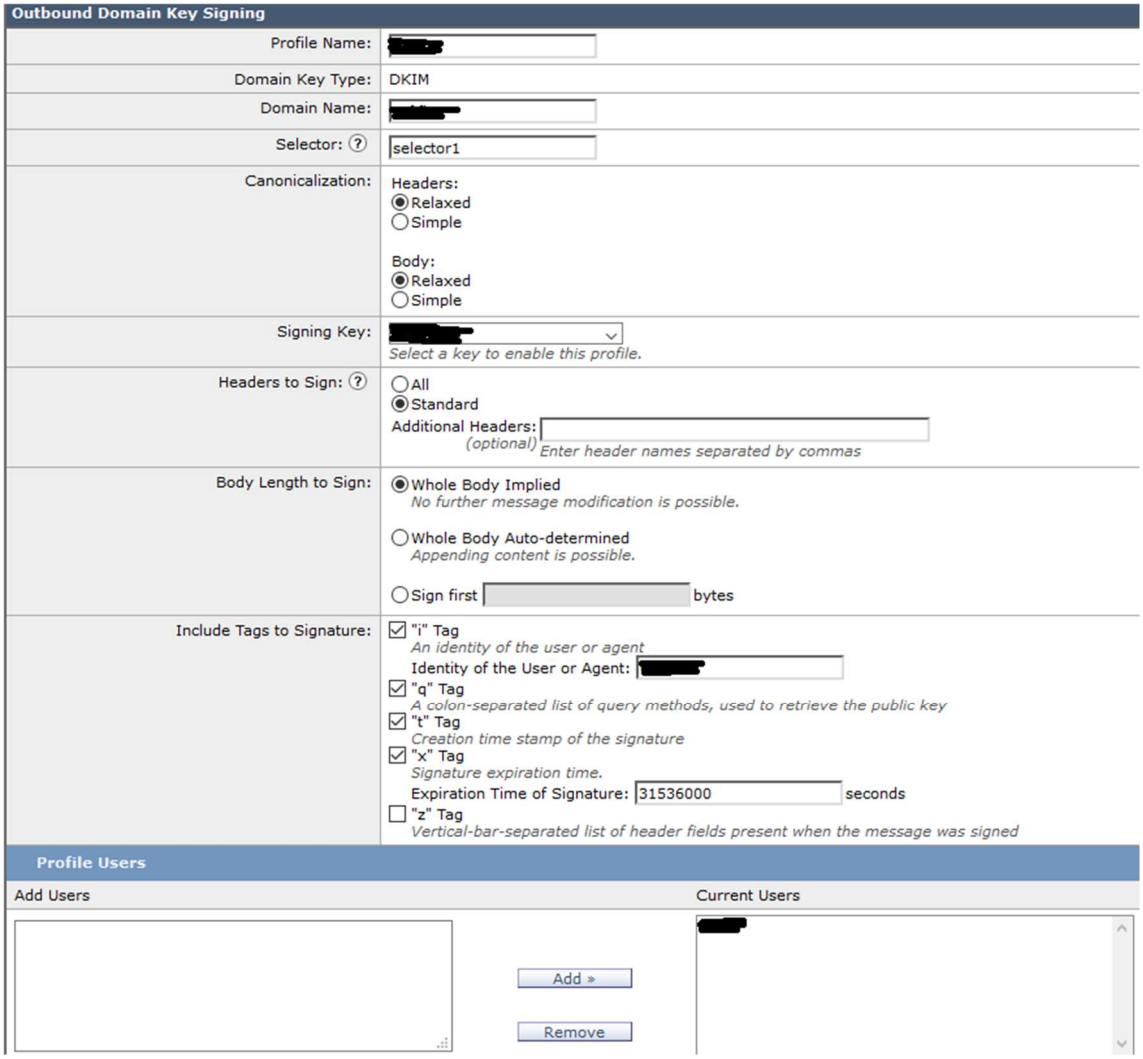
Seuraavaksi valmisteltiin lähtevään sähköpostiliikenteeseen vaikuttavat DNS-tietueet. Koska SPF-tietue oli jo aikaisemmassa yliheitossa asetettu, tämä osuus aloitettiin DKIM-allekirjoituksen määrittelyllä. DKIM-allekirjoituksen tulisi jatkossa tekemään ESA. Aluksi oli tärkeää varmistaa, ettei asiakkaan O365-järjestelmässä ole entuudestaan aktiivista DKIM-allekirjoitusta, joka löytyy EOP Admin Centerin ”protection” asetuksesta. Yleensä kun käytössä on kaksi DKIM-allekirjoitusta, ensimmäinen allekirjoitus hajoaa, koska viesti muuttuu matkalla, kun sähköpostiviestiin tulee myös toinen allekirjoitus, ja tämä voi aiheuttaa ongelmia.

