SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

TURVAPOSTIN KÄYTTÖÖNOTTO ITC-SOLUTION GROUPILLE

TEKIJÄ/T: Tomi Laatikainen

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma	
Työn tekijä(t) Tomi Laatikainen	
Työn nimi Turvapostin käyttöönotto ITC-Solution Groupille	
Päiväys 6.12.2021	Sivumäärä/Liitteet 27
Ohjaaja(t) Keijo Kuosmanen ja Janne Koponen	
Toimeksiantaja/Yhteistyökumppani(t) ITC-Solution Group Oy	

Tiivistelmä

Tämä opinnäytetyö oli projektityö, jonka tarkoituksena oli perustaa ja ottaa käyttöön turvaposti ITC-Solution Groupille. Turvapostin tuotteena käytettiin Deltagon Sec@GW – sähköpostin salausratkaisua. ITC-Solution Group halusi ottaa turvapostin ensin yrityksen sisäiseen käyttöön ja myöhemmin tarjota palvelua yritysasiakkaille.

Projektissa perustettiin ensin pilvipalvelin, johon turvapostiratkaisu asennettiin. Palvelimelle tehtiin tarvittavat määritykset ja verkkoyhteyksien avaamiset. Asennusten jälkeen toteutettiin salatun sähköpostin reititys ja lopuksi testattiin turvapostiratkaisun toimivuus. Käyttöönottoprojektin lisäksi opinnäytetyössä käydään läpi sähköpostin salausta yleisesti, EU:n tietosuoja-asetusta ja sen vaikutuksia työelämään sekä Deltagon Sec@GW -salausratkaisun toiminnallisuutta.

Työn tuloksena ITC-Solution Group sai käyttöönsä turvapostin ja projekti mahdollisti turvapostin jälleenmyynnin yritysasiakkaille. Opinnäytetyöhön tehtyä raporttia voidaan hyödyntää yrityksen sisäisessä dokumentaatiossa sekä turvapostin esittelyssä ja ohjeistuksessa asiakkaille.

Avainsanat
Turvaposti, sähköpostin salaus

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Tomi Laatikainen			
Title of Thesis Email Encryption Solution for ITC-Solution Group Oy			
Date	6 December 2021	Pages/Appendices	27
Supervisor(s) Mr Keijo Kuosmanen, Senior Lecturer and Mr Janne Koponen, Senior Lecturer			
Client Organisation /Partners ITC-Solution Group Oy			

Abstract

The goal of this thesis was to set up and deploy secure email for ITC-Solution Group Oy. The product used for email encryption was Deltagon Sec@GW. ITC-Solution Group Oy wanted to deploy secure email for internal use and later offer this service to enterprise customers.

In addition to secure email deployment project, the aim of this thesis was to review email encryption in general and find out what The European Data Protection Regulation is and how it affects businesses. Deltagon Sec@GW email encryption solution was also showcased in this thesis.

As a result, ITC-Solution Group Oy now has secure email in internal use. The project made it possible to resale the secure email product to enterprise customers. The report made for this thesis can be utilized for the company's internal documentation and for introducing the product to customers.

Keywords
Secure email, email encryption

ESIPUHE

Kiitos ITC-Solution Groupille opinnäytetyön aiheesta ja avusta opinnäytetyöhön liittyen. Erityiskiitokset ITC:n Niko Kinnuselle avusta turvapostin käyttöönottoprojektin toteutuksessa.

Kuopiossa 6.12.2021
Tomi Laatikainen

SISÄLTÖ

LYHENTEET JA MÄÄRITELMÄT

ITC = ITC-Solution Group Oy
Palvelin = Tietokone tai siinä suoritettava palvelinohjelmisto, joka tarjoaa erilaisia palveluja muille ohjelmille.
Selain, verkkoselain = Tietokoneohjelma, jolla voi selata verkkosivuja. Esimerkiksi Google Chrome, Firefox, Opera.
Plugin = Liitännäinen, joka tuo lisätoiminnallisuuksia isäntäsovellukseen.
Instanssi = Pilviympäristössä sijaitseva virtuaalikone.
Image = Pilviympäristöön perustettu virtuaalikoneen mallipohja, josta perustetaan instansseja.
SSL = Secure Sockets Layer, tietoverkkosalausprotokolla.
HTTP = Hypertext Transfer Protocol, protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
HTTPS = Hypertext Transfer Protocol Secure. HTTP:n laajennus, jossa tiedonsiirto on salattu.
Apache HTTPD = Apache-säätiön tuottama http-palvelin.
Certbot = Työkalu, jolla voi luoda sertifikaatin, joka mahdollistaa verkkosivulle HTTPS-yhteyden.
Palomuuri = Laite tai ohjelmisto, joka suodattaa saapuvaa ja lähtevää verkkoliikennettä.
SSH = Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla.
Office/Microsoft 365 = Microsoftin julkaisema tuoteryhmä, johon kuuluu erilaisia pilvipalveluja, kuten Outlook-sähköposti, Word ja Excel.
M365 = Microsoft 365
SMTP = Simple Mail Transfer Protocol. Protokolla, jota käytetään viestien välittämiseen sähköpostipalvelimelta toiselle.
TCP = Transmission Control Protocol. Tietoliikenneprotokolla tietokoneiden väliseen luotettavaan tiedonsiirtoon.
NTP = Network Time Protocol. Protokolla täsmällisen aikatiedon välittämiseen tietokoneiden välillä.
UDP = User Datagram Protocol, tietoliikenneprotokolla.
DNS = Domain Name System. Nimipalvelujärjestelmä, joka muuntaa verkkotunnukset IP-osoitteiksi.
SPF = Sender Policy Framework.
Tietue = Yksinkertainen tietorakenne, joka on itsenäinen ja looginen kokonaisuus.

1 JOHDANTO

1.1 ITC yrityksenä

ITC on Pohjois-Savon ja Pohjoisen Keski-Suomen suurin yksityinen tietotekniikan palvelutalo, joka työllistää tällä hetkellä 26 työntekijää. Yrityksellä on kiinteät toimipisteet Kuopiossa, Iisalmessa ja Viitasaarella. ITC on keskittynyt yrityspalveluihin, joihin kuuluvat muun muassa etä- ja lähituki, helpdesk, sekä ylläpitopalvelut palvelimille, työasemille, monikäyttölaitteille ja verkkolaitteille. Kuluttajamyynti ja -huolto lopetettiin kokonaan vuoden 2021 joulukuusta lähtien kysynnän hiipumisen ja toiminnan kannattavuuden takia. Viimeisempänä kuluttaja-asiakkaita palveli Kuopion toimipisteen myymälä, joka tarjosi myös huoltopalveluita eri IT-laitteille. (ITC.)

1.2 Opinnäytetyön tavoitteet

Työn tarkoitus on perustaa ITC-Solution Groupille sähköpostin salausratkaisu Deltagon Sec@GW ohjelmistoon perustuen. Tarkoituksena on ottaa turvaposti ensin käyttöön ITC:lle ja sen jälkeen tarjota palvelua yritysasiakkaille. Aiemmin ITC on ulkoistanut turvapostipalvelun ja sen hallinnoinnin yhteistyökumppanin kautta. Nyt tavoitteena on perustaa turvaposti ITC:n omalle pilvipalvelimelle ja ylläpitää sekä hallinnoida palvelua ITC:n toimesta. Opinnäytetyön tavoitteena on myös perehtyä syvemmin sähköpostin salaukseen ja tietosuojalainsäädäntöön.

2 SALATTU SÄHKÖPOSTI YLEISESTI

2.1 Mitä on salattu sähköposti?

Salatulla sähköpostilla (myös turvaposti tai suojattu sähköposti) tarkoitetaan sähköpostiviestiä, jonka yksityisyys ja luottamuksellisuus on turvattu eri tekniikoita hyödyntäen. Yleensä vähimmäistavoitteena on viestin yksityisyys eli se, etteivät ulkopuoliset pääse lukemaan viestejä. Tavallista, salaamatonta sähköpostia verrataan usein postikorttiin, koska viesti on ulkopuolisten luettavissa kaikille korttia käsitteleville. Sähköpostiviestit kulkevat useiden postipalvelimien ja erilaisten välityspalvelimien kautta. Salaamaton viesti on periaatteessa mahdollista lukea kaikkien näiden etappien välillä. Salattua sähköpostia käytettäessä viesti kryptataan eli muutetaan salattuun muotoon heti lähetysvaiheessa ja tämän salauksen voi purkaa vain viestin vastaanottaja, jolloin viesti muuttuu luettavaan muotoon. Salauksen purkamiseen voidaan myös asettaa lisävaatimuksena monivaiheinen tunnistautuminen esimerkiksi pankkitunnuksilla tai tekstiviestillä saapuvalla PIN-koodilla. Monivaiheisella tunnistautumisella voidaan varmentaa vastaanottajan identiteetti useampaa tunnistautumismenetelmää hyödyntäen. Tällä tavalla voidaan yrittää estää ulkopuolista henkilöä avaamasta viestiä, vaikka hän olisi päässyt käsiksi vastaanottajan postilaatikkoon tai jos lähettäjä olisi epähuomiossa lähettänyt viestin väärälle henkilölle. Vaikka viestin sisältö olisi salattu, niin aivan kaikkea sähköpostiviestin tietoja salatulla sähköpostilla ei ole mahdollista piilottaa, eikä ole tarkoituskaan. Näitä tietoja ovat muun muassa lähettäjä, vastaanottaja, postipalvelinten julkiset nimet ja osoitteet sekä viestin välitysajankohdat. Nämä tiedot ovat tarpeellisia viestin kulkemisen kannalta. (Kukkonen.)

2.2 Miksi käyttää salattua sähköpostia?

Tietoturvaan ja henkilötietojen asianmukaiseen käsittelyyn kiinnitetään vuosi vuodelta enemmän huomiota. Monilla yrityksillä on tiukat tietoturvaan ja henkilötietojen käsittelyyn liittyvät käytännöt, joiden laiminlyömisestä voi aiheutua sanktioita. Sähköposti on nykymaailmassa merkittävä työkalu yritysten sisäisessä ja ulkoisessa viestinnässä. Sähköpostilla kommunikoidaan kollegoiden ja asiakkaiden kanssa ja joskus nämä sähköpostikeskustelut olisivat hyvä pitää mahdollisimman salassa ulkopuolisilta. Salattua sähköpostia olisi hyvä käyttää aina, kun sähköpostin välityksellä käsitellään arkaluontoista tietoa, kuten henkilötietoja, potilastietoja, palkkatietoja, pankkitietoja, sekä luottamuksellisia ja salaisia yritys- ja viranomaistietoja. (Saikkonen, 2020.)

