EXTRANET-PALVELUIDEN TURVALLINEN JULKAISEMINEN INTERNETIIN

CASE CINIA

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Riihimäki, Tietotekniikan koulutusohjelma

kevät 2017

Janne Pankkonen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietotekniikan koulutusohjelma
Riihimäki

Tekijä Janne Pankkonen **Vuosi** 2017

Työn nimi Extranet-palveluiden turvallinen julkaiseminen internetiin.

TIIVISTELMÄ

Organisaatiot tarvitsevat turvallisen tavan julkaista sisäverkon palveluita extranet-järjestelmällä ulkopuolisille käyttäjille. Työn tarkoituksena oli ymmärtää sisäverkon palveluiden julkaisemiseen liittyvää järjestelmä-, tietoliikenne- ja sovellustietoturvaa. Tavoitteena oli selvittää ammattilaisten kokemuksia extranet-järjestelmäkoko-naisuuden tietoturvavaatimuksista.

Opinnäytetyön teoreettinen viitekehys muodostuu tietoliikenneturvallisuuden perusteista, sovellusten ja palveluiden tietoturvasta sekä extranet-palveluissa käytettävistä teknisistä ratkaisuista.

Empiirisessä osuudessa tutkimusmenetelmänä käytettiin kvalitatiivista haastattelututkimusta ja metodina puolistrukturoitua teemahaastattelua. Case-yrityksenä oli verkkopalveluita, telematiikan järjestelmäratkaisuja, ohjelmisto- ja pilvipalveluita tuottava Cinia Oy.

Tutkimustulokset osoittivat kolme eri tekijää, jotka vaikuttavat sisäverkon palveluiden turvalliseen julkaisemiseen. Näitä olivat laitteet/komponentit, tekniset menetelmät/toiminnot ja työntekijöiden inhimilliset ominaisuudet.

Teknisissä menetelmissä ja toiminnoissa on panostettava luotettavaan pääsynhallintaan. Muilla tietoturvatoiminnoilla ei ole merkitystä, jos käyttäjätunnistus sallii väärien henkilöiden pääsyn järjestelmään tai antaa liian laajat käyttöoikeudet.

Verkkosovellukset yleistyvät ja niiden tietoturvariskit kasvavat. Tämän estämiseksi sovelluksia on kehitettävä jo ohjelmointivaiheessa. Lisäksi tarvitaan inhimillisiä tekijöitä, kuten ammattitaitoa ja proaktiivisuutta estettäessä uusia kehittyneimpiä hyökkäyksiä tunkeutumasta sisäverkon palveluihin.

Jatkokehityksenä voidaan tutkia automatisoitua järjestelmän poistamisen ja palauttamisen merkitystä tietoturvaan.

Avainsanat Reverse proxy, Extranet, Tietoturva.

Sivut 41 s. + liitteet 2 s.

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Information Tecnology
Riihimäki

Author Janne Pankkonen **Year** 2017

Subject Publication of the extranet services securely to the Internet.

ABSTRACT

Organizations need a secure way to publish intranet services with extranet system to external users. The works aim was to understand the system-, telecommunication- and application security aspects in publishing intranet services. The aim was also to find out professionals experiences about the extranet system security requirements.

The theoretical framework consists of basis of the telecommunication security, security of network applications and services as well as technical implementations used in extranet services. The empirical part of the research was using qualitative research interview where semi-structured interviews were used as a method. Cinia Oy which provides network services, telematic system solutions, software- and cloud services was used as an example case-company.

The research results were showing three different factors that were affecting to the secure launch of the intranet services. These were the
devices/components, used technical methods/functions and human characteristics the employees. On technical methods and functions we should focus on the reliable access control. Other security functions do not matter if the user authentication grants access for the wrong persons to the system or gives too broad access rights.

Web applications are becoming more common and their security risks are increasing. To prevent this the applications should be developed already in the programming phase. Additionally also human factors such as the expertise and proactivity are needed when preventing new more sophisticated attacks to the internal network services.

As a further development we can investigate the usage of the system's automated removal and restoration's significance to the information security.

Keywords Reverse proxy, Extranet, Information security

Pages 41 p. + appendices 2 p.

SISÄLLYS

TERMIT JA LYHENTEET

AAA	Authentication, Authorization ja Accounting. Todentaminen, valtuutus ja tilastointi ovat menetelmiä, joilla käyttäjä tunnistetaan verkossa.
API	Application Programming Interface on ohjelmointirajapinta, jonka välityksellä sovellukset keskustelevat keskenään.
ADC	Application Delivery Controller on edistynyt kuormantasaaja, joka reitittää ja optimoi sovellusliikennettä.
BOTNET	Bottiverkko on joukko internetissä toisiinsa kytkeytyneitä tietokoneita.
CSRF	Cross-Site Request Forgery on hyökkäys, jossa käyttäjä yritetään saada suorittamaan haitallinen toiminto.
CONTENT CACHING	Reverse-proxyn toiminto, joka tallentaa web-palvelinten staattista sisältöä, joka nopeutta selainta ja vähentää web-palvelin kuormaa.
DDOS	Distributed Denial of Service, hajautettu palvelunestohyökkäys, jossa palvelua pyritään kaatamaan useasta eri lähteestä käsin.
DMZ	Demilitarized Zone on internetin ja yrityksen sisäverkon väliin sijoittuva verkkoalue, johon sijoitetaan palvelimet, joihin on tarve liikennöidä sekä internetistä että yrityksen sisäverkosta.
DOS	Denial of Service on palvelunestohyökkäys, jonka tarkoituksena pyrkiä estämään verkkopalvelun käyttö.
EXTRANET	Sisäverkon osa, mitä yritys hyödyntää tiedonjakamisessa asiakkaiden tai yhteistyökumppanien välillä.
IDS	Intrusion Detection System on epäilyttävän verkkoliikenteen havaitsemisjärjestelmä.
IPS	Intrusion Prevention System on epäilyttävän liikenteen estojärjestelmä.
LDAP	Lightweight Directory Access Protocol on käyttäjä tunnistukseen ja valtuuksien tarkistukseen käytetty protokolla.

NAT	Network Address Translation on osoitteen muutostoiminto, jolla voidaan yhden julkisen IP-osoitteen taakse piilottaa useampi yksityisen verkon osoite.
PoC	Proof of Consept on järjestelmän soveltuvuustestaus.
RBAC	Role Based Access Control on roolipohjainen tunnistusmalli, jossa oikeudet annetaan käyttäjäroolin mukaisesti.
REVERSE PROXY	Käänteinen välitys -palvelin, joka välittää internetistä web-selaimen asiakaspyyntöjä sisäverkon palvelimille piilottaen sisäverkon palvelimien osoitteen.
SPOF	Single point of failure on järjestelmän yksittäinen piste / osa, joka vikaantuessa aiheuttaa koko järjestelmän toimimattomuuden.
SSL	Secure Socket Layer on asiakas koneen ja palvelimen välisen liikenteen salaamiseen käytetty teknologia.
SSL OFFLOAD	Tarkoittaa salatun SSL liikenteen terminointia, jossa salaus puretaan hallitusti.
SSO	Single Sign-On kertatunnistusmenetelmä, jossa käyttäjän ei tarvitse tunnistautua uudelleen palveluihin.
SQL	Structured Query Language standardoitu kieli, jolla hallitaan relaatiotietokantoja ja suoritaan toimenpiteitä niihin.
SECURITY TOKEN	Vahvan tunnistuksen toteutukseen käytetty laite, jonka lisäksi käyttäjän tulee tietää siihen liittyvä PIN-koodi.
OSI	Open Systems Interconnection on malli, jonka perusteella sovellukset kommunikoivat verkossa.
OTP	One Time Password on tunnistusmenetelmä, jota käytetään vahvassa tunnistuksessa toisena tunnistuksen tekijänä.
OWASP	Open Web Application Security Project on järjestö, joka auttaa parantamaan sovellustietoturvaa.
VIRTUAL PATCH	Tarkoittaa sovellushaavoittuvuuden paikkausta sovelluspalomuuriin tehtävällä säännöllä.
VLAN	Virtual Local Area Network tarkoittaa että, fyysinen verkko voidaan jakaa loogisiksi virtuaalilähiverkoiksi.

VPN	Virtual Private Network on internetin tai runkoverkon välityksellä kahden kohteen välille muodostettu salattu liikennetunneli.
WAF	Web Application Firewall on verkkosovellus palomuuri, jolla voidaan estää sovelluksiin kohdistuvia yleisimpiä tietoturvahyökkäyksiä
XSS	Cross site scripting on sovelluksissa esiintyvä tietoturva-aukko.

1 JOHDANTO

Johdannossa esitellään aihe ja käsitellään aiheen merkitystä. Johdanto on jaoteltu kolmeen osaan, jotta aiheen merkitys, tavoite ja tarkoitus ja rajaukset tulevat selkeästi ilmi. Lisäksi johdannosta voidaan hahmottaa opinnäytetyön tiedon tarpeellisuus, uutuusarvo ja sijoittuminen teoriaan.

1.1 Aihealueen esittely ja merkitys

Opinnäytetyö käsittelee extranetin sisäverkon palveluiden turvallista julkaisemista organisaation ulkopuolisille käyttäjille. Teoriassa keskitytään tietoliikenneturvallisuuteen, sovellustietoturvaan ja teknisiin menetelmiin, joilla yritys voi tarjota palveluitaan turvallisesti asiakkaille, sidosryhmille, konsulteille ja yhteistyökumppaneille.

Andersson & Koivisto (2013, 202) painottavat, että palveluiden tarjoamisen on oltava tehokasta. Yrityksen pitää kuitenkin huomioida tiedon luottamuksellisuus ja tehokkuutta ei voida pitää ainoana kriteerinä. Luottamuksellisen tiedon käsittelyn on tapahduttava julkisen verkon (internet) välityksellä turvallisesti. Luottamuksellisuuden varmistamisen kannalta on tärkeää, että palvelua pääsevät käyttämään vain ne henkilöt, joilla on siihen oikeus.

Andersson ym. (2013, 75) jakaa verkon suojaamisen hallinnolliseen ja tekniseen suojaamiseen, joilla vastataan organisaation tietoon kohdistuviin uhkiin, vaatimuksiin ja turvallisuustarpeisiin. Extranetin välityksellä tapahtuvassa tiedonsiirrossa keskitytään teknisiin menetelmiin. Teknisillä menetelmillä pitää pystyä itse tiedon siirtoon ja estämään luvaton pääsy organisaation sisäverkon tietoihin ja palveluihin (Järvinen 2003, 29). Siksi tietoturvaa voidaan pitää extranet-järjestelmien yhtenä merkittävimmistä haasteista.

Digitalisaation käsite on hyvin ajankohtainen ilmiö. Internetin käytön laajentumisen vuoksi erilaisten verkkosovellusten määrä on lisääntynyt huomattavasti ja niitä käytetään erilaisilla päätelaitteilla paikasta ja ajasta riippumatta (Ristić 2014, 1). Tämä tekee juuri extranet-järjestelmien hyödyntämisestä hyvin ajankohtaisen aiheen.

Tieturvasta ja sisäverkon suojaamisesta on saatavilla aikaisempaa tutkimustietoa. Näissä tutkimuksissa ei ole syvennetty tutkimaan sisäverkon palveluiden julkaisua internetin välityksellä. Lehto (2008) on tehnyt pro gradu -tutkielman extranet-järjestelmien tietoturvasta, mutta tutkielmassa aihetta käsiteltiin enemmän hallinnollisesta näkökulmasta. Tämän takia on hyödyllistä lisätä tietoa juuri teknisestä näkökulmasta.

Empiirisen osuuden tavoitteena on selvittää ammattilaisten kokemusten perusteella tekijöitä, jotka ovat välttämättömiä extranet-palveluiden turvallisessa julkaisemisessa käyttöönoton ja käytön aikana. Case-yrityksenä on verkkopalveluita, telematiikan järjestelmäratkaisuja, ohjelmisto- ja pilvipalveluita tuottava Cinia Oy.

Tietoturvaa käsittelevällä teorialla on pitkä historiallinen tausta. Tietoliikenteestä ja sovelluksista löytyy uutta kirjallisuutta ja artikkeleita. Extranettia koskevaa teoreettista kirjallisuutta on taas hyvin vaikea löytää. Opinnäytetyön tekninen viitekehys muodostuu kirjoista, sähköisistä lähteistä, artikkeleista ja aikaisemmista tutkimuksista.

Tarkoituksena on se, että opinnäytetyön uusi tekninen tieto hyödyntää varsinkin tietotekniikan parissa työskenteleviä henkilöitä. Opinnäytetyö on termeiltään ja lähteiltään teknistä.

1.2 Tutkimuksen tavoite ja ongelmat

Opinnäytetyön tarkoituksena on ymmärtää sisäverkon palveluiden julkaisemiseen liittyvää järjestelmä-, tietoliikenne- ja sovellustietoturvaa. Tavoitteena on selvittää IT-ammattilaisten kokemuksia extranet-järjestelmäkokonaisuuden tietoturvavaatimuksista ja kuvata tietoturvan eri tekijöitä.

Case-yritys Cinialla on käytössään extranet-palvelu, jonka välityksellä se julkaisee taustapalveluita asiakkaille, sidosryhmille ja yhteistyökumppaneille. Taustapalveluina julkaistaan muun muassa työnohjausta ja valvontapalveluita. Nykyisen ympäristön ohjelmistot, palvelinlaitteistot ja käyttöjärjestelmä ovat vanhentuneet ja eivät nykyisellään tarjoa riittävää tietoturvatasoa.

Case-yritys on käyttänyt testauksessa avoimeen lähdekoodiin perustuvaa LemonLdap -ohjelmistoratkaisua, jolla taustapalvelut julkaistaan ulkoverkosta käytettäväksi. Julkaistavat taustapalvelut ovat testiympäristöjä, jotka vastaavat nykyisin käytössä olevia tuotantoympäristöjä. Case-yrityksessä on ilmennyt tarve löytää tietoa extranet-järjestelmäkokonaisuuden tietoturvavaatimuksista tukemaan extranet-järjestelmien suunnittelua, käyttöä ja ylläpitoa. Tämän johdosta tutkimusongelmana on löytää vastaus siihen, miten organisaatio voi tietoturvallisesti julkaista sisäverkon palveluita extranet-järjestelmällä ulkopuolisille käyttäjille?

Lisäksi alaongelmina selvitetään:

- Minkälaisia tietoturvaan liittyviä tekijöitä tulee huomioida extranet- järjestelmien suunnittelussa, käytössä ja ylläpidossa?
- Mitä järjestelmän tietoturvallisuudelta vaaditaan?
- Millä toimenpiteillä parannetaan extranet-järjestelmien tietoturvaa?

1.3 Rajaukset

Tutkimus kohdistuu extranet-järjestelmiin, niiden teknisiin ratkaisuihin, tietoliikenneturvallisuuteen ja verkkosovellusten tietoturvaan. Tutkimuksen teoriassa keskitytään aluksi tieturvaan yleisellä tasolla. Tämän jälkeen käsitellään extranetin tietoliikenneturvallisuuden kannalta tärkeitä tekniikoita.

Verkkosovelluksien ja palveluiden tietoturvan teoriassa keskitytään yleisesti verkkosovelluksiin liittyviin haasteisiin ja uhkiin. Tämän jälkeen syvennytään tarkemmin verkkosovelluksien sisältämiin yleisimpiin haavoittuvuuksiin ja suojausmenetelmiin.

Teorian viimeisessä osiossa käsitellään extranetejä yleisesti ja extranet-toteutuksissa käytettäviä teknisiä ratkaisuja. Lisäksi osiossa perehdytään sovelluspalomuuriin, liikenteen salaukseen ja kertakirjautumisjärjestelmä teknologiaan. Teorian ulkopuolelle jätetään extranetin kautta julkaistavat taustapalvelut, virustorjuntajärjestelmä, auditointi ja tunnistukseen käytettävä LDAP-pääsynhallintajärjestelmä.

Tutkimusmenetelmäksi valittiin kvalitatiivinen tapaustutkimus ja haastattelu, koska haluttiin ymmärtää kohdetta syvällisesti ja huomioida Cinia Oy:ssä vallitsevat olosuhteet ja taustat. Tapaustutkimus sopii myös menetelmäksi projekti-, kehittämis- ja arviointitutkimuksiin. (Saaranen-Kauppinen & Puusniekka 2016, 43.)

2 TEOREETTINEN OSUUS

Extranet-palveluiden turvallisen julkaisemisen teoriapohja muodostuu tietoliikenneturvallisuudesta, verkkosovellusten ja palveluiden tietoturvasta, extraneistä sekä niiden teknisistä ratkaisuista. Teorialuvuissa on esitelty empiirisen osuuden kannalta olennaisimmat teoriat.

2.1 Tietoliikenneturvallisuuden teoreettinen viitekehys

2.1.1 Tietoturvan perusta

Tietotekniikassa tietoturvalla tarkoitetaan tietojen, palveluiden, laitteiden, järjestelmien, tietoliikenteen ja sovelluksien suojaamista. Tietoturva koostuu kerroksista, joita luodaan järjestelmillä, teknisillä- ja hallinnollisilla menetelmillä.

Tietoturvan päämäärät luokitellaan luottamuksellisuuteen, eheyteen, saatavuuteen, pääsynvalvontaan, kiistämättömyyteen ja todentamiseen (Järvinen 2003, 29–34). Andreasson ym. (2013, 78) painottaa näistä erityisesti luottamuksellisuutta, eheyttä ja käytettävyyttä.

Tietojen luottamuksessa on kyse siitä, että tietoon on pääsy vain siihen oikeutetuilla henkilöillä (Järvinen 2003, 29). Luottamuksellisuuteen liittyvät suojaamisvelvoitteet, jotka perustuvat julkisuuslakiin, henkilötietolakiin ja salassapitoa koskevaan erityislainsäädäntöön (Andreasson ym. 2013, 78). Luottamuksellisessa tiedonsäilytyksessä tieto salataan, jolloin salattuun tietoon voivat päästä käsiksi vain siihen oikeutetut henkilöt. Tiedon siirrossa luottamuksellisuus toteutetaan salaamalla tiedonsiirtoyhteys hyödyntäen SSL- ja VPN-tekniikoita. (Vacca 2011, 112–113.)

Eheydellä tarkoitetaan, että luottamukselliseen tietoon ei tehdä oikeudettomia muutoksia tiedon muokkauksen, siirron tai säilytyksen aikana. Luottamuksellisesti säilytetty tai siirretty tieto ei vielä tarkoita, että tieto on säilynyt eheänä siirron ajan. Tämän johdosta luottamuksellisuus ei tarkoita eheyttä. (Järvinen 2003, 31.) Tiedon eheyden varmistamiseksi käytetään tarkistussumma menetelmää, jolla tarkistetaan, onko tieto korruptoitunut säilytyksen tai siirron aikana. Tiedon säilytyksessä tapahtuvaan korruptoitumiseen voidaan varautua tiedon varmuuskopioinnilla (Vacca 2012, 113).