ESA tarjoaa kaikki tarvittavat tiedot DKIM-allekirjoituksen määrittelyä varten. Ensimmäisenä luodaan DKIM-allekirjoitusavain. Tämä tapahtuu ESA-hallinnassa; Mail Polices -> Domain Keys -> Signing Keys. Allekirjoitusavaimelle määriteltiin nimi muodossa esimerkkifi ja avaimen pituudeksi 2048 bittiä (Kuva 16).



Kuva 16. DKIM-allekirjoitusavain

Tämän jälkeen luotiin domainille allekirjoitusprofiili: Mail Polices -> Domain Keys -> Signing Profiles (Kuva 17).



Kuva 17. Domainin DKIM-allekirjoitusprofiili

DKIM-allekirjoitusprofiiliin määriteltiin seuraavasti:

- Profile Name; Profiilin nimi muodossa esimerkkifi
- Domain Key Type; Oletuksena DKIM
- Domain Name; Domain nimi muodossa esimerkki.fi
- Selector; Valitsimien avulla domainilla voi olla samanaikaisesti useampi julkinen avain. Asiakkaalla ei ollut aikaisemmin DKIM-allekirjoitusta käytössä, joten käytimme oletuksena olevaa ”selector1” valitsinta
- Canonicalization; Algoritmi joka määrittää, että kuinka paljon viestiä voidaan muokata matkalla lähettäjältä vastaanottajalle, ilman että DKIM-allekirjoitus

hajoaa. Sekä otsikkoon, että runkoon on suositeltavaa valita ”Relaxed”, koska ”Simple” vaihtoehdolla allekirjoitus hajoaa erittäin herkästi [17]

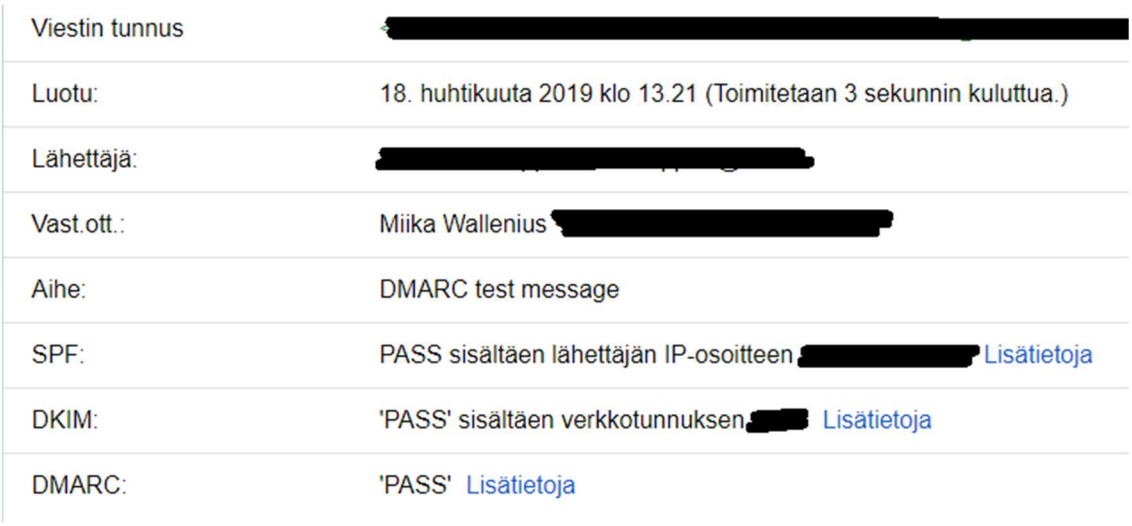
- Signing key; Tähän valittiin Kuva 16 avain
- Headers to Sign; Määritellään otsikot, jotka allekirjoitetaan. Valitussa ”Standard” asetuksessa allekirjoitetaan hyvin tunnetut otsikot. Vaihtoehto ”All” ongelmana on se, että se allekirjoittaa kaikki otsikot, myös ”Return-Path” jota ei tulisi koskaan allekirjoittaa
- Body Length to Sign; Määritellään mikä osa viestin runkoa allekirjoitetaan
- Include Tags to Signature; Tunnisteet joita halutaan allekirjoituksen sisältävän

Kun allekirjoitusprofiili oli luotu, ESA:n avulla generoitiin DKIM-tietue, joka lisättiin julkiseen DNS-palveluun. Kun muutokset olivat päivittyneet, painettiin vielä ”Test” -painiketta, joka ilmoitti, että testi on mennyt onnistuneesti läpi (Kuva 18).

