Toni Lehtinen

VMWARE-VIRTUAALIYMPÄRISTÖN TURVAAMINEN

Tietojenkäsittelyn koulutusohjelma
2015

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VMWARE-VIRTUAALIYMPÄRISTÖN TURVAAMINEN

Lehtinen, Toni
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Toukokuu 2015
Ohjaaja: Grönholm, Jukka
Sivumäärä: 41
Liitteitä: -

Asiasanat: VMware, virtualisointi, tietoturva

Tässä opinnäytetyössä käsitellään tietoturvaa virtuaalisoidussa VMware ympäristössä. Työssä tutkitaan virtualisoinnin ja tietoturvan yhdistämistä. Työssä kerrotaan mitä virtualisointi on ja mitä sillä voidaan mahdollistaa. Aihealueen rajaamiseksi työ keskittyy ainoastaan VMwaren tarjoamiin ratkaisuihin.

Tekijän oppilaitoksessa on käytetty osana koulutusta VMwaren tuotteita, joka auttoi työn aihevalinnassa ja sen rajaamisessa. VMware on myös maailman johtava virtualisointiratkaisujen toimittaja. Virtualisointi yleistyy jatkuvasti maailmanlaajuisesti yrityksissä ja organisaatioissa ja siitä on tulossa keskeinen osa jokapäiväistä IT-järjestelmien ja -palveluiden ylläpitoa.

Virtualisoinnin juuret on lähtöisin 1960-luvulta. Virtualisoinnilla viitataan useisiin erilaisiin tapoihin tehdä tietojenkäsittelyn fyysistä resursseista ja piirteistä muilta järjestelmiltä piilotettuja. Se on tietojenkäsittelyssä käytetty tekniikka, jolla mahdollistetaan fyysisten resurssien toimimisen monena virtuaalisena resurssina tai usean fyysisen resurssin näkyminen yhtenä virtuaalisena resurssina. Tällä tavoin voidaan esimerkiksi mahdollistaa useamman virtuaalisen tietokoneen ajamisen yhden tietokoneen sisällä. Virtualisoinnin keskeiset osa-alueet ovat palvelinvirtualisointi, tallennusvirtualisointi, verkkovirtualisointi ja sovellusvirtualisointi.

SECURING VMWARE'S VIRTUAL ENVIRONMENT

Lehtinen, Toni
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information Teghnology
May 2015
Supervisor: Grönholm, Jukka
Number of pages: 41
Appendices: -

Keywords: VMware, virtualization, information security

The purpose of this thesis has been to manage information security in a virtualized VMware environment. This thesis deals with combining virtualization and information security. This thesis is about what virtualization is, and what can be made possible by it. To limit the scope of the thesis's topic, the thesis will only focus on solutions offered by VMware.

In the school, in which the thesis's author is attending, VMware products have been used, which further contributed to narrowing the focus of the thesis. VMware also provides the worlds leading virtualization solutions. Virtualization is gaining more popularity in organisations and companies globally, and its also becoming the staple of everyday maintenance of IT systems and services.

The roots of virtualization originate from 1960's. Virtualization refers to several different ways in which physical resources and functions are made hidden from other systems. It is a ICT system enabling physical resources to act as multiple virtual resources, or multiple physical resources acting as one virtual resource. This method can be used to run several virtual computers inside a single computer. The primary sectors of virtualization are server virtualization, storage virtualization, network virtualization and application virtualization.

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön aiheena on virtuaaliympäristön turvaaminen, ja työni keskittyy erityisesti ohjelmistoyritys VMwaren tarjoamiin palveluihin. Työssä käsitellään virtualisointia, VMwarea ja tietoturvaa sekä näitä kaikkia yhdessä. Virtualisointi alkoi kiinnostaa minua opintojeni edetessä, koska sen suomilla mahdollisuuksilla saadaan luotua säästöjä, säästettyä aikaa ja vähennettyä laitteiston tarvetta. Yksistään virtualisointi ei kuitenkaan tuntunut sopivalta aiheelta, minkä vuoksi halusin sisällyttää aiheeseeni myös tietoturvan. Koska virtuaaliympäristön turvaaminen pelkästään olisi ollut liian laaja aihealue, halusin rajata työn koskemaan vain yhtä palveluntarjoajaa. Hyvä tietoturvan merkitys korostuu koko ajan enemmän tietojärjestelmiin painottuvassa maailmassamme. Tietolaitteiden räjähdysmäinen kasvu luo haasteita alan asiantuntijoille. Myös käyttäjien tulisi olla tietoisia mahdollisista uhista ja haavoittuvuuksista, jotta tietoturvasta saadaan sen tarjoama hyöty.

Palveluntarjoajaksi valikoitui hyvin nopeasti VMware, koska se oli minulle entuudestaan tutuin palveluntarjoaja. Lisäksi VMwaren tuotteet ovat oppilaitoksessani käytössä. Valintaan vaikutti osittain myös VMwaren suuri suosio ja laajat palvelut. Varteenotettavimmat haastajat olivat Microsoftin Hyper-V, Citrixin Xen-Server ja Red Hatin Enterprise Virtualization.