Saatavuudella tarkoitetaan, että tieto on saatavilla paikasta ja ajasta riippumatta. Saatavuuteen vaikutetaan erilaisilla teknisillä menetelmillä esimerkiksi laitteiden, järjestelmien ja tietoliikenneyhteyksien kahdentamisella (Järvinen 2003, 31).

Tietoturva pohjautuu kahdeksan eri osa-alueeseen. Näitä ovat hallinnollinen-, henkilöstö-, fyysinen-, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus. (Andreasson ym. 2013, 52.)

2.1.2 Tietoliikenneturvallisuus

Extranetin teknisen tietoturvan teoriassa keskitytään erityisesti tietoliikenneturvallisuuteen. Tietoliikenneturvallisuus tarkoittaa sitä, että organisaation tietoliikennetoiminnot ja niitä toteuttavat eri verkkojärjestelmät suunnitellaan ja rakennetaan siten, että verkossa siirrettävän tiedon eheys, luottamuksellisuus ja saatavuus pystytään riittävän hyvin suojaamaan. (Andreasson ym. 2013, 69.)

Tietoliikenneturvallisuus on otettava huomioon organisaation verkon suunnitteluvaiheessa. Tietoturvallisen verkon suunnittelussa on tunnistettava laitteet, järjestelmät ja palvelut, joita verkkoon liitetään. Tällä tunnistetaan, minkä tyyppistä tietoa verkossa siirretään. (Andreasson ym. 2013, 69.) Tiedon perusteella voidaan verkkoa jaotella fyysisesti ja loogisesti eri verkkoalueisiin. Suunnitteluvaiheessa kannattaa huomioida myös tulevaisuuden tarpeita, koska verkkotopologian muuttaminen jälkeenpäin on työläämpää ja kalliimpaa (Andreasson ym. 2013, 69–70).

Verkkotietoturvan ydinosia ovat pääsynhallinta, palomuurit, sovellustietoturva, IDS-järjestelmät (epänormaalin liikenteen tunnistus), segmentointi (verkon jaottelu), VPN, internet-tietoturva, langaton tietoturva ja virustorjunta (Cisco 2016). Seuraavissa luvuissa käsitellään tarkemmin verkkoturvallisuuden ydinosista: pääsynhallintaa, palomuuria ja segmentointia sekä IDS-järjestelmiä.

2.1.3 Pääsynhallinta

Pääsynhallinta on yksi tietoturvan keskeisimpiä asioita. Pääsynhallinnalla tarkoitetaan tietoturvan aluetta, jolla hallinnoidaan ihmisten ja järjestelmien kommunikointia toisten järjestelmien sekä resurssien kanssa. Pääsyhallinnan tärkein tarkoitus on turvata luottamuksen, kiistämättömyyden ja saatavuuden menetystä (Stewart, Chapple & Gibson 2012, 4).

Pääsynhallintaprosessissa tapahtuu tunnistus, todennus ja käyttövaltuutus. Tunnistus tarkoittaa prosessia, jossa henkilö syöttää käyttäjätunnuksen järjestelmään, jotta järjestelmä voi erottaa, kuka on tunnistautumassa (Stewart ym. 2012, 9). Todennus on prosessi, jossa henkilön todennetaan olevan tunnistamisessa väittämänsä henkilö (Stuttard & Pinto 2011, 18). Prosessissa todennusjärjestelmä tarkistaa käyttäjän syöttämän tunnus ja salasana -yhdistelmän tietokannasta. Jos molemmat löytyvät, on todennus tapahtunut. (Stewart ym. 2012, 9.)

Valtuutus tarkoittaa sitä, että tunnistetulla ja todennetulla henkilöllä on valtuudet suorittaa tietty toiminto. Valtuutuksella annetaan ja rajoitetaan oikeuksia tehdä ja suorittaa toimintoja. Todennus ei vielä tarkoita, että henkilöllä on valtuudet päästä käsiksi tiedostoon (Vacca 2012, 391). Käyttäjä voidaan käytännössä päästää sisään ilman valtuuksia suorittaa mitään toimenpiteitä. Stewart ym. (2012, 11) toteaa, että tunnistusta ja todennusta voidaan ajatella pääsynhallinnassa kaikki tai ei mitään -menetelmänä.

Vastuullisuus on tärkeä pääsynhallinnan elementti. Tämä tarkoittaa sitä, että käyttäjää pidetään vastuullisena tekemistään toimenpiteistä. Vastuullisuus toteutetaan auditoinnilla, lokituksella ja valvonnalla, jotta saadaan tietoa siitä, kuka teki, mitä teki ja milloin teki (Stewart ym. 2012, 11).

Pääsynhallintaa varten tarvitaan pääsynhallintajärjestelmä, jonka tehtävänä on toteuttaa käyttäjälle tunnistus, todennus ja valtuutus. Pääsynhallintaa suoritetaan keskitetysti tai keskittämättömästi. Keskitetty pääsynhallinta tarkoittaa sitä, että käyttäjien oikeuksia hallitaan keskitetysti yhdestä paikasta. Keskittämätön pääsynhallinta tarkoittaa, että käyttäjille on määriteltävä oikeudet erikseen jokaiselle laitteelle tai palvelimelle. Keskittämätön pääsynhallinta tuottaa enemmän ylläpidollista työtä, koska jokainen laite on yksilöllisesti määriteltävä pääsynhallintamuutosten vuoksi. (Stewart ym. 2012, 27.) Keskittämätön pääsynhallinta on tietoturvan kannalta haasteellisempi, koska esimerkiksi käyttäjille saatetaan antaa helposti enemmän käyttöoikeuksia kuin oikeasti tarvitsisi.

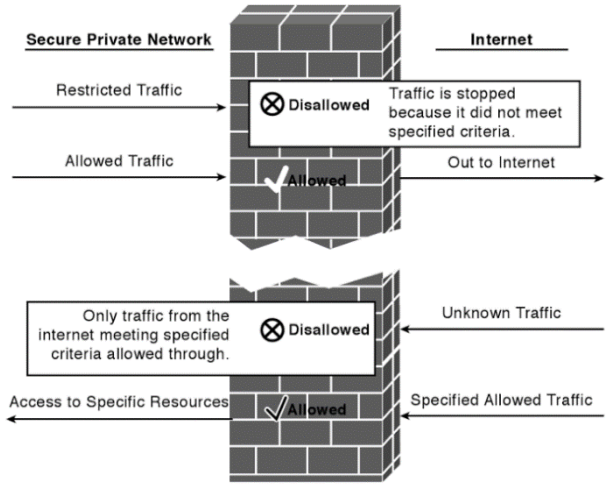
Hakemistopalvelu on tavallisesti käytössä oleva keskitetty pääsynhallintajärjestelmä, jonka tietokannassa ovat objekteina käyttäjät ja tietokoneet. Hakemistopalvelun tehtävänä on tarjota käyttäjille ja tietokoneille tunnistusta ja valtuutusta. Hakemistopalvelussa kaikki käyttäjät ja tietokoneet jakavat saman tietoturvapolitiikan. (Stewart ym. 2012, 27.)

2.1.4 Palomuuri ja segmentointi

Organisaation data ja sisäverkko on suojattava ulkoisilta tunkeutujilta. Verkon suojaukseen käytetään palomuuria. Monille organisaatioille se on ainoa verkkotason suojautumiskeino ulkoisilta uhilta. Palomuuri ei kuitenkaan yksin riitä nykyään takaamaan riittävää verkkotason tietoturvaa. (Harwood 2011, 132.)

Palomuuri on laitteisto tai sovellus, jonka tehtävänä on toimia tietoturvaporttina yrityksen sisäverkon ja ulkoisen internetin välillä, jonka lävitse kulkee kaikki liikenne sisään ja ulos. Palomuurin tehtävänä on hallinnoida, estää ja valvoa sisään- ja ulospäin kulkevaa tietoliikennettä (Harwood 2011, 132).

Palomuuriin on määritelty erilaisia sääntöjä ja pääsynhallintalistoja, joiden perusteella se suodattaa ja estää läpikulkevia tietoliikennepaketteja (Liu 2010, 1–2). Palomuuri on hyvä esimerkki sääntöihin pohjautuvasta pääsynhallintajärjestelmästä (Stewart ym. 2012, 23). Säännöillä tietoliikennepaketteja suodatetaan ja estetään pakettien protokolliin, portteihin ja lähdeosoitteeseen tai IP-pakettien sisältämään dataan perustuen. Kuvassa 1 palomuuri suodattaa sisään- ja ulosmenevää liikennettä.



Kuva 1. Palomuurin toimintaperiaate (Thomas & Stodart 2012).

Palomuuri pystyy piilottamaan ulospäin sisäverkon verkkotopologian ja IP-osoiteavaruuden. Ne eivät pysty estämään virusten pääsyä verkkoon, koska ne eivät tarkista liikennettä skannaamalla, kuten virustorjuntaohjelmistot tekevät. Palomuurien tarkoituksena on tarjota suojaa verkoille, joihin liikenne tulee palomuurin kautta. Tämä merkitsee sitä, että se ei pysty suojaamaan liikennettä, joka tapahtuu verkon sisällä. (Stewart ym. 2012, 116.)

Palomuurien ominaisuuksiin kuuluu myös NAT-osoitteenmuutostoiminto, jolla yritykset voivat käyttää julkisia IP-osoitteita julkisessa verkossa ja yksityisiä osoitteita sisäverkossa (Thomas 2015, 101). Toiminnolla suojataan sisäverkossa sijaitsevien laitteiden identiteettiä ja organisaatiot saavat enemmän joustavuutta IP-osoiterakenteiden muuntamisessa eri osoitteiksi, joita voidaan käyttää julkisessa verkossa.

Tavallisesti palomuuri sijoitetaan organisaation ja internetin välille, mutta osa organisaatioista käyttää palomuuria myös sisäverkossa eri verkkosegmenttien välillä esimerkiksi arkaluonteisen talous- ja tutkimustiedon suojaamiseen. (Harwood 2011, 133.)

Kehitys on johtanut siihen, että nykyajan moderni palomuuri on usean ominaisuuden yhdistelmä, siinä yhdistyvät käsitteet virtuaalireititin, sulautetut NAT-säännöt ja erilaiset suodatusmallien käyttö eri paikoissa (Clark, Agah 2015, 160).

Palomuureja on neljää erilaista tyyppiä, staattinen paketteja suodattava palomuuri, sovellustason palomuuri, yhdyskäytäväpalomuurit ja dynaaminen paketteja suodattava palomuuri. Staattinen palomuuri suodattaa liikennettä IP-paketin lähteen, kohteen ja TCP-paketin porttitiedon perusteella. Staattisia palomuureja kutsutaan ensimmäisen polven palomuureiksi. Reitittimet voivat myös toimia palomuureina. (Vacca 2012, 275.)

Dynaaminen paketteja suodattava palomuuri pitää yllä tietoa aktiivisista yhteyksistä varaamalla tietokantaansa tietueen jokaista yhteyttä kohdin. Se tallentaa yhteydestä IP-osoitteet ja porttinumerot. Palomuuri päästää lävitse vain ne paketit, jotka täsmäävät tietokannasta löytyvän tietueen kanssa. Se monitoroi liikennettä koko yhteyden ajan, yhteyden muodostamisesta yhteyden lopetukseen (Stewart ym. 2012, 117).

Sovellustason palomuurit toimivat sovellustasolla suodattaen liikennettä sovelluksien sisältämän tiedon perusteella. Sovellustason palomuurit monitoroivat sovelluksien käyttämää liikennettä ja havaitsevat, jos epätavallinen protokolla yrittää käyttää epätavallista palomuuriporttia. (Vacca 2012, 88.)

Segmentoinnilla tarkoitetaan verkon jakamista pienempiin verkkoihin. Segmentoinnissa IP-osoitealuetta jaotellaan pienempiin verkkolohkoihin. Jaottelua tehdään VLANeilla, missä fyysinen verkko jaetaan useammaksi loogiseksi virtuaaliverkoksi. Segmentoinnin jälkeen verkkojenvälinen liikenne kulkee reitittimien kautta. Reitittimet ja niiden pääsylistat muodostavat verkkojen välisen yhteyden. Reitittimen tehtävänä on tarkistaa pääsylistan perusteella, onko verkkojenvälinen yhteys sallittua. Segmentoinnilla on kaksi tärkeää syytä, suorituskyvyn parantaminen ja tietoturva. Verkkojen kasvaessa suureksi, verkkolaitteet saattavat ylikuormittua, jolloin kuormitusta voidaan jakaa tasaisemmin segmentoimalla verkkoa pienempiin verkkolohkoihin. (McMillan 2011, 127–128.)

Segmentoinnin tärkein syy on tietoturva, koska verkonjakaminen pienempiin lohkoihin mahdollistaa verkko-osoitteiden jakamisen verkkoon liitettävien laitteiden käyttötarkoituksen mukaan. Käyttötarkoituksen perusteella toteutettujen verkkojen tietoturvamäärittelyt ovat helpompi ottaa käyttöön. Laitteiden tai palvelinten hallintaan käytetyt yhteydet voidaan eristämällä tehdä turvallisemmaksi hallintaverkoksi (Vacca 2012, 110). Segmentointia voidaan tehdä kytkinten virtuaalilähiverkolla, reitittimellä, palomuurilla yksistään tai näiden yhdistelmillä.

Virtuaalilähiverkon luonti tehdään kytkimellä, mikä tarkoittaa fyysisen verkkotopologian jakamista loogiseen verkkosegmenttiin. Liikennöinti virtuaalilähiverkkojen välillä tapahtuu reititystoiminnolla, joko ulkoisella reitittimellä tai monikerroskytkimellä (Stewart ym. 2012, 159). Extranet ja DMZ ovat esimerkkejä verkkosegmenteistä, joissa tietoturvaa tavoitellaan eristämällä.

DMZ-verkkoalueeksi kutsutaan aluetta, joka sijaitsee yrityksen sisäverkon ja internetin välissä. DMZ-verkkoon sijoitetaan yleensä palvelimia, joihin on tarve liikennöidä sekä internetistä että organisaation sisäverkosta. DMZ-verkko sijoitetaan kahden palomuurin väliin (Vacca 2012, 267). DMZ-verkko mahdollistaa ulkoisten käyttäjien pääsyn yrityksen ulkoisille palvelimille ja estää pääsyn organisaation sisäverkkoon. Tämä lisää organisaation sisäverkon tietoturvaa (Harwood 2011, 134). DMZ-verkkoon on rajattu pääsy sekä ulkoisilla että sisäisillä käyttäjillä. (Vacca 2012, 433). Tavallisesti DMZ-verkkoalueelle sijoitetaan palveluita, kuten julkisia internet, sähköposti ja erilaisia resursseja tarjoavia palvelimia (Stewart ym. 2012, 117).

Palomuuri ja DMZ-verkkosegmentti eivät yksin riitä takaamaan riittävää suojaa organisaation sisäverkkoon kohdistuvilta internetistä tulevilta hyökkäysyrityksiltä, jotka tulevat internetistä. Lisäksi tarvitaan verkkotasolla toimivia IDS- ja IPS-järjestelmiä, joilla voidaan havaita tai estää verkossa esiintyvä epätavallinen liikenne.

2.1.5 IDS- ja IPS-järjestelmät

IDS- ja IPS-järjestelmät ovat tehokkaita verkon suojausmenetelmiä palvelunestohyökkäyksiä vastaan (Stewart ym. 2012, 590). IDS seuraa sisäänpäin tulevaa verkkoliikennettä ja vertaa sitä parametreihin, jotka perustuvat tiedossa oleviin verkkouhkiin. IDS on passiivinen turvamekanismi, jonka tehtävänä on merkata ja tallentaa epätavallinen verkkoliikenne analysoitavaksi. (Harwood 2011, 136–137.) IDS arvioi ja tutkii liikennettä allekirjoitukseen ja käyttäytymiseen perustuvalla havaitsemisella (Vacca 2012, 91). Allekirjoituksiin perustuvassa havaitsemismenetelmässä IDS monitoroi jokaisen verkossa liikennöivän paketin, joita se vertaa tietokannan haitallisen liikenteen tunnisteallekirjoituksiin (Thomas & Stoddard, 2012, 337). Toimiakseen tehokkaasti IDS:n tietokanta on päivitettävä säännöllisesti.

Käyttäytymiseen perustuvassa menetelmässä IDS nauhoittaa verkon normaalin käyttäytymisen määritellyltä ajanjaksolta. Tämän pohjalta se muodostaa lähtötilanteen, jota se vertaa aktiiviseen verkkoliikenteeseen havaitakseen epänormaalia käyttäytymistä verkossa. Menetelmässä IDS käyttää poikkeavan liikenteen havaitsemiseen muodostamaansa lähtötilannetta, heuristista arviointia ja aktiivisuustilastoja. (Stewart ym. 2012, 592–593.)

IPS on puolestaan epämääräisen verkkoliikenteen estojärjestelmä. Se suorittaa samat toimenpiteet kuin IDS, mutta lisäksi sen tarkoituksena on automaattisesti estää verkolle haitallinen liikenne (Harwood 2011, 137). IPS sijoitetaan tavallisesti verkkoon siten, että se sijaitsee organisaation palomuurin ja sisäverkon välissä, jossa kaikki sisään- ja ulospäinkulkeva liikenne ohjautuu IPS:n lävitse. IPS:n tarkoitus on estää haitallinen liikenne ennen sen päätymistä kohdelaitteisiin tai järjestelmiin (Stewart ym. 2012, 590).
Organisaatio voi suojautua sisäisiltä tietoturvauhilta sijoittamalla IDS- ja IPS-järjestelmiä organisaation sisäverkkoon.

IDS- ja IPS-järjestelmillä luodaan yksi suojakerros tietoliikenneturvallisuuteen, jolla suojaudutaan paremmin ulkoisilta uhkilta. Verkkotasonsuojausmenetelmät eivät kuitenkaan tehoa sovellustasolla tapahtuviin tietoturvahyökkäyksiin, joita suoritetaan sallitun verkkoliikenteen sisällä.

2.2 Verkkosovellusten ja palveluiden tietoturva

2.2.1 Palvelunestohyökkäykset

Erilaiset palvelunestohyökkäykset ovat yleistyneet. Niiden tarkoituksena on lamauttaa palvelin tai tietoliikenne siten, että palveluiden käyttö hidastuu tai estyy kokonaan. Palvelunestohyökkäyksessä ei varsinaisesti murtauduta järjestelmään, vaan pyritään aiheuttamaan mahdollisimman paljon taloudellista haittaa yritykselle ja palveluita käyttäville ihmisille. Palvelunestohyökkäyksien toteuttaminen ei vaadi välttämättä hyökkääjältä erikoisosaamista ja se on mahdollista toteuttaa hyvinkin pienellä kustannuksella, koska sen voi hankkia helposti internetistä valittuun kohteeseen. Tämän perusteella hyökkäyksiltä suojautuminen on työläämpää ja kalliimpaa kuin niiden toteuttaminen. (Ristić 2014, 280.)