Sähköpostin salaaminen vähentää riskiä tietovuodoille. Arkaluontoisten tietojen vuotaminen organisaation ulkopuolelle voi aiheuttaa organisaatiolle isoja menetyksiä. Liiketoimintakriittisten tietojen vuotaessa kilpailijat voivat saada tietoonsa informaatiota, joka on saattanut aikaisemmin olla suuri etu liiketoiminnan kannalta. Uutisissa ja verkossa julkaistut tietovuodot ovat monesti kova isku yrityksen maineen ja brändin kannalta. Asiakkaiden ja yhteistyökumppaneiden syvän luottamuksen rakentaminen on voinut kestää vuosikymmeniä, mutta tämä luottamus voi romuttua minuuteissa. Asiakkaat ja yhteistyökumppanit luottavat siihen, että heidän antamansa tiedot pysyvät turvassa ja että niitä käsitellään asianmukaisella tavalla. Luottamuksen menettämisen jälkeen nykyiset asiakkaat

ja yhteistyökumppanit saattavat kaikota muualle ja uusien sopimusten luominen voi olla huomattavasti haastavampaa kuin aiemmin. Rahallisten tappioiden ja maineen menettämisen lisäksi tietovuodosta voi aiheutua yritykselle myös rikosoikeudellisia toimenpiteitä. (Deltagon.)

Salattua sähköpostia käyttämällä voidaan myös tehostaa ajankäyttöä. Monissa yrityksissä luottamuksellista tietoa välitetään vain kasvotusten tai kirjeiden välityksellä perinteisellä postilla. Perinteisellä tavalla asian hoitamiseen voi mennä päiviä tai jopa viikkoja, kun se olisi voitu hoitaa salatulla sähköpostilla minuuteissa. Kirjeiden tulostamiseen ja postittamiseen kuluva aika voitaisiin käyttää muihin työtehtäviin. Myös asiakkaan kannalta on mielekkäämpää, kun viestintä on nopeaa ja helppoa, turvallisuudesta tinkimättä. (Deltagon.)

3 GDPR

3.1 Mikä on GDPR?

GDPR (General Data Protection Regulator) on EU:n tietosuoja-asetus, jota alettiin soveltaa vuonna 2018 kaikissa EU-maissa. Uuden tietosuojalain tarkoituksena on muun muassa parantaa henkilötietojen suojaa ja tietosuojaoikeuksia, vastata tietosuojaan liittyviin kysymyksiin sekä yhtenäistää kaikkien EU-maiden tietosuojasääntelyä. Lain mukaan jokaisella on oikeus tietää mitä henkilötietoja organisaatiolla on hänestä ja miten ja mihin tarkoitukseen hänen henkilötietojaan käsitellään. Tietosuoja-asetuksen mukaan jokaisella on myös oikeus muun muassa pyytää henkilötietojensa poistamista ja vastustaa henkilötietojen käsittelyä. (Tietosuojavaltuutetun toimisto.)

3.2 GDPR:n vaikutus työelämään

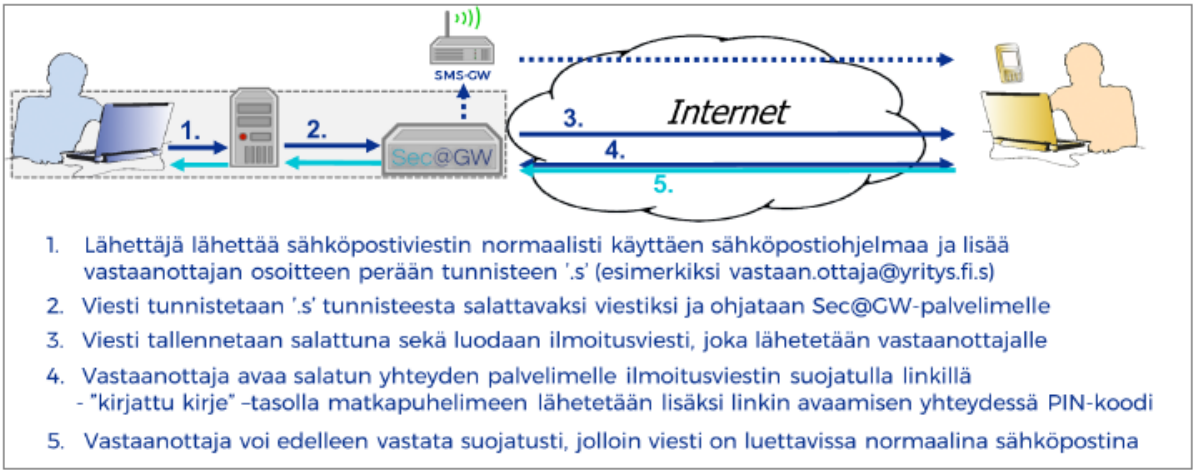
Uusi tietosuojalaki sai monet yritykset kiinnittämään entistä enemmän huomiota henkilötietojen käsittelyyn ja suhtautumaan tietosuojaan uudella tavalla. Organisaatioiden on erityisesti kiinnitettävä huomiota tietosuojaan liittyvien riskien tunnistamiseen ja ehkäisyyn, sisäisten toimintamallien kehittämiseen, uuden lainsäädännön noudattamiseen sekä monipuoliseen ja ajantasaiseen dokumentointiin. Työntekijöiden kouluttaminen ja sisäinen ohjeistus tietosuojaan ja tietoturvaan liittyen on tärkeää. Yritysten työntekijöiden olisi hyvä käydä läpi yrityksen omat tietoturvaan liittyvät käytännöt ja toimintatavat. Jokaisen työntekijän olisi hyvä tietää erilaisista tietoturvauhista ja oppia tunnistamaan niitä. Erilaiset huijaukset ja tietojenkalasteluyritykset ovat nykyään todella yleisiä ja ne leviävät jatkuvasti muun muassa sähköpostin ja tekstiviestien välityksellä. Vahingon sattuessa tai huijatuksi tullessa tulisi olla selvillä toimintatapa, jolla vahinkoja pyritään minimoimaan. Toimintatapa voi olla esimerkiksi salasanan vaihtaminen tai pikainen yhteydenotto IT-tukeen. Yritysten sisäiseen tietoturvaohjeistukseen olisi hyvä sisällyttää sähköisen viestinnän pelisäännöt. On tärkeää ohjeistaa, mitä viestintäkanavia tulisi käyttää ja mitä taas välttää, kun käsitellään arkaluontoista tietoa. Myös fyysiseen tietoturvallisuuteen tulisi kiinnittää huomiota. Fyysisellä tietoturvallisuudella tarkoitetaan muun muassa toimitilojen sekä niissä sijaitsevien laitteiden, fyysisen dokumentaation ja tietojärjestelmien suojaamista fyysisiltä uhilta. Henkilötietoja koskevia fyysisiä uhkia ovat esimerkiksi varkaudet ja väärinkäyttö. Arkaluontoista tietoa ei tulisi säilyttää fyysisesti paikoissa, joihin ulkopuolisilla on pääsy. Arkaluontoista tietoa tulostaessa tulisi tulostus hakea mahdollisimman nopeasti talteen, eikä jättää sitä tulostimeen yhtään pidemmäksi aikaa kuin on tarve. Tietokoneella arkaluontoista tietoa käsittelevän työntekijän tulisi aina lukita työasemansa, kun poistuu sen äärestä. On myös otettava huomioon, kuka pääsee milloinkin kurkkimaan olan takaa tai kuuntelemaan puhelinkeskusteluja, kun käsitellään arkaluontoista tietoa. Koronaviruspandemiasta aiheutunut etätyöskentelyn räjähdysmäinen kasvu on lisännyt omat haasteensa fyysiseen turvallisuuteen. Etätyöskentelevällä tulisi olla mahdollisuuksiensa mukaan käytössään työskentely- ja säilytystilat, jotka täyttävät nämä fyysisen turvallisuuden kriteerit. (EY Suomi, 2019; Seclion, 2021.)

Uuden lain mukaan organisaation on pakollista nimittää tietosuojavastaava, kun organisaation keskeisimmät työtehtävät muodostuvat henkilötietojen käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa tai arkaluontaisten henkilötietojen laajamittaista käsittelyä. Tietosuojavastaava on organisaation sisäinen asiantuntija, jonka tehtäviin kuuluu valvoa tietosuojasääntöjen noudattamista ja tuoda esiin havaitsemiaan puutteita. Tietosuojavastaava myös neuvoo työntekijöitä tietosuojasäännösten noudattamisessa. Tietosuojavastaava toimii rekisteröityjen yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä asioissa ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa, joka toimii Suomessa tietosuojalain valvontaviranomaisena. Organisaatiossa, joissa suoritetaan riskialtista tai laajamittaista henkilötietojen käsittelyä, on organisaation tehtävä tietosuojaa koskeva vaikutustenarviointi. Vaikutustenarvioinnilla arvioidaan, tunnistetaan ja hallitaan henkilötietojen käsittelyyn liittyviä riskejä. Jos organisaatio on nimennyt tietosuojavastaavan, auttaa hän vaikutustenarvioinnin tekemisessä ja valvoo sen toteutusta. GDPR:n mukaan organisaatioilla on ilmoitusvelvollisuus tietoturvaloukkauksista. Tapahtuneista tietoturvaloukkauksista on lain mukaan ilmoitettava valvontaviranomaiselle, jos tietoturvaloukkauksesta voi aiheutua riski henkilöiden oikeuksille ja vapauksille. Loukkauksesta tulisi ilmoittaa viivyttelemättä ja mahdollisuuksien mukaan kolmen vuorokauden sisällä siitä, kun tietoturvaloukkaus on tullut rekisterinpitäjän tietoisuuteen. Ilmoituksen tietoturvaloukkauksesta voi tehdä tietosuojavaltuutetun toimiston verkkosivuilla olevan lomakkeen kautta. Uuden tietosuojalain mukaan rekisteröidyille on annettava aikaisempaa yksityiskohtaisempia tietoja henkilötietojen käsittelyyn liittyen. Laki edellyttää, että rekisteröidyille on annettava henkilötietojen käsittelyä koskevat tiedot tiiviissä, läpinäkyvässä ja helposti ymmärrettävässä muodossa. Lain mukaan rekisteröityjen tulee saada tietää, kuka rekisterinpitäjänä toimii ja mihin tarkoitukseen henkilötietoja käytetään. Rekisteröidyille on kerrottava myös henkilötietojen säilytysaikaan ja eteenpäin luovuttamiseen liittyvät käytännöt sekä sen, miten rekisteröity voi käyttää henkilötietoihin liittyviä oikeuksiaan. Tietosuojavaatimusten tiukentumisen lisäksi niiden rikkomisesta voi aiheutua tuntuvia sakkoja. Sakot voivat nousta korkeimmillaan 20 miljoonaan euroon tai 4 prosenttiin yrityksen liikevaihdosta. (EY Suomi, 2019; Tietosuojavaltuutetun toimisto.)