Virtualisointi on kasvattanut suosiotaan viime aikoina, ja sen ai-kaisimmat vaiheet ulottuvat aina 1960-luvulle saakka. Alan edelläkävijöitä ovat IBM ja VMware. Nykyisin virtualisointitekniikkojen kehitystä ja kilpailua on useilla yrityksillä ja uusia kilpailijoita tuleekin markkinoille jatkuvasti. Virtualisoinnin muotoja on erilaisia, kuten käyttöjärjestelmä-, palvelin-, ohjelmisto-, tallennus- ja verkkovirtualisointi. VMwarella on pitkä kokemus virtualisoinnista ja se onkin tällä hetkellä markkinoiden johtava virtualisointipalveluita tarjoava yritys.

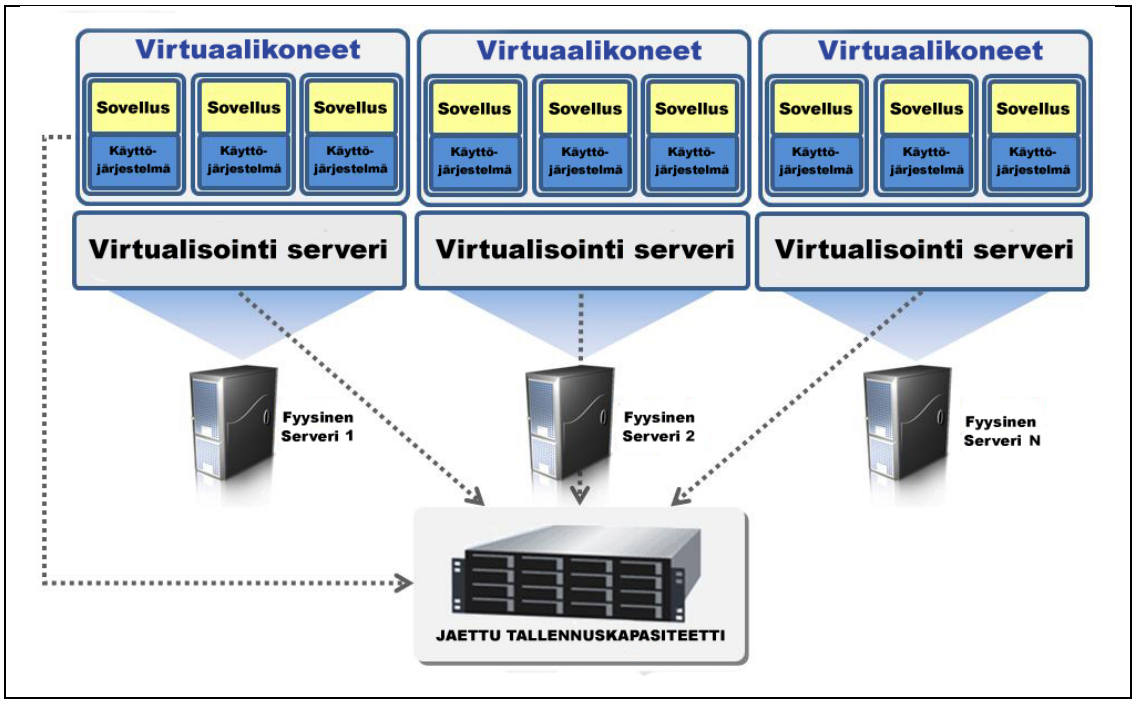
2 VIRTUALISOINTI

Virtualisointi on termi, jolla viitataan useisiin erilaisiin tapoihin tehdä tietojenkäsittelyn fyysistä resursseista ja piirteistä muilta järjestelmiltä piilotettuja. Se on tietojenkäsittelyssä käytetty tekniikka, jolla mahdollistetaan fyysisten resurssien toimiminen monena virtuaalisena resurssina tai usean fyysisen resurssin näkyminen yhtenä virtuaalisena resurssina. Virtualisoinnilla järjestelmien ja resurssien hallitseminen helpottuu riippumatta siitä, millainen niiden ulkoasu tai tekniikka on. Virtualisoinnilla saavutetaan monia etuja, mutta sen hyödyntämistä vaikeuttavat monet erilaiset virtualisointitavat.

Virtualisointiohjelmistolla muodostetaan yksi tai useampi työasema fyysiselle koneelle riippuen tämän koneen käytössä olevista resursseista, kuten kovalevytilasta, prosessorin kapasiteetista, verkkokorteista ja RAM-muistin määrästä. Virtualisointiohjemistolla luotujen virtuaalikoneiden avulla on mahdollista suorittaa useita käyttöjärjestelmiä, kuten kaikkia versioita Microsoft Windowsista, MS-DOSista ja Linuxista. Virtuaalikoneet voivat keskustella fyysisen isäntänsä ja muiden samassa verkossa olevien koneiden kanssa, aivan kuin ne olisivat tavallisia yksittäisiä fyysisiä koneita. (Ruest & Ruest 2009, 24.)