Palvelunestohyökkäykset jaetaan kahteen ryhmään, keskitettyihin ja hajautettuihin palvelunestohyökkäyksiin. Keskitetty palvelunestohyökkäys toteutetaan yleensä internetin välityksellä ja tulee yhdestä osoitteesta (Stewart ym. 2012, 62). Hyökkäyksessä aiheutetaan järjestelmälle tarpeetonta verkkoliikennettä, jonka seurauksena palvelun käyttö estyy.

Hajautetussa palvelunestohyökkäyksessä hyökkäys tulee useammasta lähteestä ja on näin huomattavasti vaikeammin estettävä kuin yhdestä lähteestä tuleva hyökkäys. Hajautetussa palvelunestohyökkäyksessä hyökkääjällä on käytössä useista eri käyttäjien tietokoneista koostuva botnet-verkko, jossa hyökkääjä on ottanut tietokoneet hallintaansa etähallittavilla haittaohjelmilla. Tämän verkon tietokoneilla hyökkääjä voi käyttäjän tietämättä suorittaa palvelunestohyökkäystä (Thomas & Stoddard, 2012, 365).

Palvelunestohyökkäykset ovat aiemmin tyypillisesti kohdistuneet verkkotasolle ja niiltä on suojauduttu erilaisilla suojausmenetelmillä. Nykypäivänä hyökkäykset ovat kehittyneempiä kuin aikaisemmin. Ne kohdistuvat laajemmin eri alueisiin esimerkiksi käyttöjärjestelmiin, palveluihin, verkkoprotokolliin ja sovelluksiin. (Stewart ym. 2012, 192.) Sovelluksiin kohdistuvilla hyökkäyksillä tavoitellaan samaa kuin resursseihin kohdistuvilla hyökkäyksillä. Sovelluksiin kohdistuvat hyökkäykset ovat hienostuneempia ja tavoitteellisempia kuin perinteiset verkkoinfrastruktuuriin kohdistuvat hyökkäykset. Ne voivat kohdistua yksittäisiin käyttäjiin tai verkkopalvelun yksittäiseen toimintoon esimerkiksi varausjärjestelmään tai maksuliikenteeseen (Stuttard & Pinto 2011, 6). Harwood (2011, 226) esittää, että nykyään noin 70 prosenttia verkkosivuihin kohdistuvista hyökkäyksistä kohdistuu sovellustasolle.

Organisaatioiden nykypäivän liiketoiminta perustuu yhä enemmän verkon palveluihin ja verkkosovelluksiin, millä moderni liiketoiminta voi toimia tehokkaasti. Tämän vuoksi sovellustasolle kohdistuvat palvelunestohyökkäykset ovat lisääntyneet merkittävästi. Verkkosovelluksien ja palveluiden turvaamisesta onkin tullut tietoturvan uusi haasteellinen alue, mikä on otettava erityisesti huomioon organisaation tietoturvastrategian luomisessa. (Harwood 2011, 142.)

2.2.2 Verkkosovellusten tietoturvahaasteet ja suojautuminen

Aikaisemmin internet koostui verkkosivuista, jotka tarjosivat staattista tietoa ja ne eivät olleet interaktiivisia. Tiedonsiirto oli yksisuuntaista selaimen ja palvelimen välillä. Sivustoilta käytännössä haettiin tietoa selaimella ja sivustoilla oli vähän käyttäjien itse luomaa tietoa. Avoimeen lähdekoodiin pohjautuvia verkkosovelluksia ei juurikaan ollut (Harwood 2011, 16). Sivustoille ei ollut tarvetta tunnistautua tai rekisteröityä ja kaikilla käyttäjillä oli samat pääsyoikeudet sivustoihin. Ne eivät sisältäneet arkaluonteista tietoa ja niistä ei ollut yhteyksiä muihin sovelluspalvelimiin tai tietokantoihin (Stuttard & Pinto 2011, 2).

Nykyään internetsivustot ovat dynaamisia verkkosovelluksia, jotka ovat interaktiivisia ja toimivat kahteen suuntaan selaimen ja palvelimen välillä. Verkkosovellukset tarjoavat esimerkiksi rekisteröitymistä, maksuliikennepalveluita ja kirjautumista. Dynaamisten verkkosovellusten käsittelemä tieto on usein luottamuksellista ja henkilökohtaista,

jota säilytetään tietokannoissa (Stuttard & Pinto 2011, 2). Ne voivat sisältää esimerkiksi maksutietoja, asiakastietoja, käyttäjätunnuksia, salasanoja, käyttöoikeuksia, tilauksia ja hintoja. Verkkosovelluksien keskeiset toiminallisuudet toimivat taustalla olevissa tietovarastoissa, joissa käytetään eri tekniikoita. Niiden sisältämää jäsenneltyä tietoa haetaan eri kysely ja kielimuodoilla sekä ne käyttävät tiedonhallintaan sisäistä logiikkaa. SQL-tietokanta ja LDAP-hakemisto ovat yleisimpiä verkkosovellusten käyttämiä tietovarastoja (Stuttard & Pinto 2011, 287).

Verkkosovellukset vaativat verkkoyhteyksiä ja käyttöoikeuksia taustalla oleviin sovellus- ja tietokantapalvelimiin, jotta ne voivat tuottaa organisaatioille tehokkaasti toimivia liiketoimintasovelluksia ja käyttäjille monipuolisia palveluita verkossa. (Stuttard & Pinto 2011, 2.) Tämä tarkoittaa sitä, että nykyiset verkkosovellukset tuovat monimutkaisuutta ja haastavuutta perinteiseen tietoturvamalliin, koska sovelluksien on päästävä liikennöimään sisäverkkoon sijoitetuille tietokantapalvelimille (Stewart ym. 2012, 349). Tietokantapalvelimet eristetään julkisesti saatavilla olevasta sovelluspalvelimesta palomuurilla, johon määritellään sääntö, joka sallii vain tarvittavan liikennöinnin tietokantapalvelimelle. Yhteys tietokantaan mahdollistaa kuitenkin hyökkääjälle luvattoman pääsyn tietokantaan. (Stewart ym. 2012, 349.) Hyökkäystavat ovat nykyään hienostuneempia kuin aiemmin. Ne kohdistuvat nykyään paljolti sovellustasolle, johon perinteiset verkkotason tietoturvaratkaisut eivät tehoa.

Organisaatiot suunnittelevat ja toteuttavat sovelluksia itse, mikä lisää teknisesti erilaisesti toteutettujen sovelluksien määrää. Tämä lisää IT-infrastruktuurin monimutkaisuutta ja tekee sovellustietoturvan toteuttamisesta haasteellista. Tämä tarkoittaa, että organisaation tietoturvansuunnittelussa ei ole vain yhtä ja ainoata tapaa suojautua ulkopuolisilta uhkilta. (Stuttard & Pinto 2011, 3.) IT-ammattilaiset ovat joutuneet uudelle tietoturvan pelikentällä dynaamisten verkkosovellusten mukana tulleiden tietoturvahaasteiden kanssa.

2.2.3 OWASP TOP 10

Organisaatioiden sovellustietoturvallisuuden lisäämisen tueksi on perustettu taloudellista voittoa tavoittelematon järjestö OWASP, jonka tarkoituksena on parantaa organisaatioissa tietoturvallisempien verkkosovellusten sovelluskehitystä, valmistusta ja ylläpitoa. (Stewart ym. 2012, 155.) Järjestö toimii samalla periaatteella kuin avoimeen lähdekoodiin perustuvat projektit. Se muodostuu maailmanlaajuisesta yhteisöstä, jonka tavoitteena on lisätä sovellustietoturvan näkyvyyttä siten, että organisaatiot ja yksittäiset käyttäjät voivat tehdä tietoisia päätöksiä paremman sovellustietoturvan parantamiseksi. OWASP jakaa ilmaiseksi työkaluja, dokumentteja ja ehdotuksia avoimen lähdekoodiin perustuvista tekniikoista, joilla sovellustietoturvaa parannetaan. (OWASP, 2013.) Se ei tue kaupallisia tuotteita tai palveluita.

OWASPin kuuluisin projekti on (OWASP Top 10) lista kymmenestä kriittisestä verkkosovellushaavoittuvuudesta, jonka se julkaisee kolmen vuoden välein. Lista keskittyy erityisesti verkkosovellusten tiedonsiirtoon ja sisältöön liittyviin ongelmiin sekä miten tietoa käsitellään selaimen sisällä (Vacca 2012, 155). Listan päätarkoitus on kehittää kehittäjien, suunnittelijoiden, arkkitehtien ja organisaatioiden tietämystä merkittävimmistä verkkosovelluksien tietoturvaan liittyvistä heikkouksista. Listalla olevat nimet viittaavat

hyökkäyksen tyyppiin, heikkouden tyyppiin tai hyökkäyksestä aiheutuviin seurauksiin. Lista tarjoaa myös tekniikoita, joilla heikkouksia vastaan suojaudutaan.

Viimeisiin lista (OWASP Top 10 2013) on julkaistu vuonna 2013:

A1. Injektio.
A2. Rikkoutunut käyttäjätunnistus ja istunnonhallinta.
A3. Verkkosivun rakenne ei säily (XSS).
A4. Turvaton suora objektiviittaus.
A5. Puutteellisesti määritelty tietoturva.
A6. Arkaluonteisen tiedon puutteellinen salaus.
A7. Puuttuva funktiotason pääsynhallinta.
A8. Puutteellinen pyynnön alkuperän tarkistus (CSRF).
A9. Tunnettuja haavoittuvuuksia sisältävien komponenttienkäyttö.
A10. Varmistamattomat uudelleenohjaukset.

2.2.4 Injektio ja rikkoutunut käyttäjätunnistus sekä istunnonhallinta

Injektio on yleisin verkkosovelluksiin kohdistuva tietoturvauhka. Verkkosovellusten käyttämät tiedot ja niiden toimintalogiikka sijaitsee erilaisissa tietokannoissa. Injektio tarkoittaa, että hyökkääjä pyrkii ohittamaan sovelluksen pääsynhallinnan ja sen myötä pääsemään käsiksi sovelluksen käyttämiin tietokantoihin. Injektiot on suunniteltu murtamaan tietokantojen käyttämät turvamekanismit ja pääsemään käsiksi niiden sisältämään dataan. Ne voivat lukea, muokata, luoda tai poistaa dataa tietokannasta. (Harwood 2011, 152.)

Injektioita on erityyppisiä, mutta selvästi yleisimpiä injektioita ovat SQL-tietokantaan ja LDAP-hakemistoon kohdistuvat injektiot, koska näiden sisältämä tieto on arvokasta ja sovelluksen tuottaman palvelun kannalta tärkeää. SQL-injektiossa hyökkääjä pyrkii verkkosovelluksen välityksellä syöttämään eli injektoimaan tai manipuloimanaan sovelluksen suorittamaa SQL-kyselyä tietokannalle (Harwood 2011, 152). Kyselyllä se pyrkii samaan luvattoman oikeuden tietokantaan ja pääsemään näin kriittiseen tietoon käsiksi. Pahimmillaan hyökkääjä voi saada SQL-tietokantaa hallinnoivan tietokantapalvelimen käyttöjärjestelmän hallintaansa täysin oikeuksin (Stuttard & Pinto 2011, 291).

LDAP-injektiossa hyökkääjä pyrkii pääsemään LDAP-protokollalla käsiksi hakemistopalveluun, joka sisältää käyttäjätunnuksia, salasanoja, nimiä ja muita henkilökohtaisia tietoja. Injektiossa hyökkääjä pyrkii syöttämään tai manipuloimaan järjestelmän suorittamaa LDAP-kyselyä ja pääsemään käsiksi LDAP-hakemistopalvelun rakenteeseen ja sen sisältämiin tietoihin (Harwood 2011, 152).

Injektio on haavoittuvuuksista helpoiten estettävissä. Tarkoituksena on estää käyttäjän syöttämiä tietokantakyselyitä tai ohjelmakomentoja päätymästä sellaisenaan sovelluksen välityksellä tietokannalle. Sovelluksen ja tietokannan välissä voidaan käyttää API-ohjelmointirajapintaa, jonka tarkoituksena on estää haitallisen koodin päätyminen suoraan tietokantaan. API käyttää parametrisoitua tietokantakyselyä, joka on tehokkain tapa suojautua injektiolta. Tässä hyökkääjä ei pääse muokkaamaan tietokannalle suoritettavaa tietokantakyselyä vaan API suorittaa kyselyn sovelluksen puolesta turvallisella tavalla. (OWASP, 2013.)

Toinen tapa estää on tarkistaa kaikki käyttäjältä tuleva syöte ja poistaa siitä erikoismerkit, joita voidaan käyttää injektointiin. Näiden lisäksi voidaan käyttää syötteen tarkistukseen valkolistausta (White List Input Validation). Listaan on määritelty etukäteen kaikki sallitut syötteet, joita voidaan ajaa tietokannalle turvallisesti. Kaikki listan ulkopuolelle osuvat syötteet estetään. Listalla voidaan määritellä myös syötteissä sallitut erikoismerkit ja syötteessä ajattavan datan suurin sallittu koko. (Stuttard & Pinto 2011, 338–339.)

Edellä mainittujen suojautumismenetelmien lisäksi on varmistettava, että sovelluksien käyttämillä tunnuksilla on vain tarvittavat oikeudet tietokannalle suoritettavia kyselyitä varten. Valtaosa sovelluksien tietokannoille tekemistä kyselyistä vaatii vain lukuoikeudet tietokantaan. Yleensä vain osa kyselyistä vaatii kirjoitusoikeutta tietokantaan ja sekin tavallisesti vain tiettyyn osaan tietokannasta. Kirjoitusoikeutta varten voidaan sovellukselle määritellä käyttöön eri tunnus kirjoitusoikeutta vaativiin tietokantasuoritteisiin. (Stuttard & Pinto 2011, 342.) Käyttöoikeuksia rajoittamalla minimoidaan merkittävästi haittavaikutuksia, joita hyökkääjä injektiolla voi saada aikaiseksi (Harwood 2011, 228).

Tietokantaa on myös kovennettava poistamalla siitä kaikki tarpeettomat toiminnot ja palvelut, koska ne tarjoavat ylimääräistä hyökkäyspintaa hyökkääjälle. Tietokantaa on myös ylläpidettävä jatkuvasti asentamalla siihen säännöllisesti ohjelmisto- ja haavoittuvuuspäivitykset. (Stuttard & Pinto 2011, 342.)

Toiseksi kriittisin verkkosovelluksiin liittyvä tietoturvauhka on OWASPin mukaan rikkoutunut käyttäjätunnistus ja istunnonhallinta. Suurin osa käytössä olevista verkkosovelluksista käyttää käyttäjätunnistusta pääsynhallinta mekanismina. Se on ensisijainen ja tärkein suojakeino sovelluksen luvattomalle käytölle (Stuttard & Pinto 2011, 159). Yleisesti verkkosovelluksissa käytetään tunnistusmallia, jossa käyttäjä syöttää käyttäjätunnuksen ja siihen liittyvän salasanan. Siinä sovellus validoi käyttäjän ja antaa sille määritellyt oikeudet sovellukseen. Yksi verkkosovellusten heikkouksista on se, että ne eivät kykene tarjoamaan riittävän vahvaa tunnistusta. (Harwood 2011, 226.) Verkkosovellusten käyttäjätunnistusmekanismeissa on monia käyttöönottoon ja suunnitteluun liittyviä ongelmia. Näiden seurauksista hyökkääjällä annetaan mahdollisuus arvata käyttäjän salasana tai muuten ohittaa tunnistusmekanismi. Tällä hyökkääjä voi saada luvattomat oikeudet sovellukseen tai järjestelmään. (Stuttard & Pinto 2011, 19.)

Suurin osa sovelluksien käyttäjätunnistukseen liittyvistä ongelmista voidaan korjata käyttämällä riittävän vahvaa tunnistusmenetelmää. Se on tärkein sovelluksen tietoturvaan liittyvä suojausmenetelmä, joka heikosti toteutettuna tarkoittaa sitä, että muilla sovelluksen sisäisillä turvamenetelmillä ei voida suojautua hyökkääjän hyödyntäessä luotetun käyttäjän tunnusta ja salasanaa. Sovelluksilla tulee olla käytössä kunnollinen tunnistushallinta, jolla luodaan vahvat salasanat ja tunnukset sekä säilytetään niitä turvallisesti. Asiakkaan selaimen ja verkkosovellusten välinen liikenne on salattava käyttäen SSL/TLS-tekniikkaa, jotta tunnustiedot eivät ole selkokielisesti ulkopuolisten luettavissa. (Stuttard & Pinto 2011, 192.) Sovelluksen käyttövaltuutuksella varmistetaan, että käyttäjällä on oikeudet vain niihin sovelluksen osiin, joita käyttäjä tarvitsee. Lisäksi on varmistettava, että itse sovellusta ajetaan minimaalisilla oikeuksilla ja paikalliset ylläpitotunnukset eivät ole hyökkääjän käytettävissä.

Istunnonhallinta tarkoittaa sovellukseen tunnistuneen käyttäjän istunnon käsittelyä ja hallintaa. Tunnistuksen jälkeen sovellus muodostaa tunnistuneesta käyttäjästä istuntotunnuksen. Istuntotunnuksella käyttäjän ei tarvitse tunnistautua sovellukseen toistuvasti uudelleen. Sovellus hyödyntää istuntotunnuksia tunnistaakseen eri käyttäjiltä tulevien pyyntöjen alkuperän. Hyökkääjä yrittää saada haltuunsa istuntotunnuksen, jolla se voi ohittaa pääsyhallinnan käyttäen luotettuun käyttäjätunnukseen liittyvää istuntotunnusta. (Stuttard & Pinto 2011, 19.)

Istunnonhallinnan rikkoutuminen estetään siten, että sovellus käyttää tehokasta ja turvallista istunnonhallintaa. Istunnonhallinta tarkoittaa tapaa, jolla sovellus käsittelee ja hallinnoi käyttäjäistuntoja (Harwood 2011, 228). Sillä varmistetaan, että käyttäjän kirjautuessa pois sovelluksesta, on sovelluksen tuhottava kyseinen käytetty istuntotunnus, jotta hyökkääjä ei voi sitä jatkossa hyödyntää. Sovelluksien tulee generoida mahdollisimman vahvoja istuntotunnuksia ja ne on luotava satunnaisessa järjestyksessä. Sovelluksilla pitää olla käytössä istuntojen aikakatkaisutoiminto, joka automaattisesti poistaa istunnon, kun se on vanhentunut.