4 DELTAGON SEC@GW – SÄHKÖPOSTIN SALAUSRATKAISU

4.1 Sähköpostin suojaaminen

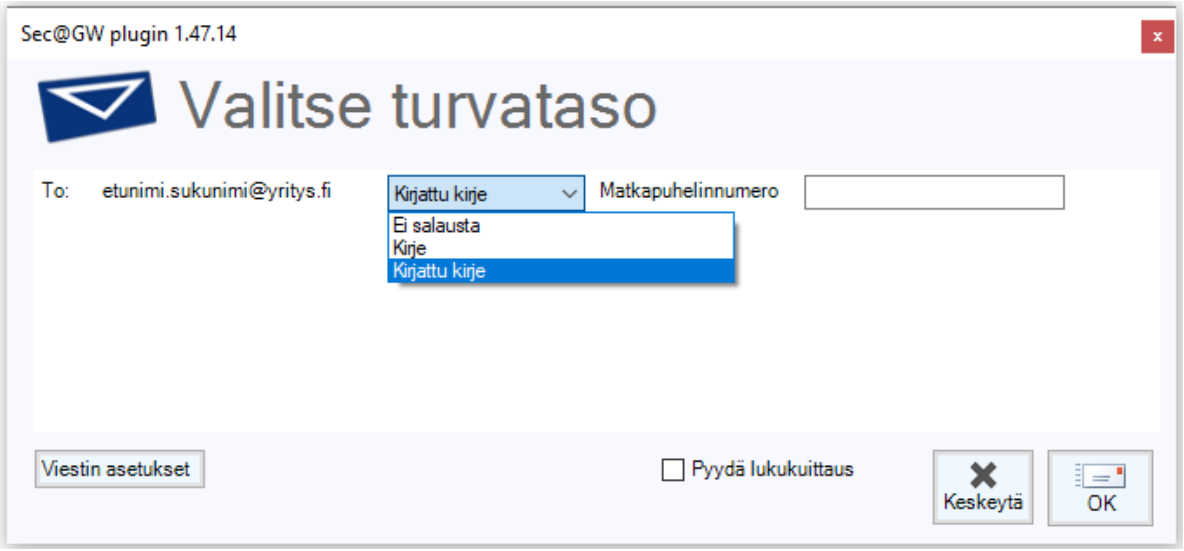
Suomalaisen Deltagon Group Oy:n kehittämällä Deltagon Sec@GW – sähköpostin salausratkaisulla voi lähettää ja vastaanottaa salattuja sähköposteja luottamuksellisesti ilman, että käyttäjän tarvitsee ladata työasemalleen ylimääräisiä ohjelmia. Deltagon Sec@GW muuntaa sähköpostiviestin selaimella luettavaan muotoon, tallentaa salatun viestin tilapäisesti palvelimelle ja lähettää vastaanottajalle suojatun linkin. Tämän linkin kautta vastaanottaja pääsee lopulta avaamaan salatun viestin. Palvelussa on kaksi eri turvatasoa, joilla viestin voi salata. ”Kirje”-tasolla viestiliikenne suojataan ja itse viesti lukitaan Deltagon MessageLock-tekniikalla. ”Kirjattu kirje” -tasolla edellisten lisäksi vastaanottajalta vaaditaan tunnistautumista SMS-autentikoinnilla. Viestiä avatessa vastaanottajan puhelimeen lähetetään tekstiviestillä PIN-koodi, jolla viestin saa lopulta avattua. (Deltagon.)



KUVA1. Esimerkki salauksen toiminnasta (Deltagon)

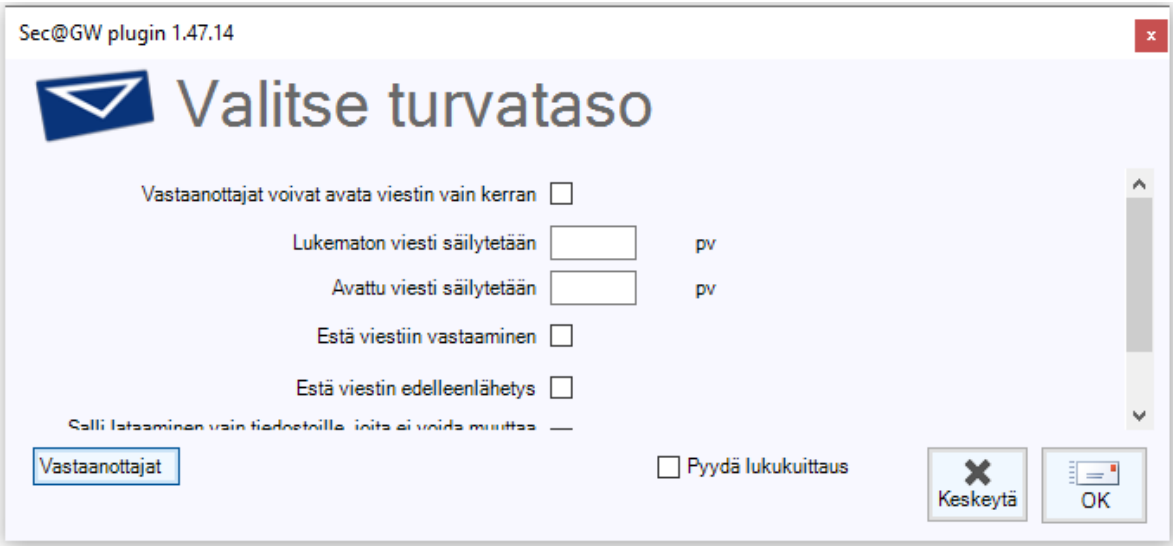
4.2 Viestin lähettäminen

Salatun sähköpostiviestin lähettäminen onnistuu lisäämällä vastaanottajan sähköpostiosoitteen perään ”.s” (esimerkiksi etunimi.sukunimi@yritys.fi.s). Jos viestin avaamiseen halutaan vaatia myös SMS-autentikointi, on vastaanottajan osoitteen perään lisättävä puhelinnumero ja ”.s” (esimerkiksi etunimi.sukunimi@yritys.fi.0501234567.s). Työasemille on myös mahdollista asentaa Outlook-sähköpostin työpöytäsovellukseen lisättävä Sec@GW plugin, eli liitännäinen. Plugin tulee näkyviin Outlookin yläpalkkiin, jota kautta salatun sähköpostiviestin lähettäminen ja turvatason valinta myös onnistuu. Pluginiin pystyy myös määrittämään asetuksen, jossa Outlook näyttää viestin turvatason valinnan aina viestiä lähettäessä. Tällä asetuksella voidaan pienentää riskiä lähettää luottamuksellinen viesti salaamattomana, kun käyttäjän olisi pitänytkin lähettää viesti salattuna.



KUVA2. Viestin turvatason valinta Sec@GW pluginilla.

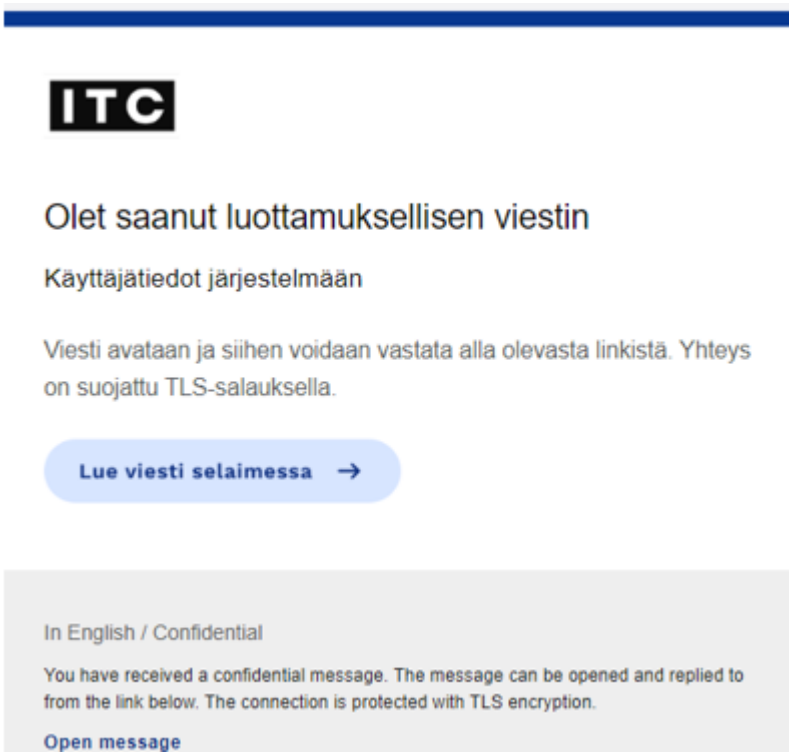
Pluginin avulla voidaan myös määrittää viestiin lisäasetuksia, kuten estää viestin edelleenlähetys, muuttaa viestin säilymisaikaa ja pyytää lukukuittaus. Lukukuittauksella lähettäjälle saapuu automaattivastaus sähköpostilla, kun vastaanottaja on avannut viestin ensimmäisen kerran.



KUVA3. Viestin lisäasetukset Sec@GW pluginilla.