Fyysisten koneiden osioinnin juuret ovat 1960-luvulla, jolloin IBM alkoi osioida palvelimiaan suorittaakseen useita käyttöjärjestelmiä samalla laitteella. Tuolloin osiointia käytettiin ajamaan useita rinnakkaisia käyttöjärjestelmiä samanaikaisesti. 1990-luvulla fyysisten järjestelmien osiointi nimettiin virtualisoinniksi. Aluksi virtualisointia käytettiin suorittamaan eri käyttöjärjestelmiä toisella alustalla, kuten Microsoft Windowsia Applen Macintoshissa. Vuonna 2003 Microsoft hankki ranskalaisen yrityksen nimeltä Connectix, joka erikoistui Windows-käyttöjärjestelmän suorittamiseen Macintosh-koneissa. Tämän ansiosta Macintosh-käyttäjät pääsivät käsiksi tuhansiin Windows-alustalle suunniteltuihin sovelluksiin. (Ruest & Ruest 2009, 24.)

VMware Corporation oli kuitenkin työskennellyt virtuaalisoinnin kanssa jo 1990-luvun lopulta asti ottamalla käyttöön VMware Workstationin. VMware Workstation oli loppukäyttäjille suunniteltu ohjelmisto, joka oli kehitetty suorittamaan useita eri 32-bittisiä käyttöjärjestelmiä. Silloin VMware ymmärsi virtuaalisoinnin mahdollisuudet ja siirtyi palvelintasolle aloittaen suuren noususuhdanteen koneiden virtuaalisoinnissa. Tämä on nähtävissä myös tänä päivänä, sillä nykyään VMware on markkinoiden johtava virtualisointipalveluiden tarjoaja. VMwarella on laaja valikoima datakeskusten virtualisointiin liittyviä tuotteita. (Ruest & Ruest 2009, 25.)



Kuva 1. Havainnekuva virtuaalisoinnista. (CommVerge 2015)

Virtualisointiteknologia on kehittynyt alkuajoistaan niin paljon, että datakeskukset voivat käyttää sitä hyväkseen useilla eri tasoilla. Useimmin virtualisoituja tasoja ovat laskenta- ja tallennuskapasiteetit. Erilaisia asiointitasoja ovat esimerkiksi laitteisto-, työpöytä-, ohjelmisto-, muisti-, tallennus-, data- ja verkkovirtualisointi. Virtualisointi on tekniikka, jolla osioidaan tietokone useaksi itsenäiseksi koneeksi, jotka pystyvät ylläpitämään erilaisia käyttöjärjestelmiä ja sovelluksia samanaikaisesti. Tällä tavoin fyysisten koneiden resursseja saadaan hyödynnettyä paremmin. Kone, joka toimii käyttäen vain kymmentä prosenttia resursseistaan, voidaan muuntaa koneeksi, jonka käyttöaste nousee 60–80 prosenttiin käyttämällä siinä useampaa virtuaalista konetta. Taustalla oleva hypervisorhallintaohjelmisto toimii suoraan laitteistolta ja hallinnoi useita käyttöjärjestelmiä virtuaalikoneessa. Tällä tavoin jokainen käyttöjärjestelmä, joka suoritetaan virtuaalikoneessa, tulee omavaraiseksi toimintaympäristöksi toimien hypervisorin päällä ja käyttäytyy kuin se olisi erillinen tietokone. (Ruest & Ruest 2009, 30.)

Virtuaalikoneet on tehty useista komponenteista, joihin yleensä kuuluvat käyttöjärjestelmä, VMware tools sekä virtuaaliset resurssit ja laitteistot, joita voi hallita suurelta osin samalla tavalla kuin fyysisiä laitteita. Virtuaalisen käyttöjärjestelmän asennus on pohjimmiltaan fyysistä asennusta vastaava. Virtuaalisen käyttöjärjestelmän asennukseen tarvitaan levykuva, joka sisältää asennettavat tiedostot. Fyysinen laitteisto määrittää virtuaalikoneen tuetut ominaisuudet, kuten BIOSin, suorittimien maksimimäärän, suurimman muistin koon ja muut laitteistojen tyypilliset ominaisuudet. Virtuaalikoneen laitteiston versio määräytyy sen mukaan, mikä ESXi:n versio virtuaalikoneeseen on asennettu. (VMware haku 2013.)

Vaikka fyysinen kone tarvitsisi vain kymmenen prosenttia resursseistaan, kuluttaa se täyden määrän virtaa, tarvitsee täyden jäähdytyksen ja suuren määrän tilaa datakeskuksissa ympäri maailman. Sen sijaan hyvin määritelty virtualisoitu palvelin voi suorittaa samoilla ominaisuuksilla yli kymmentä virtuaalista konetta, palvelinta tai työpöytää tarvitsematta kuitenkaan jokaiselle koneelle omaa virtaa, eivätkä kaikki vaadi omaa tuuletusta tai tarvitse omaa tilaa. Silti kaikki koneet pystyvät tarjoamaan saman kuin fyysisessä-

kin muodossa. Jokainen kone on vain joukko tiedostoja kansiossa. Tässä muodossa kone on helppo siirtää palvelimelta toiselle, sulkea, käynnistää uudelleen tai tehdä mitä tahansa kuin normaaleillekin koneille. (Ruest & Ruest 2009, 34.)