Istuntotunnuksia on säilytettävä turvallisesti koko niiden olemassaolon ajan ja ne pitää suojata kuljetuksen ajan salaamalla liikenne selaimen ja verkkosovelluksen välillä. Verkkosovelluksen ja taustaverkossa sijaitsevan tietokantapalvelimen välinen liikenne tulee myös salata, jotta istuntotunnukset voidaan kuljettaa käyttäjän selaimen ja tietokantapalvelimen välillä turvallisesti. Istunnonhallintamenetelmää tulisi myös valvoa, lokittaa ja sen pitäisi pystyä muodostamaan hälytys epänormaalista istuntoihin liittyvästä toiminnasta (Stuttard & Pinto 2011, 252).

2.2.5 XSS-hyökkäys ja turvaton objektiviittaus

XSS-hyökkäys on verkkosivun rakenteen muutoshyökkäys, jossa sovellus ei tarkasta ja käsittele käyttäjän selaimelta tullutta syötettä ennen kuin lähettää sen takaisin käyttäjälle. Tämä antaa hyökkääjälle mahdollisuuden kaapata toisen käyttäjän istuntotunnuksen, jossa se voi syöttää käyttäjän selaimelle haitallista koodia tai ohjata käyttäjä haitalliselle sivustolle.

XSS-hyökkäyksessä haitallinen koodi ajetaan käyttäjän selaimessa, jossa hyökkääjä syöttää verkkosovellukselle haitallista koodia, mihin käyttäjä on yhteydessä (Harwood 2011, 226). Tällä hyökkääjä yrittää ohjata käyttäjän verkkosovelluksen kautta haitalliselle sivustolle esimerkiksi vääristetyllä linkillä. Siinä ei vahingoiteta itse verkkosovellusta, vaan hyödynnetään verkkosovelluksen haavoittuvuutta, jolla hyökkääjä pääsee käyttäjän selaimella keräämään henkilökohtaisia tietoja käyttäjästä. (Harwood 2011, 175.) XSS-hyökkäystä pidetäänkin toisiin käyttäjiin kohdistuvien hyökkäysten kummisetänä (Stuttard & Pinto 2011, 432).

XSS-hyökkäyksiltä suojaudutaan tarkistamalla käyttäjältä tuleva syöte palvelimella siten, että palvelin ei välitä haitallista koodia takaisin vastauksessa. Valkolistausmenetelmä (White List) on tehokas tapa suojautua XSS-hyökkäyksiltä, siinä määritellään kaikki sallitut syötteet, joita palvelin saa lähettää vastauksen mukana käyttäjälle. Syötteen tarkistamisessa tulee ottaa huomioon myös syötteen datan pituus, merkit ja muoto. (OWASP, 2013.)

Neljäntenä listalla on turvaton objektiviittaus. Tämä syntyy, kun verkkosovelluspalvelimen tiedosto- ja kansio-oikeudet on väärin määritelty. Hyökkääjä pystyy selaimelle syötettyä osoitetta muokkaamalla päästä selaamaan ja muokkaamaan esimerkiksi www-palvelimella olevien muiden käyttäjien tiedostoja ja kansioita.

Turvaton objektiviittaus estetään parhaiten käyttämällä istunto- ja käyttäjäkohtaisia epäsuoria objektiviittauksia, joissa käyttäjän oikeudet tarkistetaan jokaisen viittauksen yhteydessä. Tarkoituksena on suojata käyttäjän käytettävissä oleva tieto. Epäluotettavasta lähteestä tuleva suora objektiviittaus on aina tultava pääsynhallinnan lävitse ja käyttöoikeudet on tarkistettava. (OWASP, 2013.) Järjestelmäylläpitäjien on rajattava verkkosovelluspalvelimen tiedostojen ja kansioiden käyttöoikeudet (Harwood 2011, 153).

2.2.6 Puutteellisesti määritelty tietoturva ja arkaluonteisen tiedon salaus

Puutteellisesti määritelty tietoturvahaavoittuvuus syntyy siten, että verkkosovellusta tarjoavan teknologia kokonaisuuden ohjelmistoja ei kovenneta ja niihin ei asenneta säännöllisesti ohjelmisto- sekä haavoittuvuuspäivityksiä. Ohjelmistoihin sisältyy palvelinkäyttöjärjestelmä, verkkosovellus- ja taustapalvelimet esimerkiksi tietokantapalvelimet. Käyttöjärjestelmien, sovelluksien ja palveluiden puutteellisesti määritelty tietoturva tarjoaa hyökkäysmahdollisuuden ulkopuoliselle. (Vacca 2012, 156.)

Haavoittuvuus estetään koventamalla ja ylläpitämällä kaikki ohjelmistot verkkosovellusta palvelevasta kokonaisuudesta, joka sisältää sovelluksen lisäksi siihen liittyvät muut taustapalvelut, kuten tietokanta-, tunnistus- ja tiedostopalvelua tarjoavat palvelimet. Koventamisessa poistetaan ylimääräiset portit, toiminnot ja palvelut, jotka ovat tarpeettomia sovelluksen toiminnan kannalta tai ovat turvattomia (OWASP, 2013).

Haavoittuvuuden riskiä merkittävästi pienentää, jos versio- ja haavoittuvuuspäivityksiä asennetaan säännöllisesti. Lisäksi sovelluksissa ja käyttöjärjestelmissä kannattaa käyttää mahdollisimman vähäisillä käyttöoikeuksilla määriteltyjä tunnuksia. Erityisesti on kiinnitettävä huomioita ylläpitoon käytettävien yhteyksien ja tunnuksien hallintaan sekä sovelluksien käyttämien prosessien käyttöoikeuksiin. Sovelluksilla tulee olla käytössä vahva arkkitehtuuri, jossa eri komponentit ovat eriytetty toisistaan tietoturvallisesti. Haavoittuvuuksien havainnointiin tulee olla käytössä skannaus- ja auditointimekanismeja (OWASP, 2013).

Arkaluonteisen tiedon puutteellinen salaus syntyy, kun verkkosovelluksissa ei käytetä riittävän vahvaa salausta tai sitä ei käytetä lainkaan. Arkaluontoisen tiedon esimerkiksi henkilökohtaisten tunnistus-, luottokortti- tai taloustietojen salaamattomuus antaa mahdollisuuden hyökkääjälle saada sille kuulumattomia tietoja haltuunsa. Tämä tietoturvauhka voi tapahtua tiedonsiirrossa, tiedonvarastoinnissa tietokannassa tai varmistuksissa (OWASP, 2013). Julkisuudessa esiin tulevat tietomurrot liittyvät usein internetissä toimivan palvelun asiakkaiden luottokorttitietojen, salasanojen varastamiseen tai asiakkaiden henkilökohtaisten tietojen julkaisemiseen.

Kaikki luottamuksellinen tieto, salasanat, luottokortti- ja taloustiedot on salattava säilytyksessä siten, että niitä ei voida luvattomasti lukea tai muokata. Tiedon salauksessa on käytettävä riittävän vahvaa salausalgoritmia ja vahvoja salausavaimia, jotta salausta on mahdollisimman vaikea purkaa. Salaukseen käytettäviä yksityisavaimia on säilytettävä turvallisessa paikassa. Avaimia on säilytettävä verkon ulkopuolella ja niihin tulee olla rajattu pääsy. Tarpeettoman luottamuksellisen tiedon säilytystä tulee välttää. Luottamuksellisen tiedon siirtäminen, käyttäen mitä tahansa erilaista siirtomediaa, on turvattava salaamalla tieto tiedonsiirron aikana. (Harwood 2011, 159.)

2.2.7 Puuttuva funktiotason pääsynhallinta ja CSRF-hyökkäys

Puuttuva funktiotason pääsynhallinta tarkoittaa, että hyökkääjä pääsee hyödyntämään sovelluksen toimintojen palvelimelle suorittamaa puutteellista tunnistusta. Useimmat verkkosovellukset suorittavat käyttövaltuutuksen sovelluksen toiminnoille, joihin käyttäjällä on oikeudet. Toiminnot tulevat tämän jälkeen käyttäjälle näkyviin käyttöliittymään. Verkkosovelluksen on lisäksi tarkistettava palvelimelta erikseen käyttöoikeudet jokaisen toiminnon kohdalta, kun käyttäjä sitä käyttää. Pyynnön saatuaan palvelin vahvistaa sen takaisin sovellukselle, jos oikeudet ovat kunnossa. Tietoturvauhka syntyy, kun palvelin ei varmenna pyyntöä sovellukselle takaisin. Tämä mahdollistaa hyökkääjän esimerkiksi väärentää varmistus ja saada luvaton pääsy palvelimeen. Sovelluksen hallintaan ja ylläpitoon käytettävät toiminnot ovat erityisesti hyökkääjien pääkohteita. (OWASP, 2013.)

Puuttuvasta funktiotasonhallinnasta johtuva haavoittuvuus estetään sovelluksen eri toiminnoille erikseen tehtävällä pääsynhallintatarkistuksella, jolla varmistetaan, että käyttäjällä on varmasti oikeudet suorittaa haluttu toiminto. Sovelluskäyttöliittymän pääsynhallintamalli, jossa käyttäjältä piilotetaan toiminto tai linkki, ei vielä takaa tietoturvaa, vaan tarkistukset tulee suorittaa myös sovelluksen taustalla olevissa sovellus- ja liiketoiminta logiikassa. Toiminnoissa tulee käyttää rooleihin perustuvaa tunnistusmenetelmää (RBAC) ja käyttäjäkohtaisesti myönnettyjä oikeuksia tulee välttää. (OWASP, 2013.)

CSRF-hyökkäys tapahtuu, kun käyttäjä on kirjautuneena luotetulle sivustolle, johon hyökkääjä suorittaa haitallisia toimenpiteitä. Hyökkääjä huijaa käyttäjää kuvalla, lomakkeella tai väärennetyllä linkillä, joilla syötetään väärennettyjä http-pyyntöjä käyttäjän selaimelta luotetulle sivustolle. Esimerkiksi hyökkääjä pääsee hyödyntämään uloskirjautuneen käyttäjän auki jäänyttä istuntotunnusta. (Harwood 2011, 154.) Tällä se pääsee aiheuttamaan käyttäjälle haittaa muun muassa tekemällä ostoja käyttäjän nimissä. Erityisen alttiina hyökkäyksille ovat sovellukset, jotka käyttävät http-evästeitä tunnistukseen käytettävien istuntotunnuksien välittämiseen (Stuttard & Pinto 2011, 506).

Tärkein suojautumiskeino hyökkäyksien varalta on sovelluksen istunnonhallinta, jossa sovelluksesta uloskirjautuneen käyttäjän istuntotunnus tuhotaan heti uloskirjautumisen jälkeen ja istuntotunnukset sisällytetään piilotettuun kenttään html-muodossa (Harwood 2011, 154). Sovelluksien istuntotunnuksien käsittelyssä tulee välttää evästeitä, jotka altistavat CSRF-haavoittuvuudelle (Stuttard & Pinto 2011, 508).

2.2.8 Haavoittuvuuksia sisältävät komponentit ja uudelleen ohjaukset

Tunnettuja haavoittuvuuksia sisältävien komponenttien käyttö altistaa sovellukset erilaisille hyökkäyksille esimerkiksi injektioille, XSS-hyökkäyksille ja pääsynhallinnan murtamiselle. Sovellukset sisältävät erilaisia ohjelmistokomponentteja ja kirjastoja, jotka eivät ole päivitettyjä. Tämän vuoksi ne sisältävät haavoittuvuuksia, joita hyökkääjä voi hyödyntää. Niitä suoritetaan usein liian laajoilla käyttöoikeuksilla. Haavoittuvuuksia sisältävien komponenttien havaitseminen on vaikeaa, koska edes ohjelmistojen kehittäjillä ei ole aina tiedossa, mitä komponentteja, kirjastoja tai riippuvuuksia sovellukset sisältävät. Sovelluskehittäjät eivät kiinnitä riittävästi huomiota sovelluksien versiopäivityksissä niiden sisältämien komponenttien, kirjastoversioiden ja haavoittuvuuksien päivittämiseen. Kaikkiin sovelluskomponentteihin ei yleisesti tehdä haavoittuvuuspäivityksiä. (OWASP, 2013.)

Sovelluskehityksessä tulee ottaa huomioon sovelluksien sisältämät eri komponentit, kirjastot ja riippuvuudet varmistamalla, että niihin ei liity haavoittuvuuksia. Sovelluksen lisäksi sen komponentteja täytyy pystyä päivittämään. Ylläpitäjien tulee olla tietoisia käytössä olevista sovelluksista ja sovelluksen sisältämistä komponenteista ja riippuvuuksista, jotta haavoittuvuudet voidaan korjata. Sovelluksen komponentteja voidaan myös koventaa poistamalla niistä toimintoja, jotka ovat tarpeettomia. (OWASP, 2013.)

Viimeisenä haavoittuvuutena listalla on varmistamattomat uudelleenohjaukset. Nämä syntyvät, kun hyökkääjä yrittää väärennetyllä linkillä ohjata käyttäjä haitalliselle sivustolle. Hyökkääjä lähettää käyttäjälle haitallisen linkin sähköpostilla tai tarjoaa linkin verkkosivuston kautta, jossa se ohjaa käyttäjän haitalliselle sivustolle. Hyökkääjä voi yrittää myös itse saada uudelleenohjauksella oikeudeton pääsy luotetulle sivustolle. Haavoittuvuus ei ole kovin yleinen ja se on helposti havaittava. (OWASP, 2013.)

Tehokkain tapa estää haavoittuvuus on olla käyttämättä verkkosovelluksissa uudelleenohjauksia. Sovelluskehittäjien tulisi välttää sovelluksissa uudelleenohjaustekniikkaa, jossa käyttäjän syöttämää dataa menee uudelleenohjauksen kohteeksi (Stuttard & Pinto 2011, 546).

Valtaosa edellä käsitellyistä haavoittuvuuksista voidaan estää sovelluksien sekä käyttöjärjestelmien osalta riittävän vahvalla tunnistuksella, syötteen tarkistuksella ja istunnonhallinnalla. Nämä kolme osa-aluetta muodostavat sovelluksien tietoturvan pääsuojausmekanismit, joihin sovelluskehittäjien ja IT-ympäristöjen ylläpitäjien tulee erityisesti kiinnittää huomiota (Harwood 2011, 226).

Lisäksi organisaatioiden tulee ottaa tietoturva huomioon jo sovelluksien kehitysvaiheessa ja sovelluskehittäjiä tulee kouluttaa tietoturvallisten sovelluksien ohjelmointiin, jotta he ymmärtävät ja noudattavat tietoturvallisia ohjelmointimenetelmiä (Bosworth, Kabay & Whyne, 2014, 330). Verkkosovellusten valvonnalla voidaan varautua ennalta tunnistettuihin tietoturvauhkiin ja tunnistaa uusien haavoittuvuuksien löytymistä sovelluksista ennakoivasti. (Harwood 2011, 243.)

Sovelluksien ja palvelimien ohjelmistoversiot on pidettävä ajan tasalla. Tietoturvapäivitykset ja päivitykset on asennettava säännöllisesti sekä tietoturvan toteuttamisen tulee olla ennakoivaa (Harwood 2011, 243).

Useat käytössä olevat verkkosovellukset sisältävät haavoittuvuuksia ja kaikkiin sovelluksiin ei julkaista päivityksiä edes sovelluksen tarjoajan toimesta. Sovelluksen muuttaminen jälkikäteen tietoturvallisemmaksi ylläpitäjien toimesta on usein vaikeaa, hidasta ja siihen vaaditaan erikoisosaamista. Verkkosovelluspalomuuri (WAF) tuo lisävaihtoehdon verkkosovellusten tietoturvalle (Vacca 2012, 998).

2.2.9 Web Application Firewall (WAF)

Verkkosovelluspalomuuri (WAF) on palvelin tai ohjelmisto, joka sijoitetaan verkkosovelluksen eteen valvomaan, suodattamaan ja estämään haitallista liikennettä pääsemästä sovellukseen. (Vacca 2012, 998.) Se suojaa verkkosovelluksia uhkilta, joihin perinteiset verkkopalomuurit ja IDP-järjestelmät eivät pysty.

WAF pystyy käsittelemään sovellusprotokollien käyttämää liikennettä ja suorittamaan liikenteen sisältöön perustuvia suojaustoimenpiteitä (McMilllan 2009). Se suojaa muokattavilla säännöillä verkkosovelluksia yleisimmiltä hyökkäyksiltä (Bosworth ym. 2014, 264). WAF eroaa verkkopalomuureista ja IPS-järjestelmistä siten, että se analysoi sovelluskerroksessa tapahtuvaa verkkosovelluslogiikkaa (McMillan 2009).

WAF on suunniteltu parantamaan sovellusten tietoturvaa ja sen ensisijainen tehtävä on suojata olemassa olevia sovelluksia havaituilta tietoturvahaavoittuvuuksilta (Vacca 2012, 998). WAF käyttöönotossa ei tehdä muutoksia itse sovellukseen tai lähdekoodiin, mikä tekee käyttöönotosta nopeaa ja helppoa. Uuden haavoittuvuuden esiintyessä ylläpitäjät voivat nopeasti päivittää säännöstöä (Virtual Patching) ja estää haavoittuvuus erillisessä kerroksessa koskematta itse sovellukseen (Ristić 2010, 5).

Sovelluksien päivittäminen ei ole helppoa tuotantoympäristöissä, koska sovellukset ovat monimutkaisia ja sisältävät riippuvuuksia toisiin järjestelmiin sekä tietokantoihin. Muutosten tekeminen sovelluksille jälkeenpäin on hankalaa ja kallista tai jopa mahdotonta. Sovellukset ovat usein heikosti dokumentoituja ja päivityksistä aiheutuvista palvelukatkoista voi tulla liiketoimintahaittoja.

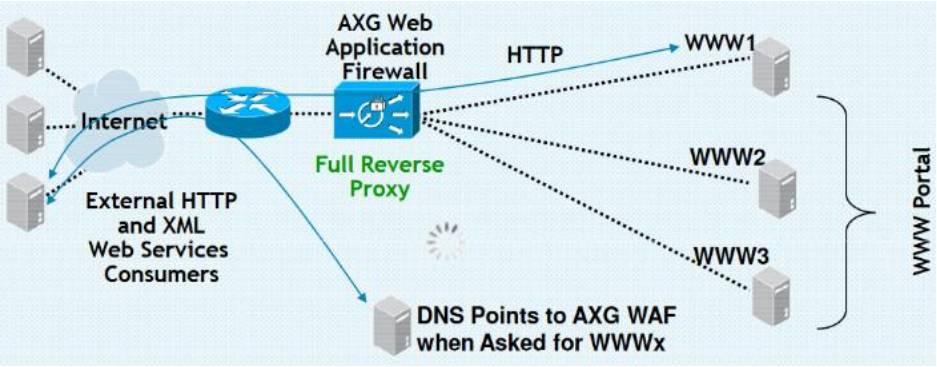
WAF:n ydintoiminnallisuuksia ovat reaaliaikainen verkkosovelluksen liikenteenvalvonta, pääsynhallinta ja liikenteen täydellinen nauhoitus. Reaaliaikaisella liikenteenvalvonnalla on mahdollista tutkia http-liikennettä reaaliaikaisesti. Lisäksi liikenne voidaan halutessa nauhoittaa ja tutkia jälkeenpäin. (Ristić 2010, 5.)