4.3 Viestin lukeminen

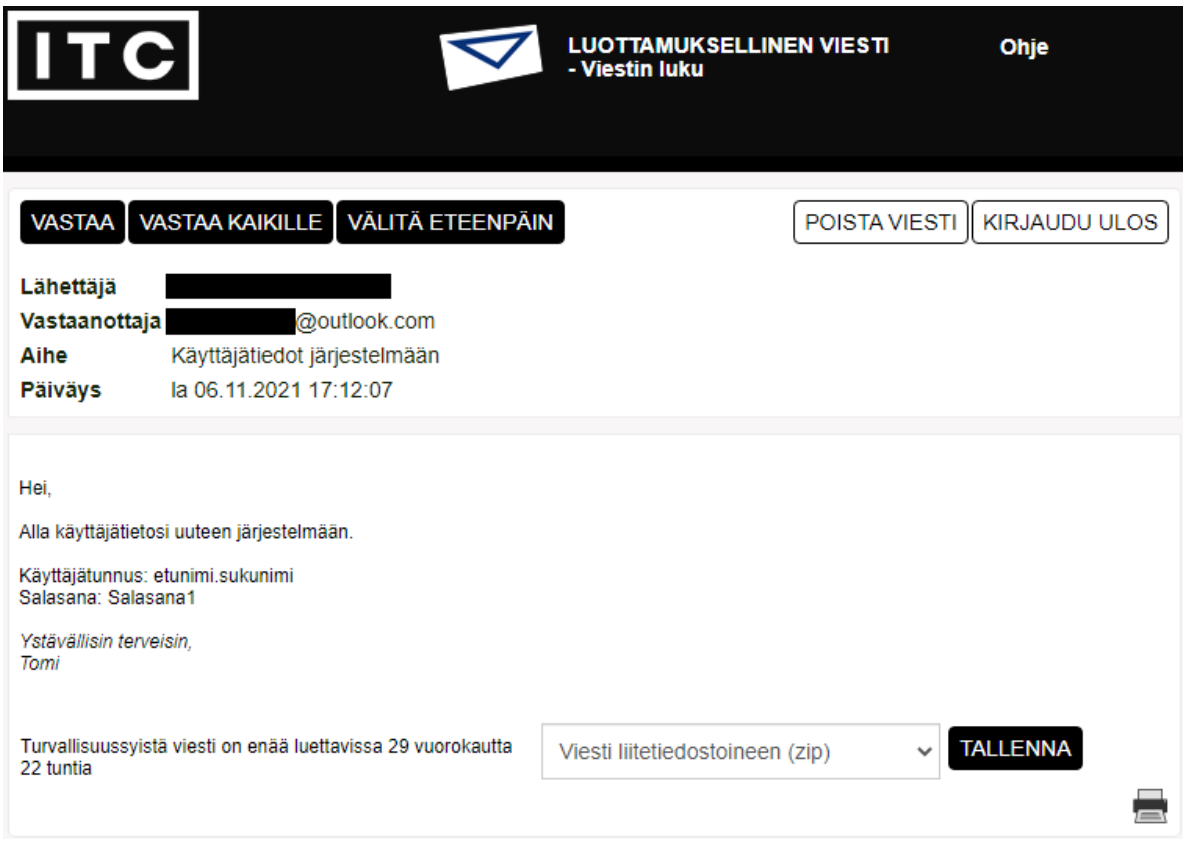
Kun salattu sähköpostiviesti on lähetetty, saapuu vastaanottajan sähköpostiin ilmoitusviesti lähettäjältä. Ilmoitusviestissä on linkki, jota kautta salatun viestin voi lukea selaimessa.



KUVA4. Ilmoitusviesti.

Linkin avaamisen jälkeen käyttäjää huomautetaan, että painamalla ”Jatka” käyttäjä antaa palvelun tarjoajalle luvan kerätä tarvittavat henkilötiedot, jotta palvelun ja salatun viestinnän toiminta olisi mahdollista. Käyttäjä voi myös halutessaan valita ”Keskeytä”, jolloin istunto sulkeutuu. Käyttäjän valitessa ”Jatka” avautuu käyttäjälle salattu viesti luettavassa muodossa. Jos lähettäjä oli valinnut turvatasoksi SMS-autentikoinnin, vaaditaan viestin avaamiseen vielä PIN-koodi, joka lähetetään vastaanottajalle tekstiviestillä äsken mainitun ”Jatka”-napin painamisen jälkeen.

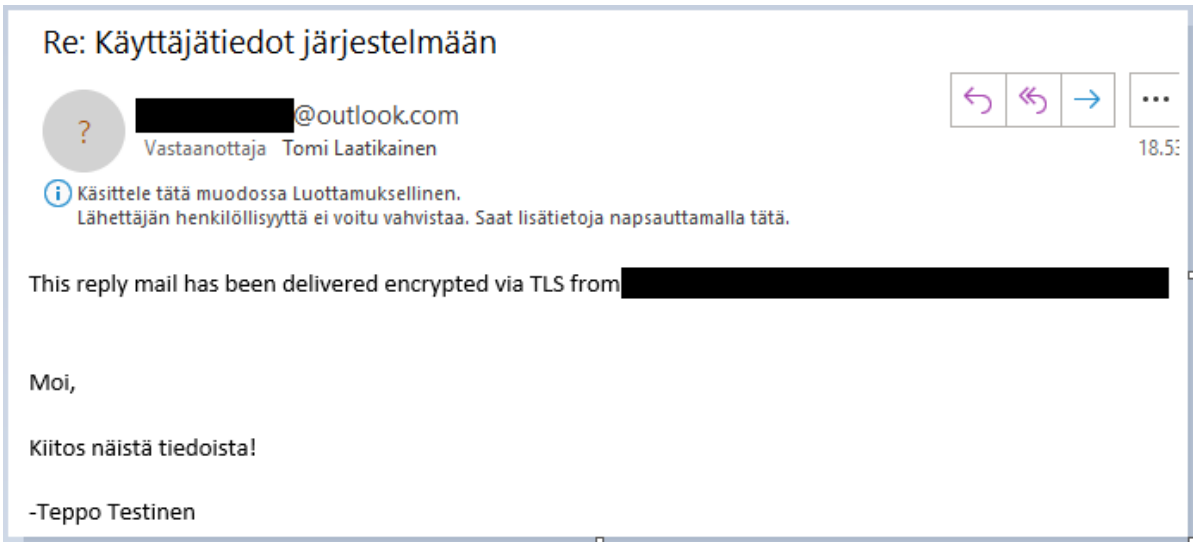
Lukunäkymän kautta viestiin voi vastata ja sen voi välittää eteenpäin. Jos lähettäjä oli määrittänyt, ettei viestiä voi välittää eteenpäin, niin kyseinen valinta on piilotettu. Käyttäjä voi myös poistaa viestin lopullisesti, tallentaa sen valitsemassaan tiedostomuodossa koneelle, tulostaa viestin sekä kirjautua ulos järjestelmästä.



KUVA5. Salatun viestin lukeminen.

4.4 Viestiin vastaaminen

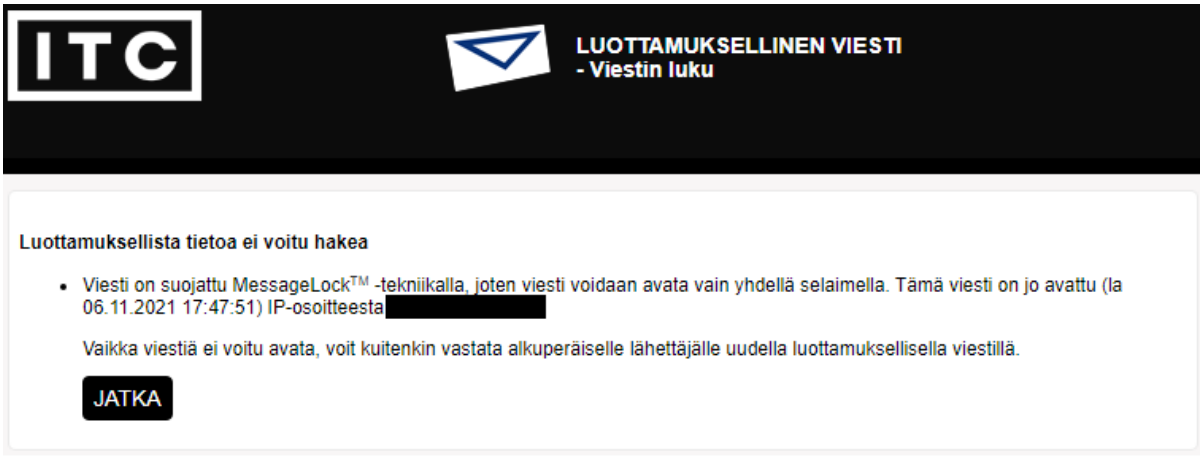
Viestiin voi vastata valitsemalla “Vastaa” tai ”Vastaa kaikille”. Käyttäjälle avautuu uusi välilehti, jossa vastauksen voi kirjoittaa ja lähettää. Vastaus lähetetään salattuna viestinä automaattisesti, joten käyttäjän ei tarvitse sitä erikseen valita. Vastaus saapuu alkuperäiselle lähettäjälle perinteisen näköisenä sähköpostiin, mutta viestin alussa mainitaan viestin olevan luottamuksellinen ja että viesti on salattu.



KUVA6. Vastattu viesti.

4.5 Viestin sulkeminen

Viestin uudelleenavaaminen vaatii tunnistautumista. Käyttäjän on siis otettava huomioon viestin sulkemistapa, jos hän aikoo avata viestin myöhemmin uudelleen. Viesti suljetaan hallitusti valitsemalla ”Kirjaudu ulos”, jonka jälkeen käyttäjä ohjataan poistumissivulle. Käyttäjää pyydetään valitsemaan tunnistautumistapa viestin uudelleenavaamista varten. Vaihtoehtoina ovat salasana tai eväste, joista käyttäjälle ehdotetaan oletuksena salasanaa. Valitsemalla salasana, viestin voi avata uudelleen vain käyttäjän määrittelemällä salasanalla. Tämä vaihtoehto mahdollistaa viestin uudelleenavaamisen mistä tahansa sijainnista ja miltä tahansa selaimelta. Toisena vaihtoehtona on eväste, joka tallennetaan käyttäjän selaimeen. Evästeellä käyttäjä tunnistetaan automaattisesti, kun viesti avataan uudelleen. Tällä vaihtoehdolla viesti voidaan avata vain tietystä verkko-osoitteesta ja vain tietyllä selaimella. Jos käyttäjä yrittää avata viestin uudelleen eri selaimella tai eri sijainnista, niin hänelle avautuu sivu, joka antaa virheilmoituksen ”Luottamuksellista tietoa ei voitu hakea” ja kertoo milloin ja mistä sijainnista viesti on avattu (katso KUVA7). Eväste-vaihtoehdolla viestin uudelleenavaus ei ole enää mitenkään mahdollista, jos selaimesta poistetaan evästeet tai jos valinta oli tehty käyttämällä yksityistä selainikkunaa, jossa evästeitä ei tallenneta. Viestiin vastaaminen on kuitenkin mahdollista, vaikkei viestiä pääsisikään enää lukemaan. Vastaanottaja voi täten vastata lähettäjälle suoraan ja pyytää lähettämään viestin uudelleen tarvittaessa. Käyttäjän sulkiessa salattu viesti hallitsemattomasti ilman uloskirjautumista (esimerkiksi sulkemalla selainikkuna, jossa viesti oli), valitaan käyttäjän puolesta tunnistautumisvaihtoehdoksi eväste.