Kuva 18. DKIM-allekirjoitusavain, josta generoitu DKIM-tietue ja suoritettu testi

DKIM-allekirjoituksen jälkeen vuorossa oli DMARC:n käyttöönottaminen. Aluksi varmistettiin, ettei asiakkaalla ole jo valmiiksi käytössä DMARC:a. Ennen DMARC:n määritystä luotiin asiakkaalle käyttäjätunnus DMARCAnalyzer -palveluun, jolla DMARC:n keräämät tiedot analysoidaan. Menettelytavaksi tietueelle asetettiin ”none”, koska aluksi haluttiin ainoastaan kerätä dataa. Lisäksi mahdolliset aliverkkotunnukset noudattivat samaa menettelytapaa. Raportit kerättiin tapauksista, joissa joko SPF tai DKIM epäonnistuvat. Kun kaikki asetukset oli määritetty, palvelu generoi DMARC TXT-tietueen, joka lisättiin julkiseen DNS-palveluun. Kun tiedot olivat päivittyneet, varmistettiin sekä DKIM:in että DMARC:n toimivuus lähettämällä asiakkaan testitunnuksella sähköpostia gmail-sähköpostiosoitteeseen (Kuva 19). Gmail-sähköposti on testaamiseen hyvä työkalu, koska tietueiden toimivuudesta on helppo saada tieto. Tietueiden toimivuuden jälkeen jätettiin DMARC:n toimintatavaksi vielä ”none”, eli epäonnistuneille SPF ja DKIM sähköposteille

ei vielä tehtäisi mitään, vaan DMARC:n tehtävä oli ainoastaan kerätä dataa. Datan keräämiselle oli varattu enintään kaksi viikkoa, aika riippuisi sähköpostiliikenteen määrästä.