WAF mahdollistaa http-liikenteen täydellisen lokitus mahdollisuuden sovelluksen tietoturvaan liittyville toimenpiteille, joita web-palvelimet tavallisesti lokittavat hyvin niukasti. Järjestelmä mahdollistaa erilaisten lokitus variaatioiden käytön tietoturvatoimenpiteisiin. (Ristić 2010, 5.)

Näiden lisäksi WAF mahdollistaa erilaisten sovellusten tietoturvaan liittyvien uhkien ennaltaehkäisyn. Sitä voidaan hyödyntää seuraamalla järjestelmän käyttäytymistä ja löytää siitä ennakoivasti epänormaalia käyttäytymistä. WAF:lla tehdään myös sovelluksen koventamista, rajataan pois tarpeettomat palvelut ja tehdään istunnonhallintaa. (Ristić 2010, 5.)

WAF sijoitetaan verkkotasolle tai palvelintasolle sovelluksen yhteyteen. Verkkotasolla se sijoitetaan DMZ-verkossa sijaitsevalle reverse proxylle, joka välittää liikenteen verkkosovelluksille piilottaen verkkosovelluspalvelimien identiteetit käyttäjiltä. Kuvassa 2 WAF on sijoitettu reverse proxyn yhteyteen suojamaan useita www-sovelluksia. Reverse proxy terminoi eli purkaa https-liikenteen salauksen, jotta WAF voi analysoida liikenteen sisältöä (Pirc, DeSanto, Davison & Gragido 2016, 137).

Toteutusmallissa WAF:lla suojataan useita sovelluksia luomalla niiden eteen etuoven suodattamaan haitallista liikennettä. Sillä muodostetaan erillinen arkkitehtuuri ja tietoturvakerros, jossa pääsynhallinta, valvonta ja lokitus on helposti toteutettavissa keskitetysti. Toteutusmallin haittana on, että se muodostaa arkkitehtuuriin yksittäisen pisteen, jossa sääntömuutokset vaikuttavat kaikkiin reverse proxyn taakse sijoitettuihin sovelluksiin. Virheellisesti tehty muutos saattaa lopettaa kaikkien sovelluksien toiminnan. (Ristić 2010, 8.) Sääntöjen tulee olla geneerisiä, jotta kaikki sovellukset säilyttävät toimintansa.



Kuva 2. Verkkosovellus palomuurin toimintaperiaate. (Cisco, 2008).

Toisessa toteutusmallissa WAF sijoitetaan sovelluksen eteen esimerkiksi sovellusta pyörittävälle palvelimelle, jossa se sisällytetään osaksi www-palvelin konfiguraatiota. Tässä toteutusmallissa etuna on se, että sillä voidaan tehdä tarkempia sovelluskohtaisia sääntöjä vaikuttamatta muiden sovellusten toimintaan. Verkkosovelluspalvelin ja WAF yhdessä kuluttavat enemmän palvelimen muisti- ja prosessorikapasiteettiä. (Ristić 2010, 7–8.)

2.2.10 SSL/TLS

Internetin käytön lisääntyminen on muuttanut ihmisten tapaa kommunikoida. Ihmiset kommunikoivat puhelinten ja tietokoneiden välityksellä, mitkä ovat liitetty internetiin. Internetissä siirrettävän tiedon määrä on kasvanut ja siksi on huolehdittava luottamuksellinen tiedon turvaamisesta. Tähän tarpeeseen on kehitetty SSL/TLS-tekniikka, jolla voidaan suojata siirrettävä tieto. Tällä hetkellä suuri osa laitteiden välisestä tiedonsiirrosta nojautuu SSL/TLS-tekniikkaan (Ristić 2014, 1).

SSL ja TLS ovat tekniikoita, jotka mahdollistavat selaimen ja www-palvelimen välisen kommunikoinnin salattuna turvattomassa verkossa. Tämä tarkoittaa, että yhteyden muodostuttua selaimen ja palvelimen välinen liikkeenne salataan ja molemmat tietävät, kenen kanssa tietoa vaihdetaan. (Ristić 2014, 1). SSL-teknologia takaa selaimen ja palvelimen välissä siirrettävän tiedon luottamuksellisuuden ja koskemattomuuden (Stuttard & Pinto 2011, 8). SSL toimii OSI-mallissa sovellus- ja verkkokerroksen välissä. Toimiminen verkkokerroksen yläpuolella mahdollistaa tiedon siirtämisen salattuna salatun yhteyden ylitse ja sen, että asiakas ja palvelin tunnistautuvat toisilleen ennen tiedon siirtämistä.

TLS on uudempi versio SSL-teknologiasta, joka toimii samalla tavoin kuin SSL, mutta sisältää parannuksia tietoturvaan. TLS käyttää vahvempia salaus- ja tunnistusprotokollia (Stewart ym. 2012, 153). TLS pystyy salauksen ja tunnistuksen lisäksi varmistamaan, ettei salattua tietoa peukaloida, salakuunnella tai väärennetä tiedonsiirron aikana. SSL ja TLS koostuvat kahdesta eri protokollasta, kättely- ja tietueprotokollasta. (Cross & Fisher 2011, 402–404.) Tietueprotokolla vastaa tiedon kuljetuksesta ja salaamisesta. Se jakaa tiedon osiin, jotta se voi salata ja tarvittaessa pakata tiedon. Kättelyprotokollan tehtävä on hoitaa yhteyden osapuolten välinen tunnistus ja salakirjoitusmenetelmän neuvottelu. (Vacca 2012, 435.)

2.3 Extranetit ja niiden tekniset ratkaisut

2.3.1 Extranet-järjestelmät

Extranet on organisaation yksityinen verkko, jonka kautta se julkaisee palveluita ja tietoa liiketoiminnastaan asiakkailleen ja sidosryhmilleen tietoturvallisesti käyttäen internet-teknologiaa (Finneran Dennedy, Fox & Finneran 2014, 13). Curtis & Cobham (2008, 191) mukaan järjestelmien käytön ja tiedon jakamisen laajeneminen organisaation ulkopuolelle muodostaa extranet-järjestelmän. Sen kautta jaetaan tietoa, jota ei voida jakaa organisaation julkisen internet-sivuston kautta.

Extranetillä hallitaan organisaation tietoihin ja sovelluksiin pääsyä rajoittamalla käyttöoikeuksia tietyille käyttäjille tai käyttäjäryhmille (Lloyd & Boyle 1998, 56). Järjestelmän käytöllä organisaatiot voivat jakaa eri käyttäjäryhmille yksilöllistä tietoa (Lloyd & Boyle 1998, 55). Se mahdollistaa ulkopuolisten käyttäjien työskentelyn organisaation sisäisten työntekijöiden kanssa.

Extranetit on suunniteltu parantamaan ja tehostamaan organisaation sekä asiakkaiden välisiä asiakassuhteita. Niillä organisaatiot pystyvät tarjoamaan ja ylläpitämään organisaation sekä asiakkaidensa välistä yksilöllistä suhdetta. Se mahdollistaa internetillä edullisen ja nopean tavan jakaa asiakkaalle räätälöityä tietoa keskitetysti, jota voidaan luoda dynaamisesti ja muokata perustuen määriteltyihin käyttöoikeuksiin. (Lloyd & Boyle 1998, 55.)

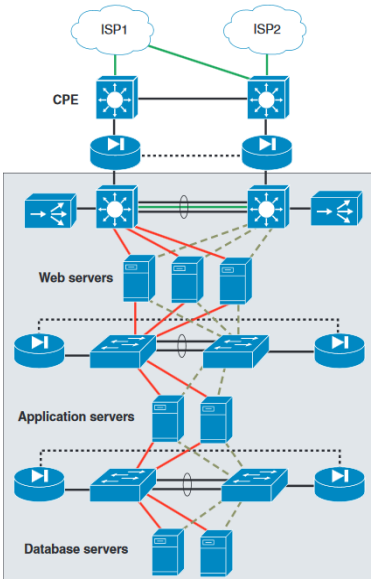
Extranetin tärkeimpiä etuja ovat prosessien ja tiedon nopea jakaminen, alhaiset kustannukset, hyvät asiakassuhteet ja kokonaisuudessaan liiketoiminnan tehostaminen (Rainer & Cegielski 2010, 344).

Aikaisemmin organisaatioiden väliset yksilöllisesti toteutetut extranetit olivat kustannuksiltaan kalliita ja heikosti skaalautuvia toisiin organisaatioihin. Jokaista extranetin toteutusta varten rakennettiin oma järjestelmä ja yksilöllinen yhteys. Nykyään internetteknologiaan perustuvat extranet-järjestelmät ovat suhteellisen edullisia toteuttaa ja ne ovat joustavia, integroituvia ja skaalautuvia nykyaikaisiin erilaisiin integroituihin järjestelmä- ja verkkosovellusympäristöihin. Nykyaikaiset extranetit lisäävät merkittävästi organisaatioiden välistä verkostoitumista.

Extranet-toteutuksissa merkittävä haaste on niiden tietoturva. Toteutuksissa joudutaan tasapainottelemaan käytännöllisyyden ja tietoturvan välillä. Liiketoimintakriittisen tiedon tarjoaminen extranetin kautta on toteutettava tehokkaasti, mutta samalla on pystyttävä suojaamaan organisaation sisäinen verkko ja järjestelmät ulkoisilta uhilta. Sisäverkon ulkoisen uhan muodostaa se, että internetistä on sallittava yhteys sisäverkkoon. Extranet-järjestelmät koostuvat sovelluksista, joista usein on yhteyksiä sisäverkossa olevalle tietokantapalvelimille.

Extranet-järjestelmissä käytetään N-tier (kerros)-arkkitehtuuria, jossa extranetin sovelluskomponentit ovat jaettu eri kerroksiin. Näitä ovat esitys-, sovelluslogiikka- ja tietokantakerros. Kerrokset ovat verkkoteknisesti eristetty omiin verkkosegmentteihin, jolloin jokaisessa kerroksessa voidaan käyttää yksilöllistä verkkopolitiikkaa. Ne on eristetty toisistaan palomuurilla ja niissä voidaan käyttää yksilöllisiä verkon turvamekanismeja.

Kuvassa 3 extranetin sovelluskomponentit on jaettu verkkoarkkitehtuurissa yllä mainittuihin kolmeen kerrokseen. Organisaatiolle kriittinen tieto pidetään sovellus- ja tietokantakerroksissa. Esityskerros on sijoitettu DMZ-verkkoalueelle, josta käyttäjille tarjotaan extranetit-käyttöliittymä (Front end) (Microsoft, 2016).

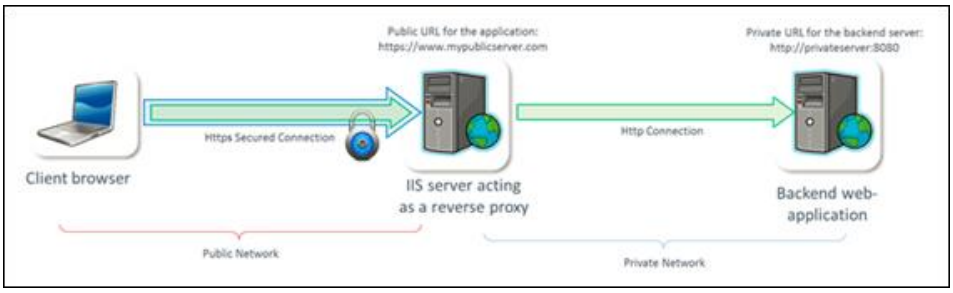


Kuva 3. N-Tier-arkkitehtuuri. (Cisco, 2013).

Extranet-järjestelmätoteutuksissa yhdistyvät useat erilaiset teknologiat, jotka mahdollistavat palveluiden tarjoamisen tehokkaasti organisaation ulkopuolelle. Extranet-toteutuksissa käytettäviä tekniikoita ovat reverse proxy-, kuormantasaus-, high availability-, vahva tunnistus-, SSO- ja SSL/TLS -tekniikka.

2.3.2 Reverse Proxy

Reverse proxy on laitteisto tai palvelu, jonka tehtävänä on välittää internetistä tulevia http-pyyntöjä organisaation web-palvelimille suojaamalla varsinaisten web-palvelinten identiteettiä. Sen roolina on toimia keskitettynä yhdyskäytävänä internetin ja organisaation web-palvelimien välillä. Sitä käytetään organisaation sisäverkon web-palvelimien suorituskyvyn ja tietoturvan parantamiseksi. Tyypillisesti se on sijoitettu palomuurin taakse organisaation sisäverkkoon. Kuvassa 4 http-pyyntö ohjautuu taustapalvelimelle siten, että internetistä yhteyttä ottava asiakas-selain näkee vain reverse proxy -osoitteen (Stewart 2013, 262).



Kuva 4. Reverse Proxy:n toimintaperiaate (Microsoft, 2016).

Reverse proxyt toimivat myös kuormantasaajina taustapalvelimille. Kuormantasauksen tehtävänä on jakaa sen kautta tulevat pyynnöt tasaisesti pyyntöjä vastaanottaville palvelimille, mikä vähentää taustapalvelimille kohdistuvaa kuormaa ja nopeuttaa pyyntöjä kutsuvaa selaimen toimintaa.

Lisäksi reverse proxyt suorittavat muita niille tyypillisiä toimenpiteitä, kuten sisällönkytkentää, liikenteenoptimointia ja käyttäjätunnistusta. Sisällönkytkentä on toiminnallisuus, jolla sisään tuleva liikenne voidaan reitittää palvelupyyntöjen sisältämän tiedon perusteella oikealle palvelimelle. Internetliikennettä tutkitaan sovellustasolla, jossa http-pyynnön sisältämillä yksityiskohdilla liikenne ohjataan oikealle palvelimelle. Sisällönkytkentä on edistynyttä kuormantasausta, jossa ohjauspäätös tehdään yksityiskohtaisemmalla tavalla kuin perinteisessä verkkotason kuormantasauksessa. (Citrix 2015.)

Liikenteen optimointiin reverse proxy käyttää content-caching ja ssl-offload -toiminnallisuuksia. Content-caching -toiminallisuudella se tallentaa välimuistiin web-palvelimien tarjoaman staattisen sisällön, mikä vähentää web-palvelimille ohjautuvien turhien pyyntöjen määrää samalla vähentäen niiden työkuormaa (Stewart 2013, 263).

SSL-offload-toiminallisuudella reverse proxy purkaa salatun ssl-liikenteen taustalla olevien web-palvelinten puolesta erillisessä arkkitehtuurissa, mikä nopeuttaa näiden toimintaa (Ristić 2014, 248). Liikenteen sisältöön perustuvaa ohjausta ja suodatusta voidaan tehdä salauksen purun jälkeen.

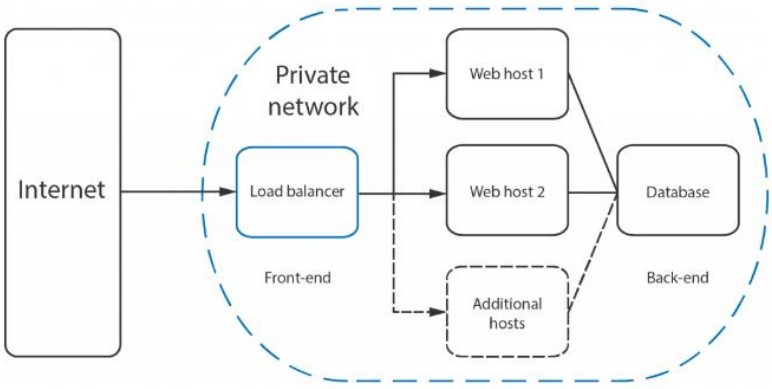
Verkkosovelluspalomuurin (WAF) käyttö on tavallista reverse proxyn yhteydessä, missä liikenne ohjataan WAF:n lävitse salatun liikenteen purkamisen jälkeen (Bosworth ym. 2014, 269). Reverse proxy voi myös salata uudelleen purkamansa liikenteen, ohjatessaan sitä eteenpäin taustapalveluille.

Reverve proxy suorittaa keskitettyä pääsynhallintaa käyttäen erilaisia tunnistusmekanismeja tai näiden yhdistelmiä. Ne tukevat myös SSO-kirjautumismenetelmää. Reverve proxy suorittaa käyttäjätunnistuksen web-palvelinten puolesta, mikä estää oikeudettomat pääsyt eteenpäin. Tämä yksinkertaistaa web-palvelinten käyttäjähallintaa ja ylläpitoa sekä parantaa tietoturvaa.

Reverse proxyjä käytetään extranet-toteutuksissa, koska niillä voidaan lisätä tietoturvaa luomalla epäsuora pääsy julkisesta verkosta organisaation sisäverkon palveluihin (Stewart 2013, 263).

2.3.3 Load Balancing

Kuormantasauksella (Load Balancing) tarkoitetaan menetelmää, jossa palvelinresursseihin kohdistuvaa käyttökuormaa jaetaan tasaisesti palvelinresursseja tarjoaville palvelimelle. Kuormantasaajiksi kutsutaan kuormantasausta suorittavia palvelimia, joiden tehtävänä on jakaa sovelluspyynnöt tasaisesti. Kuormantasaajat samalla parantavat resurssipalvelimen saatavuutta, koska yhden sovellusresursseja tarjoavan palvelimen vikaantuessa, kuormantasaus huolehtii sovelluspyyntöjen ohjauksen seuraavalle toimivalle palvelimelle. (Citrix 2015.) Kuvassa viisi kuormantasaaja tasaa taustapalvelimille kohdistuvaa liikennekuormaa.



Kuva 5. Kuormantasaajan toimintaperiaate (UpCloud, 2016).

Kuormantasaajan ydintoiminnallisuudet ovat verkko- ja sovellustasolla tapahtuva kuormantasaus. Verkkotasolla tapahtuvassa kuormantasaamisessa ohjauspäätökset perustuvat verkko-ja kuljetuskerrosprotokollien dataan, kuten TCP-portteihin ja IP-osoitteeseen. (Citrix 2015.) Kuormantasaaja purkaa myös tcp-paketeista tarvittavat osoitetiedot, joiden perusteella se tekee reitityspäätöksen (NGINX 2016).