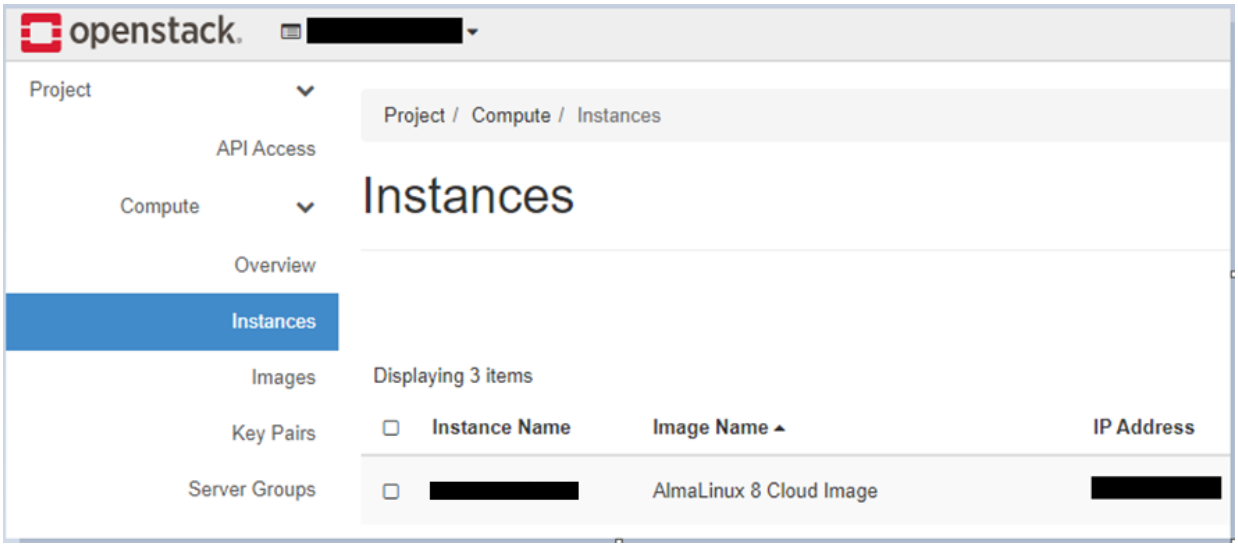
KUVA7. Viestiä ei voitu avata uudelleen, tunnistautumistapana eväste.

5 ITC-TURVAPOSTIN KÄYTTÖÖNOTTOPROJEKTI

5.1 Valmistelut

5.1.1 Palvelimen asennus

Turvapostiratkaisu tulee toimimaan ITC:n hallinnoimalla pilvipalvelimella. Pilvipalvelin perustetaan laitesalipalveluntarjoajan TNNet Oy:n pilviympäristöön. Projektissa oli alun perin tarkoitus asentaa palvelin Deltagonin ohjeiden mukaan. Ohje oli kuitenkin tarkoitettu fyysisen palvelimen asennukseen, mutta koska kyseessä on pilvipalvelin, piti palvelimen ja käyttöjärjestelmän asennus toteuttaa eri tavalla. Ohjeen mukaisessa asennuksessa palvelimelle asennettaisiin AlmaLinux 8 -käyttöjärjestelmä asennuslevyltä ja asennukseen tulisi käyttää myös Deltagonin lähettämää kickstart-tiedostoa, joka määrittää palvelimelle tietyt määritykset. Tämän jälkeen olisi ollut tarkoitus tehdä palvelimen levyosiointi ohjeen mukaisesti. Kokeilimme ensin luoda pilvipalvelimen instanssin käyttämällä TNNetin luomaa AlmaLinux 8 -imagea ja lisäämällä kickstart-konfiguraatiotiedoston asennusvaiheessa. Kickstart-tiedostolla ei kuitenkaan ollut mitään vaikutusta palvelimen kokoonpanoon. Kokeilimme myös luoda pilviympäristöön oman AlmaLinux imagen, mutta ongelmaksi tuli, ettei image syystä tai toisesta tunnistanut kiintolevyjä. Tässä vaiheessa olimme yhteydessä TNNetin tukeen asiaan liittyen. Heidän mukaansa kickstart-tiedoston tilalle on tullut cloud init, joka ajetaan palvelimelle instanssin luonnin yhteydessä. Asian selvityksen jälkeen sovimme TNNetin kanssa, että he suorittavat pilvipalvelimen ensiasennukset nykyaikaisella tavalla tietojemme perusteella ja tekevät tarvittavat kickstart-tiedostossa olevat määritykset käsin. Myös palvelimen levyosiointi tehtiin heidän toimestaan sovitulla tavalla. Palvelimen ensiasennusten jälkeen TNNet lähetti meille palvelimen root-tunnukset, joilla pääsemme palvelimeen käsiksi.

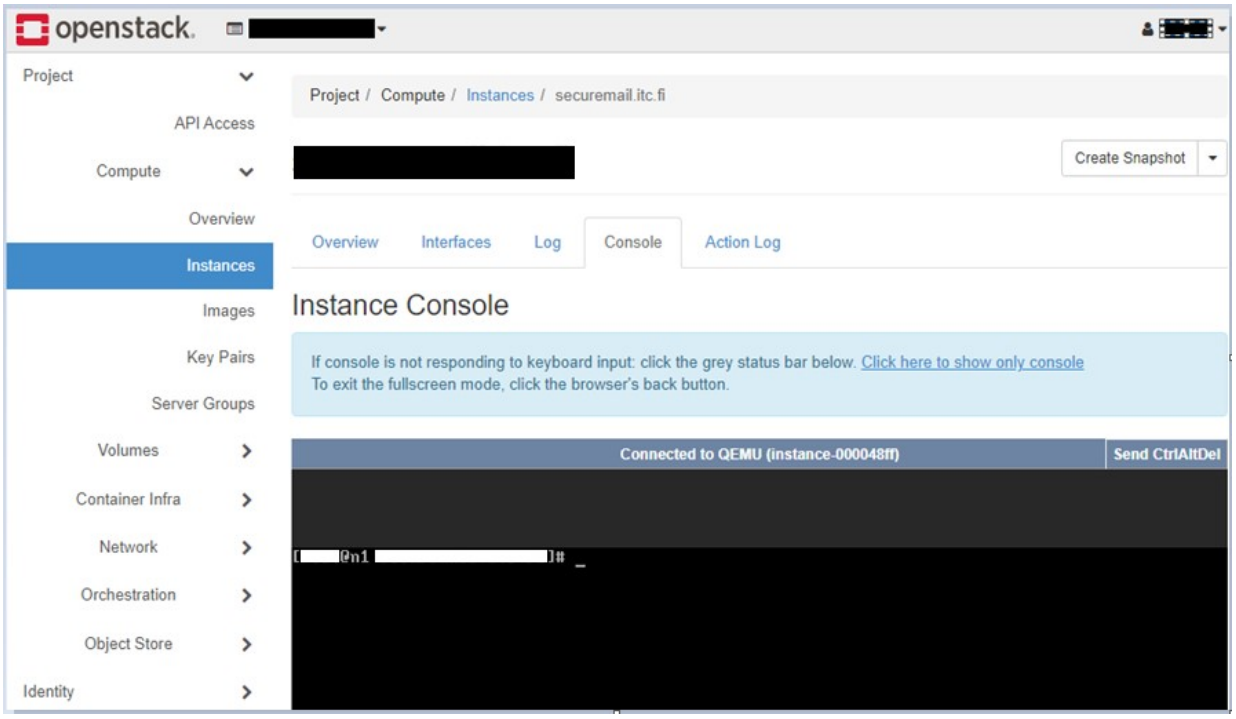


KUVA8. Turvapostipalvelimen instanssi pilviympäristössä.

5.1.2 Verkkoyhteyksien avaamiset

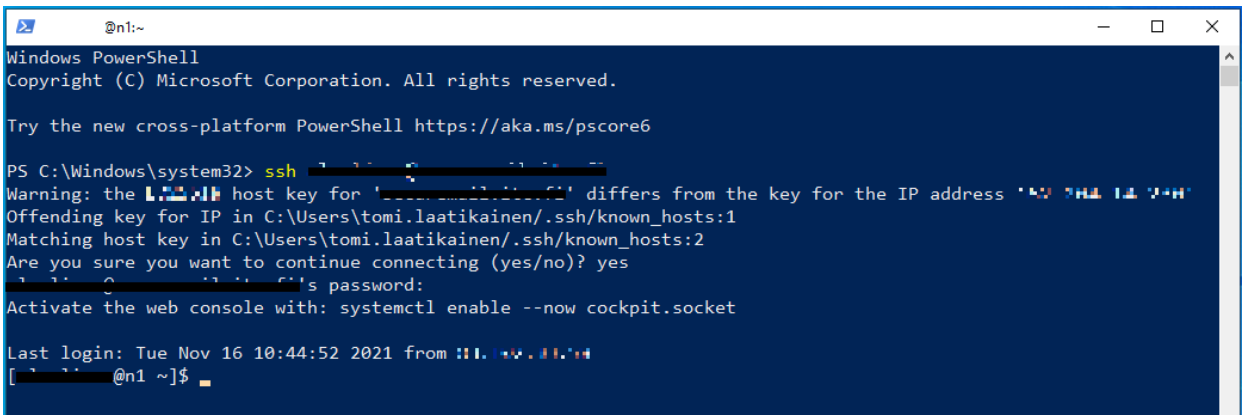
Turvapostiratkaisu tarvitsee toimiakseen verkkoyhteyksiä. Turvapostipalvelimen palomuuri estää oletuksena kaiken verkkoliikenteen, joten palomuuriin on tehtävä tarvittavat avaukset. Palomuurinsääntöjen muokkaukseen käytettiin iptables-työkalua, koska asennusohjeen mukana tulleessa kickstart-tiedostossa oli määritetty palvelimelle asennettavaksi iptables palomuurisääntöjen muokkausta varten.