Virtualisointia hyödynnetään organisaatioissa useilla eri tavoilla heille luotujen toimintamallien mukaan. Virtualisointi nousee esille usein silloin, kun organisaation laitteisto alkaa käydä vanhaksi ja tulee aika ostaa uusia laitteita. Tällöin siirtyminen virtualisointiin usein tulee ajankohtaiseksi, ja sen toteuttaminen on helpompaa. Virtuaalisoinnilla organisaatio saa vakautta laitteiston resursseihin, lyhennettyä huoltoaikoja, helpotusta myöhempiä muutostöitä varten sekä mahdollisuuden vapaampaan ylläpitoon ja paljon joustavuutta. Virtualisoinnilla mahdollistetaan laitteiden sijoittaminen muihin tiloihin, kuitenkin säilyttäen työasemaympäristöjen muokattavuus. Tämän lisäksi virtualisoinnilla annetaan lisää varmuutta sekä turvatoimia ilman suuria kustannuksia. (Williams & Garcia 2007, 40, 41.)

2.1 Virtualisoinnin muotoja

Virtualisoinnin tyyppejä on olemassa kolmea erilaista, nämä muodot ovat palvelin-, työpöytä- ja sovellusvirtualisointi. Palvelinvirtualisointi on näistä kolmesta tyypistä kaikkein laajin ja organisaatioissa kaikkein yleisin virtualisointityyppi. Palvelinvirtualisoinnin ansiosta yhdellä fyysisellä palvelimella pystytään ajamaan useampaa virtuaalista palvelinta. Työpöytävirtualisointi tarkoittaa koko työpöydän virtualisoimista. Virtualisoitua työpöytää voidaan ajaa etänä palvelimelta. Tällöin käytetyllä fyysisellä päätelaitteella ei ole niin suurta merkitystä, koska prosessointi siirtyy palvelimille. Sovellusvirtualisoinnilla kapseloidaan sovelluksia toimimaan käyttöjärjestelmästä ja sen muista ohjelmista. Tämä tekee sovelluksista täysin siirrettäviä, eikä sovelluksessa tapahtuva virhe vaikuta ollenkaan käyttöjärjestelmään. Sovellusten virtualisointi vaatii kuitenkin erillisen virtualisointikerroksen.

2.1.1 Palvelinvirtualisointi

Palvelinvirtualisoinnin muotoja on olemassa kahta tyyppiä. Ohjelmistovirtualisointia käytetään usein virtualisointiprojektien alussa, koska se pohjautuu helppoihin ja usein ilmaisiin tekniikoihin. Kyseinen tekniikka on hieman tehottomampi, koska taustalle tarvitaan aina isäntäkäyttöjärjestelmä. Tämä käyttöjärjestelmä tarvitsee resursseja, jotka myös suorittavat virtuaalikoneita sisällään. Tästä syystä organisaatiot eivät käytä tätä muotoa muuhun kuin testaamiseen ja kehitykseen. (Ruest & Ruest 2009, 32.)

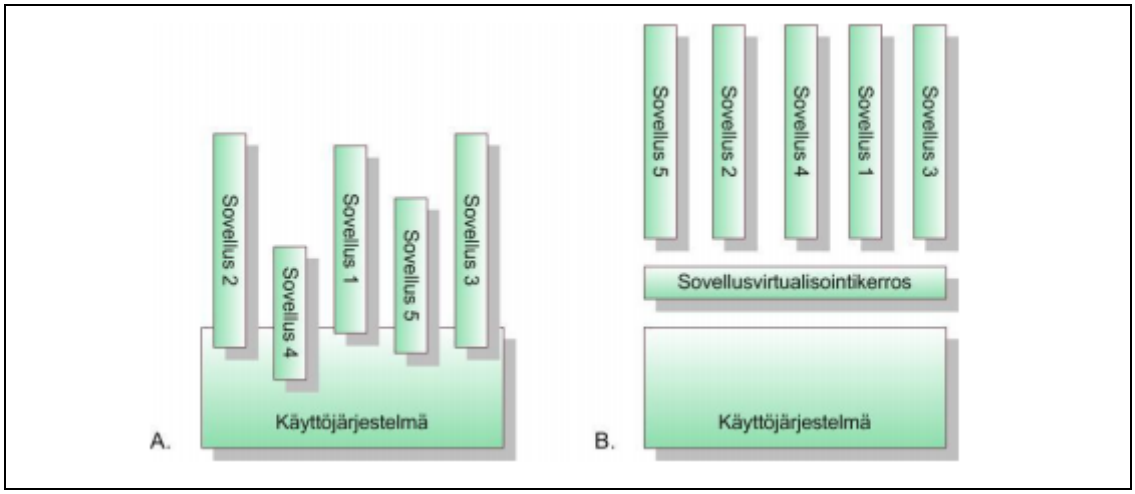
Toinen tyyppi on laitteistovirtualisointi. Tällöin hypervisorin koodi integroidaan suoraan laitteistoon ja näin virtuaalikoneiden asentaminen onnistuu ilman isäntäkäyttöjärjestelmää suoraan laitteeseen, lähelle fyysisiä resursseja. Tämä mahdollistaa mahdollisimman monen virtuaalikoneen suorittamisen. Kun virtuaalikoneiden isäntä ei sisällä normaalia käyttöjärjestelmää, se ei vaadi yhtä usein päivittämistä. Tämä minimoi hypervisorin vaikutuksen koneisiin, joita se hallitsee. (Ruest & Ruest 2009, 32, 33.)