Kuormantasaajat käyttävät verkkotasolla eri metodeja suorittaakseen tasausta. Yleisimmin käytettyjä kuormantasaus algoritmeja ovat round-robin ja least-connection. Round-

robin metodissa sovelluspyynnöt ohjataan aina järjestyksessä seuraavalle palvelimelle, jolloin samalle palvelimelle ei ohjata kahta peräkkäistä sovelluspyyntöä (NGINX 2015).

Least connection-metodissa jokainen sovelluspyyntö ohjataan palvelimelle, jolla on vähiten yhteyksiä auki. Metodi ei huomio kohdepalvelimen kuormaa ohjauspäätöksessä. Kuormantasaus on yksinkertainen tapa hyödyntää tehokkaasti palvelinkapasiteettiä. (NGINX 2015.) Palvelinlaitteiden laskentatehojen kasvu on alentanut verkkotason kuormantasauksen merkitystä (NGINX 2016).

Sovellustason kuormantasaajat tekevät ohjauspäätökset tarkemmalla tasolla kuin verkkotasolla toimivat kuormantasaajat. Nykyiset modernit kuormantasaajat toimivat myös reverse proxyinä, joissa ohjauspäätökset tehdään perustuen sovelluskerroksen dataan, kuten http-paketin sisältöön ja sen sisältämiin eri attribuutteihin esimerkiksi http-tunnisteeseen (Citrix 2015).

2.3.4 Application Delivery Controller

Application Delivery Controller (Sovellusten toimitusjärjestelmä)-nimitystä käytetään uuden sukupolven kuormantasaajalaitteista. ADC:t suorittavat perinteisten kuormantasaajien tekemien toimintojen lisäksi toiminnallisuuksia, kuten sovellustason liikenteenohjausta ja keskitettyä pääsynhallintaa sekä tarjoavat taustapalveluille sovellustason tietoturvaa. ADC:llä voidaan myös valvoa taustapalveluiden tilaa ja tarjota SSL-VPN etäkäyttöpalvelua. (Citrix 2016.)

ADC:n tarkoituksena on vastata nykyvaatimuksiin vähentäen verkossa olevien laitteiden määrää käyttäjien ja sovellusten välillä. Tavallisesti näiden toimintojen toteuttamista varten on tarvittu useammasta laitteesta koostuva ympäristö.

Yhä enemmän kehitetään uusia teknologioita ja erilaisia protokollia, joilla sovelluksiin ja tietoon päästään käsiksi, mistä ja millä tahansa. ADC:n rooli on integroida nämä uudet teknologiat nykyisiin verkkoihin. (F5 Networks Inc 2012.)

2.3.5 Multi-Factor Authentication

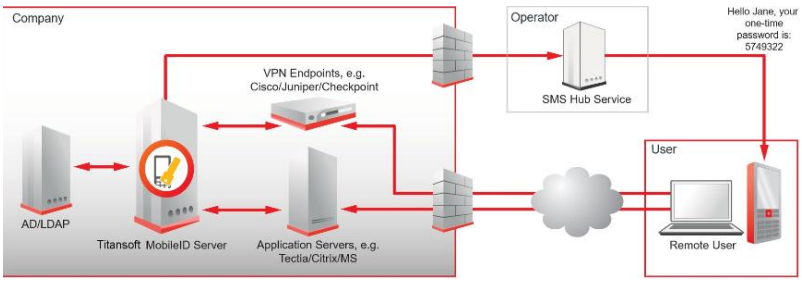
Multi-Factor Authentication on vahva tunnistusmenetelmä, joka käyttää kahta tai useampaa tekijää tunnistukseen (Stewart ym. 2012, 21). Tekijät ovat kaksi toisistaan erillistä itsenäistä tunnistusmenetelmää, jotka molemmat käyttäjän on läpäistävä, jotta tunnistus voi tapahtua. Tyypillisesti ensimmäinen tekijä on käyttäjätunnus ja salasana -yhdistelmä, jonka käyttäjä tietää. Tekijöistä toinen on käyttäjällä hallussa oleva fyysinen laite, jota käytetään samassa tunnistusprosessissa. Ei riitä, että käyttäjä tietää salasanan, vaan käyttäjällä on oltava jotain henkilökohtaista mukana tunnistushetkellä. (Thomas & Stoddard, 2012, 161.)

Vahvoissa tunnistusmenetelmissä käytetään toisena tekijänä tavallisesti tokeneita ja biometrisiä tunnisteita. Perinteiset rautapohjaiset tokenit, joihin generoituu dynaamisesti PIN-koodi, ovat olleet jo pitkään organisaatioilla käytössä esimerkiksi VPN-

yhteyksissä. Ne soveltuvat käytettäväksi rajattuun käyttöön, koska niiden hallinta on työlästä ja laite-kustannukset kasvavat isoissa ympäristöissä. (Bosworth ym. 2014, 330.)

Toinen pitkään käytössä ollut menetelmä on sms-pohjainen (one-time password OTP). Otp-tekstiviestitunnistusta pidetään turvallisena, koska viesti on kertakäyttöinen ja voimassa tietyn hetken. Lisäksi viesti ei tallennu puhelimeen siten, kuin tavalliset tekstiviestit. OTP:n käyttö isoissa käyttäjämäärissä on edullisempaa kuin laitepohjaisten tokeneiden käyttö (Bosworth ym. 2014, 290).

OTP-tunnistusprosessissa käyttäjän syöttäessä tunnuksen ja salasanan, OTP-palvelin (Radius) varmentaa Active Directory hakemistopalvelusta, että käyttäjän syöttämä käyttäjätunnus ja salasana täsmäävät. Tämän jälkeen OTP-palvelin lähettää käyttäjälle yksilöllisestä esimerkiksi ajasta tai käyttäjän puhelinnumerosta generoidun tekstiviestin (tokenin), jonka käyttäjä syöttää määriteltyyn kenttään. Tässä vaiheessa otp-järjestelmä tarkistaa, että käyttäjän syöttämä token on oikein ja sallii pääsyn. Kuvassa 6 esitetään OTP-tekstiviestitunnistuksen toiminta.



Kuva 6. OTP:n toimintaperiaate (Titansoft, 2016).

Tavallisesti verkkosovelluksien tunnistukseen käytetään käyttäjätunnusta ja salasanaa, joka ei ole riittävän vahva tunnistusmenetelmä kriittistä ja arkaluonteista tietoa sisältävään palveluun tai järjestelmään. Varsinkin extranetit ovat järjestelmiä, joissa pitää käyttää vahvaa kaksivaihetunnistusta, koska organisaation on oltava varma ulkopuolisten käyttäjien identiteetistä. Käyttäjille sallitaan pääsy extranet-portaaliin ja sieltä eteenpäin sisäverkon palveluihin ja -järjestelmiin. (Bosworth ym. 2014, 330.)

Pankkien internet palveluissa vahva kaksivaiheinen tunnistus on ollut käytössä jo pitkään. Vahvan tunnistuksen käyttö on laajentunut muissakin palveluissa, kuten erilaisissa pilvipalveluissa. Sen lisäksi extranet-palveluissa käytetään SSO-kertakirjautumismenetelmää, jossa käyttäjän ei tarvitse kirjautua palveluihin erikseen. Menetelmää kuvataan seuraavassa luvussa.

2.3.6 Single Sign-On SSO

SSO on keskitetty pääsynhallintatekniikka, joka sallii käyttäjän pääsyn verkon eri resursseihin yhdellä tunnistuksella. Tunnistuksen jälkeen käyttäjän ei tarvitse tunnistautua uudelleen käyttäessään verkon resursseja ja sovelluksia (Stewart ym. 2012, 27).

Organisaatioiden käytössä olevat SSO-tekniikat jaetaan käyttötarkoituksen mukaan luokiteltuihin toteutusmalleihin. Toteutusmallit ovat työasemaympäristö SSO, enterprise SSO ja extranet SSO. Usealla organisaatiolla on käytössä kaikki kolme edellä mainittua SSO-toteutustapaa (Microsoft, 2017).

Työasemaympäristön SSO tarkoittaa organisaation sisällä eri resurssien ja sovelluksien käyttöä yhdellä tunnistuksella. Enterprise SSO-toteutuksessa organisaation ja liikekumppanin välille perustetaan federoitu luottosuhde, jossa käyttäjät voivat käyttää toisen organisaation verkon resursseja ja sovelluksia yhdellä tunnistuksella (Microsoft, 2017).

Extranet SSO:lla (Web SSO) tarkoitetaan organisaation extranet-toteutusta, jossa ulkopuoliset käyttäjät pääsevät extranetin kautta julkaistuihin palveluihin yhdellä kirjautumisella (Microsoft, 2017).

SSO:ta pidetään tietoturvaa lisäävänä mekanismina, koska käyttäjien ei tarvitse kirjoittaa eri järjestelmien käyttäjätunnuksia ja salasanoja muistiin. Sen käyttö vähentää myös järjestelmien tunnuksien hallintaan liittyvää ylläpitotyötä. (Stewart ym. 2012, 28.)

3 EMPIIRINEN OSUUS

Empiirisen osuuden luvut sisältävät case-yrityksen ja valitun tutkimusmenetelmän sekä tutkimusmetodin esittelyn. Tämän jälkeen on kuvattu tutkimuksen kulku ja aineiston analysointimenetelmä. Lisäksi empiirisessä osuudessa on arvioitu tutkimuksen luotettavuutta, pätevyyttä ja oikeellisuutta.

3.1 Case-yrityksen esittely

Cinia Oy on vuonna 1998 perustettu suomalaisessa omistuksessa oleva ICT-alan yritys, joka työllistää tällä hetkellä 220 henkilöä. Cinia on verkkoyhteyspalveluita, telematiikan järjestelmäratkaisuja, ohjelmisto- ja pilvipalveluita tuottava yritys. Tämän lisäksi se tuottaa valvontapalvelua yritysten IT-infrastruktuureille ja niiden palveluille.

Cinian tarjoamat verkkoyhteysratkaisut on suunniteltu erityisesti yritykselle, joiden liiketoiminta vaatii nopeita ja luotettavia yhteyksiä. Cinia suunnittelee asiakaskohtaisesti räätälöityjä verkkoyhteyksiä kokonaispalveluna. Cinialla on käytössä yli 10 000 kilometrin laajuinen runkoverkon, joka mahdollistaa yrityksille luotettavan IT-ympäristön ja datakeskuskeskeisen toimintaympäristön.

Ohjelmistopalvelut, joka työllistää noin 100 henkeä, tuottaa asiakkaan vaatimusten pohjalta räätälöityjä ohjelmistopalveluita. Ohjelmistopalvelut ovat mukana järjestelmähankkeissa, joissa asiakkaiden järjestelmä suunnitellaan, toteutetaan, viedään tuotantoon ja ylläpitoon.

Cinia tuottaa myös kapasiteettipalvelua yksityisenä (Private Cloud) pilvipalveluna, joka sijaitsee Suomessa korkean turvallisuuden datakeskuksessa. Palvelun tarkoituksena on tarjota yrityksille mahdollisuus siirtää omaa infrastruktuuriaan ja palveluitaan yksityiseen virtuaaliseen konesaliin, johon sisältyvät luotettavat ja nopeat verkkoyhteydet.

Tutkimuskohteeksi valikoitui Cinia Oy, koska siellä on käytössä extranet-palvelu, jonka kautta se julkaisee taustapalveluina muun muassa työnohjaus -ja valvontapalveluita asiakkailleen, sidosryhmilleen ja yhteistyökumppaneilleen. Nykyisen extranetin ohjelmistot ja laitteistot ovat vanhentuneet ja eivät nykyisellään tarjoa riittävää tietoturvatasoa.

Tutkimuksessa hyödynnettiin avoimeen lähdekoodiin perustuvaa LemonLdap -järjestelmää, joka voi toimia reverse proxynä taustapalveluille. Järjestelmä tarjoaa myös keskitettyä käyttäjätunnistusta ja sso-toiminnallisuutta.

3.2 Tutkimusmenetelmä ja metodi

Opinnäytetyön tutkimus menetelmänä käytetään kvalitatiivinen tapaustutkimusta ja haastattelua. Tutkimusongelma määrittää sen, mikä tutkimusmenetelmä sopii ongelman ratkaisuksi (Hirsjärvi 2007, 179). Opinnäytetyössä tarkoituksena on etsiä vastausta, miten organisaatio voi tietoturvallisesti julkaista sisäverkon palveluita extranet-järjestelmällä ulkopuolisille käyttäjille? Laadullisen tutkimus vastaa kysymykseen, miten ja miksi (Saaranen-Kauppinen & Puusniekka 2006). (Hirsjärvi 2007, 134) lisää, että laadullisen tutkimuksen tarkoitus on olla kartoittava ja kuvaileva. Opinnäytetyön tulokset kuvaavat

extranet-järjestelmän osa-alueita ja kartoittavat sisäverkon turvallisen julkaisemisen eri tekijöitä.

Tutkimusmetodina on puolistrukturoitua teemahaastattelu. Teemahaastattelussa keskitytään pieneen haastateltavien määrään, mutta haastateltavien kokemuksiin, uskomuksiin ja tuntemuksiin syvennytään tarkemmalle tasolle. (Hirsjärvi & Hurme 2008, 47–48.) Cinia Oy:ssä IT-järjestelmien ylläpidosta ja kehittämisestä vastuussa on muutama henkilö ja heillä on laaja osaaminen erilaisten IT-ympäristöjen ylläpidosta.

Puolistrukturoiduissa teemahaastattelussa haastattelu kohdennetaan valittuihin teemoihin, jotka haastattelija pitää samana kaikilla haastateltavilla. Haastattelurunkoa laadittaessa ei määritellä yksityiskohtaista kysymysluetteloa vaan teema-alueluettelo. Teemojen alle laaditut kysymykset toimivat haastattelijan muistilistana. Teemojen alla kysymykset voivat tarvittaessa vaihdella tai itse haastattelutilanteessa teema-alueen sisällä tutkija voi esittää tarkentavia kysymyksiä. (Hirsjärvi & Hurme 2008, 66.)

3.3 Tutkimuksen kulku

Teorian ja opinnäytetyön ongelman perusteella suunniteltiin teemahaastattelun teemat ja muistilistaksi kysymykset. Haastateltavat valittiin case-yrityksestä. Haastateltavien valintakriteerinä oli Cinia yrityksessä työskentelevät henkilöt, jotka vastaavat Cinian IT-järjestelmien ylläpidosta ja kehittämisestä. Haastatteluun osallistuneista on koottu liitteeseen 2 opinnäytetyön kannalta oleelliset taustatiedot, kuten ammattinimike, haastattelu ajankohta ja kesto.

Hirsjärvi & Hurme (2008, 127) neuvoo, että litterointi voidaan tehdä koko aineistosta tai valikoiden teema-alueiden mukaisesti. Tässä opinnäytetyössä litterointi on suoritettu teema-alueiden mukaisesti.

3.4 Aineiston analysointimenetelmä

Hirsjärvi & Hurme (2008, 143–144) mukaan analyysissa on tarkoituksena eritellä ja luokitella tietoa. Aineistokokonaisuudesta muodostetaan osia, aineistoa luokitellaan ja luokkia yhdistellään. Laadullisessa tutkimuksessa tulkintaa tapahtuu koko prosessin ajan, eikä pelkästään analysointivaiheessa.

Synteesissä muodostetaan kokonaisuuksia, tulkitaan syvällisesti ja hahmotetaan ilmiötä uudelleen. Tarkoituksena on muodostaa kokonaiskuva ja esitellä tutkittava ilmiö uudessa perspektiivissä. (Hirsjärvi & Hurme 2008, 143–144.)

Haastattelut purettiin litteroimalla. Aineiston analyysissa teemojen mukaisesti muodostuivat extranet-järjestelmän osa-alueet. Tämän jälkeen informaatiota tyypiteltiin ja löydettiin kolme luokkaa, joista muodostuivat sisäverkon turvallisen julkaisemisen tekijät.

3.5 Tutkimuksen reliabiliteetti ja validiteetti

Tutkimuksen reliaabelius tarkoittaa luotettavuutta ja mittaustulosten toistettavuutta. Kaikissa tutkimuksissa tulee arvioida tutkimuksen luotettavuutta. Laadullisen tutkimuksen luotettavuutta lisää tarkka selostus tutkimuksen toteuttamisesta. (Hirsjärvi 2007, 226–227.) Tässä opinnäytetyössä on selitetty tutkimusmenetelmän ja metodin valinta, tutkimuksen kulku ja analysointimenetelmät. Opinnäytetyössä on myös haastatteluotteita aineiston kuvaus luvussa (4.1). Suorat haastatteluotteet ovat todisteita siitä, mihin opinnäytetyön tulokset perustuvat. Näiden voidaan nähdä lisäävän opinnäytetyön reliabiliteettia.

Mittaustulosten toistettavuus tarkoittaa sitä, että tutkimus ei anna sattumanvaraisia tuloksia (Hirsjärvi 2007, 226). Tämä tarkoittaa sitä, että samalla aineistolla on päästävä samoihin tuloksiin. Laadullisessa tutkimuksessa myös tutkimuksen ajankohta vaikuttaa saatuihin tuloksiin. Varsinkin tietotekniikan alalla järjestelmät kehittyvät nopeasti ja samat kysymykset esittämällä valituille haastateltaville, päästäisiin hyvin todennäköisesti eri tuloksiin kuin tässä opinnäytetyössä.

Tutkimuksen validiteetti tarkoittaa pätevyyttä ja sitä voidaan arvioida, joko koko tutkimuksen, metodin valinnan tai mittarin pätevyyden osalta (Saaranen-Kauppinen & Puusniekka 2006). Mittarin tai tutkimusmenetelmän validius tarkoittaa sen kykyä mitata juuri sitä, mitä sen on tarkoituskin mitata (Hirsjärvi 2007, 226).

Mittaria pitää käyttää oikeaan kohteeseen, oikealla tavalla ja oikeaan aikaan. Jos mittausvälineenä käytetään haastattelua, voidaan esimerkiksi epäonnistua haastateltavien valinnassa ja haastattelun ajankohdassa. Haastateltavan ja haastattelijan välinen henkilökemia voi myös vaikuttaa mittaustulokseen, joka aiheuttaa epäluotettavuutta mittaustuloksessa (Saaranen-Kauppinen & Puusniekka 2006).

Lisäksi pätevyys tarkoittaa sitä, onko tutkimus perusteellisesti tehty ja ovatko saadut tulokset sekä tehdyt päätelmät oikeita. Voidaan esimerkiksi tehdä virheellisiä päätelmiä suhteista tai kysyä vääriä kysymyksiä (Saaranen-Kauppinen & Puusniekka 2006).

Opinnäytetyön haastattelukysymyksiä voidaan pitää pätevinä, koska kysymykset on suunniteltu käytännön käyttöönottoprojektin suunnittelutyön ja luetun teorian perusteella. Lisäksi haastateltavat on valittu yrityksen IT-ammattilaisten joukosta, jolloin he ymmärtävät kysymykset ja käytetyt ammattitermit. Päätelmien validiteettia voidaan pitää riittävänä, koska päätelmät perustuvat mitattuihin tuloksiin ja johtopäätöksiä tehtäessä tuloksia on vertailu teoriaan.

