LAUREA AMMATTIKORKEAKOULU Uuden edellä

Citrix -
Jaetun teknologian tietoturvan kartoitus

Vaahterikko, Jari

2014 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Citrix - Jaetun teknologian tietoturvan kartoitus

Vaahterikko Jari
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2014

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Tietojenkäsittelyn koulutusohjelma

Vaahterikko, Jari

Citrix - Jaetun teknologian tietoturvan kartoitus

Vuosi 2014 Sivumäärä 37

Tämä opinnäytetyö tarkoituksena on kartoittaa virtuaalijärjestelmän tietototurvaa, erityisesti Citrix-järjestelmän osalta.

Yritysten liiketoiminta-alueet ovat kasvaneet viimeisen vuosikymmenen aikana ja liiketoimintaa tehdään nykyisin osaksi tai jopa kokonaan verkossa. Asiakaspalvelu, tavaroiden tilaaminen ja maksaminen tapahtuu verkon välityksellä. Tämä on johtanut tilanteeseen jossa tietojärjestelmien kasvu on asettanut uudenlaisia haasteita tietotekniikan kehitykselle. Lisäksi palvelinjärjestelmien kasvu toi uudenlaisia haasteita yhtiöiden liiketoimintaan. Virtuaalisointi ja sen tuomat edut yrityselämässä on huomattu ja tietototekniikassa virtuaalisointia pidetään tämän päivän johtavana trendinä.

Tämän opinnäytetyön tavoitteena on tutkia, mitä tietoturva tarkoittaa Citrix-järjestelmässä ja millaisia parhaita tietoturvakäytänteitä käytetään parantamaan järjestelmän tietoturvallisuuden ominaisuuksia.

Opinnäytetyön tutkimuksellinen osuus toteutettiin kvalitatiivisella eli laadullisella tutkimusmenetelmällä valitsemalla tutkimusmenetelmäksi kirjallisuustutkimus. Kirjallisuustutkimuksessa tutkittiin alan kirjallisuutta ja artikkeleita virtuaalisoinnista kuin Citrixistä sekä tietoturvasta.

Tutkimuksessa selvisi, että Citrix-järjestelmä on turvallinen järjestelmä käyttää, kun järjestelmä toimii suojatun verkon sisällä ja suojausmenetelmät ovat asianmukaisesti käytössä ja ajan tasalla.

Asiasanat Citrix, tietoturva, virtuaalisointi

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Vaahterikko, Jari

Citrix – The security mapping of the shared technology

Year 2014 Pages 37

The purpose of this bachelor's thesis was to investigate the Citrix system, its functionality and information security. The thesis focuses on what information security means in the Citrix system and what has to be taken into consideration in the operation of the system when information security is maintained. In the thesis information security is surveyed at a general level: what it means today's working life and what it means to the company.

Companies' business areas have increased during the last decade and nowadays business is conducted partly or totally in the network. The customer service, ordering of goods and paying take place through the network. This has led to the situation in which the growth of information processing systems has set new challenges for the development of the information technology. Furthermore, the growth of server systems brought new challenges to the business of companies. Virtualization and the advantages that it brought for the companies have been noticed and in information technology virtualization is considered to be today's leading trend.

The objective of this thesis is to study what information security means in the Citrix system and which best practices are used to improve the information security of the system.

The research method of this thesis was the qualitative method and the research study was literature study. Articles and books on virtualization, Citrix and the information security have been used as literary sources.

In the study it became clear that the Citrix system is a safe system to use, when the system functions inside the protected network and when the protection methods are in use and updated duly.

Keywords Citrix, information security, virtualization

Sisällys

1 Johdanto

Tietotekniikan kehitys alkoi kun matemaatikko Alan Turing vuonna 1936 kehitti teoreettisen mallin, kuinka tietokone toimii. Turingin konetta pidetään alkusykäyksenä tietojenkäsittelytieteelle ja siitä syntyi myöhemmin matemaattisen logiikan haara, joka on myöhemmin sulautunut tietojenkäsittelytieteeseen. Ensimmäiset varsinaiset tietokoneet toi markkinoille 1950-luvulla International Business Machines (IBM), joka aikaisemmin oli valmistanut mekaanisia reikäkorttikoneita. Suomeen ensimmäinen tietokone tuli vuonna 1958, joka oli IBM 650. Alkuaikoina tietokoneet olivat jättikokoisia ja niiden varastoimiseen tarvittiin isoja tiloja. Vain harvalla yrityksellä oli tietotekniikan alkuaikoina varaa lähteä kehitykseen mukaan. Tietotekniikan kehitys kuitenkin valtasi yrityksissä enemmän alaa 1980 luvun lopussa, kun Microsoft toi Windows käyttöjärjestelmän markkinoille. Windowsin saatua markkinat lähes täysin haltuunsa, alkoi henkilökohtaisten tietokoneiden (pc) aikakausi. Suurtietokoneet aikakausi alkoi kääntyä laskuun, kun järjestelmiä alettiin korvata Microsoftin toimittamalla Windows käyttöjärjestelmällä. Tämän seurauksena yritysten katseet kohdistuivat Microsoftin palvelinjärjestelmiin, koska yhtiöissä alkoi olla Microsoft Windows käyttöjärjestelmällä toimivia pc-koneita. Microsoftin palvelinjärjestelmät tulivat varteen otettavaksi vaihtoehdoksi korvata suurtietokoneet, koska niiden toiminta alkoi käydä yhteensopivuusongelmien takia vaikeaksi. Microsoftin palvelimet olivat seuraava askel yritysten järjestelmien kehityksessä, koska tällöin pc-laitteiden käyttöjärjestelmä ja palvelinjärjestelmä olivat samalta toimittajalta. Microsoftin palvelimet toimivat hyvin siihen asti, kun yksi järjestelmä käytti yhtä palvelinta. Järjestelmästä alettiin käyttää nimitystä yksi palvelin - yksi ohjelma. Kun toinen järjestelmä alkoi käyttää samaa palvelinta, saattoi järjestelmä hidastua tai jopa kaatua. Tämä johti kierteeseen, jossa yhtiöt alkoivat kasvattaa palvelinjärjestelmiään. Järjestelmien kasvu alkoi tuoda muunlaisia ongelmia yhtiöiden toiminnalle. Tilantarve palvelimille kasvoi valtavaksi, minkä lisäksi sähkönkäyttö, niin palvelimissa kuin palvelintilojen ilmastoinnin järjestämiseksi kasvoi. Syntyi palvelinkeskuksia, joiden kasvava palvelinkapasiteetin hallinnointi vaati myös lisää henkilöstöä, mutta tästä huolimatta palvelinten hallinnointi alkoi käydä vaikeaksi (Portnoy. M. 2012, 3-6.)

Sähköinen liiketoiminta alkoi tehdä tuloaan 1990 luvun lopussa yritysten liiketoimintaan Internetin käytön yleistymisen myötä. Yhtiöiden liiketoiminnan kasvu tapahtui verkossa, jossa tavaroiden myynti, rahansiirrot ja asiakaspalvelu yleistyivät, minkä johdosta edelleen palvelinjärjestelmien koko kasvoi. Oli välttämätöntä keksiä uusia tapoja laajentuvan palvelinkapasiteetin hoitamiseksi ja yksi palvelin - yksi ohjelma käsite alkoi olla rasite yhtiöiden liiketoiminnalle. Ratkaisuksi alettiin kehittää palvelinjärjestelmien virtuaalisointia, joka oli jo kehitetty 1960 – luvulla. Virtuaalisoinnin avulla pystyttiin yhdessä fyysisessä laitteessa ajamaan

useita käyttöjärjestelmiä ja sovelluksia, minkä johdosta suuria palvelinkapasiteetteja ei enää tarvittu. Virtuaalijärjestelmän käyttöönotto toi myös yrityksille säästöä tilantarpeen vähenemisellä, energian kulutuksessa, ylläpidettävyydessä ja hallinnossa. Virtuaalisointi on tämän päivän ehdottomia kuumia trendejä tietotekniikan alalla, mutta virtuaalisointi tuo myös uusia haasteita järjestelmien hallittavuuteen, vakauteen ja tietoturvallisuuteen.

Tietojärjestelmien käyttö tämän päivän liike-elämässä on tärkeässä roolissa yhtiöiden liiketoiminnassa. Tietojärjestelmien avulla liiketoiminta on tehostunut, nopeutunut ja joissain tapauksissa se on jopa tehnyt liiketoiminnan mahdolliseksi. Liiketoiminnan raaka-aineena käytetään dataa, joka on liiketoiminnan perusta. Yhtiön prosesseissa data on jalostettu hyödylliseksi ja mielekkääksi muodoksi, jonka jälkeen sitä kutsutaan tiedoksi. Kun tietojärjestelmä käsittelee dataa joka on saatu käyttökelpoiseen muotoon, tulee siitä hyödynnettävä omaisuus yhtiön liiketoiminnan tarpeisiin (Sargadharan, M. ym. 2010, 9). Tietojärjestelmä voidaan määritellä toisistaan riippuvaisiksi komponenteiksi, jotka toimivat yhdessä yhteisen päämäärän saavuttamiseksi, hyväksymällä syötteet ja tuottamalla tuotoksia organisoidussa muunnosprosessissa (Sargadharan, M. ym. 2010, 19).

Tietojärjestelmiä käytetään yleisesti yhtiön sisäisissä prosesseissa, sisäverkon välityksellä, mutta myös julkisen verkon välityksellä salatulla yhteydellä. Tämän päivän työkulttuurissa vaatimukset ovat kasvaneet ja työnteon funktio on laajentunut niin, että työntekijät käyttävät tietojärjestelmiä niin kotoaan kuin asiakkaidensa luona. Vaatimukset työn tekemiselle on muuttunut aikojen saatossa ja teknisen kehityksen myötä tietojärjestelmien käyttö on monipuolistunut. Kehitys myös mahdollistaa nykyisin erimuotoisen työn tekemisen.

Globaalissa yhteiskunnassa yhtiöiden toiminta voi ylittää valtioiden rajat jolloin liiketoiminta pitkälti määrittää millaisia tietojärjestelmiä yhtiön on parasta käyttää. Kun yhtiön liiketoiminta eri maissa tai toimipaikoissa perustuu samaan tietojärjestelmään, voidaan samaa jaettua järjestelmää käyttää julkisen verkon välityksellä salatusti. Tällainen jaetun teknologian käyttö antaa synergiaa ohjelmistokehitykselle, testaukselle kuin myös itse järjestelmän käytölle, kun tietojärjestelmää ja siinä käytettäviä ohjelmia ei tarvitse asentaa kuin yhdelle palvelinjärjestelmälle. Käytetyimpiä jaetun teknologian ohjelmistoja ovat Symantecin pcAnywhere ja Citrix Systemsin Citrix-järjestelmä, joista tässä opinnäytetyössä keskityn Citrix-järjestelmään. Julkisen verkon käyttö tällaisissa järjestelmissä asettaa vaatimuksia käyttöjärjestelmien tietoturvallisuudelle, sen toiminnalle kuin myös käytettävyydelle.

2 Tavoitteet, tutkimusongelma, rajaus ja rakenne

Opinnäytetyö kartoittaa Citrix-järjestelmän tietoturvan tasoa, mitä tietoturva tarkoittaa virtuaalijärjestelmässä, millaisin ylläpitäjän ja myös käyttäjän toimenpiteitä ja käytänteitä tar-

vitaan, joilla tietoturvaa järjestelmässä parannetaan. Työssäni käyn läpi niin ohjelmallisia kuin myös parhaita käytäntöjä tietoturvan näkökulmasta, että järjestelmästä voidaan saada paras mahdollinen tietoturvan taso käyttöön.

Opinnäytetyö jakautuu tietoturvan teoreettisesta viitekehyksestä, tietoturvapolitiikasta, virtuaalijärjestelmästä ja sen toiminnasta, Citrix-järjestelmästä, sen toiminnallisesta ympäristöstä ja siihen liittyvistä tietoturvallisuus asioista. Verkkoon liittyvät tietoturvauhat, järjestelmän konfiguraatioon liittyvät uhat sekä järjestelmän tietoturvaan liittyvät riskit.

3 Tietoturva

Kun tietojärjestelmiä käyttävän yhtiön liiketoiminta usein perustuu sen omaisuutena olevaan tietoon, nousee järjestelmien turvaamisen merkitys tärkeään osaan. Siksi järjestelmien tietoturvallisuuden takaaminen on yhtiön menestymisen ja usein myös toiminnan jatkuvuuden edellytys. Tietoturva pitää sisällään kaiken sähköisesti tuotettavan ja käsiteltävän tiedon turvaamista, sisältäen kaiken mitä liittyy yksittäiseen tietoon, sähköiseen järjestelmään, palveluun tai tietojen siirtämisestä tietoliikenteen avulla. Lisäksi se myös kattaa kaiken muun yhtiön liiketoimintaan liittyvän toiminnan, kuten tietojärjestelmän käyttäjien toimet. Tietoturva pitää sisällään myös sen, että tietojärjestelmässä olevaan tietoon ei pääse käsiksi sellaiset tahot jotka eivät ole siihen oikeutettuja.

3.1 Tietoturvan perus- ja laajennettu määritelmä

Tietojärjestelmissä olevaa tietoa käsitellään ja säilytetään digitaalisesti tietovarastoissa, jotka ovat palvelusta tai järjestelmästä riippuen joko sisäverkon ja/tai julkisen verkon käytettävissä. Näitä järjestelmiä tulee käyttää oikein ja turvallisesti, taaten tiedon oikeellisuus ja luottamuksellisuus. Kun yhtiön tietojärjestelmissä olevan tiedon määrä kasvaa ja ne ovat siten riippuvaisia sähköisesti tallennetun tiedon arvosta, tulee järjestelmän tietoturvaan kiinnittää erityistä huomiota. Kaikki häiriöt tai virheet järjestelmän toiminnassa voidaan jaotella luokkiin, joilla määritellään vahinko yhtiön liiketoiminnan näkökulmista. Tällaisia luokkia ovat

- käytettävyyden menetys
- luottamuksellisuuden menetys
- eheyden menettäminen.