2.1.2 Työpöytävirtualisointi

Samaa tekniikkaa, joka suorittaa palvelinvirtualisointia, voidaan käyttää myös työpöytien virtualisoinnissa. Työpöytävirtualisointi keskittää työasemien käytön siten, että saadaan täysi hallinta niistä sallien käyttäjiä pitämään useita päätteitä, joista on pääsy virtuaaliympäristöön. Vaikka yhdessä virtuaalityöpöydässä tapahtuu jotain ikävää, se ei vaikuta muihin samalla palvelimella suoritettaviin työpöytiin. Virtuaalisoiduilla työpöydillä on mahdollista testata päivityksiä ja huoltopaketteja tai tarjota koulutusta loppukäyttäjille ja teknikoille. Kun testaus tai harjoittelu tulee päätökseen, on virtuaalikone helppo palauttaa alkutilaan ja aloittaa alusta. (Ruest & Ruest 2009, 39.)

2.1.3 Sovellusvirtualisointi

Sovellusvirtualisoinnin avulla sovellus kapseloidaan toimimaan erillään käyttöjärjestelmästä ja muista sen ohjelmista. Sovellus-virtualisointi tuo sovelluksen tai palvelun paketoituna erillisen virtualisointitason läpi käyttöjärjestelmään. Se vaatii toimiakseen erillisen käyttöjärjestelmän. Sovellusvirtualisointi suojelee käyttö-järjestelmää kaikilta muutoksilta, joita sovelluksen asennuksen yhteydessä voi tapahtua. VMware tarjoaa ratkaisua, joka ei tarvitse lainkaan agenttiohjelmaa kohteen työpöydällä toimiakseen. Tämä vapauttaa sovellukset kaikilta sidoksilta ja tekee niistä täysin siirrettäviä, joten samojen ohjelmien eri versioita voidaan ajaa samanaikaisesti. Virtualisoidut sovellukset toimivat kaikissa Windowsin versioissa. (Ruest & Ruest 2009, 40, 42, 43, 273.)



Kuva 2. Sovellusten käyttäytyminen (A) ilman sovellusvirtualisointia ja (B) sovellusvirtualisoinnilla. (Ruest & Ruest 2009, 43.)

2.2 Hyödyt

Virtualisoinnin suurin hyöty on raha, jota säästää virtualisoimalla niin pienissä kuin suurissakin organisaatioissa. Virtualisoitu järjestelmä tarvitsee vähemmän fyysisiä laitteita, minkä takia jäähdytyksen ja tilan tarve vähenee sekä sähkönkulutus laskee.

Virtualisoitu järjestelmä on myös siirrettävyydeltään parempi. Virtuaalipalvelimet eivät paina mitään, koska ovat vain kasa tiedostoja. Virtuaalipalvelimen siirtäminen fyysisestä palvelimesta toiseen on helppoa, kun esimerkiksi vanha palvelin rikkoutuu tai siirrytään uudempaan. Virtuaalipalvelimen siirto onnistuu fyysiseltä palvelimelta toiselle ilman sammuttamista, tämä mahdollistaa palvelimen siirron jopa toimipisteestä toiselle vain asennuskansiota siirtämällä. Myös laitesalin muutossa vähempi määrä fyysisiä laitteita on helpompi siirtää vaikkapa toiseen rakennukseen. Virtualisointi mahdollistaa palvelimen pystyttämisen huomattavasti fyysistä nopeammin ja jopa kokonaan etätyönä.

Virtualisoidessa saadaan fyysisten koneiden resursseja hyödynnettyä paremmin. Kone joka toimii käyttäen vain kymmenen prosenttia resursseistaan, voidaan muuntaa koneeksi jonka käyttöaste nousee 60–80 prosenttiin käyttämällä siinä useampaa virtuaalista konetta. Kun olemassa olevia resursseja hyödynnetään paremmin, tarvittavia laitteita voidaan vähentää, ja niiden tarvitsemien huoltosopimuksien määrää laskea. Näin laitteiden jättämä hiilijalanjälki pienenee, kun ilmastoinnin ja sähkön tarve laskee, tämä näkyy myös pienempinä kustannuksina. (Ruest & Ruest 2009, 30.)