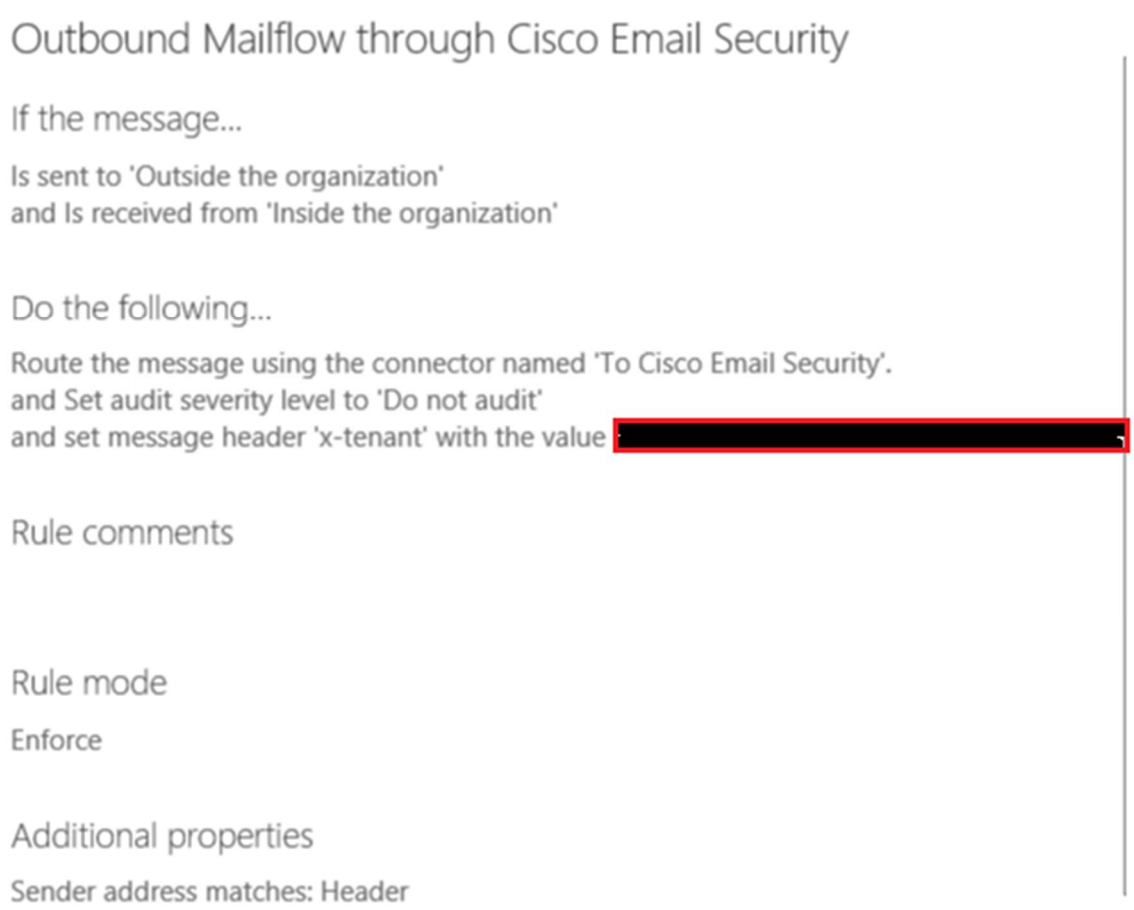


Kuva 19. Testiviestissä todetaan DNS-tietueiden toimivuus

DMARC:n dataa kerätessä huomiota herätti epäonnistuneiden DKIM allekirjoitusten määrä, joka oli erittäin suuri. Asiaa selvitellessä vika löytyi julkisen DNS-palvelun DKIM-tietueen virheellisestä asetuksesta. Asetuksen korjauksen jälkeen lukemat normalisoituivat, ja muita poikkeamia ei havaittu. Tämä kuitenkin hidasti projektin etenemistä, koska datan kerääminen jouduttiin aloittamaan uudelleen korjaamisen jälkeen. Kun tarvittava datamäärä oli kerätty ja todettu, että toimenpiteitä ei tarvita, muutettiin DMARC:n menettelytavaksi ”quarantine”.

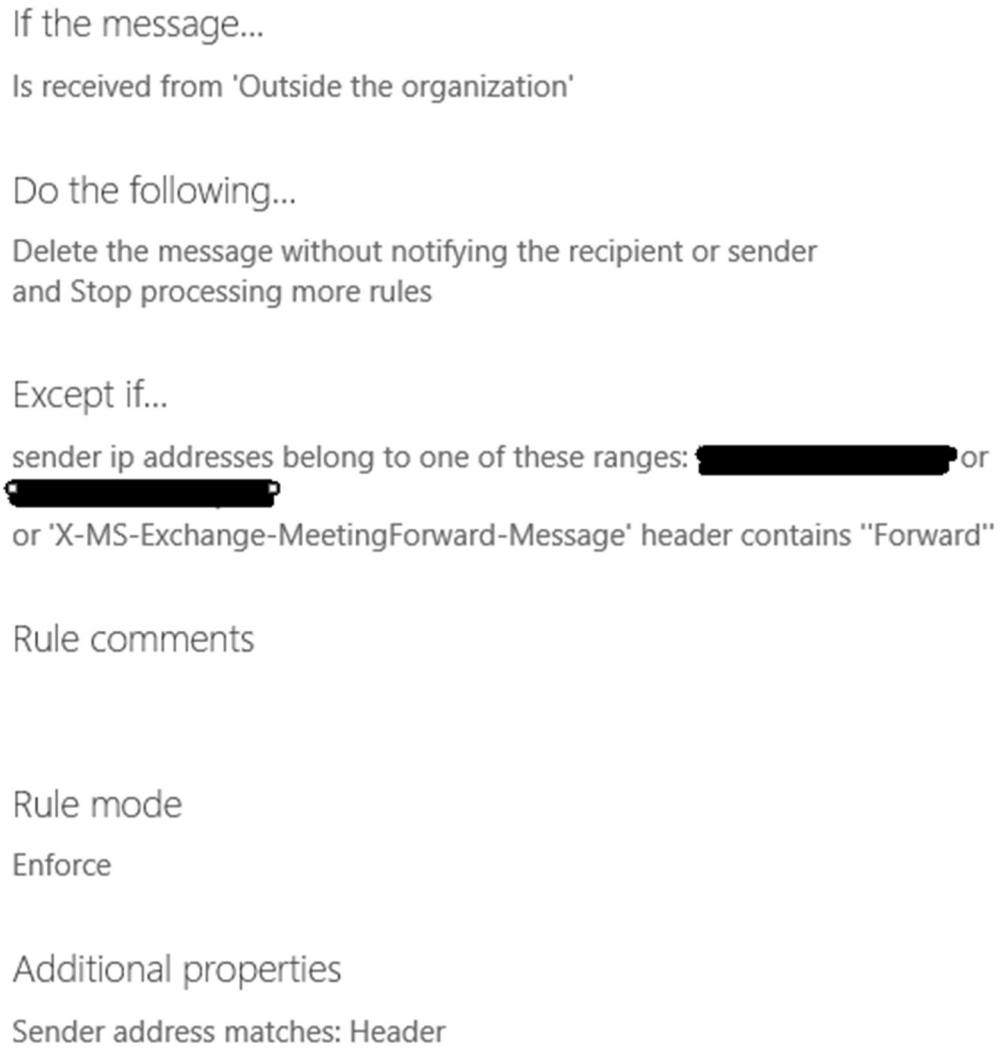
6.3.5 Lähtevän sähköpostiliikenteen yliheitto