Palvelimen hallintaa ja asennuksia varten on ensin sallittava palvelimelle sisääntuleva verkkoliikenne ITC:n ja Deltagonin verkko-osoitteista porttiin 22 SSH-yhteyttä varten. SSH-yhteydellä palvelimeen pääsee etänä käsiksi käyttäjätunnusta ja salasanaa käyttämällä. Tämä ensimmäinen SSH-yhteyksien mahdollistava palomuuriavaus on luotava palvelintarjoaja TNNetin pilviympäristössä Openstackissa palvelimen instanssin oman konsolin kautta. Tämä ”huoltokonsoli” on tarkoitettu käytettäväksi, kun muu konsoliyhteys (kuten SSH-yhteys) ei ole mahdollinen.



KUVA9. ”Huoltokonsoli” Openstackissa.

Palomuuriavaus SSH-yhteyden sallimiseen luodaan iptables-työkalulla komennolla **iptables -A INPUT -s 12.345.67.89/32 -p tcp --dport 22 -j ACCEPT**. Valitsimella **-A INPUT** määritellään, että luodaan uusi palomuurisääntö, joka koskee sisääntulevaa liikennettä. Valitsimella **-s 12.345.67.89/32** (osoite muutettu) määritetään, mistä verkko-osoitteesta liikenne sallitaan. Valitsimella **-p tcp** määritellään, että sääntö koskee TCP-paketteja. **--dport 22** -valitsin määrittää, että sääntö koskee palomuurin porttiin 22 tulevaa liikennettä ja valitsin **-j ACCEPT** määrittää, että kyseiset paketit hyväksytään. Komennon syöttämisen jälkeen SSH-yhteyden luominen on mahdollista määritellystä verkko-osoitteesta. (Linux, 2021.)



KUVA10. SSH-yhteys luotu palvelimelle onnistuneesti PowerShellin kautta ITC:n verkko-osoitteesta.

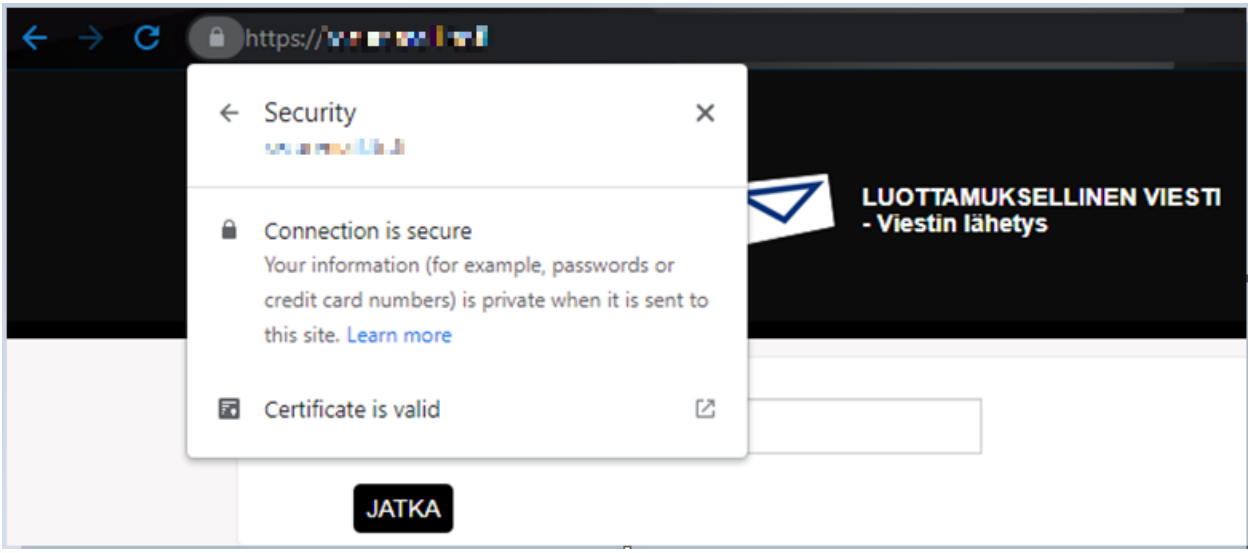
ITC:n lisäksi myös valtaosa ITC:n yritysasiakkaista käyttää työsähköpostejaan Office 365 -ympäristössä. Jotta sähköpostien välittäminen olisi mahdollista Office 365 postipalvelinten ja ITC:n turvapostipalvelimen välillä, on sallittava sisääntuleva liikenne Officen SMTP-osoitteista. Palomuuriin on myös sallittava kaikista lähteistä sisääntuleva TCP-liikenne portteihin 443 ja 80, jotta turvapostin käyttäjät saavat yhteyden palvelun verkkosivuille.

Turvapostipalvelimen käyttöjärjestelmäpäivityksiä ja Sec@GW-turvapostiratkaisun päivityksiä varten palomuuriin on sallittava ulospäin liikenne tarvittaviin päivityspalvelimien osoitteisiin. Käyttöjärjestelmä Alma Linuxin päivityksiä varten on sallittava verkkoliikenne Alma Linuxin päivityspalvelimiin ja Deltagon Sec@GW -turvapostiratkaisun päivityksiin on sallittava yhteys Deltagonin päivityspalvelimen verkko-osoitteeseen. Turvapostissa käytettäviä vastaus- ja ilmoitusviestejä varten on sallittava ulospäin liikenne kaikkiin osoitteisiin SMTP-porttiin 25. Jotta turvapostipalvelimen kello pysyisi ajan tasalla, on palvelimen oltava yhteydessä NTP-palvelimeen, joka jakaa turvapostipalvelimelle tarkan aikatiedon. Palomuuriin on täten sallittava ulospäin liikenne NTP-palvelimen verkko-osoitteeseen UDP-porttiin 123. Palomuuriin on myös tehtävä avauksia DNS-palvelimien eli nimipalvelimien osalta. Internetin laitteet kommunikoivat toistensa kanssa numeeristen IP-osoitteiden avulla. Nimipalvelin muuttaa verkko-osoitteiden nimet (esimerkiksi www.google.com) IP-osoitteiksi (esimerkiksi 111.222.33.44). Jotta tämä verkko-osoitteiden kääntäminen olisi mahdollista, on palomuuriin sallittava ulospäin liikenne TNNetin käyttämiin DNS-palvelimiin. (Hostingpalvelu.)

Vaikka palomuuriin sallitaan tiettyjä yhteyksiä ulospäin, eivät nämä yhteydet toimi ilman paluuliikenteen sallimista. Esimerkiksi kun otetaan yhteys Alma Linuxin päivityspalvelimeen, niin paketit pääsevät palomuurista ulos, mutta päivityspalvelimen lähettämä vastaus ei kuitenkaan pääse takaisin perille, koska sisääntulevaa liikennettä ei ole erikseen sallittu. Tämän takia palomuuriin on lisättävä sääntö, joka sallii saapuvat paketit, jotka kuuluvat jo avoinna olevaan yhteyteen. Kyseinen sääntö luodaan komennolla **iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT**. Säännöllä sallitaan siis paketit, jotka ovat osa jotakin avattua yhteyttä (ESTABLISHED) tai muuten liittyvät johonkin avoinna olevaan yhteyteen (RELATED). Kun säännön luomisen jälkeen otetaan ulospäin yhteys toiseen palvelimeen, niin palomuuri päästää läpi myös sisäänpäin toisen palvelimen lähettämät vastaukset. (Linux, 2021.)

5.1.3 Sertifikaatti

Palvelimelle on asennettava SSL-sertifikaatti, joka salaa nettisivulla kävijän ja palvelimen välisen yhteyden. Tällä voidaan estää ulkopuolisia henkilöitä lukemasta käyttäjän sivulle antamiaan henkilötietoja. Sertifikaatin ollessa voimassa nettisivun käyttäjä myös näkee osoiteriviltä, että sivu on turvallinen. Jos sertifikaattia ei olisi, ei osoiterivillä näkyvä ”Ei turvallinen”-teksti herättäisi asiakkaan luottamusta kyseistä sivua ja palvelua kohtaan. ITC:n turvapostipalvelimelle otettiin käyttöön Let’s Encrypt -sertifikaatti. Sertifikaatti on asennettu palvelimelle Apacheen Certbotilla, joka uusii sertifikaatin automaattisesti 60 päivän välein. (Suomen hakukonemestarit)



KUVA11. Voimassa oleva sertifikaatti.

5.2 Sec@GW-ratkaisun asennus ja konfigurointi

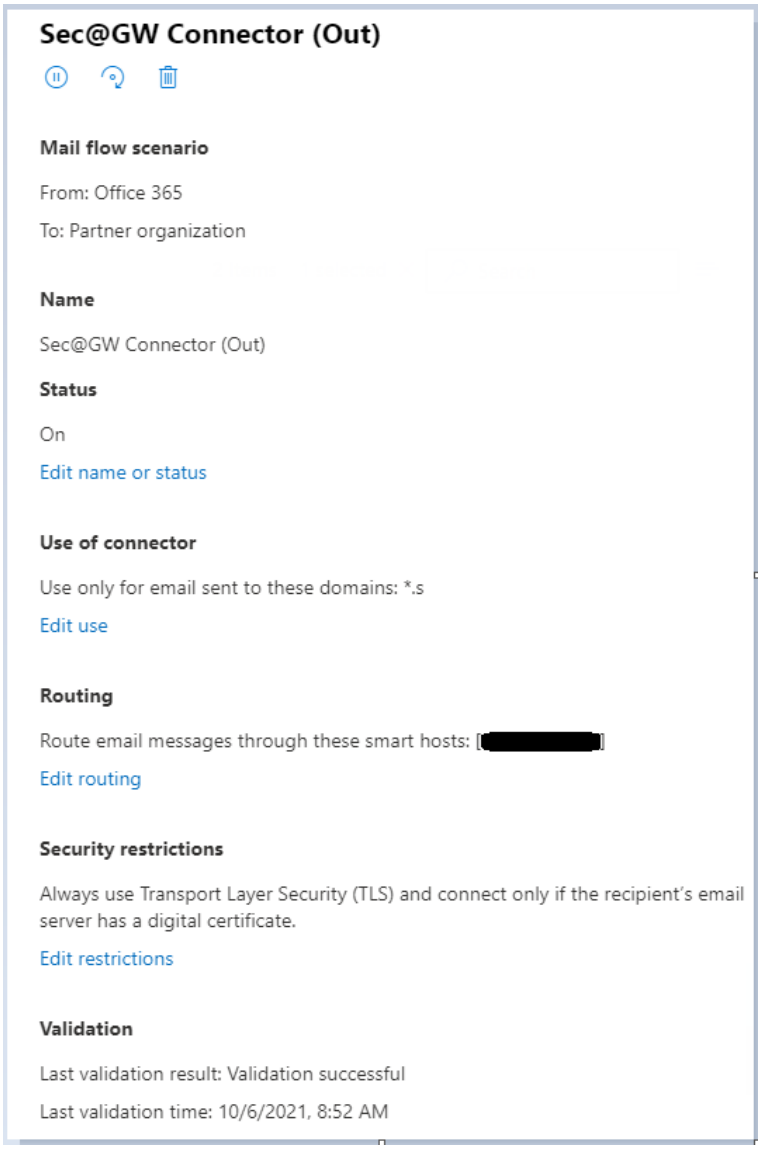
Verkkoyhteyksien avausten jälkeen palvelimelle luotiin Deltagonin käyttöön käyttäjätunnus ja salasana SSH-yhteyttä varten. Sec@GW-turvapostiratkaisun asennus ja pohjakonfigurointi tehtiin Deltagonin toimesta suojattua SSH-yhteyttä käyttäen.