Käytettävyyden menettämisellä tarkoitetaan sitä, että yhtiön tietoliikennejärjestelmään tulee katkos joka aiheuttaa toiminnassa pysähdyksen. Tällaiset ovat esimerkiksi asiakastapahtumiin liittyvät pysähdykset, kuten ostojen kirjaukset, rahansiirrot, pankkitapahtumien kirjaukset tai muut tuotantoprosessien katkokset. Käytettävyyden määritelmä pitää myös sisällään

sen, että tietoliikennelaitteiden ja – järjestelmien tehokkuus ovat riittävällä tasolla sekä järjestelmissä olevat ohjelmat soveltuvat hyvin järjestelmissä olevien tietojen käsittelyyn. Pyrkimyksenä on lisäksi automatisoida tiedon jalostus mahdollisimman pitkälle, jolloin käyttäjien tulisi saada haluamansa tiedot järjestelmästä itselleen sopivassa muodossa, kuten valmiina raportteina tai yhteenvetoina (Hakala, M. ym. 2006, 4).

Luottamuksellisuus on tiedon saatavuutta ja näkymistä niille käyttäjille, joilla on tietoon oikeutus. Tämä tarkoittaa sitä, että tietojärjestelmiin pääsy on käyttäjätunnuksien ja salasanojen takana. Luottamuksellisuuden menetys yhtiön liiketoiminnassa voi johtaa vakaviin menetyksiin. Jos luottamuksellisuus menetetään, on asiakasluottamuksen takaisin saaminen hyvin vaikeaa, usein myös mahdotonta.

Eheyden menetys on yhtiön tietojärjestelmissä oleva tiedon korruptoitumista tai väärää tietoa, mistä voi aiheutua yhtiön tuotantoprosessissa virheitä ja väärää informaatiota. Eheyteen pyritään pääasiassa ohjelmointiteknisin ratkaisuin. Sovelluksiin ohjelmoidaan erilaisia syöttörajoitteita tai syötteen tarkistuksia, tallennus- ja tiedonsiirto-operaatioihin varmistussummia tai tiivisteitä. Laitteistolla pyritään estämään virheet käyttämällä esim. virheenkorjaavia muisteja tai väyliä. Tietoliikenneratkaisuissa suositetaan virheen tunnistus- ja korjausmekanismeilla varustettuja protokollia ja laitteita (Hakala, M. ym., 2006, 5).

Nykyisin edellä mainittu kolmen kohdan tietoturva määritelmä on usein koettu riittämättömänä, minkä johdosta tietoturvamääritelmää on laajennettu nykyaikaisen yritysten tarpeita vastaaviksi. Tästä syystä tietoturvallisuuden kokonaisuus pilkotaan usein pienempiin, helpommin käsiteltäviin alueisiin, joista perinteinen tapa on jakaa tietoturva kahdeksaan alueeseen

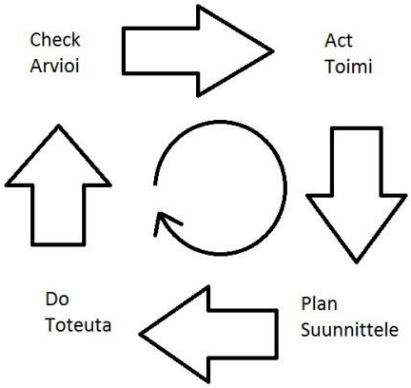
- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöstöturvallisuus
- tietoaineistoturvallisuus
- ohjelmistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus
- käyttöturvallisuus

Hallinnollisella tietoturvallisuudella, Kansallisen Turvallisuusauditointikriteeristön (myöhemmin KATAKRI) mukaan, tarkoitetaan turvallisuuden johtamista. Kokonaisuuden perusteena käsitellään turvallisuuden johtamisjärjestelmää ja sen osa-alueiden vaadittavaa suojaustasoja. Hallinnollinen turvallisuus on myös tietoturvallisuustoiminnan järjestelyjen, organi-

soinnin ja ylläpidon muodostama kokonaisuus, jonka tulos on kuvaus tietoturvallisuustoiminnan periaatteista, tietoturvatyön järjestelyistä, organisoinnista, arvioinnista, ylläpidosta ja kehittämisjärjestelmästä sekä kunkin työhön osallistuvan tieto omista vastuistaan ja tietoturvatehtävistään. Hallinnollisen turvallisuuden prosesseissa kuvataan toimintalinjat, vastuut ja tehtävät, järjestelyt, resurssit sekä tietoturvatyölle yleensä että tietoturvan ohjeistukselle, koulutukselle, valvonnalle ja raportoinnille. Se on siten organisaatiossa tietoturvallisuuden perusta.

Organisaation tietoturvapolitiikka määrittää tietoturvallisuuden pääperiaatteet ja miten tehtävät jakautuvat eri vastuuhenkilöiden kesken. Tietoturvasta vastuussa olevien tehtävänä on tietoturvasta tiedottaminen, seuraaminen ja tietoturvan puutteista ja laiminlyönneistä huomauttaminen. Tietoturvallisuuden koulutus on jatkuvaa ja koko organisaation kattavaa. Tietoturvallisuudesta vastaaville annetaan korkean luokan turvallisuus- ja valmiuskoulutusta sekä henkilöstölle perustason koulutusta tietoturvallisuuden ylläpitämiseksi. Usein vahingot syntyvät työntekijöiden huolimattomuudesta, perusturvallisuuden laiminlyönneistä. Perusturvallisuuteen liittyvät asiat on organisaatiossa suunniteltava, määriteltävä, toteutettava ja testattava. Joissain tapauksissa ylimitoitetut ja epäkäytännölliset tietoturvaratkaisut saattavat johtaa tietoturvan alenemiseen, koska työntekijät eivät jaksa käydä läpi tietoturvaratkaisuja, jos ne ovat liian vaikeita hahmottaa tai sisäistää. Perustason käyttäjien koulutus tulee olla yksinkertaista ja selkeästi hahmotettavaa, ei liian yksityiskohtaista tai liian teknistä.

Tietoturvan hallintajärjestelmän kehittämisessä suositellaan PDCA – mallia, jonka suomenkielinen vastine on Suunnittele-Toteuta-Arvioi-Toimi. PDCA – mallissa aluksi suunnitellaan, minkä jälkeen toimitaan. Tekemisen jälkeen tarkistetaan ja tehdään tarvittavat korjaukset, minkä jälkeen palataan alkuun, eli suunnitteluun. Jokaisen kierroksen jälkeen tavoite on lähempänä, minkä lisäksi toimintatapa ja tiedot karttuvat kierrosten aikana.



Kuva 1: PDCA -malli (www.tietojesiturvaksi.fi)

KATAKRIn mukaan fyysisessä turvallisuudessa keskitytään toimitilaturvallisuuteen, mutta siinä huomioidaan myös muunlaisia fyysisen turvallisuuden elementtejä. Perusajatuksena on suojata sensitiivisen tai suojattavan tiedon salassa pysyminen kuiriajatteluun pohjautuen siten, että pääsy edellä mainittuihin tietoihin estetään mahdollisimman varhaisessa vaiheessa ja tiukennetaan suojaamisvaatimuksia sitä mukaa, mitä lähemmäs fyysisesti tietoon päästään. Tärkeimpiä suojattavia kohteita ovat usein tietojärjestelmien kriittisiä osia sisältävät laitetilat (KATAKRI. 2011, 60). Fyysisen tietoturva käsittää tietojen hallittua käyttöympäristöä, jossa tiedon käsittely ja siinä tarvittava tekniikka on suojattu fyysisten rakenteiden ja niiden vikojen aiheuttamilta tuhoilta ja vahingoilta. Fyysiseen tietoturvallisuuteen liittyy siten laitetilojen ja kiinteistöjen suunnitteluun ja valvontaan sekä kulunvalvontaan liittyvät käsitteet, jolloin estetään asiattoman pääsy tiloihin, joissa tietoa käsitellään. Fyysinen turvallisuus on hyvin laaja-alainen käsite ja hyvin vaikeasti hallittava kokonaisuus. Turvallisuuden perusta tulisikin jo lähteä rakennuksen rakentamisen suunnittelusta liikkeelle. Fyysisen turvallisuuden perusteet luovat perustan tietoturvalle ja ilman niitä hallinnolliset ja tekniset tietoturvaratkaisut ovat tehottomia.

Henkilöstöturvallisuus on KATAKRI:n mukaan henkilöstön toimista aiheutuvien ja heihin kohdistuvien tietoturvauhkien hallintaa. Henkilöstön, joka joutuu käsittelemään salassa pidettäviä tietoja tai sensitiivistä tietoa, jonka turvallisuusmääräysten vastainen käyttö voisi aiheuttaa vakavaa vahinkoa työnantajalle (KATAKRI. 2011,47). Henkilöstöturvallisuuden perusta luodaan luotettavalla rekrytoinnilla, jossa määritetään ennen henkilön palkkaamista, tuleva toimenkuva ja toimialuevaltuudet. Rekrytoitavan henkilön tulee olla luotettava ja tehtäviinsä soveltuva, joka tuntee itselleen asetetut tietoturvavaatimukset omaan toimenkuvaansa ja rooliinsa liittyen. Organisaatiolle tuottavan henkilöstön tulee tuntea tiedonsaantioikeutensa, käyttöoikeutensa, sijaisuus- tai muihin työtä koskeviin järjestelyihin liittyvät toimet, oma tietosuojansa sekä velvollisuutensa ja oikeutensa työsuhteen alkaessa ja päättyessä. Henkilöstön tehtäväkuvauksia ylläpidetään siten, että tehtävistä on johdettavissa tehtävien edellyttämät henkilökohtaiset tietojärjestelmien käyttöoikeudet. Tietojärjestelmien käyttäjistä pidetään ajantasaista rekisteriä, josta ilmenee käyttäjän yksilöintitietojen lisäksi käyttäjärooli. Organisaation tietojärjestelmiä käsittelevistä henkilöiltä edellytetään vastaavien tehtäväkuvauksien ylläpitoa käyttäjärekisteriä varten.

Valtiohallinnon tietoturvakäsitteistön (VAHTI-ohjeet) mukaan tietoaineistoturvallisuus on tietoaineistojen, kuten asiakirjojen, tietueiden ja tiedostojen luottamuksellisuuden hallintaa sekä estää tietojen tuhoutuminen tai tahaton muuttuminen. Tallenteet tulee säilyttää ja suojata oikeassa muodossa ja muuttumattomana sekä tietojen jatkuva varmistaminen ja oikeanlainen hävittäminen. Tietoaineistoturvallisuuteen liittyy myös tiedon jakaminen turvaluokkiin, sen tärkeyden perusteella. Aineisto voi olla täysin julkinen, luottamuksellinen tieto, salattu tieto tai erittäin salainen. Käyttäjät, jotka ovat oikeutettuja käyttämään salattua tietoa,

käyttävät aina henkilökohtaisia käyttäjätunnuksia tai muita varmennettuja menetelmiä kirjautuessaan järjestelmään. Tietoaineistoturvallisuus on myös tiedon hallintaa siten, että säädösten mukaisesti taltioidut tiedot säilyvät ja ovat saatavissa käyttötilanteen edellyttämässä ajassa, tarkoituksenmukaisessa muodossa ja järjestyksessä sekä hävitetään säädösten mukaisesti (Tietoaineistoturvallisuus, 2009).

Ohjelmistoturvallisuus on VAHTI -ohjeen mukaan kaikkien ohjelmistojen, kuten käyttöjärjestelmät, tulee valita siten että niiden käyttötarkoitus ja sopivuus huomioidaan organisaation osaamisen ja kokemuksen perusteella. Lisäksi ohjelmistoja valittaessa tulee ottaa huomioon käytettävyys, saatavuus ja toimivuus sekä se, että käytössä olevat ohjelmistot suojaavat sisältämänsä tiedon asetettujen vaatimusten mukaisesti (Ohjelmistoturvallisuus, 2009).

Laitteistoturvallisuus on päätelaitteiden, palvelimien ja muiden tiedon käsittelyssä käytettävien laitteistojen suojausta, asennusta ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään laitteiden omistaja ja turvaluokka, sekä laitteiden valvonta ja niiden kapasiteettien suunnittelua. Laitteistoturvallisuudella turvataan laitteistojen tarkoituksenmukaisuus, käytettävyys ja saatavuus sekä toiminnan tarpeita tyydyttävä toiminta. Ylipäätään laitteistoturvallisuudella turvataan laitteiston elinkaarta, johon myös kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa (Laitteistoturvallisuus, 2009).

Laitteiston elinkaareen liittyvät palvelusopimuksien palvelun tasoa määrittelevien rajojen ja vasteaikojen sopimisella voi olla merkittäviä vaikutuksia tietoturvatason ylläpidettävyyteen ja tietoturvapoikkeamiin reagointiin. Palvelusopimusten vasteaikoihin tukeutumalla voidaan vähentää varastoitavaa varalaitteistoa, mutta toisaalta riippuvuus toimittajan kyvystä toimia vasteaikojen puitteissa kasvaa. Erityisen tärkeää on määritellä sopimuksilla tilanteissa, joissa joko koko palvelu sijaitsee palvelun tarjoajalla tai osa organisaation laitteista sijaitsee siellä, jolloin joudutaan kiinnittämään huomiota yksittäisen laitteen fyysisen turvallisuuden järjestämiseen toisen osapuolen tiloissa ja tilojen pääsynhallintaan poikkeamatilanteissa. Näissä tapauksissa palvelusopimukset ulotetaan koko järjestelmään ja vaaditaan riittävän tarkat selvitykset verkkoyhteyksistä ja fyysisestä pääsystä järjestelmään työajan ulkopuolella, mikäli palvelun täytyy olla jatkuvasti asiakkaiden käytettävissä. Laitteiston ylläpidossa huolehditaan, että kaikki tiedot laitteista voidaan milloin tahansa palauttaa, kun toivutaan poikkeamasta. Tämä tarkoittaa, että laitteiston käyttöjärjestelmistä, ohjelmistoista ja niiden asetuksista on olemassa varmuuskopiot. Samaa edellytetään tietenkin niiden sisältämästä operatiivisesta tiedosta. Kaikkia järjestelmän laitteita on kyettävä jatkuvasti valvomaan ohjelmien avulla ja niiden käyttöasteiden kehittymistä seuraamaan säännöllisesti. Järjestelmien tietoturvapäivityksiä varten tarvitaan selkeät ohjeet ja ne testataan ennen tuotantojärjestelmän asennusta.