DNS-tietueiden valmistelujen jälkeen projektin seuraava vaihe oli lähtevän sähköpostiliikenteen yliheitto. Ensimmäisenä asetettiin asiakkaan O365 toimittamaan kaikki lähtevät sähköpostit ESA:n kautta (Kuva 20). Tämä tapahtui luomalla sähköpostivirtaa koskeva sääntö O365 EOP Admin Centerissä. Sääntöä käytetään silloin, kun palvelimelle saapunut sähköpostiviesti on saapunut organisaation sisältä, ja sen vastaanottaja on organisaation ulkopuolella. Sähköpostiviestin reitittämiseen käytetään Kuva 15 luotua yhdistintä, viestiä ei tarkisteta O365 toimesta ja sähköpostiviestin otsikkoon lisätään x-tenant, jonka arvo on aikaisemmin määritelty MD5-tarkistussumma.



Kuva 20. Sääntö ohjaa kaikki lähtevät sähköpostit ESA:een

Viimeisenä toimenpiteenä estettiin kaikki saapuva sähköpostiliikenne, jota ESA ei ole välittänyt asiakkaan O365-järjestelmään. Myös tämä tapahtuu luomalla sääntö asiakkaan O365-järjestelmään. Sääntöä käytetään, kun sähköpostiviesti saapuu organisaation ulkopuolelta, jolloin viesti poistetaan ilman että siitä ilmoitetaan lähettäjälle tai vastaanottajalle. Poikkeuksena on se, jos sähköpostiviestin lähettäjä on toinen ESA-palvelimista tai kun kalenterikutsun otsikko sisältää ”Forward”. Säännölle annettiin priorisointi arvoksi ”0”, joka tarkoittaa sitä, että se on ensimmäinen sääntö, jonka O365 huomioi (Kuva 21).



Kuva 21. Sääntö estää sähköpostiviestit, jotka eivät ole ESA:n välittämiä

6.4 Lopputoimet ja projektin lopetus

Kun järjestelmän käyttöönotto oli valmis, asiakas ilmoitti hyvin nopeasti, että uusi sähköpostisuodatin oli ehkä liian tiukka, koska järjestelmä oli ohjannut käyttäjälle osoitetun sähköpostiviestin karanteeniin. Tämä yksittäinen sähköpostiviesti ei ollut ongelma, mutta asiakkaalla oli huoli, että tarpeellisia sähköpostiviestejä saattaisi päätyä karanteeniin, mikäli sähköpostisuodattimen määritykset olisivat liian tiukka.

Tutkimisen jälkeen selvisi, että kyseinen sähköpostiviesti oli lähetetty gmail.com -domainista, reply-to eli vastausosoite oli eri kuin osoite, josta viesti oli lähetetty, ja otsikosta päätellen viesti saattoi sisältää liitetiedoston tai linkin. Liitetiedosto tai linkki yksistään ei ohjaisi postia karanteeniin, mutta kun muut tekijät lisätään yhtälöön, oikea toimenpide oli siirtää viesti karanteeniin. Tästä ilmoitettiin käyttäjälle ja yhteyshenkilölle.