5.3 Postin reititys

Asennusten jälkeen ITC:n domainin eli verkkotunnuksen SPF-tietueeseen lisättiin turvapostipalvelimen IP-osoite. SPF-tietueella kerrotaan vastaanottaville sähköpostipalvelimille, millä kaikilla palvelimilla on lupa lähettää viestejä yrityksen verkkotunnusta (esimerkiksi yritys.fi) käyttäen. Kun sähköpostipalvelin ottaa viestin vastaan, tarkistaa vastaanottava palvelin viestin lähettäjän sähköpostiosoitteen tiedoista, onko osoitteen verkkotunnukselle määritelty SPF-tietue. SPF-tietueen löytyessä vastaanottava palvelin tarkistaa, onko SPF-tietueeseen lisätty sallittujen listalle viestin lähetyksessä käytetty palvelin. Jos kyseistä palvelinta ei ole sallittu SPF-tietueeseen, niin sähköposti ohjataan roskapostiin tai viesti estetään kokonaan. SPF-tietueella voidaan siis estää huijausviestien saapuminen vastaanottajan postilaatikkoon, mutta myös toisaalta ehkäistä aitojen ja harmittomien viestien joutuminen roskapostiin. (Creamailer, 2021.)

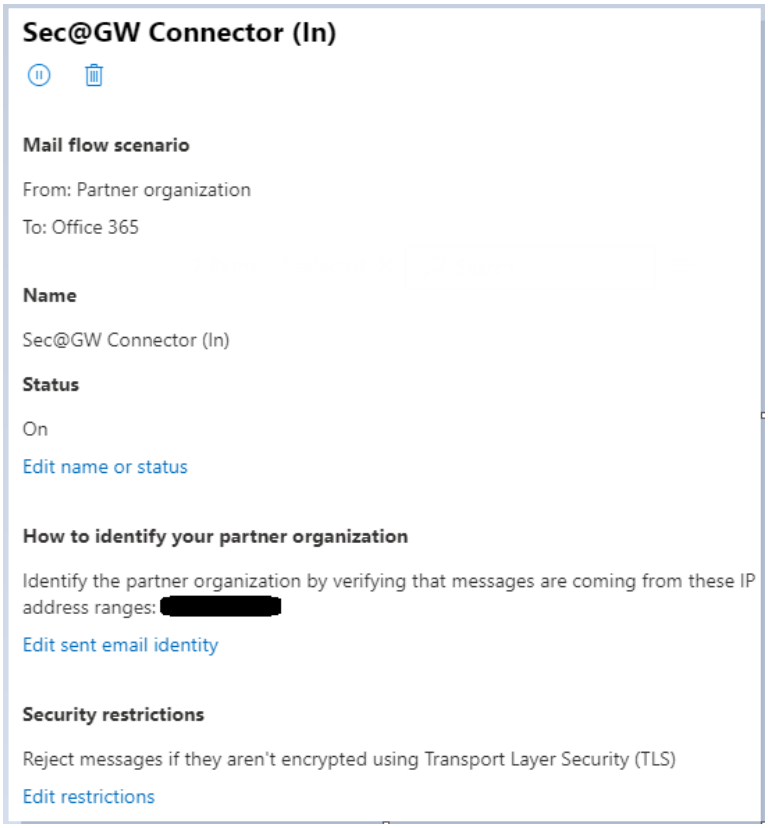
SPF-tietueen lisäksi tuli lisätä myös PTR-tietue. Kun nimipalvelu DNS kääntää selkokieliset verkko-osoitteet IP-osoitteiksi, niin käänteisnimipalvelu eli reverse DNS puolestaan kääntää IP-osoitteet selkokielisiksi verkko-osoitteiksi. PTR-tietueita käytetään reverse DNS hauissa. Jotkut sähköpostin roskapostisuodattimet käyttävät käänteisnimipalvelua tarkistaakseen sähköpostiosoitteiden verkkotunnukset ja arvioivat PTR-tietueen avulla, onko viesti lähetetty sallitulta sähköpostipalvelimelta. PTR-tietueen lisäämisellä vältetään turvapostipalvelimen kautta kulkevien viestien joutuminen vastaanottajan roskapostiin. PTR-tietueen lisäämisestä oli tehtävä pyyntö palvelintarjoaja TNNetille, koska tämä tietueen lisääminen ei ollut mahdollista meidän toimestamme. (Cloudflare.)

Jotta turvapostia pystyisi lähettämään lisäämällä vastaanottajan osoitteen perään ”.s”, on tätä varten luotava sääntö. ITC:n sähköpostit toimivat Microsoft 365 -ympäristössä, joten säännöt luotiin ITC:n M365 hallintakeskuksen alla olevaan Exchangen hallintakeskukseen. Exchangen hallintaan luotiin aluksi Outbound-yhdistin ”Sec@GW Connector (Out)”. Outbound-yhdistimellä määritetään, että kaikki sähköpostit, joiden vastaanottajan osoitteen perässä on ”.s”, reititetään ITC:n turvapostipalvelimen kautta. Yhdistimellä myös määritetään, että ”.s”-päätteellä lähetetty sähköposti lähetetään salattua yhteyttä käyttäen, joka vaatii toimiakseen voimassa olevan sertifikaatin turvapostipalvelimella.

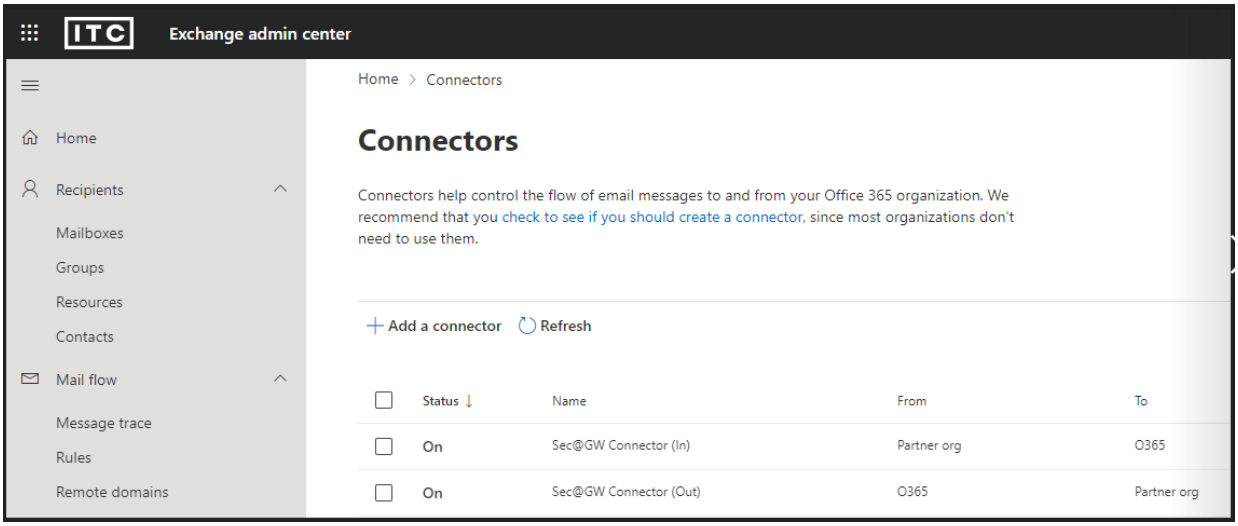


KUVA12. Outbound-yhdistin.

Exchangen hallintakeskukseen luotiin Outbound-yhdistimen lisäksi myös Inbound-yhdistin ”Sec@GW Connector (In)”. Inbound-yhdistimen avulla turvapostipalvelimen kautta saapuviin turvapostin vastausviesteihin luotetaan. Inbound-yhdistimessä on myös määritetty, että turvapostipalvelimelta tulevat viestit estetään, jos niitä ei ole salattu.