4 TUTKIMUKSEN KESKEISET TULOKSET JA HAVAINNOT

Tutkimuksen keskeiset tulokset sisältävät aineiston kuvauksen ja opinnäytetyön keskeiset tulokset. Aineiston kuvauksessa on haastatteluotteita, jotka kuvaavat esimerkkejä teeman sisällä esiintyneistä tyypillisistä vastauksista tai poikkeavista havainnoista. Haastatteluotteet ovat muokkaamattomia puhekielisiä otteita, joiden tarkoitus on lisätä tuloksien reliabiliteettia.

Tulososiossa sisäverkon palveluiden turvallinen julkaiseminen on jäsennetty tyypillisten tapausten mukaisesti uudeksi kokonaisuudeksi. Tarkoituksena on ollut esittää tulokset selkeänä ja tiiviinä taulukkona.

4.1 Aineiston kuvaus

4.1.1 Extranet-järjestelmiin (käyttöjärjestelmä) liittyvä tietoturva

Useamman haastateltavan mukaan käyttöjärjestelmien tietoturvaa parantavina menetelminä pidettiin järjestelmällistä ja säännöllistä ohjelmisto- ja tietoturvapäivitysten asentamista. Tuotantopäällikkö kuvaa: *siellä pitää tietenkin huomioida on se käyttöjärjestelmä ja siihen liittyvät sovelluskomponentit, niitten päivitykset niin päivitykset pitää tehdä ne pitää tehdä järjestelmällisesti mielellään automaattisesti.*

Lisäksi haastateltavat esittivät, että käyttöjärjestelmille on tehtävä tietoturvakovennuksia, jotka pienentävät järjestelmiin kohdistuvaa hyökkäyspintaa. Asiantuntija: *niihin tulis tehdä tämmösiä käyttöjärjestelmäkovennuksia sitten tota vois ajatella näin, että ne palvelut, mitä siellä palvelimella sitten pyöritetään niin pitäisi karsia minimiin eli pyörittää vain ja ainoastaan niitä palveluita, mitä tarvitaan sen niin kun toiminnallisuuden saavuttamiseksi ja kaikki muu ylimääräinen pitäisi karsia pois.*

Aineistossa esille nousi järjestelmäylläpitäjien aktiivisuuden ja suunnitelmallisuuden merkitys, mitä asiantuntija kuvaa: *tietyllä tavalla se, että sillä ylläpidolla olisi aikaa tietyllä tavalla tutustua siihen niihin järjestelmiin, jotta se olis niin kuin se niin kuin tietyllä tavalla pysyttäis siinä mukana ja sinne ei vaan arvattais niitä asetuksia kohdilleen*.

Aineistossa esille nousi järjestelmien käyttöönoton ja suunnittelun merkitys järjestelmätietoturvalle. Tuotantopäällikkö: *sillon kun niitä järjestelmiä pystytetään niin tavallaan turvallisuus otetaan siinä vaiheessa huomioon et mietitään, että millaseen verkkoon ne esimerkiks tulee ja ketkä niihin ottaa yhteyttä, miten niihin voidaan päästä käsiks.* Teoriaosuudessa Andreasson ym. (2013, 69) painottaa, että organisaation on tunnistettava suunnitteluvaiheessa verkkoon liitettävät laitteet ja palvelut. Tämän perusteella tunnistetaan, mitä tietoa verkossa siirretään.

Kaikkien haastateltavien mukaan käyttäjätunnuksille on annettava vain tarvittavat oikeudet suorittaa toimenpiteitä järjestelmässä ja käyttöoikeudet on myönnettävä käyttäjäroolin perusteella. Tuotantopäällikkö kuvaa asiaa: *käyttäjätunnuksella annetaan vaan sen roolin vaatimat oikeudet mukaan luettuna myös se, että admin tunnuksellekin*

annetaan vaan ne oikeudet, mitä tarvitaan ja toteaa lisäksi: *perinteinen mahdollisimman vähän oikeuksia periaate on se, millä ensimmäisenä lähdetään, jokaisella on yksilölliset käyttäjätunnukset.*

Aineistosta nousi esille järjestelmän palveluiden ja prosessien käyttämien tunnusten käyttöoikeudet. Järjestelmän palveluille ja prosesseille tulee antaa mahdollisimman vähän oikeuksia. Asiantuntija toteaa: *ne palvelut, mitä siellä palvelimella ajetaan, niin niitä ei ajeta pääkäyttäjätunnuksin, jos se vaan on sen sovelluksen kannalta mitenkään mahdollista.*

4.1.2 Extranetin tietoliikenneturvallisuus

Haastateltavat pitivät tietoliikenneturvallisuutta lisäävänä tekijänä sitä, että extranetin komponentit sijoitetaan eri verkkosegmentteihin, joilla luodaan järjestelmäkokonaisuuteen tietoturvaa kerroksilla. Asiantuntija kuvaa kerrosmallia: *ajatus, että on erilaisia erilaisia tämmösiä tasoja eli ja sitten, kun sen reverse-proxyn kautta mennään, sitten siihen sovellukseen sitten, mitä halutaan julkaista niin, sitten siinä sovelluksessa on oma esityskerros, sitten siellä takana voi olla joku tämmönen middleware-kerros ja sitten voi olla joku tämmönen tietokantakerros vielä riippuen vähän järjestelmästä eli tämmöisellä hierarkialla pystyy sitten tätä tietoliikenneturvallisuutta parantamaan tai ainakin sitä minimoimaan sitä.*

Haastateltavien mukaan extranet-komponentit tulee eriyttää eri verkkoihin ja verkkojenvälinen liikenne on palomuuritettava. Asiantuntija: *sulla on joku frontti niin siinä välttämättä ei oo edessä vielä ihan hirveesti muuria, mutta sit se et se liikennöi sinne seuraavalle tasolle niin taas kerran mennään jonkunnäkösen turvakomponentin, onko se sitten muuri onko se sitten joku suodattava proxy.*

Extranetien merkittävä tekijä verkkoturvallisuudelle on DMZ-verkko, jonka kautta yrityksen sisäverkon palveluita julkaistaan internetiin. Asiantuntija: *ajatus on oikeastaan se että internetistä pystytään liikennöimään vain ja ainoastaan siihen dmz-verkkoon niin kuin IP-reititys mielessä ja sitten vasta siitä DMZ-verkosta sitten siinä oleva sitten tää reverse-proxy pystyy juttelemaan sitten palomuurin läpi sitten sisäverkon palvelimien kanssa.*

Taustajärjestelmiä suojataan sallimalla vain taustajärjestelmien toiminnallisuuden vaatimat palomuuriavaukset. Asiantuntija kuvaa DMZ-verkon ja ldap-tunnistusjärjestelmän välistä yhteyttä: *meillä reverse proxy on yleensä siellä dmz alueella niin ja sitten yleensä tämä ldappi on jossain taustaverkossa niin tota siinä on yleensä aina muuri välissä voi olla useampikin muuri ja verkkotopologisesti se on layer kolme mielessä eriytetty niin, että tota niiltä palvelimilta ei pääse sitten tota muuta, kun sillä ldap protokollalla liikennöimään sitten sen palomuurin läpi.*

Extranetissä tiedon luottamuksellisuus tiedonsiirron aikana turvataan salaamalla yhteys asiakasselaimen ja reverse-proxyn välillä käyttäen SSL/TLS -tekniikkaa. Asiantuntija esittää*: jos ajatellaan että käytetään nettiselaimella extranet palveluita niin tota yleensä ne on käytettävissä vain ja ainoastaan sitten salatun yhteyden yli eli varsinkin jos on sitten*

jotain tämmöstä palvelua, joka vaatii autentikointia niin tota ei yleensä haluta lähettää niitä autentikointitietoja salaamattomana siitä internetin yli.

Yhteyden salaus edustapalvelusta (front end) taustapalveluihin asti nousi esille kaikkien haastateltavien keskuudessa. Yhteyden salauksella alusta loppuun voidaan olla melko varmoja tiedon luottamuksellisuuden säilymisestä. Asiantuntija: *kyl se aika pitkälti nykypäivänä on sillä tavalla, että hyvin paljon niin kun uusista palveluista niin tiedonsalaus on vaikka se on sisäverkossa niin on hyvin usein TLS -protokollalla suojattuja.* Toinen asiantuntija korostaa luottamuksen säilyttämistä, kun käytetään sertifikaattipohjaista salausta: *mut periaatteessa siihen ei kenenkään pitäis päästä väliin silloin kun se on sertifikaatein suojattua liikennettä.*

Haastateltavien mielestä hallintaan käytetyt yhteydet on turvattava. Kaikkien mukaan hallintayhteydet tulisi eriyttää asiakasliikenteestä omaksi dedikoiduksi yhteydeksi. Asiantuntija kuvaa asiaa: *Ideaalitapaus olisi sellainen, että asiakasliikenne kulkisi oman IP-liitännän kautta eli palvelimessa, jossa pyöritetään joko loadbalancer tai reverse-proxy toiminnallisuutta niin asiakasliikenne menisi omaa IP-liitäntää pitkin ja sitten olisi erillinen hallintaliitäntä siinä palvelimessa.*

Hallintayhteyksien rajaaminen siten, että IP-tasolla jo rajataan tiettyyn pisteeseen, mistä sallitaan hallintayhteydet extranetin-hallintaliittymään. Asiantuntija toteaa: *mä kuitenkin näkisin, että jonkunnäkönen tämmönen yks hallintapiste, joka ois sitten turvattu erityisen hyvin ja sieltä ois sitten hallintayhteydet mä näkisin näin, että se ois et sä niitä hallintaportteja ei avattais kaikille, vaan se pidettäisi se hallintaportti hyvin suppeena.*

Aineistossa nousi esille, että extranet-järjestelmän hallintanäkymään tunnistamiseen voidaan käyttää kaksivaiheista tunnus ja salasana -yhdistelmää, jolla varmistutaan ylläpitäjän identiteetistä. Asiantuntija: *kyllä mun mielestä pitäis olla jonkunnäköset aika vahvat salasanat ja sit mieluummin ihan vaikka sitten hallintayhteydessäkin jonkunnäkönen Two-Factori jossain vaiheessa.*

Verkkoliikenteen havainnointi- ja estämisjärjestelmiä pidettiin olennaisena tietoliikenneturvallisuudelle. Asiantuntija: *noihan on kovia juttuja noi, mutta ne sitten kans aika high level juttuja noi tämmöset niin, kun järkevämmät tämmöset oikein detection systeemit tai prevention systeemit IPSit IDSit*. Asiantuntija painottaa liikenteen tarkempaa tutkimista: *verkkojen välillä on jonkinnäköinen suodattava elementti, turvaelementti, jossa mahdollisesti skannataan sitten liikennettä vähän tarkemmin kuin vain porttitasolla, sehän ois se vähän niin kuin se optimitilanne, et sitä pystyttäis sitä liikennettä kuuntelee myös niin kuin, mitä siellä menee.*

Aineistossa esiintyi yksittäisenä seikkana eri sovellus- ja laitevalmistajien tuotteiden käyttäminen. Asiantuntija: *ehkä mä lähtisien sillä et sitten olis esimerkiks erilaisia tuotteita siinä matkan varrella, et jos yhdessä löytyykin tietoturva-aukko niin, se ei välttämättä ole sit siinä toisessa.*

Esille nousi haastatteluissa IDS-järjestelmien kehittyminen verkkotasolta järjestelmä- ja palvelintasolle. Asiantuntija: *nythän on viime vuosina sitten alkanut tulee tämmöisiä niinsanottuja host based intrusion detection systems tai sitten host based prevention systems eli tavallaan, että se toiminnallisuus, joka aiemmin on tehty ehkä erillisessä laitteessa verkkotasolla niin tuodaan nyt sitten ihan sinne sinne palvelin tasolle.*

Yksi haastateltavista esitti näkemyksen, kun lisätään tietoturvaa parantavia komponentteja, se tuo monimutkaisuutta sen hallintaan ja vianetsintään. Asiantuntija: *siinä on sitten taas sellainen ongelma tai problematiikka, että mitä enemmän näitä kerroksia lisää niin vianmetsästäminen on silloin kohtalaisen paljon hankalampaa.*

Laitteilla ja järjestelmillä ei yksistään voida tietoturvallista ympäristöä toteuttaa. Näiden lisäksi tarvitaan osaavaa ja kehittymishaluista henkilöstöä, ketkä proaktiivisesti tunnistavat mahdollisia uhkia. Päällikkö esitti asiasta yksittäisen näkemyksen: *järjestelmä ei sinänsä auta mitään, vaan se et jos sulla on järjestelmä, sun pitää hankkia ihmisiä töihin, jotka osaa oikeesti järjestelmii käyttää, jotta ne tunnistaa ne osaa tunnistaa oikeesti niistä heikoista signaaleista, et mikä on todellinen uhka ja mikä on vaan pelkkää taustakohinaa.*

4.1.3 Extranet sovellustietoturva

Taustasovelluksien suojaamisessa nousi kaikkien haastateltavien keskuudessa esille käyttövaltuutuksen merkitys taustapalveluihin kirjautuessa. Asiantuntija: *taustajärjestelmissä pitää sitten laittaa minimaaliset oikeudet sille käyttäjälle eli tämmöinen least privilege malli, että mihin on oikeus ja mitä voi tehdä niin ne pitää aina katsoa taustajärjestelmäkohtaisesti, että ei voi tehdä mitä tahansa.*

Esille nostettiin syötteen tarkistuksen merkitys, joko sovelluksessa tai muussa keskitetyssä skannauspisteessä, missä voidaan estää mahdolliset SQL-injektio-tyyppiset hyökkäysyritykset. Päällikkö kuvaa asiaa: *sulla voi olla vaikka maailman paras järjestelmä missä on autentikoinnit, oikeudet ja muut kunnossa ja jos siinä on semmonen haavoittuvuus missä kirjottamalla tähti tähti ja painamalla enter mennään läpi niin se ei hirveesti lohduta.*

Asiantuntija tarkentaa, että syötteen tarkistus tulee tehdä edustan lisäksi taustasovelluksessa. Asiantuntija: *extranetissä jo katottais, et siitä ei saa mennä, mitä tahansa lävitte, mut myös siel taustajärjestelmässä katottais, et hei minä en ota vastaan ihan mitä tahansa.*

Sovelluskehittäjien tulee huomioida tietoturva sovelluksen suunnittelu- ja ohjelmointivaiheessa. Asiantuntija: *siellä on lukuisia kehittäjiä* kehittämässä *ja kyllä se tietenkin sieltä aina lähtee se tietoturvaosaaminen, osaamista olisi myös sitten tai huomioimista vähintään siellä koodausvaiheessa.*

Aineistossa esiintyi sovelluspalomuurien tarpeen merkitys, millä suojataan sovellustasolle kohdistuvia hyökkäysyrityksiä. Asiantuntija: *Webi-pohjaisten niin kuin aplikaatioiden palomuuria ja siellä ajatus on se että siellä on tälläsiä sääntöjä, jotka sitten tutkii, että onko yrittääkö hyökkääjä vaikkapa jotain sql-injektiota tai jotain muuta vastaavaa tämmöstä hyökkäystä tehdä ja niillä pystytään ainakin pienentämään sitä puolta.*

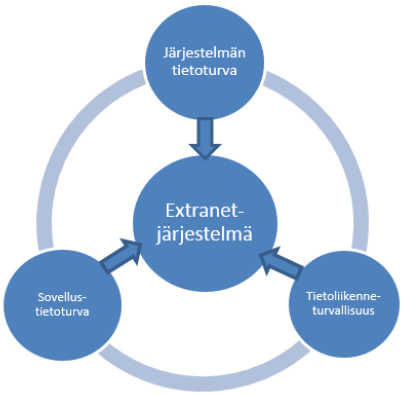
Yhden haastateltavan mukaan kaksitasoisen tunnistuksen käyttäminen taustasovelluksille on tärkeää, millä varmistutaan käyttäjän identiteetistä. Asiantuntija: *maailmalla hyvin yleisesti käytössä on kakstasoinen autentikointi eli on käyttäjätunnus ja jonkinäkönen salasana, voi olla pin-koodi tai mikä se on sitten missäkin, mutta sitten on tää toinen vaihe eli kertakäyttösalasana sen lisäksi.* Asiantuntija viittaa samalla, että roboteilla tehtäviä salasanahyökkäyksiä pystytään menetelmällä estämään. Asiantuntija: *sillä pystytään sitten aika pitkälti niin kuin tämmöset koneellistetut hyökkäysmenetelmät poistamaan.*

Aineistossa esiintyi havaintona proaktiivisuus, joka tarkoittaa ennakoivaa IT-teknologioiden kehittymisen seuraamista ja uusien uhkien sekä haavoittuvuuksien seuraamista. Tuotantopäällikkö: *aika tärkeetä on sellasii, että käytännössä pysytään ajantasalla tekniikan kehittymisessä sitten et, mitä yleensä ottaen niin kun maailmalla tapahtuu, mitä haavoittuvuuksia tulee, mitä epäillään, mitä jotain voitas käyttää väärin tai muuta.* Päällikkö nopean reagoimisen merkityksestä: *jos tulee jotain selkeesti haavoittuvuuksia tai tälläsia niin et ne pitää päivittää nopeeta.*

Yksi haastateltavista esitti uutena asiana automatisoinnin merkityksen sovellustietoturvaa parantavana menetelmänä. Siinä sovelluksia pyörittävät virtuaalipalvelimet tuhotaan säännöllisesti ja ne rakennetaan uudelleen tallessa olevilla asetuksilla, jolloin aina aloitettaisiin puhtaasta lähtötilanteesta. Asiantuntija: *se ois paljon tietoturvallisempaa, et me tuhottais esimerkiksi tietyt tietokoneet, tai virtuaalikoneet, niin ne aina välillä sanottais, et wipe tai delete, meillä ois ne konfit tallessa ja ne tehtäisi uudestaan.*

4.2 Tutkimuksen tulokset

Sisäverkon palveluiden julkaiseminen muodostuu kolmesta eri osa-alueesta, jotka muodostuivat teemojen perusteella. Osa-alueet esitetään kuvassa 7.



Kuva 7: Extranet-järjestelmän osa-alueet.

Aineistoa uudelleen tyyppien mukaisesti luokittelemalla muodostuivat sisäverkon turvallisen julkaisemisen tekijät, jotka ovat laitteet / komponentit, tekniset menetelmät / toiminnot ja inhimilliset tekijät. Sisäverkon palveluiden turvallisen julkaisun eri tekijät taulukossa yksi liittyvät kaikkiin extranet-järjestelmän osa-alueisiin.