Lopuksi pidimme projektin lopetuspalaverin, johon osallistui lisäksi ohjaajani ja asiakasyrityksen yhteyshenkilö, kuten aloituspalaverissa. Palaverissa verrattiin suunniteltua aikataulua ja toteutunutta aikataulua sekä syitä viivästyksille. Projekti oli aikataulutettu kestämään yhteensä viisi viikkoa, mutta todellisuudessa aikataulu melkein tuplaantui. Osittain tämän selittivät SPF-tietueen ongelmat erillisen palvelimen kanssa sekä DMARC:n käyttöönoton aikana havaittuun virheeseen DKIM-määrityksissä. Kävimme myös läpi mitä osapuolet ovat projektista oppineet. Tulevaisuudessa DMARC:n datan keräämiselle on varattava enemmän aikaa, koska tässä projektissa ei oltu varattu aikaa sille, että dataa jouduttaisiin keräämään uudestaan testissä havaitun virheen takia. Positiivisia asioita oli kommunikaatio asiakkaan kanssa, ja että DNS muutokset saatiin nopeasti suoritettua. Vaikka projektin aikataulu venyi runsaasti, asiakas oli erittäin tyytyväinen sekä tekniseen toteutukseen, että projektin hallintaan ja aikataulutukseen. Tämä johtuu todennäköisesti siitä, että käyttökatkoja ei juurikaan syntynyt ja että kaikista suunnitelmista ja toimista ilmoitettiin asiakkaalle hyvissä ajoin.

7 YHTEENVETO

Opinnäytetyön toimeksiantona oli parantaa asiakasyrityksen sähköpostiliikenteen tietoturvaa ottamalla käyttöön Cisco ESA -järjestelmä. Tavoitteena opinnäytetyössä oli selvittää, miksi Cisco ESA:n kaltaisia järjestelmiä tarvitaan, sekä ottaa järjestelmä onnistuneesti käyttöön. Opinnäytetyössä käy ilmi selkeästi sähköpostin nykyinen asema, historia, tekninen toimintaperiaate, siihen liittyvät uhat ja se, kuinka näitä uhkia vastaan voidaan puolustautua. Lisäksi ennen käyttöönottoa tutustuttiin Cisco ESA -tuotteen toimintaan ja ominaisuuksiin.

Lähes jokaisella Internetin käyttäjällä on sähköpostitili. Voisi kuvitella, että pikaviestintäpalvelut ja sosiaalisen median suosion myötä sähköpostin käyttö olisi vähentynyt. Näin ei kuitenkaan ole, vaan nämä palvelut ovat tulleet sähköpostiviestinnän rinnalle. Vuosien aikana sähköpostiviestintä on integroitunut niin vahvasti osaksi Internetiä, että todennäköisesti sen asema pysyy vakaana niin kauan, kuin tuntemamme Internet on olemassa.

Teoriaosuudessa tavoitteena oli saada selkeä kokonaiskuva sähköpostiviestinnästä yleisellä ja teknisellä tasolla. Yleisellä tasolla todettiin, että sähköpostilla on vielä tänäkin päivänä vakaa asema, ja sen käyttö kasvaa vielä 50 vuoden jälkeen. Vakaan suosion ja kasvun myötä se on myös merkittävä tietoturvauhka, ja tämä antoi käytännön osuudelle selkeän tarpeen. Teoriaosuudessa saatiin kuvaus sähköpostiviestinnän toimintaperiaatteelle, joka on välttämätön, kun halutaan parantaa sähköpostiliikenteen tietoturvatasoa.

Käytännönosuudessa Cisco ESA otettiin käyttöön asiakasyrityksen ympäristöön ja työ suoritettiin projektina. Projekti koostui työvaiheiden suunnittelusta sekä niiden toteutuksesta. Suunnitteluvaiheessa kartoitettiin asiakasyrityksen sähköpostiympäristö, sekä asiakkaan kanssa käytiin läpi työvaiheet ja aikataulu. Toteutuksessa suoritettiin suunnitellut toimenpiteet ja muutosten jälkeen testattiin, että kaikki toimivat toivotulla tavalla. Projektin aikana ilmeni, että itse työvaiheisiin saattaa kulua vähemmän aikaa kuin suunnitteluun ja viestintään asiakkaan kanssa. Toteutusvaihe oli oppimisen kannalta erittäin onnistunut, koska siinä näki selvästi tehtyjen toimenpiteiden vaikutukset käytännön tasolla. Oppiminen oli helpompaa, kun teorian lisäksi asiat voitiin todeta myös käytännössä.