Ohjelmistosuunnittelijoille virtuaalisoinnista saadaan suuri hyöty ohjelmistojen testauksessa. Kehitettäviä ohjelmistoja tai ohjelmistojen päivityksiä pystytään testaamaan turvallisessa ympäristössä ennen niiden jakamista loppukäyttäjille. Testiympäristöistä saadaan identtisiä tai erilaisia. Virtuaalikoneeseen tullut vika on helppo korjata palauttamalla kone, tilanteen tallentavien tilannekuvien avulla, virhettä edeltäneeseen tilaan. Virtuaalikoneesta on myös mahdollista ylläpitää peilattua kopiota, joka on heti käytettävissä, jos päävirtuaalikoneeseen tulee ongelmia.

Samassa fyysisessä koneessa sijaitsevat virtuaaliset koneet ajattelevat käyttävänsä omia resurssejaan. Myös erillisiä verkkoja voidaan rakentaa virtualisointitekniikoilla. Virtuaalikoneiden muokkaaminen tapahtuu vain liu-

kusäädintä siirtämällä, mikä tekee resurssien uudelleen jakamisesta helppoa ja nopeaa.

2.3 Uhat

Tietoturva pitää ottaa huomioon jo virtualisointia suunnitellessa. Perinteisten palvelinten rinnalle voi lisätä kytkimiä ja palomuureja. Kun palvelimia virtualisoidaan, ne asetetaan usein samaan virtuaaliseen verkkosegmenttiin. Tällöin palvelinten rinnalle ei pysty enää asentamaan tavallisia kytkimiä ja palomuureja, mutta virtuaaliverkkoon voi kuitenkin ottaa käyttöön samoja suojaratkaisuja. Se vaatii kuitenkin asiaan perehtymistä, mikä tuo lisäkustannuksia.

Virtualisoidessa usein ajatellaan vain kustannussäästöjä ja tällöin on vaarana, että tietoturva jää vähäiseksi tai unohtuu jopa kokonaan. Myyntimiesten lupaamat hurjat kustannussäästöt laskevat kuitenkin nopeasti, kun lisätään edes vähän tietoturvaa. Tämä voi asettaa tietoturvan toissijaiseksi jos keskitytään vain säästöihin. (Tietoviikko 2013a.)

Tutkimusyhtiö Gartnerin (Gartner 2010.) tutkimuksen mukaan 60 prosenttia virtuaalipalvelimista ei yllä tietoturvan puolesta samalle tasolle kuin fyysiset palvelimet, joita korvataan virtuaalipalvelimilla. Tutkimusyhtiö kuitenkin uskoo, että parin vuoden kuluttua virtuaalipalvelinten tietoturva on kohentunut huomattavasti, ja vuonna 2015 enää 30 prosenttia virtuaalipalvelimista on fyysisiä palvelimia heikommin tietoturvattuja. (Tietoviikko 2013b.)

Työpöytien virtualisointi tehdään yleensä lataamalla työpöytä ja käyttöjärjestelmä valmiista levykuvasta. Tällöin yleisenä vaarana on, että tätä levykuvaa päivitetään aivan liian harvoin. Käynnissä oleva työpöytä toki päivittyy, mutta kun työpöytä joudutaan käynnistämään uudelleen, voivat tietoturvapäivitykset olla jopa puoli vuotta vanhoja. Vaikka työpöytä alkaa päivittymään heti, se on jonkin aikaa verkossa ilman asianmukaista suojaa.

Täydellisten tietoturvapäivitysten saaminen voi kestää tunteja. (Tietoviikko 2013b.)

Virtualisointiin siirtyminen voi aluksi olla melko kallista. Virtualisoinnin ajamiseen ja hallintaan tarvitaan tehokas laitteisto, joka on jo itsessään kallis. Lisäksi kustannuksia syntyy mahdollisesti tarvittavista tallennusjärjestelmistä ja verkkolaitteista. Käyttöjärjestelmien, ohjelmistojen ja sovellusten lisensoiminen vaatii myös resursseja. (Williams & Garcia 2007, 12–13.)

Vaikka huoltosopimusten määrä laskee, ylläpidon tarve laitetta kohti kasvaa. Tarve tehokkaalle ylläpidolle kasvaa laitteiden määrän mukaan. Ylläpitoa varten on toki olemassa erilaisia hallintatyökaluja, joista on apua. Työkaluista tulee lisää kuluja, eikä niitä ole suunniteltu suoraan sopivaksi tietylle yritykselle. Yritys voi palkata ohjelmistokehittäjiä kehittämään juuri sille sopivia hallintatyökaluja, joilla saadaan manuaalisen ylläpidon tarvetta laskettua.

2.4 Ongelmat

Virtualisointi voi mennä pieleen jo suunnitteluvaiheessa, jolloin sillä haettuja säästöjä ei saadakaan. Parhaiden tulosten saavuttamiseksi tarvitaan osaavaa työvoimaa usealle osa-alueelle, kuten suunnitteluun, ylläpitoon ja ongelmatilanteiden ratkaisuun. Joidenkin ohjelmistojen lisensointi määräytyy isäntäkoneen suorittimen ydinten määrän mukaan, vaikka virtuaalikoneen käytössä olisi vain osa ytimistä.