Taulukko 1: Sisäverkon turvallisen julkaisemisen tekijät.

Laitteet/komponentit	**Tekniset menetelmät / toiminnot**	**Inhimilliset tekijät**
Reverse proxy	SSL/TLS Sertifikaattipohjainen yhteyden salaaminen asiakasselaimen ja tausta palvelun välillä	Ammattitaito
Load Balancer	Kaksivaiheinen vahva tunnistus asiakas- ja hallintayhteyksille	Proaktiivisuus
Verkkopalomuuri	Least privilege -malli	Huolellisuus
Internet DMZ-verkko	Roolin mukaiset rajatut käyttöoikeudet	Järjestelmällisyys
Pääsynhallinta järjestelmä LDAP / OTP	Käyttövaltuuksien tarkistus palvelimissa ja sovelluksissa	Suunnitelmallinen
Keskitetty hallintapiste ”Hyppykone”	Asiakas- ja hallintaliikenteen eriytys (L2/L3)	Nopea reagointikyky
Verkkosovelluspalomuuri (WAF)	Auditointi Kuka tekee, mitä tekee ja miksi tekee?	Paineensietokyky
IDS / IPS- järjestelmät Epänormaalin verkkoliikenteen tunnistus- ja esto.	Hallintayhteydet keskitetyn ja turvatun pisteen kautta	Viitseliäisyys
Taustaverkot	Verkkosegmentointi	Tehokkuus
HIDS / HIPS-järjestelmät	Rajatut palomuuriavaukset	Kokonaisuuksien hallinta
Virustorjunta	Tietoturvapäivityksien säännöllinen asennus	
Käyttöjärjestelmä	Palvelimien ja sovelluksien tietoturvakoventaminen	
Sovellukset	Palvelin ja sovelluspäivitykset	
	Tietoturvan huomioiminen ohjelmistokehityksessä	
	Syötteen tarkistus	
	Istunnon hallinta	
	SSO	

	Kerrosarkkitehtuuri (N-Tier)	
	Testaaminen	
	Automatisointi	
	Muutoshallinta ja dokumentointi	
	Epänormaalin järjestelmätoiminnan tunnistaminen	

5 JOHTOPÄÄTÖKSET

Extranet-järjestelmän tietoturvan osa-alueet ovat järjestelmä-, sovellus- ja tietoliikennetietoturva. Aineistoa luokiteltaessa löytyi kolme eri tekijää, jotka vaikuttavat sisäverkon palveluiden turvalliseen julkaisemiseen. Näitä ovat laitteet / komponentit, tekniset menetelmät ja toiminnot sekä työntekijöiden inhimilliset ominaisuudet.

Extranet-järjestelmään kuuluu oleellisesti seuraavat järjestelmä- ja verkkolaitekomponentit: palvelimet, reverse proxy, load balancer, pääsynhallintajärjestelmä, verkot, internet-DMZ ja palomuuri. Teoriaosuudessa eri komponentteja kuvattiin varsin kattavasti. Empiirisessä osuudessa aineistosta löydettiin uutena seikkana HIDS- ja HIPS-järjestelmät, jotka ovat palvelin-ja järjestelmätasolla tapahtuvan epänormaalin toiminnan havainnointiin ja estämiseen tarkoitettuja järjestelmiä.

Tekniset menetelmät ja toiminnot kuuluvat oleellisesti sekä järjestelmä-, sovellus- että tietoliikenneturvallisuuteen. Teknisillä menetelmillä ja toiminnoilla suoritetaan järjestelmän toiminnan ja tietoturvan kannalta oleellisia tehtäviä. Teoriaosuudessa Stewart ym. (2012, 4) esittävät, että pääsyhallinnan tärkein tarkoitus on turvata järjestelmien ja niiden sisältämien tiedon luottamus, kiistämättömyys ja saatavuus. Nämä turvataan vahvalla käyttäjätunnistuksella, käyttöoikeuksilla, tiedon siirron salauksella, verkkotason eriyttämisellä ja hallintayhteyksien turvaamisella. Perusteena tälle johtopäätökselle on se, että muilla tietoturvatoiminnoilla ei ole merkitystä, jos käyttäjätunnistus sallii väärien henkilöiden pääsyn järjestelmään tai antaa liian laajat käyttöoikeudet.

Verkkosovellukset yleistyvät ja niiden tietoturvariskit kasvavat, kun sallitun verkkoliikenteen sisällä yritetään luvattomasti päästä sisäverkonpalveluihin käsiksi. Teoriaosuudessa Harwood (2011, 226) painotti, että nykyään noin 70 prosenttia verkkosivuihin kohdistuvista hyökkäyksistä kohdistuu sovellustasolle. Tästä johtuen sovellustietoturvan osa-alueella nousi esiin sovellusten ohjelmointi, jossa tietoturva on huomioitava jo sovelluksien suunnittelu- ja kehitysvaiheessa.

Tulokset osoittavat, että laitteet ja tekniset menetelmät sekä tehtävät toiminnot eivät yksin riitä. Tietoturvallisuuteen olennaisesti vaikuttavat ihmisten ominaisuudet, kuten ammattitaito, järjestelmällisyys, suunnitelmallisuus, proaktiivinen toimintatapa ja reagointikyky.

Case-yrityksessä oli tarve kartoittaa tietoturvavaatimuksista tukemaan extranet- järjestelmien suunnittelua, käyttöä ja ylläpitoa. Näissä käytön eri vaiheiden onnistumisessa korostuvat inhimilliset ominaisuudet.

Extranet-järjestelmän käyttöönottoprojekti on suunniteltava huolellisesti ja aikataulutettava. IT-ammattilaisten on oltava huolellisia määritellessään järjestelmän asetuksia. Käyttöönotossa voi olla liian kiireinen aikataulu, jolloin organisaatiossa voi vallita kokeilukulttuuri.

Inhimilliset ominaisuudet korostuvat myös extranet-järjestelmien ylläpidon perusasioiden hoitamisessa. Järjestelmien ylläpidossa pitää olla proaktiivinen, joka tarkoittaa pal-

velin -ja sovelluspäivityksien pitämistä ajan tasalla ja haavoittuvuuksien aktiivista seurantaa. Proaktiivisuuteen vaikuttaa usein organisaatioiden henkilöresurssien rajallisuus, mikä ilmenee kiireenä, huolimattomuutena ja suunnitelmallisuuden puutteena.

Käyttäjätunnistuksien ylläpidossa korostuu huolellisuus, järjestelmällisyys ja viitseliäisyys. Esimerkiksi käyttäjätunnukset voivat olla teknisesti oikein määriteltyjä, mutta ylläpitäjä tai loppukäyttäjä ei huolehdi tiedon turvallisesta säilyttämisestä tai henkilömuutosten yhteydessä ei poisteta tai rajata käyttöoikeuksia.

Laadullisia tutkimustuloksia ei voida laajasti yleistää muihin organisaatioihin suoraan samoin kuin määrällisen tutkimuksen tuloksia. Laadullisessa tutkimuksessa voidaan puhua siirrettävyydestä (Saaranen-Kauppinen & Puusniekka 2016, 51). Kaikkien organisaatioiden tietoturva koostuu järjestelmä-, sovellus- ja tietoliikennetietoturvasta ja siten extranet-järjestelmän osa-alueet voidaan yleistää kuuluvaksi muidenkin organisaatioiden extranet-järjestelmien tietoturvakokonaisuuteen.

Sisäverkon turvallisen julkaisemisen tekijöistä laitteet ja komponentit sekä tekniset menetelmät ja toiminnot ovat siirrettävissä toisiin organisaatioihin, mutta inhimillisiä tekijöitä ei voida samalla tavalla siirtää muihin organisaatioihin. Haastateltavien kokemiin inhimillisiin tekijöihin käyttöönottoprojektin tai ylläpidon aikana vaikuttavat osaksi työntekijän luonne ja persoona. Lisäksi monessa organisaatiossa on tiukat aikataulut ja rajalliset resurssit, jotka vaikuttavat stressin tasoon ja proaktiivisuuteen.

Verkkosovellusten yleistymisen myötä tietoturvahyökkäykset ovat hienostuneempia ja niitä vastaan on vaikeampi suojautua perinteisillä verkkotason suojausmenetelmillä, jonka johdosta ammattitaito ja proaktiivisuus ovat tärkeitä ominaisuuksia myös muissa organisaatioissa.

Tulevaisuuden jatkotutkimuskohteena voi olla automatisoinnin hyödyntäminen järjestelmien ja sovelluksien tietoturvassa. Automatisointi prosessilla poistetaan tuotannossa olevat sovellukset ja palvelimet säännöllisesti sekä rakennettaan ne uudestaan tallessa olevilla virtuaalikuvilla ja konfiguraatioilla. Tämä vaikeuttaa tietoturvahyökkäyksen suorittamista.

LÄHTEET

Andreasson, A. & Koivisto, J. (2013). *Tietoturvaa toteuttamassa*. Tallinna: AS Pakett.

Bosworth, S., Kabay, M & Whyne, E. (2014) *Computer Security Handbook, Set (6).* Indianapolis: John Wiley & Sons, INC

Buecker, A., Patel, N., Rahnenfuehrer, D., Herzele, J & IBM Redbooks. (2012). *Enterprise Single Single-On Design Guide IBM Security Access Manager for Enterprise Singel Sign-On 8.*

Clark, P. & Agah, A. (2015). Modeling Firewalls for Behavior Analysis. Procedia Computer Science, 159–166. Haettu 28.11.2016 osoitteesta http://www.sciencedirect.com.ezproxy.hamk.fi/science/article/pii/S1877050915025648

Cisco, (2008). *Verkkosovelluspalomuurin toiminta periaate*. Haettu 22.1.2017 osoitteesta http://www.cisco.com/c/dam/global/en_sg/training-events/security_techbyte/files/webapplication_firewall.pdf

Cisco, (2013). N-Tier arkkitehtuuri. Haettu 22.1.2017 osoitteesta http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/2_Topolo.html

Cisco (2016). *What Is Network Security?* Haettu 26.11. 2016 osoitteesta http://www.cisco.com/c/en/us/products/security/what-is-network-security.html

Citrix (2016). *What is Application Delivery Controller (ADC)?* Haettu 5.3.2017 osoitteesta https://www.citrix.fi/products/netscaler-adc/resources/what-is-an-adc.html

Citrix (2015). *What is Load Balancing?* Haettu 17.10.2015 osoitteesta https://www.citrix.fi/glossary/load-balancing.html

Cross, M. & Fisher, M. (2011). *Developer's Guide to Web Application Security.* Rockland: Syngress Publishing,Inc. Haettu 11.12.2016 osoitteesta: Ebrary-tietokanta.

Cowley, S. (2005). G*aining speed, Citrix buys Netscaler*. Haettu 17.10.2015 osoitteesta http://www.networkworld.com/article/2321586/software/gaining-speed--citrix-buys-netscaler.html

Curtis G. & Cobham D (2018) *Business Information Systems: Analysis, Design and Practice.* Harlow: Pearson Education.

Fabbi, M. & Lerner, A. (2014). *Citrix Positioned for the Eighth Consecutive Year in the Leaders Quadrant for Application Delivery Controllers MQ.* Haettu 17.10.2015 osoitteesta https://www.citrix.com/news/announcements/oct-2014/citrix-positioned-for-the-eighth-consecutive-year-in-the-leaders.html

Finneran Dennedy, M., Fox, J & Finneran, T. (2014). *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value.* New York: Apress Media.

Harwood, M. (2011). *Security Strategies in Web Application and Social Networking.* Mississauga: Jones & Bartlett Learning.

Hirsjärvi, S. & Hurme, H. (2008). *Tutkimushaastattelu.* Helsinki: Gaudemus Helsinki University Press.

Järvinen, P. (2003). *Salausmenetelmät.* Porvoo: Docendo Finland Oy

Layland, R. (2008). *Application delivery controllers: Moving toward the application-centric network.* Haettu 13.10.2015 osoitteesta http://searchnetworking.techtarget.com/tip/Application-delivery-controllers-Moving-toward-the-application-centric-network

Lehto, J. (2008). *Extranet-järjestelmien tietoturva.* Turun Kauppakorkeakoulu, Pro gradu –tutkielma.

Liu, A. (2010). *Computer and Network Security : Firewall Design and Analysis.* Singapore: World Scientific. Haettu 27.11.2016 osoitteesta: Ebrary-tietokanta.

Lloyd, P. & Boyle, P. (1998). *Web-Weaving.* Oxford: Butterworth-Heinemann.

MacMillan, J. (2009). *What is a the Difference Between an IPS and a Web Application Firewall*? Haettu 8.1.2016 osoitteesta https://www.sans.org/security-resources/id-faq/what-is-the-difference-between-an-ips-and-a-web-application-firewall/1/25

McMillan, T. (2011). *Cisco Networking Essentials (1).* Indianapolis: John Wiley & Sons, INC. Haettu 27.11.2016 osoitteesta Ebrary-tietokanta.

Microssoft, (2016). *Understanding SSO.* Haettu 22.1.2017 osoitteeesta https://msdn.microsoft.com/en-us/library/aa546809.aspx

Microsoft, (2016). *Reverse Proxy:n toiminta periaate.* Haettu 22.1.2017 osoitteesta https://blogs.msdn.microsoft.com/friis/2016/08/25/setup-iis-with-url-rewrite-as-a-reverse-proxy-for-real-world-apps/

Microsoft, (2016). *Chapter 19: Physical Tiers and Deployment.* Haettu 1.3.2017 osoitteesta: https://msdn.microsoft.com/en-us/library/ee658120.aspx

Nginx, (2016). *What is layer 4 load balancing?.* Haettu 18.1.2017 osoitteesta https://www.nginx.com/resources/glossary/layer-4-load-balancing/

OWASP, (2013). *Open Web Applications Security Project*. Haettu 18.12.2016 osoitteesta https://www.owasp.org/index.php/Top_10_2013

OWASP, (2013). *Open Web Application Security Project.* Haettu 26.12.2016 osoitteesta https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf

Pirc, J., DeSanto, D., Davison, I. & Gragido, W. (2016). *Threat Forecaasting: Leveraging Big Data for Predictive Analysis.* Cambridge: Syngress.

Rainer, K. & Cegielski, C. (2010). *Introduction to Information Systems: Enabling and Transforming Business.* Indianapolis: John Wiley & Sons.

Ristić, I. (2014). *BULLETPROOF SSL AND TLS Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications*. London: Feisty Duck Limited.

Ristić, I. (2010). *ModSecurity Handbook.* London: Feisty Duck Limited.

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). *Menetelmäopetuksen tietovaranto KvaliMOTV*. Haettu 4.2.2017 osoitteesta http://www.fsd.uta.fi/menetelmaopetus/

Salchow, K. (2012). *Load Balancing 101: The Evolution to Application Delivery Controllers.* Haettu 13.10.2015 osoitteesta https://f5.com/resources/white-papers/load-balancing-101-the-evolution-to-application-de

Stewart, J., Chapple, M. & Gibson, D. (2012). *CISSP: Certified Information Systems Security Professional Study Guide : Certified Information Systems Security Professional Study Guide (6).* Indianapolis: John Wiley & Sons, INC. Haettu 20.11.2016 osoitteesta: Ebrary-tietokanta.

Stewart, M. (2013). *Network Security, Firewalls and VPNs.* Burlington: Jones and Bartlett

Stuttard, D. & Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition.* Indianapolis: John Wiley & Sons, INC.

Thomas, T. & Stoddard, D. (2012) *Network Security First-Step*. Indianapolis: Cisco Press.

Thomas, T., (2005). *Verkkojen tietorva*. Helsinki: IT-Press

Titansoft, (2016). *OTP:n toiminta periaate.* Haettu 22.1.2016 osoitteesta http://titansoft.fi/wp-content/uploads/2016/06/Titansoft_MobileID_Datasheet.pdf

UpCloud, (2016). How to Configure Load Balancing with Nginx. Haettu 2.3.2017 osoitteesta: https://www.upcloud.com/support/how-to-set-up-load-balancing/

Vacca, J. (2012). *Computer and Information Security Handbook (2).* Waltham: Morgan Kaufman. Haettu 20.11.2016 osoitteesta: Ebrary-tietokanta.

Liite 1

TEEMAHAASTATTELU

- **Teema 1. Taustatiedot**
- Haastateltavan asema ja tehtävä organisaatiossa?
- Kokemus IT-alalta?
- Aikaisempi kokemus vastaavien järjestelmien ylläpidosta?

- **Teema 1 Extranet-järjestelmiin (käyttöjärjestelmä) liittyvä tietoturva**

- Millä ylläpidollisilla ja teknisillä menetelmillä järjestelmän (käyttöjärjestelmät) tietoturvaa voidaan parantaa? (kovennukset / tietoturva ja sovelluspäivitykset)
- Mitä käyttäjätunnuksiin ja käyttöoikeuksiin liittyviä asioita tulee huomioida järjestelmässä ja sen ylläpidossa?

- **Teema 2 Extranetin tietoliikenneturvallisuus**

- Miten Extranet-järjestelmän eri komponentit tulisi sijoittaa verkkotopologisesti?
- Miten verkkosuunnittelussa tulee huomioida extranet-järjestelmään liittyvät toiset järjestelmät esimerkiksi tunnistus-järjestelmät?
- Mitä tulee huomioida extranetissä julkaistavien palveluiden tietoliikenneturvallisuudessa?
- Miten voidaan turvata tiedon luottamuksellisuus tiedonsiirrossa asiakkaan ja taustasovelluksien välillä?
- Miten hallintayhteydet (Management) tulisi verkkoteknisesti toteuttaa? Tulisiko käyttää eri yhteyttä hallinnalle ja asiakasyhteyksille?
- Miten hallintayhteydet / pääsyt tulee rajata ja suojata?
- Mitä muita tietoliikenneturvallisuutta parantavia teknisiä menetelmiä mielestänne tulisi käyttää? IDS, IPS, yms.?

- **Teema 3 Extranet sovellustietoturva**

- Millä menetelmillä taustajärjestelmien hyökkäyspintaa voidaan pienentää?
- Mitä nykyaikaisia suojausmenetelmiä voidaan käyttää sovelluksiin kohdistuvien tietoturvahyökkäyksien estämiseksi?
- Mitä ennakoivia toimia tulisi tehdä, jotta sovelluksiin kohdistuvia erilaisia tietoturva haavoittuvuuksia ja uhkia voidaan estää tehokkaasti etukäteen?

Liite 2

LUETTELO EMPIIRISEN OSUUDEN HAASTATELTAVISTA HENKILÖISTÄ

Haastateltavan tehtävänimike	**Haastattelupäivä**	**Kesto**
Järjestelmäasiantuntija	08.02.2017	32 min.
Järjestelmäasiantuntija	09.02.2017	32 min 40 sek.
IT Tuotanto päällikkö	16.02.2017	10 min 4 sek.