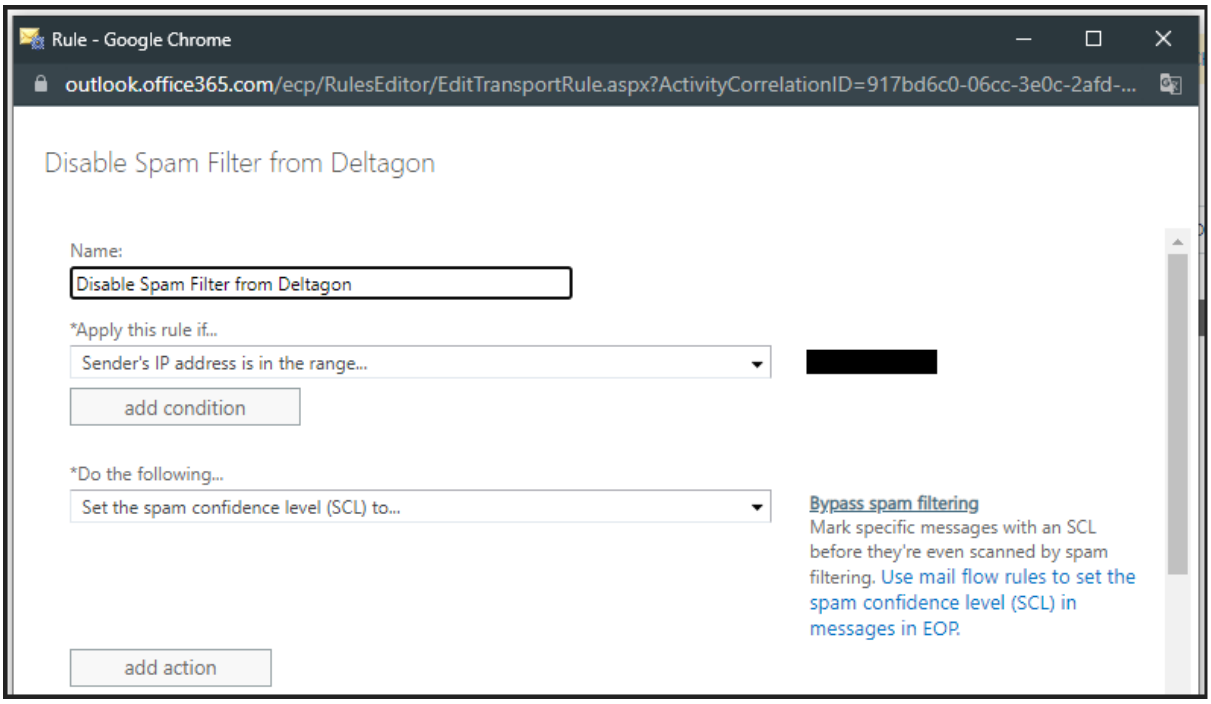


KUVA13. Inbound-yhdistin.



KUVA14. Luodut yhdistimet Exchangen hallintakeskuksessa.

Yhdistimien lisäksi ITC:n Exchange-hallintakeskuksessa luotiin sääntö roskapostisuodattimen ohittamiseksi, kun sähköposti saapuu ITC:n turvapostipalvelimen osoitteesta. Tällä säännöllä vähennetään mahdollisuutta siihen, että turvapostit päätyisivät vastaanottajan roskapostiin.



KUVA15. Roskapostisuodattimen ohitus.

5.4 Toimivuuden testaus

Yhdistimien luonnin jälkeen oli vuorossa turvapostin toimivuuden testaaminen. Salattujen sähköpostiviestien lähettämistä ja vastaanottamista testattiin ensin ITC:n ja Deltagonin välillä. Ensin salattu sähköpostiviesti lähetettiin Deltagonin ilmoittamaan osoitteeseen käyttämällä ”.s”-päätettä. Deltagon kuittasi salatun viestin saapuneen perille, mutta kyseiseen viestiin ei pystynyt vastaamaan. Yrittäessä vastata salattuun viestiin Deltagonin sähköpostilokiin tuli seuraava herja: ”Access denied, banned sending IP [*ITC:n turvapostipalvelimen osoite*]. To request removal from this list please visit https://sender.office.com/ and follow the directions.” Microsoft 365 oli lisännyt turvapostipalvelimen IP-osoitteen estolistalle, jonka takia viestiliikenne turvapostipalvelimen ja Microsoftin palvelimien välillä oli estynyt. Microsoft lisää estolistalle IP-osoitteet, jotka on merkattu mahdollisiksi uhkiksi Microsoftille syystä tai toisesta. Microsoft ei julkaise estolistalle päätymisen syytä. Turvapostipalvelimen määritysten ja yhdistimien ollessa kunnossa, pyysimme IP-osoitteen poistamista estolistalta ohjeistuksen mukaisesti. Microsoft poisti ITC:n turvapostipalvelimen IP-osoitteen estolistalta, jonka jälkeen salattua sähköpostia pystyi taas lähettämään ja nyt myös viestiin vastaaminen onnistui.

Onnistuneiden testausten jälkeen Deltagon lähetti salatun sähköpostin käyttöön liittyvät ohjeistukset, joiden avulla turvapostia alettiin testaamaan kattavammin yrityksen sisäisesti ITC:llä. Sisäisessä testauksessa havaittiin, ettei vastaanottajan puhelimeen koskaan saapunut viestin avaamiseen tarvittavaa PIN-koodia, kun sähköposti lähetettiin ”Kirjattu kirje”-valinnalla. Tekstiviestitunnistautumisen konfigurointi oli tehty palveluntarjoajan toimesta, kuten oli sovittu. Tekemäämme vikailmoitukseen vastattiin, että PIN-koodin lähetykseen tarvittava palomuuriavaus oli jossain välissä kadonnut.

Palomuuriavauksen uudelleen lisäämisen jälkeen PIN-koodit saapuivat perille ja salatun viestin sai auki myös, kun viesti oli lähetetty ”Kirjattu kirje”-valinnalla. Sisäisessä testauksessa testattiin myös Sec@GW Outlook-pluginin toimivuutta ja salatun sähköpostin lähetystä pluginin avulla. Aiemman PIN-koodin saapumisen toimimattomuuden lisäksi testauksessa ei ilmennyt muita ongelmia.

6 YHTEENVETO

Projekti saatiin onnistuneesti maaliin ja ITC-Solution Group sai käyttöönsä turvapostiratkaisun, joka toimii ITC:n hallinnoimalla pilvipalvelimella. Projekti mahdollisti turvapostiratkaisun jälleenmyynnin yritysasiakkaille. Projektissa ilmenneistä erinäisistä ongelmista huolimatta itse turvapostin lopputuotteen toiminnallisuuteen ja käytettävyyteen oltiin tyytyväisiä. Opinnäytetyöhön tehtyä raporttia voidaan hyödyntää yrityksen sisäisessä dokumentaatiossa sekä turvapostin esittelyssä ja ohjeistuksessa asiakkaille. Kyseisen projektin toteutus ja opinnäytetyön raportin kirjoittaminen edellyttivät minulta uusien asioiden ja tekniikoiden opettelua. Myös ennestään tuttuihin aiheisiin piti perehtyä syvemmin ymmärtääkseni ne paremmin. Koen, että tämä opinnäytetyö toi minulle tärkeää osaamista palvelimiin, pilviympäristöihin ja sähköpostin salaukseen liittyen.

7 LÄHDELUETTELO

ITC, julkaisuaika tuntematon. Yrityksemme. Verkkojulkaisu. https://www.itc.fi/yrityksemme/. Viitattu 29.10.2021.

Kukkonen, julkaisuaika tuntematon. Salattu sähköposti - Opas asiakasviestinnän suojaamiseen. Pdf-tiedosto. https://kirjasto.tietosi.fi/aineisto/salattu-sahkoposti-opas-asiakasviestinnan-suojaamiseen?c=blog&utm_source=blog. Viitattu 30.10.2021.

Saikkonen Paavo, 2020. Osaako yrityksesi sähköpostin salaamisen käytännöt? Rauhalan blogi. 15.6.2020. https://www.rauhala.fi/blog/osaako-yrityksesi-sahkopostin-salaamisen-kaytannot. Viitattu 31.10.2021.

Deltagon, julkaisuaika tuntematon. 10 syytä salata yrityksesi sähköpostit. Deltagonin blogi. https://www.deltagon.com/fi/blogi/10-syyta-salata-yrityksesi-sahkopostit. Viitattu 31.10.2021.

Tietosuojavaltuutetun toimisto, julkaisuaika tuntematon. Usein kysyttyä EU:n tietosuoja-asetuksesta. Verkkojulkaisu. https://tietosuoja.fi/gdpr. Viitattu 1.11.2021.

Seclion, 2021. Mitä on fyysinen tietoturvallisuus? Blogi. Julkaistu 7.1.2021. https://blog.seclion.fi/turvallisuus/fyysinen-tietoturvallisuus. Viitattu 28.11.2021.

EY Suomi, 2019. Täyttääkö organisaatiosi EU:n yleisen tietosuoja-asetuksen (GDPR) vaatimukset? Verkkojulkaisu. Julkaistu 28.10.2019. https://www.ey.com/fi_fi/law/tietosuoja-asetus. Viitattu 2.11.2021.

Tietosuojavaltuutetun toimisto, julkaisuaika tuntematon. Tietosuojavastaavat. Verkkojulkaisu. https://tietosuoja.fi/tietosuojavastaavat. Viitattu 28.11.2021.

Tietosuojavaltuutetun toimisto, julkaisuaika tuntematon. Vaikutustenarviointi. Verkkojulkaisu. https://tietosuoja.fi/vaikutustenarviointi. Viitattu 28.11.2021.

Tietosuojavaltuutetun toimisto, julkaisuaika tuntematon. Ilmoitus tietoturvaloukkauksesta. Verkkojulkaisu. https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta. Viitattu 28.11.2021.

Tietosuojavaltuutetun toimisto, julkaisuaika tuntematon. Kerro käsittelystä rekisteröidylle. Verkkojulkaisu. https://tietosuoja.fi/rekisteroidyn-informointi. Viitattu 28.11.2021.

Deltagon, julkaisuaika tuntematon. Sec@GW internal instruction ITC. Pdf-tiedosto. FI_Sec@GW_internal_instruction_ITC.pdf. Viitattu 3.11.2021.

Suomen hakukonemestarit, julkaisuaika tuntematon. Mikä on SSL-sertifikaatti, ja miksi kotisivut tarvitsevat sellaisen? Verkkojulkaisu. https://www.hakukonemestarit.fi/blogi/mika-on-ssl-sertifikaatti-ja-miksi-kotisivut-tarvitsevat-sellaisen/. Viitattu 9.11.2021.

Linux, 2021. iptables. Verkkojulkaisu. https://www.linux.fi/wiki/Iptables. Viitattu 20.11.2021.

Hostingpalvelu, julkaisuaika tuntematon. Mikä on domainin nimipalvelin/nimipalvelu (DNS). Verkkojulkaisu. https://www.hostingpalvelu.fi/ohjeet/yleiset-domain-ohjeet/mika-on-domainin-nimipalvelinnimipalvelu-dns/. Viitattu 20.11.2021.

Creamailer, 2021. SPF-tietue. Verkkojulkaisu. https://tuki.creamailer.fi/hc/fi/articles/115001428332-SPF-tietue. Viitattu 23.11.2021.

Cloudflare, julkaisuaika tuntematon. What is a DNS PTR record? Verkkojulkaisu. https://www.cloudflare.com/learning/dns/dns-records/dns-ptr-record/. Viitattu 29.11.2021.