Ongelmat lisensoinnissa on vähitellen poistumassa, koska ohjelmistojen tuottajat ovat ymmärtäneet virtuaalisoinnin tulevan yhä suositummaksi. Kaikkia sovelluksia ei ole kehitetty toimimaan virtuaalisessa ympäristössä, joten ongelmatilanteissa ei välttämättä heti ilmene, johtuvatko ongelmat sovelluksesta tai virtuaalisesta ympäristöstä. Kaikkiin ohjelmiin ei välttämättä ole saatavissa asiakastukea, jos niitä suoritetaan virtualisoidussa ympäristössä.

3 VMWARE

VMware, Inc. on amerikkalainen ohjelmistoyritys, joka tunnetaan parhaiten virtuaalisoinnin ja pilvipalveluiden saralla. Yrityksen ohjelmistot mahdollistavat useiden virtuaaliympäristöjen ja virtuaalikoneiden luomisen. Esimerkiksi yksi fyysinen tietokone tai palvelin voi ylläpitää useita virtuaalisia järjestelmiä, joskus jopa yli sataa. Yrityksille erityisen hyödyllistä on mahdollisuus luoda useita palvelinjärjestelmiä ilman tarvetta hankkia jokaiselle järjestelmälle omaa laitteistoa. Tämä säästää paljon aikaa, rahaa ja tilaa.

VMware julkaisi ensimmäisen tuotteensa toukokuussa 1999, tämä ohjelmisto oli VMware Workstation. VMware laajensi pilvipalvelumarkkinoille huhtikuussa 2011, kun yritys julkaisi tuotteen nimeltä Cloud Foundry. Nykyään VMware kehittää ja markkinoi useita virtualisointiin liittyviä ohjelmistoja suurimmaksi osaksi yrityksille, mutta yksityiset käyttäjät voivat hyödyntää joitakin yrityksen ohjelmistoja.

Virtualisointi mahdollistaa useamman käyttöjärjestelmän toimimisen yhdellä fyysisellä alustalla. Virtualisointi mahdollistaa säästöjä hankintakustannuksissa ja ylläpidossa. Virtuaalikoneet vaativat vähemmän fyysisiä tietokoneita kuin tavalliset, koska virtuaalisia koneita saa useamman yhteen fyysiseen koneeseen. Vikasietoisuuden takaamiseksi tarvitaan kuitenkin edelleen erillinen fyysinen tietokone. Koska fyysisiä laitteita tarvitaan vähemmän, säästetään tilaa, sähköä ja ilmastointikuluja. Virtuaalisoinnilla pystytään myös hyödyntämään tietokoneiden resurssit paremmin.

Virtualisointi keskittyi alkutaipaleellaan vain järeisiin palvelimiin, mutta on viime aikoina alkanut yleistyä myös kevyemmissä työasemissa. Virtuaalikoneet ovat myös yhä enemmän muuttuneet laitteistoon ja käyttöjärjestelmiin integroiduiksi ominaisuuksiksi, jotka tarjoavat näin aiempaa suorituskykyisemmän ja yhteensopivamman alustan usean käyttöjärjestelmän käyttämiseen. Tämä tarkoittanee sitä että VMware ja muut virtualisointiratkaisut muuttunevat yhä enemmän vain virtuaalisoinnin hallintaohjelmiksi.

3.1 Mahdollisuudet

Uusien ominaisuuksien ja palveluiden määrä kasvaa VMwaren tuotteissa nopeassa tahdissa. VMware on lisännyt jokaisen uuden version myötä paljon uusia ominaisuuksia, joiden käyttöönotto on tehty yksinkertaiseksi. Virtuaalisoinnin myötä palvelinfilosofia muuttuu dynaamisemmaksi, mikä voi mahdollistaa virtuaalikoneiden tehokkuuden optimointia. Palvelinten hyötykäyttösuhde paranee ja rahaa säästyy etenkin sähkönkulutuksen kannalta.

Yrityssovellus on päivittäistä laskentaa. Asiakkuuksien koon mukaan on palvelinten suorituskyky ainoastaan rajana. Virtualisointi VMwaren tuotteilla mahdollistaa asiakkuuksien profiloinnin resurssitarpeiden mukaan ja erittelee asiakkuudet täysin omiksi yksiköikseen. Kaikki palvelut voidaan pitää omina virtuaaliympäristöinään, näin erotetaan palvelut ja asiakkuudet paremmin toisistaan.

3.2 Tuotteet

VMware vSphere, joka aiemmin tunnettiin nimellä Infrastucture, on nimitys VMwaren tuoteperheen kokonaisuudelle. vSphere on kokonaisuus teknologioita ja tuotteita, joilla virtualisointi toteutetaan täydellisesti x86-arkkitehtuurin laitteissa. vSphere on kuin Microsoft Office -paketti, johon kuuluu monia ohjelmia kuten MS Excel, MS Word, MS Access ja niin edelleen. Kuten Office-paketti, niin myös vSphere on kokoelma tuotteita, joita ovat esimerkiksi ESXi, ThinApp, vCenter ja niin edelleen. vSphere on siis vain nimi paketille, joka sisältää erilaisia komponentteja.