Opinnäytetyöstä saatavia tietoja ja menetelmiä voidaan soveltaa Cisco ESA -järjestelmän lisäksi myös muissa järjestelmissä ja tietoturvan kehityksissä, koska suurin osa

vaiheista perustuu yleiseen sähköpostiliikenteen toimintaperiaatteeseen sekä avoimien standardien käyttöön.

Sähköpostiviestinnän toimintaperiaate ei ole vuosien aikana kokenut suuria muutoksia. Kuitenkin sen käyttö kasvaa vielä tänä päivänäkin, joten opinnäytetyö antaa selkeän kuvan sähköpostin tekniikasta, jota voidaan hyödyntää myös jatkossa sen tietoturvan parantamisessa.

LÄHTEET

[1] The Radicati Group. Email Statistics Report, 2018-2022; saatavilla: https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf. Viitattu 15.6.2019.

[2] Leppänen J. 2019. Cisco ESA -järjestelmän käyttöönotto yrityksessä; saatavilla: https://www.theseus.fi/bitstream/handle/10024/171216/Leppanen_Juuso.pdf?sequence=2&isAllowed=y Viitattu 20.10.2019

[3] Pharsee 2019. A brief history of email: dedicated to Ray Tomlinson; saatavilla: https://phrasee.co/a-brief-history-of-email/. Viitattu 30.6.2019

[4] Hildebrandt R, Koetter P, Back M, Haycox I, Rusenko D, Taylor C, McDonald A. 2009. Linux E-mail; saatavilla O'Reilly -palvelusta. Viitattu 19.10.2019

[5] Hostinger. POP3, SMTP and IMAP Ports and Protocols Explained; saatavilla: https://www.hostinger.com/tutorials/email/pop3-imap-smtp-protocols-explained-ports. Viitattu 30.6.2019

[6] Bradley T. 2006. Essential Computer Security: Everyone's Guide to Email, Internet and Wireless Security; saatavilla O'Reilly -palvelusta. Viitattu 13.10.2019

[7] Symantec Corporation. ISTR Email Threats 2017; saatavilla: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-email-threats-2017-en.pdf. Viitattu 3.8.2019

[8] Proofpoint 2019. Proofpoint Q2 2019 Threat Report – Emotet's hiatus, mainstream impostor techniques, and more; saatavilla https://www.proofpoint.com/us/threat-insight/post/proofpoint-q2-2019-threat-report-emotets-hiatus-mainstream-impostor-techniques Viitattu 26.10.2019

[9] Zoner. SPF, DKIM ja DMARC tietueet parantavat sähköpostien läpimenoa; saatavilla: https://www.zoner.fi/spf-dkim-ja-dmarc-tietueet-parantavat-sahkopostien-lapimenoa/. Viitattu 13.8.2019

[10] Dmarcian. What is DKIM?; saatavilla: https://dmarcian.com/what-is-dkim/ Viitattu 13.10.2019

[11] Dmarc.org. Background; saatavilla https://dmarc.org/overview/. Viitattu 13.8.2019

[12] Dmarcian. Policy Modes: Quarantine vs Reject; saatavilla: https://dmarcian.com/policy-modes-quarantine-vs-reject/. Viitattu 13.8.2019

[13] The Privacy Guide. PGP; saatavilla: https://theprivacyguide.org/tutorials/pgp.html Viitattu 25.8.2019

[14] Kukkonen M. Salattu sähköposti – Opas asiakasviestinnän suojaamiseen; saatavilla: https://kirjasto.tietosi.fi/aineisto/salattu-sahkoposti-opas-asiakasviestinnan-suojaamiseen?c=blog&utm_source=blog. Viitattu 25.8.2019

[15] Cisco Systems. Cisco Email Security Advanced Email Protection; saatavilla: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/datasheet-c78-739910.pdf. Viitattu 22.9.2019

[16] Porter C. 2012. Email Security with Cisco IronPort; saatavilla O'Reilly -palvelusta. Viitattu 13.10.2019

[17] Word to the Wise. DKIM Canonicalization – or – why Microsoft breaks your mail; saatavilla https://wordtothewise.com/2016/12/dkim-canonicalization-or-why-microsoft-breaks-your-mail/ Viitattu 30.9.2019