Päivitysten peruminen tulee olla mahdollista, mikäli päivityksessä havaitaan ongelmia (Laitteistoturvallisuus, 2009).

Tietoliikenneturvallisuus on taata turvatut tiedonsiirtoyhteydet. Siihen tähtääviä keinoja ovat laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen (Tietoliikenneturvallisuus, 2009.) Tietoliikenneturvallisuus kattaa tietoliikenneverkon ja sen laitteiden kokoonpanon, ylläpidon ja muutosten hallinnan sekä tietoliikenneverkon tapahtumien määrällisen ja laadullisen hallinnan. Tietoliikenneturvallisuus lähtee liikkeelle jo tietoverkon suunnittelusta, koska myöhemmin tehtävät turvallisuuteen liittyvät korjaukset eivät usein pysty korjaamaan verkon rakentamisessa tehtyjä virheitä ja lisäksi ne ovat jälkeenpäin tehtynä hyvin kalliita toteuttaa. Suunnitteluvaiheessa tehty dokumentaatio tietoverkon rakenteesta ja toiminnasta auttaa myöhemmässä vaiheessa turvallisuuskorjausten tekemistä. Dokumentaatiota tule myös ylläpitää säännöllisesti, kun verkon toiminnassa tapahtuu muutoksia. Tietoverkon tietoturvan tärkeänä osana ovat palomuurit. Niiden tehtävänä on erottaa eri verkkosegmentit toisistaan ja kontrolloida niiden välistä liikennettä palomuureihin asennettujen sääntökantojen mukaisesti. Palomuurit voivat olla ohjelmisto, joka toimii tietokonelaitteistossa tai erillinen laite, joka toimii erillisenä laitteena tietoliikenneverkossa.

Käyttöturvallisuus on yhtiössä päivittäisten tehtävien ja toimintojen turvaamista, joka sisältää kaikki manuaalisen ja automaattisen tietojenkäsittelyn suojaukset, kuten salasanojen hallinnointi ja järjestelmän valvonta. Käyttöturvallisuuteen liittyvät siten käyttöoikeuksien hallinta ja tunnistus- sekä todennusmenetelmät, joilla pyritään järjestelmän ja palveluiden tehokkaaseen ja tarkoituksenmukaiseen sekä turvalliseen käyttöön. Käyttöturvallisuutta edistetään koulutuksella. Tahattomia tietoturvaloukkauksia pystytään estämään, kun järjestelmään on luotu käyttäjäryhmiä, joilla oikeudet käyttää tietokantaa. Käyttäjien tunnistamisella on myös tarkoituksensa tietoturvauhkien ehkäisyssä. Lokitiedostoja ylläpitämällä ja niitä tutkimalla voidaan selvittää myös tietoturvauhkia.

3.2 Tietoturvapolitiikka

Tietoturvapolitiikka määrittää yhtiön tietoturvan tason, vastuut ja keinot, millä tietoturvaa ylläpidetään. Yhtiön ylin johto määrittää tietoturvanpolitiikan perusteet ja se toimii säännöstönä, selkeine ohjeineen ja periaatteineen henkilöstölle siitä mitä tietoturvapolitiikka pitää sisällään. Sen tarkoituksena on taata yhtiön toiminnan laatu, taso sekä jatkuvuus. Yhtiön tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tavalla liiketoiminnalleen tärkeitä tietoja, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen. Määrittelyssä ote-

taan huomioon tietoturvan yleinen taso ja siihen liittyvät vaatimukset sekä kuinka tietoturvan tasoa hallitaan sekä jaetaan tietoturvasta vastaajien vastuualueet. Tietoturvapolitiikan tulee myös koskea yhtiön sidosryhmiä ja sen tulee olla lyhyt ja helposti omaksuttava. Riskienhallinta toimittaa olennaista osaa tehokkaassa turvallisuus-strategiassa taaten sen että tietoturvallisuus toimenpiteet ovat yhdessä linjassa yhtiön liiketoiminnan tarpeiden kanssa. Yhtiön tietoturvapolitiikassaan määrittämät tasot ja niiden valvonta ovat elintärkeitä varmistamaan sen, että tietoturvallisuus-strategiaa toteutetaan tehokkaasti ja siinä korostuu oleellisesti riskienhallinnan prioriteetit. Erityisesti yhtiön tarkoitusperiä varten räätälöity turvallisuus sisältää käyttäjähallinnan kriteerit, mihin ryhmään käyttäjä kuuluu Active Directoryssä ja tietoturvauhkien auditointi säännöllisesti ja järjestelmällisesti. Haavoittuvuuksien ja niiden korjaus muutostiedostojen avulla on tietojärjestelmän turvallisuuden edellytys. Tietototuturvapolitiikka määrittää tietoturvavaatimusten määrittämisen ja millaisilla resursseilla sitä ylläpidetään. Tietoturvallisuuteen liittyvistä puutteista tai tietoturvaohjeiden vastaisesta toiminnasta määritellään toimintatavat, kuinka niitä käsitellään sekä sanktiot rikkeistä. Tietoturvasta vastuussa olevat henkilöt määrittävät liiketoiminnan jatkuvuuden kannalta kriittisille prosesseille laaditaan jatkuvuussuunnitelmat, jota tulee testata ja säännöllisesti päivittää. Tietoturvasta vastuussa olevat tulee toteuttamaan yhtiön tietoturvaa ajanmukaisin ja käytettävyydeltään käyttäjäystävällisin ratkaisuin.

Tärkeänä korostettavana asiana tietoturvapolitiikassa on henkilökohtaisten käyttäjätunnusten käyttöä koskeva säännöt. Jokaisella tulee olla henkilökohtaiset käyttäjätunnukset, kun käsitellään luottamuksellisia tai salaisia tietoja. Kun käyttäjätunnukset ovat henkilön omassa käytössä, voidaan todentaa jälkeenpäin kuka tietoja on käyttänyt tai hakenut. Yrityksen järjestelmiin tulee päästä vain todennetut henkilöt, jossa käyttäjätunnus ja siihen kuuluva salasana ovat pääsyn edellytyksenä. Tietojärjestelmän käytöstä on jokainen käyttäjä vastuussa ja käyttöön kuuluu aina työtehtävään kuuluva käyttöoikeus järjestelmään. Käyttäjätunnusta ja salasanaa ei siten voida luovuttaa toisen henkilön käyttöön. Salasanojen vaihtaminen täytyy tapahtua säännöllisesti ja salasanan luontiin on tietoturvapolitiikassa annettava ohjeet, niin että salasana tulee olla tarpeeksi vaikeasti murrettavissa. Yleisesti ohjeena on että salasana on vähintään 8 merkkiä pitkä ja sisältää isoja kirjaimia sekä numeroita.

4 Jaettu teknologia

Jaettu teknologia voidaan käsittää teknologiana, jossa järjestelmässä ja sen tarjoamissa ohjelmistoissa ja resursseissa on useita käyttäjiä samanaikaisesti. Käyttäjät voivat samanaikaisesti käyttää järjestelmän tarjoamia resursseja, ilman että toinen käyttäjä voi nähdä mitä resurssia toinen käyttää. Ohjelmistojen ja resurssien jakaminen tapahtuu palvelimella, missä järjestelmän ylläpitäjä (administrator) jakaa käyttöoikeudet ohjelmistojen ja resurssien käyttöön. Ohjelmat ajetaan siten palvelimella, mistä etäpäätteen käyttäjä lähettää komentoja ja

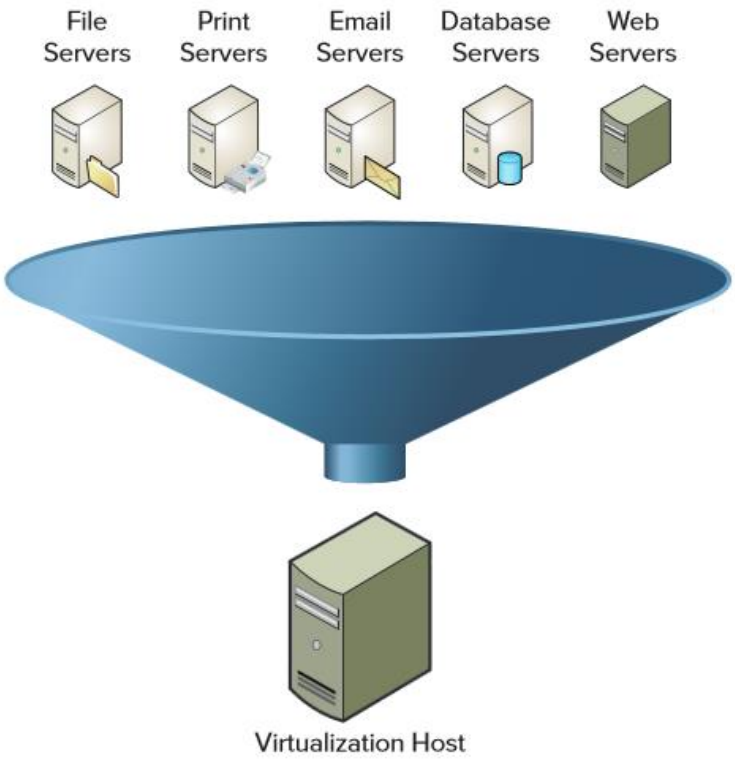
näkee tapahtumat näytöllään. Tällainen toiminta mahdollistaa sen, että käyttäjät voivat käyttää jaettuja resursseja verkon yli millaisella päätelaitteella tahansa, kunhan verkkoyhteys on salattu ja turvattu. Jaettu teknologia käsitetään nykypäivänä hyvin pitkälle myös pilvipalveluiksi, joissa Internetin välityksellä käytetään järjestelmä- ja ohjelmapalveluita. Pilvipalveluille tyypillisiä ominaisuuksia ovat koko tietohallintopalveluiden siirto toisen yhtiön hoidettavaksi, joko osittain tai kokonaan sekä Web-hosting. Pilvipalveluissa maksetaan laitteiden ja resurssien käytöstä, ei laitteiden ostosta. Pilvipalveluiden oston hyötyinä yritykselle on esimerkiksi se että laitetilat voidaan muuttaa liiketiloiksi, koska tietojärjestelmän vaatimat laitteet ovat vuokraajan hallussa.

4.1 Virtuaalisointi

Virtuaalisointi on saanut viime vuosina hyvin laajalti huomiota, mm. pilvipalveluiden tarjonnan ja käytön myötä. Virtuaalisointi tuo organisaatioille uusia tapoja tuottaa ja tarjota sovelluksia ja järjestelmiä sekä tuoda ne suuremmalle käyttäjäryhmälle. Sillä pystytään tuomaan järjestelmät käyttöön hyvin nopealla aikataululla, jopa minuuteissa, kun aikaisemmin niihin saattoi mennä viikkoja. Virtuaalisointi on siten tällä hetkellä yksi kuumimmista trendeistä IT teknologian alueella ja se on tuonut ja tuo edelleen mahdollisuuksia laajentaa työn tekemisen käsitettä. Työtä voidaan tehdä pois toimistolta, asiakkaiden luona tai kotona, ilman että järjestelmän toiminnallisuudesta joudutaan karsimaan.

Virtuaalisointi on tehokas teknologia, joka voi yksinkertaistaa käytettävät tietokoneet, mutta tuo mukanaan lisäkapasiteetin tallennukseen, muistinkäyttöön ja prosessoritehoon. Se tuo yhtiölle etua fyysisten laitteiden käyttöasteen muodossa, nopeuttaa toipumista ongelmatilanteista ja laskee virrankulutusta. Se tuo mukanaan mahdollisuuden suorittaa ohjelmia, käyttöjärjestelmiä tai muita resursseja erillään ympäristöstä, joissa ne tavallisesti ovat olleet käytettävissä, yksittäisessä fyysisessä tietokoneessa. Palvelimien virtuaalisoinnissa voidaan yhdessä fyysisessä laitteessa ajaa monia virtuaalipalvelimia, kun yhdessä fyysisessä laitteessa pystytään ajamaan vain yhtä palvelinta. Viimeisten viiden vuosikymmenen aikana tietotekniikan keskeiset suuntaukset loivat perustavanlaatuiset muutokset sille, miten tietotekniikan palveluja tarjotaan. Suurtietokoneet tulivat käyttöön 60- ja 70-luvuilla, mikrotietokoneet ja palvelinjärjestelmät 80- ja 90-luvulla. Internetin käyttö ja sitä seurannut digitaalisen viestinnän kasvu on jatkanut laajentuvaa tietoteknistä kehitystä näihin päiviin asti. Virtuaalisointia voidaan pitää häiritsevänä teknologiana, joka särkee sen käsityksen miten olemme viime vuosikymmenten aikana tietokoneet ymmärtäneet. Virtuaalisoinnilla on ja tulee olemaan syvällisiä vaikutuksia nykyiseen tietojenkäsittely-ympäristöön ja sen merkitys tulee vielä muuttumaan. Sitä mukaa, mitä tietojenkäsittelyn määre on laajentunut etenkin Internetin ja älypuhelimien käytön kanssa, palvelujen tarjonta ja saatavuus on lisääntynyt merkittävästi. Kasvu tulee edelleen jatkumaan.

Virtuaalisointi tietojenkäsittelyssä viittaa jonkin fyysisen osan abstraktion loogiseen osaan ja virtuaalisoimalla objektin voidaan saada hyöty jonkin suuremman mitan resursseista, jota objekti käsittää. Esimerkkinä voidaan käyttää virtuaaliverkkoja (VLAN), jotka tarjoavat parempaa suorituskykyä kuin fyysiset verkot, mutta myös parempaa verkon hallinnointia kun verkko on erotettu fyysisestä järjestelmästä (Portnoy, M. 2012, 1-2).



Kuva 2: Järjestelmän virtuaalisointi (Portnoy, M. 2012. 10)

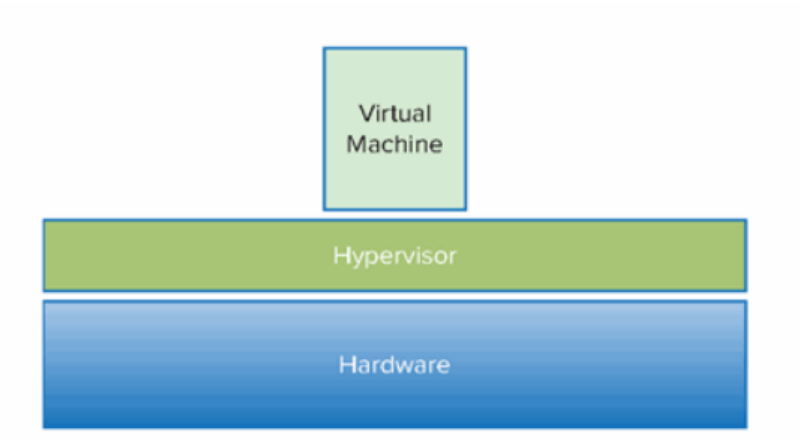
Virtuaalisointiratkaisujen tullessa markkinoille vuosituhannen alussa, VMwaren toimesta vuonna 2011, järjestelmä alkoivat muodostua nykyiseen muotoonsa. Avoimen lähdekoodin virtuaalisointijärjestelmä Xen tuli markkinoille v. 2003, jossa järjestelmä käytti hypervisor ohjelmistoa fyysisen laitteiston ja virtuaalijärjestelmän välissä tai suoraan asennettuna fyysiseen laitteeseen.

Richard McDougall & muut kirjoittavat tutkimuksessaan Virtualization Performance, Perspectives and Challenges Adead virtuaalijärjestelmien tulevaisuudennäkymästä. Tämä voi olla tulevaisuudessa yksi virtuaalijärjestelmien elinehdoista. Koska järjestelmien yksi keskeisiä elementtejä on sen suorituskyky, on järjestelmän yksi mittareista tehokkuus ja toimintakyky. Kun yritysten järjestelmien toiminnalle annetaan virtuaalisoinnilla lupaus siitä, että järjestelmä yksinkertaistaa tietotekniikan hallinnoinnin ja ylläpidon, mutta myös tarjoaa loistavan

suorituskyvyn. Virtuaalijärjestelmien suorituskykyyn liittyy kuitenkin useita eri ulottuvuuksia. Sovellukset, jotka virtuaalijärjestelmässä toimivat, oletetaan myös toimivan samalla tehokkuudella kuin se toimisi omassa fyysisessä laitteessa. Virtuaalijärjestelmän perustavoitteena on ollut, että järjestelmä kykenee suorittamaan monia tehtäviä samanaikaisesti. Tehtävistä täytyy suoriutua käyttäjän määrittelemässä ajassa, yleensä sitä verrataan fyysisen laitteen suoritusaikaan. Useat virtuaalijärjestelmät toimivat samassa palvelimessa, täytyy järjestelmän skaalata ja jakaa resurssit optimaalisesti. Onneksi sovellusten toimittajatahot ovat ottaneet virtuaalisointialustat oletusarvoisesti mandaatiksi uusien sovellusten kehittelyssä, minkä lisäksi laitteiden teknologiat ovat kehittyneet niin, että liikakuormitukselta järjestelmässä on pystytty vielä hoitamaan.

4.2 Hypervisor

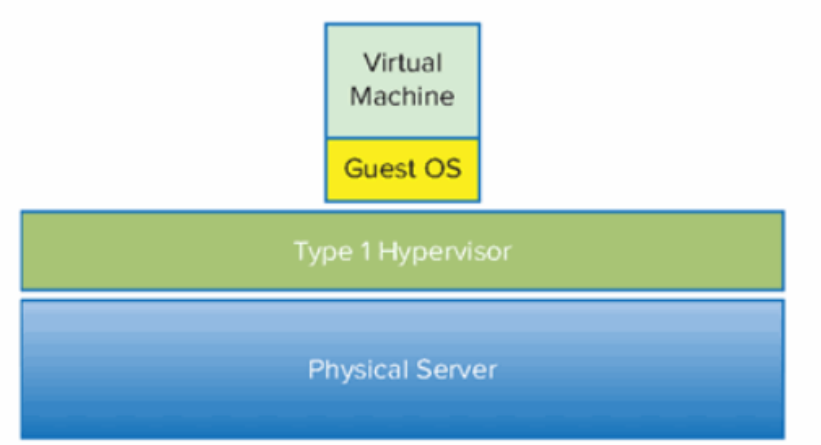
Hypervisor on valvontaohjelmisto, joka kontrolloi isäntäkoneen resursseja ja jakaa niitä virtuaalijärjestelmille. Aikaisemmin sitä kutsuttiin Virtual Machine Monitor (VMM), mutta termi on jäänyt pois hypervisor nimityksen tieltä, mutta sitä näkee vielä käytettävän. Hypervisor mahdollistaa monen virtuaalijärjestelmän toiminnan samalla isäntäkoneella niin, että virtuaalikoneet eivät näe toisiaan. Ilman hypervisoria käyttöjärjestelmät keskustelisivat suoraan fyysisen koneen kanssa. Levyjärjestelmät kommunikoivat levyjärjestelmän kanssa ja alijärjestelmät ja muistitoiminta noudetaan suoraan fyysisestä muistista. Samassa fyysisessä laitteessa Ilman hypervisoria toimivat useammat käyttöjärjestelmät haluavat kontrolloida laitteistoa, joka johtaa kaaokseen. Hypervisor hoitaa vuorovaikutuksen kunkin virtuaalikoneen ja fyysisen laitteiston välillä, jonka ne jakavat.



Kuva 3: Hypervisor virtuaalijärjestelmässä (Portnoy, M. 2012, 20)

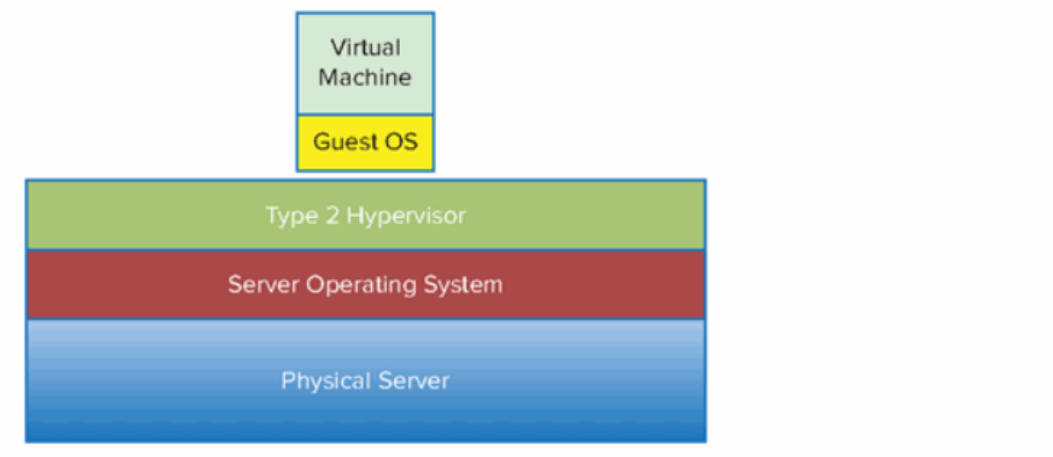
On olemassa kahdenlaisia hypervisoreita, Type 1 ja Type 2. Ainoa ero näiden välillä on, miten ne ovat otettu käyttöön. Type 1 hypervisor on suorassa yhteydessä laitteeseen, ilman käyttö-

järjestelmää. Koska välissä ei ole kerrosta hypervisorin ja fyysisen järjestelmän välissä sitä on kutsuttu bare-metal toteutukseksi. Koska Type 1 kommunikoi suoraan järjestelmän raudan kanssa, on se tehokkaampi kuin Type 2 hypervisor. Type 1 hypervisor on myös todettu turvallisemmaksi käyttää (Portnoy, M. 22). Type 1 hypervisor tarjoaa myös parempaa suorituskykyä ja sitä pidetään toiminnaltaan varmempana kuin Type 2 hypervisoreita.



Kuva 4: Type 1 Hypervisor (Portnoy, M. 2012. 22)

Type 2 hypervisor on sovellus, joka toimii perinteisen käyttöjärjestelmän, kuten Windows, Linux tai OS/2 päällä. Perinteinen käyttöjärjestelmä käsittelee laitteistoon liittyviä resursseja ja Type 2 hypervisor käyttää sitä hyväkseen. Etuna tässä on, että Type 2 voi hyödyntää laitteiston kapasiteettia paremmin omina resursseina. Type 2 hypervisorit ovat helppo asentaa ja ottaa käyttöön, koska pääosa laiteasetuksista, kuten verkkoliikenne ja muistinkäyttö ovat jo oletuksena käytössä perinteisen käyttöjärjestelmän toimesta. Type 2 hypervisorit jäävät jälkeen Type 1 tehoissa, koska käyttöjärjestelmän tuoma ylimääräinen kerros hypervisorin ja laitteiston välillä tuo hitautta. Joka kerta, kun virtuaalijärjestelmä käyttää levyjärjestelmää tai verkkoa, se antaa komennon hypervisorille joka antaa sen käyttöjärjestelmälle. Käyttöjärjestelmä käsittelee sen jälkeen pyynnön, jonka jälkeen se palauttaa tiedon takaisin hypervisorille (Portnoy, M. 2012, 23).



Kuva 5: Type 2 Hypervisor (Portnoy, M. 2012. 23)

5 Citrix-järjestelmä

Citrix Systems on perustettu 1989 ja yhtiö julkaisi ensimmäisen menestyneen tuotteen nimeltään WinView, vuonna 1993. Sen toiminta-ajatuksena oli DOS ja Windows 3.1 ohjelmistojen etäkäyttö, jossa useat käyttäjät pystyivät käyttämään sovelluksia. Vuonna 1995 Citrix julkaisi monikäyttö ohjelmiston Windows NT:n käyttöön, joka sai nimeksi WinFrame, joka perustui MultiWin ohjelmistoon. Tämä mahdollisti monen käyttäjän kirjautua ja ajaa ohjelmia WinFrame palvelimella.

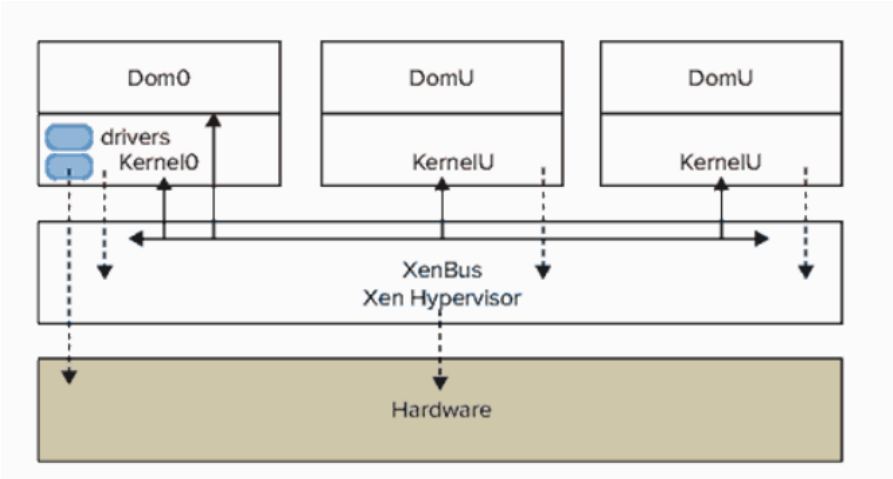
Citrix esitteli XenApp 6.0 maaliskuussa 2010, jolloin yhtiö oli kirjoittanut järjestelmän toimimaan Windows 64-bittisessä järjestelmässä, pohjana Windows Server 2008 R2. Tämä mahdollisti järjestelmän tehokkaamman toiminnan ja laajennettavuutta eri alustoille. Uusi versio, XenApp 6.5 julkaistiin elokuussa 2011 jolloin järjestelmään tuli lisää uusia ominaisuuksia ja parannuksia tehokkuuteen sekä nopeutuneen sovellusten käynnistämisen (Musumeci, G. 2012, 7-8).

Citrix on palvelinohjelmisto, joka sisältää monia ratkaisuja virtuaalisointiin. Citrix Delivery Center on päästä päähän virtuaalisointijärjestelmä, johon kuuluvat XenDesktop, XenApp, XenServer ja Netscaler - ohjelmat. Näillä ohjelmilla pystytään virtuaalisoimaan palvelinympäristö, työpöytä, työasemat ja sovellukset. Citrix toimii ns. terminaalipalveluna, jolloin millä tahansa päätelaitteella, joka voi olla tietokone, älypuhelin, kämmentietokone, tai muu vastaava laite pääsee käyttämään järjestelmää. Päätelaitteelle ladataan Citrix Receiver - ohjelma, joka tunnettiin aikaisemmin nimellä ICA (Independent Computing Architecture). Ohjelma toimii tietoliikenneyhteyden protokollana palvelimen ja päätelaitteen välillä. Citrix Reciver - ohjelmisto soveltuu käytettäväksi kaikilla käyttöjärjestelmillä kuten Windows, Mac, iOS2, Android, Windows 8/RT, Linux, Windows CE sekä Java, BlackBerry ja Unix järjestelmil-

lä. Kun käyttäjä on muodostanut yhteyden, hänellä on käytössään yhtiön järjestelmä ja käyttäjätunnukselle varatut resurssit. Koska ohjelmien ja sovelluksien suoritus tapahtuu palvelimella, tietoliikennekuormitusta ei tapahdu. Vain ohjelmien kuvat, hiiren klikkaukset ja näppäimistön painallukset kulkevat salattuna tietoverkkoja pitkin. Ohjelmia voidaan käyttää hyvin vaatimattomilla päätelaitteilla, jossa on vain tarvittavat ohjelmistot asennettuna ja muistikapasiteetin ei tarvitse olla iso. Tällaisia laitteita kutsutaan thin client'eiksi.

5.1 Citrix Xen hypervisor

Xen hypervisor projekti alkoi 1990 – luvun lopulla Cambridgen yliopistolla. Projektin tarkoituksena oli kehittää tehokas alusta jakaa tietoteknisiä resursseja. Vuonna 2002 ohjelmisto valmistui avoimen lähdekoodin periaatteella, jossa jokainen pystyi osallistumaan ja antamaan panoksensa kehitystyöhön. XenSource perustettiin 2004 tuomaan Xen hypervisor markkinoille ja tämä projekti on edelleen avoin kaikille ohjelmistokehittäjille. Red Hat, Novell ja Sun lisäsivät tuotevalikoimiinsa v. 2005 Xen hypervisorin, jolloin se pääsi kunnolla markkinoille. Vuonna 2007 Citrix Systems hankki järjestelmän täydentääkseen sovellusratkaisujaan (Portnoy, M. 29).



Kuva 6: Xen hypervisor arkkitehtuuri (Portnoy, M. 30)

Xen arkkitehtuuri on Type 1 hypervisorin mukainen, suoraan laitteeseen yhteydessä oleva järjestelmä. Xen järjestelmässä on asetettu käyttäjä Domain 0 (kuvassa Dom0), joka toimii erityisenä ohjausyksikkönä suoraan laitteeseen. Sillä on täydet hallintaoikeudet järjestelmään, toisin kuin muilla järjestelmän käyttäjillä. Se hallinnoi järjestelmän muiden käyttäjien syötteitä ja niiden vastauksia sekä laitteessa olevia ajureita. Kun toinen käyttäjä tekee pyynnön käyttää laitteen resursseja, menevät pyynnöt hypervisorin kautta ensin Dom0:lle, joka lähettää pyynnön eteenpäin. Pyyntö palautuu samaa reittiä myös takaisinpäin käyttäjälle.

5.2 XenServer

Xen hypervisorin hoitaessa kommunikoinnin laitteiston kanssa, XenServer toimii käyttöjärjestelmänä. Se käyttää paravirtualisoinnin ja laitteistopohjaisen virtuaalisoinnin yhdistelmää. Paravirtualisointi on tehokas ja kevyt virtuaalisointitekniikka, jossa ei tarvita kaikkia virtuaalisoinnin tekniikoita otettavaksi käyttöön hyödyntääkseen isäntäkoneen resursseja. Paravirtualisoinnissa virtuaalikone ja käyttöjärjestelmä toimivat paremmin yhdessä laitteiston resursseja käyttääkseen. XenServerissä paravirtualisointia käytetään myös jakamaan laitteiston suorituskykyä virtuaalikoneiden välillä, jos siihen on tarvetta. Tämä voi toisaalta aiheuttaa virtuaalijärjestelmässä hitautta. Citrix XenServerin käytön hyötyinä on että toimivat virtuaalikoneet voidaan siirtää uudelle palvelimelle ilman palvelun keskeytystä (Gohar, A. 9).

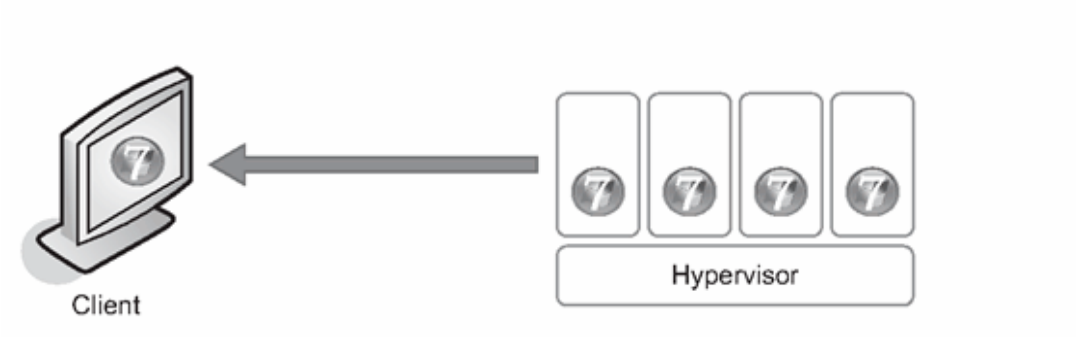
5.3 XenApp

Citrix XenApp, joka tunnettiin aikaisemmin nimellä Citrix Presentation Server, on markkinoita johtava ohjelmisto ohjelmistojen virtuaalisointiin ja sovellusten toimitukseen. Se mahdollistaa käyttäjien ottaa yhteyttä palvelimeen, jolla sovellukset ovat ja käyttää niitä. Käyttäjä saa palvelimelta käyttöön sen resurssit, kuten muistin ja prosessorit. Sovellukset toimivat samalla tavoin, kuin ne olisivat asennettuna päätelaitteelle. Yksi Citrix XenAppin ominaisuuksista on, että yhteys voidaan muodostaa miltä tahansa päätelaitteelta, käyttöjärjestelmästä riippumatta. Päätelaitteessa tulee vain olla Citrix Receiver asennettuna. XenAppin avulla määritetään käyttäjäoikeudet järjestelmään ja mitä ohjelmia käyttäjät voivat käyttää.
Kun ohjelmistojen varsinaista virtuaalisointia ei vielä ollut käytössä, oli käytössä sovellusten hostaus. Tämä tarkoitti palvelun hallinnoinnin siirtämistä toiselle, palveluntarjoajan hallintaan kuten palveluntarjoajan sivustolle.

5.4 Citrix XenDesktop

Työpöytävirtuaalisointi, josta käytetään nimeä Virtual Desktop Infrastructure (VDI), on laaja käsite joka sisältää paljon erilaisia virtuaalisointi teknologioita. Työpöytävirtuaalisoinnilla toteutetaan ja hallitaan käyttäjien työpöytäympäristöä. VDI on ollut käytössä 2000- luvun alkupuolelta lähtien ja sen tarkoituksena on isännöidä käyttäjän tarvitsemia ohjelmistoja palvelimelta käsin, ei käyttäjän koneelta käsin. Perusidean on kehittänyt Hewlett-Packard v. 2005, jossa ensimmäisessä versiossa oli ideana ottaa telineellinen Blade tietokoneita ja asentaa kuhunkin Windows XP -käyttöjärjestelmä. Tämän jälkeen käyttäjät pystyivät käyttämään käyttöjärjestelmää normaalia Microsoft RDP -protokollaa (Remote Desktop Protocol) käyttäen. Konseptina järjestelmän toiminta täytti vaativammatkin standardit, mutta työpöytävirtuaalisointi on vasta myöhemmin tullut jokapäiväistä. Nykyään pystytään käsittelemään yli 30 työpöytää yhdellä palvelimella. Citrix on julkaissut testituloksen, jolla pystytään käsittelemään 130 työ-

pöytävirtuaalisointia yhdessä 72 GB Dual Socket, quad-core Intel Xeon x5570 tietokoneessa. Testissä pystyttiin jakamaan yhdelle työpöydän käyttäjälle 512 MB muistia (James G.R., 1.) Alla yksinkertainen esimerkki työpöytävirtuaalisoinnista (kuva 3).



Kuva 7: Työpöytävirtuaalisointi (James, G. 2010, 2)

5.5 Citrix Netscaler

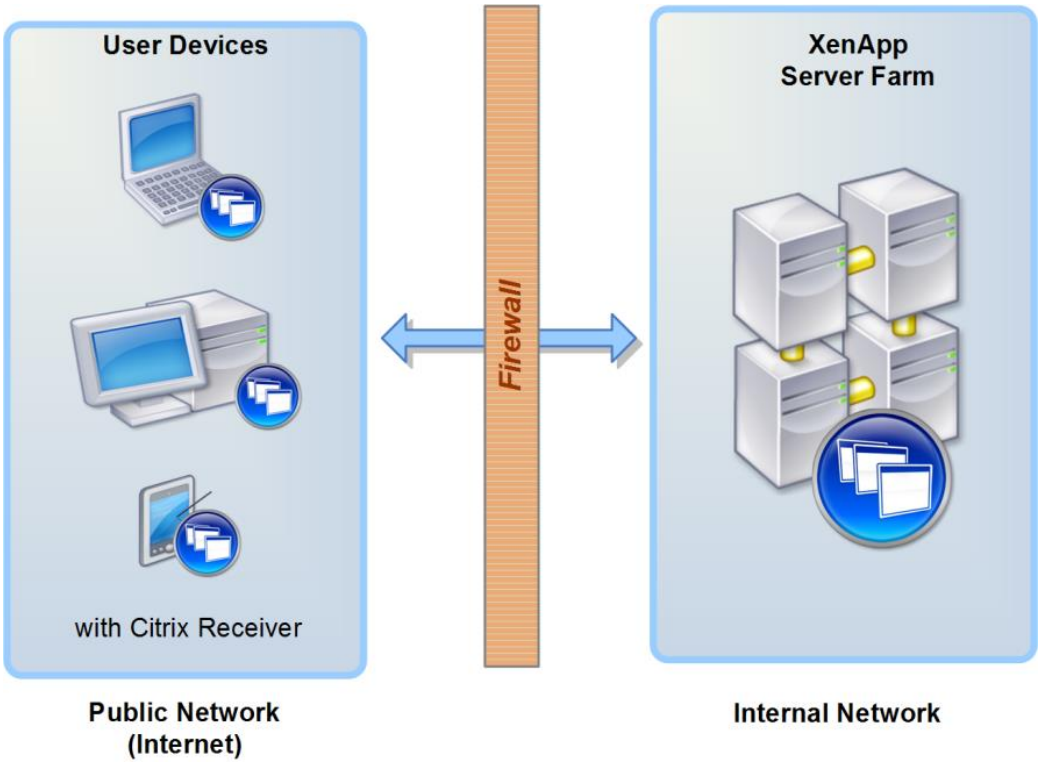
Citrix Netscaler toimii järjestelmässä tietoturvallisuuden ja verkon kuormituksen tasaajana. Sen ominaisuuksia on toimia palomuurina järjestelmän ja avoimen verkon välillä sekä hallinnoida SSL (Secure Sockets Layer) ja VPN yhteyksiä. Citrix Netscaler - järjestelmä voidaan asentaa joko Demilitarisoidulle (myöhemmin DMZ) alueelle tai sisäverkon järjestelmän osaksi. Sisäverkossa käytettynä Netscaler tukee järjestelmän sisäisiä käyttäjiä ja toimii suojavyöhykkeenä Internetin ja suojatun verkon välillä.

6 Citrix XenApp ja XenDesktop turvallisuusstandardit

Yhtiöiden liiketoimintaympäristöt vaativat luotettavan, joustavan ja sitä turvaavat toimenpiteet tietojen välittämiseen julkisessa ja luotettavassa verkossa eri sidosryhmille. Tietoturva asettaa haasteita järjestelmien käytölle, kuin myös käyttäjille. Yhtiöiden liiketoiminnan periaatteisiin kuuluu, että henkilökunta pääsee yhtiön tietojärjestelmiin useammista paikoista ja useammilla tavoilla kuin ennen. Järjestelmien etäkäyttö ovat tulleet kuvaan mukaan päivittäisten työsuoritusten tekemiseen. Citrix tuotteet tarjoavat käyttäjille valikoiman erilaisia turvallisuusominaisuuksia, joita Citrix-järjestelmän käyttöönoton yhteydessä tulee ottaa käyttöön. Kun järjestelmää suunnitellaan, yhtiössä tulee tehdä tarkat suunnitelmat, kuinka järjestelmä toteutetaan, esimerkiksi kuinka toteutetaan käyttäjien ja Citrix-järjestelmän välinen tietoliikenneyhteys. Citrix käyttää turvallisuusstandardina Amerikan Yhdysvaltojen hallituksen määrittämää FIPS 140 – standardia (Federal Information Processing Standards). FIPS 140 määrittää vaatimukset salaustekniikalle jotka käsittävät niin laitteiston kuin myös ohjelmistot (FIPS PUB 140-2.)

6.1 Citrix-järjestelmä käytettäessä SSL salausta

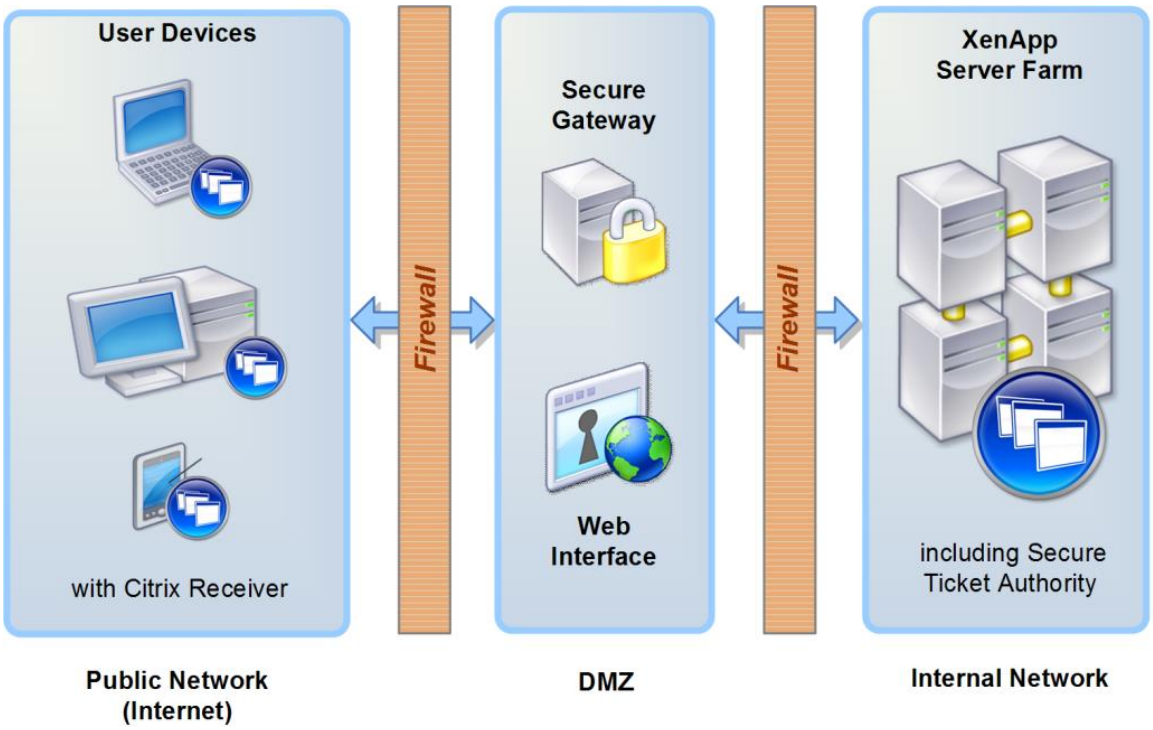
SSL salaus (Secure Sockets Layer) tai nykyisin TLS (Transport Layer Security) on salattu yhteys, jolla suojataan tietoliikenneyhteys Internet-sovellusten välillä IP verkkojen yli. Nykyisin tämä tapa on tavallisimpia tapoja suojata tietoliikenneyhteys ja se mahdollistaa yhteyden vahvan salaamisen palvelimen ja päätelaitteen välillä. Citrix käyttää salausta XenServerin ja käyttäjän laitteessa olevan Citrix Receiverin välillä. SSL salaus toimii välittäjänä yhteydenpidossa asiakaslaitteiden ja XML-palvelun välillä kullakin palvelimella. Kukin asiakaslaite todentaa SSL:n välityksen vertaamalla SSL:n välityksen palvelinsertifikaattia luotettavien varmenteiden luetteloon. Tämän todentamisen jälkeen, asiakaslaitteen ja SSL:n välitys neuvottelee pyyntöjä salatussa muodossa. SSL:n välitys avaa pyynnöt ja siirtää ne XenAppin palvelimiin. Kaikki tieto, joka on lähetetty palvelimista asiakaslaitteeseen, menee SSL salauksen lävitse, joka salaa tiedot ja lähettää sen eteenpäin asiakaslaitteeseen, missä tieto avataan. Tällä tavoin varmistetaan tiedon eheys ja koskemattomuus (Citrix).



Kuva 8: Citrix-järjestelmä käytettäessä SSL salausta (Citrix)

6.2 Citrix ja Secure Gateway (Single-Hop)

Secure Gatewayn käyttöönotto riippuu useista tekijöistä, kuten mitkä komponentit Citrix-järjestelmästä on verkossa käytössä. Secure Gateway on suunniteltu toimimaan yhdessä Citrix XenAppin kanssa. Secure Gateway toimii yhdessä web rajapinnan kanssa käyttäjän todennuksen, käyttövaltuutuksen ja ohjaimena Citrix XenApp – palvelimen resursseihin. Citrix suosittelee DMZ asentamista kahden palomuurin välille jolloin voidaan taata tietojenvälityksen täysi turvallisuus. Secure Gateway käyttää SSL/TLS salausta, jolloin salattu tietoliikenne selaimen ja palvelimen välillä on HTTPS yhteys. Lisäksi ICA liikenne voidaan myös salata käyttämällä IPSec salausta (Citrix).



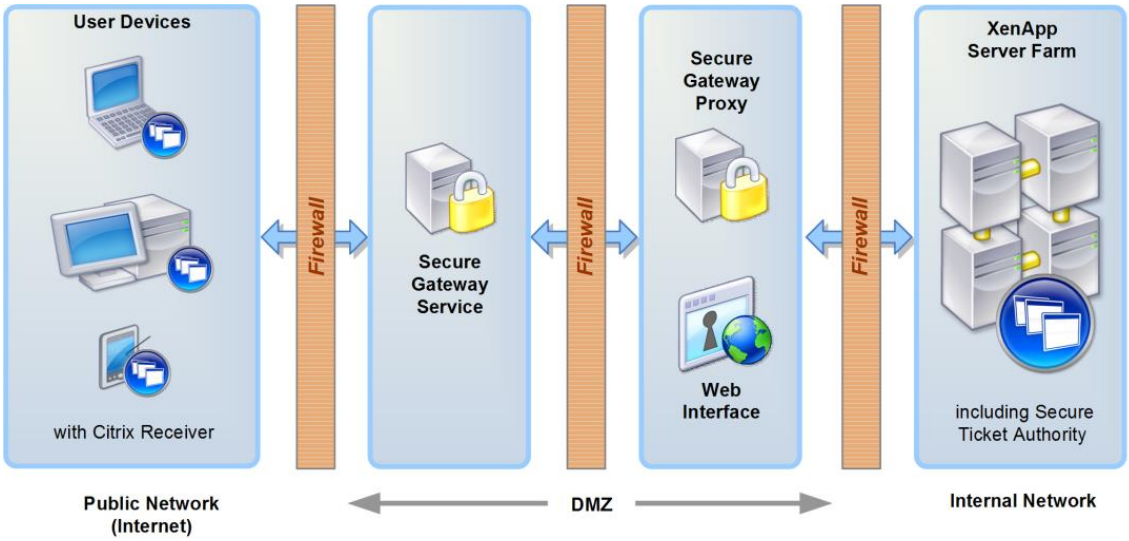
Kuva 9: Citrix ja Secure Gateway (Single-Hop) (Citrix)

6.3 Citrix ja Secure Gateway (Double-Hop)

Tässä kokoonpanossa käytetään Secure Gateway – suojausta niin, että DMZ on jaettu kahteen erilliseen segmenttiin, jolloin Secure Gateway - palvelin on ensimmäisen DMZ vyöhykkeen segmentissä. Palomuurilla suojatun DMZ vyöhykkeen ja Internetin välillä portti 443 on avoimena. Web-rajapinta ja Secure Gateway välityspalvelin asennetaan erillisille palvelimille DMZ:ssä, jolloin palvelinfarmi on turvatussa verkossa. Palomuuri, ensimmäisen ja toisen DMZ välissä on portit 80 ja 443 avoimena.
Secure Gateway, jota on käytetty ensimmäisessä DMZ segmentissä, on vastuussa kaikesta sisään tulevan tietoliikenteen sieppaamisesta. Web-rajapinta vastaa käyttäjätunnistuksesta ja

käyttövaltuuksista. Käyttäjän todentamisen jälkeen Secure Gateway välityspalvelin on vastuussa kaiken datan välittämisestä, jota on vaihdettu Secure Gateway ja palvelimien välillä, jolloin välitys tapahtuu turvatussa verkossa. Palomuuri toisen DMZ - segmentin välillä ja turvatun verkon portit 80, 443, ja 1494 ovat avoimena (Citrix).

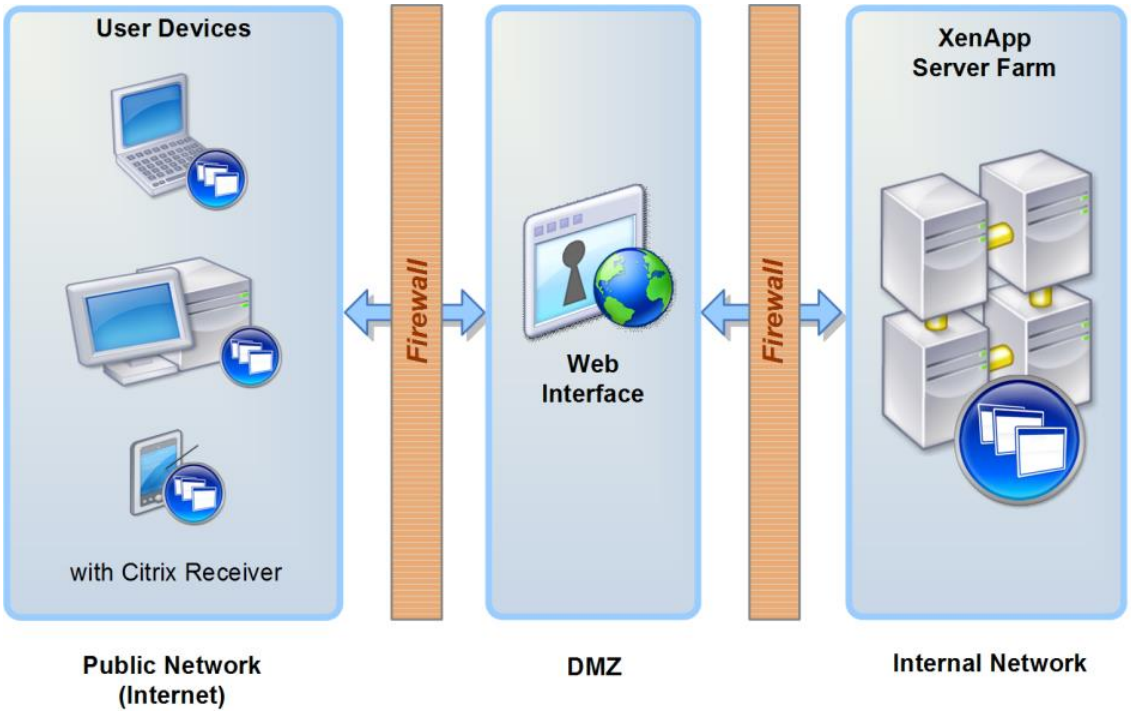
Secure Gateway tässä kokoonpanossa tarjoaa lisäsuojausta, koska mahdollinen hyökkääjä täytyy tunkeutua useisiin erillisiin turvallisuusvyöhykkeisiin tavoittaakseen palvelimet turvatussa verkossa.



Kuva 10: Citrix ja Secure Gateway (Double_hop) (Citrix)

6.4 Citrix käyttäen SSL salausta ja Web rajapintaa

Tässä kokoonpanossa SSL salaus toimii välittäjänä asiakaslaitteiden, web-rajapinnan ja XML-palveluiden välillä. Kukin asiakaslaite todentaa SSL:n välityksen vertaamalla SSL:n palvelinsertifikaattia luotettavien varmenteiden luetteloon, jolloin hyväksytyn todennuksen jälkeen asiakaslaite ja SSL neuvottelee pyyntöjä salatussa muodossa. SSL avaa pyynnöt ja siirtää ne XenApp palvelimille. Kaikki se tieto mitä järjestelmä lähettää, menee SSL salauksen lävitse palvelimista asiakaslaitteeseen, missä tieto avataan. Tällä menettelyllä varmistetaan tiedon eheys ja koskemattomuus (Citrix).



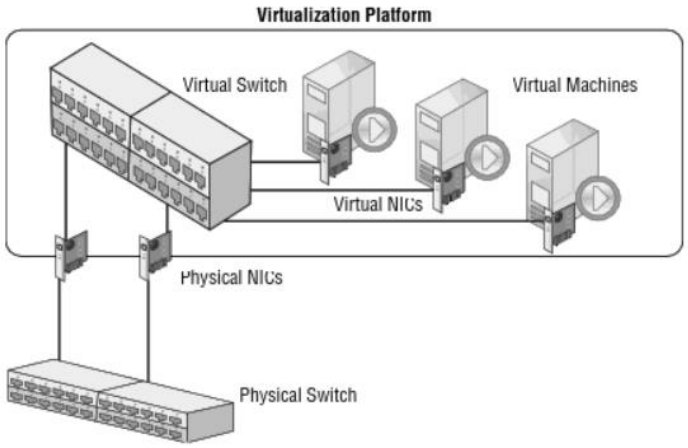
Kuva 11: Citrix SSL salaus ja Web rajapinta (Citrix)

7 Virtuaaliverkon tietoturva

Virtuaaliverkot ovat keskeinen elementti suunniteltaessa turvallista virtuaalijärjestelmää. Kaikilla hypervisor alustoilla on virtuaaliverkon komponentteja, joiden määrittely verkon osina näyttelee merkittävää osaa kuinka verkko toimii ja kuinka turvallinen verkko on. On otettava huomioon virtuaalijärjestelmää suunniteltaessa, kuinka yhdistäminen virtuaaliverkon ja fyysisen verkon kanssa toteutetaan, kun jokaisella komponenteilla on omat kapasiteetit ja rajoitteet (Shackleford, D. 2012, 93).

Virtuaaliverkon komponentteihin lukeutuu fyysiset verkkosovittimet (NIC), joiden käyttöönotossa on otettava tarkkaan huomioon se, minkä laajuista verkkoliikennettä virtuaaliympäristössä tulee olemaan. Fyysisten verkkosovittimien vastaparina virtuaalijärjestelmässä ovat virtuaaliset verkkosovittimet (Virtual NIC). Ne ovat ohjelmistopohjaisia virtuaalikomponentteja, joka siirtää tietoliikennettä fyysisen verkkosovittimen ja virtuaaliympäristöjen välillä. Virtuaaliset verkkosovittimet ovat järjestelmässä keskeinen komponentti, jotka yhdistävät virtuaaliympäristön komponentit toisiinsa niin virtuaalikoneet, fyysisen laitteiston, tietovaraston ym. Verkkoturvallisuuskomponentteihin lukeutuu fyysisen verkon palomuuri ja tunkeutumisen havaitsemisjärjestelmä (IDS). Useissa tapauksissa tällaisia järjestelmiä voidaan myös käyttää virtuaalijärjestelmän osana, eli niiden toiminta ulottuu myös virtuaalijärjestelmään (Shackleford, D. 2012, 93-94.)

Kun käytetään virtuaalijärjestelmässä ei-virtuaalisen verkon turvajärjestelmiä, voivat ne osaltaan aiheuttaa hitautta virtuaaliverkossa (Ahlm, E.).



Kuva 12: Virtuaaliverkon komponentit (Shackleford, D. 2012, 94)

Virtuaaliverkon hallinta tulee tapahtua oman hallintaverkon kautta, joka on eristetty virtuaaliverkosta tai järjestelmänvalvojan työasemien kautta. Tällä tavoin estetään komentojen tulemasta suoritetuksi suoraan virtuaalijärjestelmässä tai mahdollisen hyökkääjän pääsemisestä tuotantoverkkoon. Hallintayhteyden salaaminen SSL:llä tai TLS:llä estää ulkopuolisen hyökkääjän kuuntelemasta tietoliikenneyhteyttä, jolloin hallintaverkon ja virtuaaliverkon välinen tietoliikenne pysyy salattuna (Shackleford, D. 2012, 99).

8 Virtuaalijärjestelmän uhat

Yrityksen lähiverkko on lähes aina yhteydessä julkiseen verkkoon ja alttiina kaikenlaisille tietoverkkohyökkäyksille. Lähiverkon turvaaminen on erittäin tärkeä toimenpide kun kyseessä on yrityksen liiketoiminnallisesti tärkeistä järjestelmistä ja laitteista. Lähiverkon turvaamiseksi käytetään yleisesti palomuurijärjestelmiä. Palomuurijärjestelmät suojaavat sisäverkkoa hyökkäyksiltä, mutta nykyisin suositaan vielä rakennettavaksi DMZ -vyöhyke, joka sijaitsee sisäverkon ja julkisen verkon välissä.

Virtuaalisointi parantaa palvelinympäristöjen hallittavuutta, joka on myös siten hyödyksi sen tietoturvallisuuden kannalta. Virtuaalijärjestelmissä usein tallennuskapasiteetti on erillään itse sovelluksesta, joten jos haittaohjelma pääsee järjestelmään, on se helppo eristää. Pelkkä virtuaalisointi ei kuitenkaan uhkia poista ja kaikki tietotekniikkaympäristöt kohtaavat uhkia, oli kyse yksittäisestä laitteesta tai kokonaisesta tietotekniikkajärjestelmästä. Kaikki fyysisiin kuin virtuaalisiin järjestelmiin kohdistuvat ulkopuoliset hyökkäykset, työntekijöiden inhimillisyyteen perustuva virheellinen toiminta järjestelmässä tai tietojen varastamiseen liittyvä

toiminta ovat uhkana järjestelmien toiminnalle. Virtuaalijärjestelmän uhat ovat samanlaiset kuin kaikissa muissakin tietojärjestelmissä.

Virtuaalijärjestelmän turvallisuutta koskevia asioita on useita, joihin järjestelmän hallinnollisin keinoin tulee kiinnittää huomiota. Pääkohtina ovat hyökkäykset sisältä ja ulkoa virtuaalijärjestelmää kohtaan, sen käyttöjärjestelmiä ja sovelluksia. Järjestelmä tulee aina päivittää viimeisimpään ohjelmistoversioon, jolla taataan järjestelmän turvallisuus. Muutostiedostojen ja ohjelmistopäivitysten ajaminen virtuaalijärjestelmään on haastavampaa kuin fyysiseen. Usein ylläpidettäviä virtuaalijärjestelmiä on usein enemmän kuin fyysisiä järjestelmiä. Erityisesti isäntäkoneen haavoittuvuus koko järjestelmän tietoturvalle on merkitsevä. Haittaohjelman saastuttama isäntäkone on suurempi uhka tietoturvan kannalta, kuin yksittäisen virtuaalikoneen. Virtuaalijärjestelmän koneet, vaikka samassa isäntäkoneessa toimivat, harvoin kommunikoivat keskenään. Jos niin tapahtuu, on se tietoturvan kannalta uhkatekijä. Haittaohjelmat saattavat näin päästä leviämään koko virtuaalijärjestelmään. Virtuaalijärjestelmän palvelinympäristö on verkkotopologialtaan erilainen verrattuna fyysisen järjestelmään, että ne kommunikoivat virtuaalisten verkkosovittimien kautta. Näiden verkkosovittimien virheellinen asennus tai ohjelmointivirhe voi avata aukkoja järjestelmään pääsylle. Turvallisempi ratkaisu, joskin tehottomampi on ohjata kaikki verkkoliikenne aina fyysisen verkon kautta. Tällöin voidaan pääsynvalvonta ja verkkoliikenteen kontrollit hoitaa tutuilla toimenpiteillä, kuten palomuureilla.

Yhden merkittävän uhan virtuaalijärjestelmälle Pék G ja muut esittelee tutkimuksessaan. Se koskee hylättyjä virtuaalijärjestelmiä, jotka ovat jääneet unohduksiin tai hylätty kokonaan. Tällaiset järjestelmät ovat uhka samassa fyysisessä järjestelmässä toimiville toisille järjestelmille. Uhka muodostuu siitä, että järjestelmä on haavoittuvainen muutostiedostojen puuttumisen tai pääsynvalvonnan vuoksi. Lisäksi tällaisissa järjestelmissä voi olla jäljellä salattuja tietoja, joita mahdollinen hyökkääjä voi käyttää hyväkseen murtautuessa toisiin järjestelmiin.

Toisenlaisen näkökulman antaa virtuaalijärjestelmien uhkista suojautumiselle Jeramiah Bowling artikkelissaan Virtual Security: Combating Actual Threats. Hän kehottaa järjestelmää rakennettaessa rakentamaan tuotantojärjestelmän kahtena. Kun järjestelmässä on varalaitteet valmiina, kuten virtalähteet ja levyjärjestelmät, pystytään järjestelmä saamaan toimivaksi nopeasti. Aina kannattaa olla varmuuskopio järjestelmästä, mistä sen voi nopeasti palauttaa toimintaan. On monia tapoja varmuuskopioida järjestelmiä. Datatasolla virtuaalijärjestelmän käyttäjien järjestelmätiedot ja levytila on helppo ja yksinkertaista kopioida toiseen paikkaan. kuten fyysisen järjestelmän levylle. Huonompi puoli asiassa kuitenkin on, että käyttäjä täytyy sulkea järjestelmästä ulos. Tähän on ratkaisuna kehitetty sovelluksia, joilla voidaan ottaa tilannevedos (snapshot) järjestelmästä, ilman että järjestelmää tarvitsee sulkea. Tällainen ohjelma on XenServerissä Quorum Systemsin Alike.

8.1 Virtuaalikoneen kaappaus

Yksi uhkatekijä on virtuaalikoneen kaappaus. Virtuaalijärjestelmät ovat kokoelma tiedostoja ja ohjelmia, joihin käyttäjillä on pääsy. Käyttäjä, jolla on pääsyoikeus järjestelmään tai ulkopuolinen, joka on päässyt sisään järjestelmään, pystyy kopioimaan tai tuhoamaan tietoa järjestelmästä. Virtuaalijärjestelmä käyttää samoja fyysisiä resursseja isäntäkoneen kanssa, mutta kuitenkin yleensä säilyttää itsenäisen asemansa omana järjestelmänään.

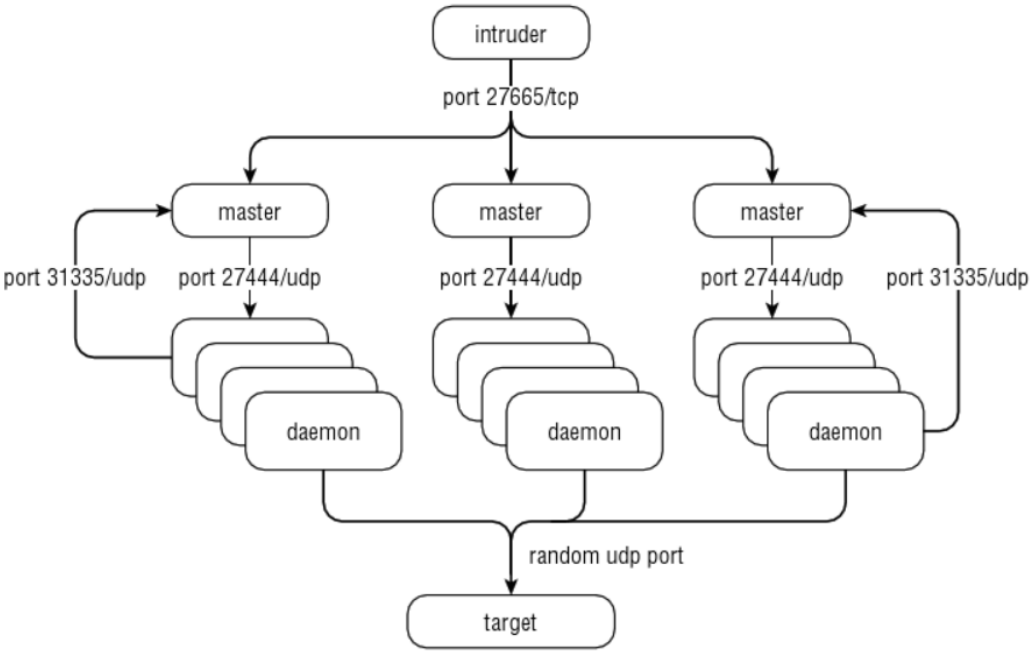
Virtuaalijärjestelmät ovat suunniteltu niin, että yhdessä järjestelmässä suoritusta tekevä ohjelma ei pysty tarkkailemaan, mitä toisessa virtuaalijärjestelmässä tai isäntäkoneessa tapahtuu tai kommunikoimaan niiden kanssa. Todellisuudessa virtuaalijärjestelmää käyttävät organisaatiot käyttävät joustavaa eristäytymistä järjestelmien välillä, joka tarkoittaa sitä että järjestelmät pystyvät käyttämään resursseja paremmin. Tällainen tilanne mahdollistaa sen, että hyökkäys yhteen järjestelmään altistaa muutkin, niin isäntäkoneen kuin toiset virtuaalijärjestelmät vaaraan. Tällaista hyökkäystä kutsutaan virtuaalijärjestelmän paoksi (VM Escape) (J. Reuben, 2007).

8.2 Palvelunestohyökkäys

Virtuaalikonearkkitehtuurissa virtuaalijärjestelmä ja isäntäkone jakavat käytettävissä olevia fyysisiä resursseja, kuten prosessori sekä muisti- ja verkkoresurssit. Siksi on mahdollista että järjestelmään pääsevä ulkopuolinen hyökkääjä määrittää palvelunestohyökkäyksen (Denial of Service, DOS) käyttäjille, jotka ovat sisällä samassa järjestelmässä. Palvelunestohyökkäys käynnistetään yleisesti yhdestä tai useammasta järjestelmästä, jotka tunkeutuja on saanut haltuunsa. Palvelunestohyökkäys virtuaalijärjestelmässä voidaan kuvailla hyökkäykseksi, jossa hyökkääjä ottaa järjestelmän resurssit omaan käyttöön. Tästä johtuen järjestelmä torjuu kaikki muut käyttäjät, jotka tekevät pyynnön käyttää tarvittavia resursseja. Paras tapa estää käyttäjiä varaamasta virtuaalijärjestelmän kaikkia resursseja on rajoittaa käyttäjille varattuja resursseja. Citrix-järjestelmä tarjoavat mekanismeja rajoittaa resurssien käyttöä, joilla voidaan rajata resurssien käytön tiettyyn rajaan asti. Tällä estetään järjestelmän kohdistuvat palvelunestohyökkäykset (Reuben, J. 2007).

Yksi tunnettu ohjelmisto jota on käytetty palvelunestohyökkäyksiin, on trin00. Siinä hyökkääjät lisäsivät käytettävien resurssien syvyyttä saavuttaakseen korkeamman tason vahinkoa ja väistämään suojaavia mekanismeja. Kun järjestelmien kapasiteetit nousivat tasolle, joka vähentää yksinkertaisten DoS hyökkäysten tehoa, hyökkääjät löysivät keinon lisätä hyökkäyksen voimaa lisäämällä kapasiteettia. Nämä keinot tulivat kahdesta keinosta. Joko järjestelmä, jossa oli suuri kaistanleveys ja suuri laskuteho tai monta pientä tietokonetta toimimaan yhdessä tukkimaan palvelun verkkokapasiteetin. Tällaisen hyökkäyksen estäminen vaatii massii-

visen suojausjärjestelmän. Vaikka suojaus onnistuisi, se kuitenkin jättäisi kuitenkin merkkinsä järjestelmän toimivuuteen.



Kuva 13: Trin00 yleinen DoS kaava (Ottenheimer, D. ym, 112)

Hajautettu palvelunestohyökkäys (Distributed Denial of Service, DDoS) on hyökkäys järjestelmää kohtaan useista eri tietokoneista yhtä järjestelmää kohtaan. Usein tällaiset hyökkäykset tulevat bottiverkoista (Botnet), jotka ovat kytkeytyneet toisiinsa Internetin välityksellä. Usein hyökkäykseen osallistuvat tietokoneet ovat saastuneet viruksella, joka käynnistää hyökkäyksen (Five Ways to Protect Against DDoS Attacks). DDoS hyökkäys perustuu raakaan voimaan, jossa pyritään useista eri IP-osoitteista tukkimaan palvelu.

9 Virtuaalijärjestelmän turvaaminen

Pitämällä virtuaalipalvelimensa sisäverkossa yritys suojaa järjestelmänsä, mutta tällaisella menettelyllä on myös yleishyödyllisiä vaikutuksia. Mitä vähemmän virtuaalipalvelimia näkyy suoraan Internetiin, sitä vähemmän ne houkuttelevat hakkereita ja sitä epätodennäköisempää on epidemioiden ryöstäytyminen käsistä. Perinteisiä tietoturvaohjelmistoja ei ole suunniteltu suoraan virtualisoitujen ympäristöjen turvaamiseen ja tietoturvayhtiöt kehittävätkin virtuaalipalvelimiin sovitettua ennalta ehkäisevää tietoturvaa virtuaalisointiohjelmien tekijöiden avustuksella.

Kuitenkin virtuaalijärjestelmän turvallisuuteen pätevät samat säännöt, kuin yksittäisen tietokoneen käyttöjärjestelmän tietoturvallisuuteen. Virtuaalijärjestelmän turvallisuuden takaamiseksi tulee järjestelmä pitää mahdollisimman ajantasaisena, ohjelmistopäivitysten ja muutostiedostojen (Patch) avulla. Myös hypervisorin ja virtuaalijärjestelmän suojaaminen päivitystiedostojen avulla on tärkeää.

Pearce M. ja muut kirjoittavat tutkimuksessaan Virtualization: Issues, security threats, and solutions virtuaalijärjestelmän parannellusta luottamuksellisuudesta ja käytettävyydestä, kun käyttöjärjestelmä asennetaan suoraan virtuaalijärjestelmään, ei välissä ole käyttöjärjestelmää joka operoi fyysisen laitteiston kanssa. Näin saadaan paremmin eristettyä samassa fyysisessä koneessa operoivat virtuaalijärjestelmät toisistaan, joka siten parantaa koko järjestelmän luottamuksellisuutta. Tämän lisäksi virtuaalijärjestelmän käytettävyys paranee normaaliin järjestelmään verrattuna merkittävästi, kun käytössä on järjestelmän varmuuskopiointi ja järjestelmän palautustoiminto. Näin on mahdollista ottaa koko virtuaalijärjestelmästä kopio muistista, kovalevystä, kuin myös muista järjestelmään asennetuista laitteista. Järjestelmän palautus voidaan suorittaa hyvin nopeasti ja jopa niin, että järjestelmä on käynnissä (Pearce, M. 2013).

Virtuaalijärjestelmän turvallisuudesta kirjoittavat myös Pék G. ja muut tutkimuksessaan A Survey of Security Issues in Hardware Virtualization, että käyttöjärjestelmällä on aina enemmän oikeuksia kuin siihen asennettuun virtuaalijärjestelmällä on. Käyttöjärjestelmä pystyy ohjaamaan laitteiston resursseja joko suoraan tai hypervisorin kautta. Tästä syystä Citrix-järjestelmässä käytettävä Xen hypervisorin kanssa ei suositella käytettäväksi erillistä käyttöjärjestelmää, koska se sekoittaa virtuaalijärjestelmän oikeuksien käsittelyn joka osaltaan johtaa myös tietoturvan heikkenemiseen (Pék G. ja muut. 2013).

Paras turva virtuaalijärjestelmän tietoturvallisuuden, tehokkuuden, resurssien hallinnan ja synkronisen toiminnan kannalta on se, että järjestelmässä on käytössä Type 1 – hypervisor, jossa ei ole käyttöjärjestelmää fyysisen koneen ja virtuaalijärjestelmän välissä. Lisäksi virtuaalijärjestelmä tulee olla näkymättömissä. Tämä virtuaalijärjestelmän näkymättömyys toisille järjestelmille ja ohjelmille on ehdoton turvallisuuden tae. Fyysisessä laitteessa toimivat useammat virtuaalijärjestelmät tulee olla tasavertaisia sekä näkymättömiä myös toistensa kanssa. Koska hypervisor pitää yllä järjestelmän täyttä valvontaa se valvoo myös resurssien käyttöä se voi myös muuttaa järjestelmän asetuksia jos se havaitsee järjestelmässä uhkia. Joissain tapauksissa on mahdollista, että virtuaalijärjestelmään ohjelmistoja kehittävät ohjelmoijat suunnittelevat ohjelmat niin, että uskovat järjestelmän jossa ohjelmat toimivat olevan jo hyvin turvattu ja jättävät tietoturvatarkistukset vähemmälle kuin normaalisti.

10 Citrix tietoturvan parhaat käytännöt

Tietoturvallisuudesta puhuttaessa on otettava huomioon, että verkkoympäristö ei ole koskaan täysin suojattu. Pääasiassa tarkoitus on tehdä ulkopuoliselle tunkeutujalle mahdollisimman hankalaksi ja aikaa vieväksi pääsy järjestelmän sisälle. Kun turvallisuutta suunnitellaan, on tehtävä tasapaino suojatun verkon ja verkossa työtä tekevien henkilöiden pääsy verkkoon tekemään töitä. Hyvä turvallisuussuunnitelma ottaa huomioon yhtiön kyvyn suojata järjestelmä ja siihen käytettävissä olevan teknologian. Yhtiön on määritettävä minimitaso tietoturvalle, jolloin pystytään valitsemaan keinot ja teknologia vähintään sen tason ylläpitämiseksi. Lisäksi on tunnistettava ne riskit, joita järjestelmää uhkaa (Azad, T. 2008, 354.)

Citrix XenApp palvelinjärjestelmän suojaaminen on tärkeä tehtävä järjestelmän ylläpitäjälle. Aluksi on selvitettävä, millaisia uhkia järjestelmä saattaa kohdata. Citrix Systems suosittelee seuraavanlaisia parhaita käytänteitä XenApp palvelinjärjestelmän suojaamiseksi. File Association ominaisuus on pois kytkettynä asiakaslaitteesta palvelimeen uudelleenohjauksessa. Julkaistujen sovellusten komentokehotteessa on aina huomioitava, että yleismerkit (kuten % ja *) eivät ole käytössä ohjelmistojen poluissa. Järjestelmässä olevien sovellusten nimeämiskäytännöt ovat tehtävä vaikeasti ymmärrettäviksi tai hahmotettaviksi, että hyökkääjä ei pysty arvaamaan niitä. XenApp ohjelmistoja ei voida käyttää suojatusta verkosta, vaan ainoastaan turvatun verkon kautta. Lisäksi on pääsynvalvonta toteutettava niin, että käyttäjillä on vain ne resurssit käytössään, mitä he tarvitsevat (Azad, T, 355).

Citrix Systems antamat ohjeet parhaiksi käytäntöihin Citrix XenDesktopin järjestelmän osalta on, että järjestelmä on aina pidettävä ajantasaisena muutostiedostojen (Patch) avulla. Kaikki järjestelmän laitteet on suojattava laitekohtaisilla antivirusohjelmistoilla ja kaikki järjestelmän laitteet ovat asetettu palomuurien sisällä, sisäverkossa. Erityisesti ohjeistus korostaa palomuurien asettelua niin, että kaikki järjestelmän laitteet tulevat suojatuiksi palomuurien avulla. Lisäksi kaikki tietoliikenneyhteydet tulee olla salattuja järjestelmän sisällä, Windows laitteiden välillä käytetään IPSec salausta (Citrix Security Best Practices).

11 Yhteenveto ja pohdinta

Yhtiöiden tietojärjestelmien käyttö on kasvanut merkittävästi viimeisten vuosikymmenten kuluessa. Liiketoimintaa tehdään verkossa, tavaroiden myynti, asiakaspalvelu, rahansiirrot ovat tämän päivän yrityksissä arkipäivää. Tietojärjestelmien kehitys on tapahtunut yhdessä tietotekniikan kehityksen kanssa, yhdessä kulttuurillisissa ja ympäristöllisissä raameissa. Virtuaalijärjestelmät ovat tuoneet ratkaisun moneen ongelmaan, kun palvelinjärjestelmien koko alkoi saada suureelliset mittasuhteet.

Virtuaalijärjestelmät ovat tietoturvallisia, kun ne pidetään suojassa sisäverkossa, joita suojaa palomuurit ja muut fyysiset suojausjärjestelmät. Mutta jos tietoturvallisuuden tasosta lähdetään joiltain osin tinkimään, tuo se uhkia järjestelmään. Virtuaalijärjestelmän uhat ovat hyvin toisenlaisia, kuin fyysisten järjestelmän uhat. Virtuaalijärjestelmässä on laajemmalti haavoittuvaa pinta-alaa, kuten virtuaaliset verkon komponentit, hypervisor, sovellukset minkä lisäksi fyysisen järjestelmän osat, käyttöjärjestelmä, fyysinen verkko ja laite, jossa järjestelmä toimii. Tämä johtaa monimutkaisiin suojaustoimenpiteisiin, kun käytetään virtuaalijärjestelmän ja fyysisen järjestelmän suojaustoimenpiteitä yhdessä. Virtuaalijärjestelmät muuttavat myös tietoturvallisuuden käsitteitä. Normaalit fyysisen verkon komponentit, aliverkot ja DMZ - vyöhykkeet sekä palomuurit ovat normaalia suojausta fyysisissä verkoissa, mutta virtuaalijärjestelmissä tarvitaan uusia ohjelmia ja ratkaisuja samanlaisen verkkojärjestelmän luomisessa.

Virtuaalijärjestelmiä hallinnoidaan järjestelmän ylläpitäjän työasemalta, jolloin kyseisen koneen suojauksen murtaminen on hyökkääjälle kuin päävoitto. Työasemalla usein on järjestelmän tietoturvan kannalta tärkeät tiedot, kuten verkon tiedot, salasanat ja IP-osoitteet. Jos järjestelmään murtautuja vielä asettaa botti - tai näppäilyn tallennus (key loggers) ohjelman työasemalle, voi hän saada käyttöönsä huomattavan määrän tietoa joilla horjutetaan järjestelmän vakautta.

Citrix virtuaalijärjestelmän käytön etuina on tietoturvallisuus, jos järjestelmän suunnittelussa ja toimintaan saattamisessa tietoturvallisuuteen panostetaan. Etuina ovat myös siitä saatavat synergiaedut. Samaa järjestelmää voidaan käyttää eri toimipaikoissa, millä laitteella tahansa, maasta tai sijainnista riippumatta, minkä yhteyden kautta halutaan. Tietoliikenneyhteyden nopeudella ei ole varsinaista merkitystä, koska Citrix Desktop - sovellus tuo loppukäyttäjän päätteelle kuvan ohjelmasta, ei kokonaista raskasta sovellusta. Etäkäyttöohjelman tietoliikenneyhteys palvelimelle on salattu joko VPN yhteydellä tai SSL/TSL salauksella. Järjestelmien kehitys, testaus ja tuotantoon otto voidaan tehdä keskitetysti ja se on heti tuotantoon oton jälkeen kaikkien käyttäjien saatavilla.

Virtuaalijärjestelmissä kuten kaikissa muissakin järjestelmissä on riskinsä. Joskus tulee eteen myös sellaisia riskejä, joita ei voi ennalta ottaa huomioon. Yksi mahdollinen riskitekijä on henkilökuntaan kuuluvat henkilöt ja henkilöt, jotka ovat irtisanottu tehtävistään. Tällaisesta tapauksesta Michael Davis kirjoittaa Virtualization Security Checklist – artikkelissa. Vuonna 2011 helmikuussa IT toimihenkilö irtisanottiin tehtävistä lääkealan yrityksestä. Henkilöltä ei ollut poistettu käyttäjätunnuksia järjestelmään, jolloin kyseinen henkilö pääsi kirjautumaan järjestelmään tunnuksilla, jotka olivat vielä voimassa. Hän pystyi poistamaan käytössä olevan palvelimen, jolla oli yhtiön liiketoiminnan kannalta tärkeitä sovelluksia, mukaan lukien sähköposti-, talousjärjestelmät ja tilausten hallinta. Tutkivan viraston (FBI) mukaan yhtiön kär-

simät tappiot liikkuivat 800.000 dollarin luokassa. Ja tämä tapahtui vain muutamalla näppäimen painalluksella (Davis, M.).

Lähteet

Ahlm, E. Server virtualization: Top 5 security concerns. Viitattu 31.01.2014. http://www.informationweek.in/informationweek/news-analysis/175042/server-virtualization-security-concerns

Azad, T. 2008. Securing Citrix XenApp Server in the Enterprise. Burlington, MA. USA. Syngress Publishing Inc.

Bowling, J. 2011. Virtual Security: Combating Actual Threats. Linux Journal. Volume 2011 Issue 205. Houston, TX. USA. Belltown Media.

Gohar, A. 2013. Implementing Citrix XenServer Quickstarter. Birmingham. UK. Packt Publishing Ltd.

Citrix. Product Documentation. Viitattu 3.3.2014. http://support.citrix.com/proddocs/topic/xenapp65-sec/ps-sec-sample-a-ssl-relay-xa6.html

Citrix Security Best Practices. Product Documentation. Viitattu 29.4.2014. http://support.citrix.com/proddocs/topic/xendesktop-bdx/cds-admin-security-best-practices-bdx.html

Davies, M. 2011. Virtualization Security Checklist. Information Week

FIPS PUB 140-2. Security Requrements for Gryptigraphic Modules. Department of Commerse, USA. Viitattu 30.3.2014. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Five Ways to Protect Against DDoS Attacks. 2014. IT Business Edge. Viitattu 30.3.2014 http://www.itbusinessedge.com/slideshows/show.aspx?c=96534

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo. Docendo Finland.

James, G.R. 2010. Citrix XenDesktop Implementation, a practical guide for IT professionals. Burlington, MA, USA. Syngress.

Katakri Kansallisen turvallisuusauditointikriteeristö, versio II. 2011. Viitattu 19.3.2014. http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Laitteistoturvallisuus. Vahti-ohjeet. Valtionvarainministeriö. 2009. Viitattu 30.3.2014. https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus

McDougall, R. & Anderson, J. 2010. Virtualization Performance, Perspectives and Challenges Adead. ACM.

Musumeci, G. 2012. Getting Started with Citrix XenApp 6.5. Olton Birmingham, GBR. Packt Publishing Ltd.

Ohjelmistoturvallisuus. Vahti-ohjeet. Valtionvarainministeriö. 2009. Viitattu 30.3.2014. https://www.vahtiohje.fi/web/guest/ohjelmistoturvallisuus

Ottenheimer, D., Wallace, M. 2012. Securing the Virtual Environment: How to Defend the Enterprise Against Attack (with DVD). Hoboken, NJ, USA. Wiley.

Pearce, M., Zeadally S., Hunt R. 2013. Virtualization: Issues, Security Threats, and Solutions. NY, USA. ACM Computing Surveys.

Pék G., Buttyán, L., Bencsáth B. 2013 A Survey of Security Issues in Hardware Virtualization. NY, USA. ACM Computing Surveys.

Portnoy, M. 2012. Essentials : Virtualization Essentials. Hoboken, NJ, USA. Sybex.

Reuben, J. 2007. A Survey on Virtual Machines Security. Viitattu 22.1.2014. http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf

Sarngadharan, M., Minimol, M.C. 2010. Management Information System. Mumbai, Intia. Global Media.

Shackleford, D. 2012. Virtualization Security : Protecting Virtualized Environments. Somerset, NJ, USA. Wiley.

Tietoaineistoturvallisuus. Vahti-ohjeet. Valtionvarainministeriö. 2009. Viitattu 30.3.2014. https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus

Tietojesi Turvaksi. Laakso, M. 2014. Viitattu 9.4.2014. http://www.tietojesiturvaksi.fi/content/tietoturvan-hallintaj%C3%A4rjestelm%C3%A4

Tietoliikenneturvallisuus. Vahti-ohjeet. Valtionvarainministeriö. 2009. Viitattu 30.3.2014. https://www.vahtiohje.fi/web/guest/tietoliikenneturvallisuus

Kuvat