VMware ESXi on VMware-tuoteperheeseen kuuluva tyypin 1 hypervisor, joka toimii suoraan fyysisen laitteen päällä ja omaa suoran pääsyn palvelinten resursseihin. Kaikki virtuaaliset koneet asennetaan ESXi:lle. Asennus, hallinnointi ja pääsy näille virtuaalikoneille, jotka ovat ESXi:llä, vaatii toisen osan vSphere-paketista. Tarvittava osa on vSphere Client. Kun vSphere

Client on asennettu, mahdollistaa se järjestelmänhallitsijan yhdistämisen ESXi:lle. (TechTarget 2013a.)

VMware Workstation on VMware tuoteperheeseen kuuluva ohjelmisto, jolla järjestelmänhallitsija voi luoda ja ajaa virtuaalikoneita suoraan työpöydältä. Workstationin avulla voidaan ajaa yhden fyysisen koneen päällä yhtä tai useampaa virtuaalista konetta. Jokaisessa näissä virtuaalikoneessa voi toimia eri käyttöjärjestelmä. Joten esimerkiksi Windowsin ajaminen omassa ikkunassa Linuxin työpöydällä on mahdollista. VMware Workstationista on tarjolla myös ilmainen tutustumisversio VMware Player. Player on kuitenkin karsittu versio Workstationista. VMwaren pääkilpailija on Oraclen ilmainen VirtualBox. (TechTarget 2013b.)

VMware ThinApp, joka aiemmin tunnettiin nimellä ThinStall, on VMwaren tuoteperheeseen kuuluva agentiton ohjelmisto sovellusvirtualisoinnin toteuttamiseen. Agentiton sovellusvirtualisointi mahdollistaa ThinApp-ohjelmistolla paketoitujen sovellusten jakamisen ilman erillisten agenttiohjelmien asentamista käyttäjän koneille. (Ruest & Ruest 2009, 292.)

ThinApp paketoi kokonaisen Windows-sovelluksen tiedostot ja sen asetukset yhdeksi paketiksi. Järjestelmän ylläpitäjä voi asentaa, hallita ja päivittää ThinApp-paketteja itsenäisesti. Virtualisoidut sovellukset eivät tee mitään muutoksia taustalla toimivaan isäntäkäyttöjärjestelmään. Sovellusvirtualisointi ThinAppilla poistaa sovelluksen ja käyttöjärjestelmän välisen yhteensopivuus ongelman. (VMware verkkosivut 2013.)

Näin sovelluksen kopioiminen toiselle koneelle vastaa lähinnä kansion kopioimista. Sovellusten päivittäminen tapahtuu yksinkertaisesti vain korvaamalla vanha sovellus päivitetyllä sovelluksella, tätä varten ThinApp sisältää ohjelman nimeltä AppSync. AppSync päivittää automaattisesti paketoidut sovellukset, jos sovelluksen *.ini-tiedostoon määritelty lähdeosoite on tismalleen oikea.

VMware NSX on VMwaren tietoverkon virtualisointi- ja suojausohjelmistoperhe. NSX:n tarkoitus on järjestää virtuaalisia tietoverkkoympäristöjä luomalla, jakamalla, snapshoteilla, poistamalla ja palauttamalla monimutkaisia tietoverkkoja ohjelmiston avulla. NSX mahdollistaa datakeskusten operaattoreita saavuttamaan kokoluokkaa paremman nopeuden, taloudellisuuden ja valikoiman. (VMware verkkosivut 2013.)

Virtuaalikone on kokoelma ohjelmia, jotka esittelevät loogisen suorittimen, muistin ja tallennuskapasiteetin sovelluksille. Näin toimii myös virtualisoitu tietoverkko, se esittää loogiset tietoverkon komponentit, kytkimet, reitittimet, palomuurit ja paljon muuta kytketyille laitteille. Tietoverkko sekä suojauspalvelut on jaettu ja liitetty virtuaalikoneisiin verkkoyhteydellä.

4 VIRTUAALIYMPÄRISTÖN TIETOTURVA

Virtualisoinnissa tietoturva-aukkoja on mahdollista hyödyntää useilla eri tavoilla. Virtualisointi ei itsessään poista haavoittuvuuksien uhkaa sovelluksista. Haavoittuvuudet ovat hyödynnettävissä samaan tapaan kuin perinteisissäkin ratkaisuissa. Myös sillä, suoritetaanko virtuaalisoituja sovelluksia normaalin käyttäjän vai järjestelmänvalvojan oikeuksin, on edelleen merkitystä. (Hoppe & Seeling 2010, 294–295.)

Normaalissa käyttäjätilissä haavoittuvuuksia hyödyntävä hyökkääjä saa vastaavat oikeudet ja pääsyn resursseihin, jotka käyttäjälläkin alun perin on. Hyökkääjä pystyy myös tarkkailemaan käyttäjän tekemisiä etäyhteyden DLL-injektiohyökkäyksellä, kun koodia sisältävä DLL-tiedosto pakotetaan prosessin osoiteavaruudessa latautuvaksi. Tällainen yhteys on kuitenkin mahdollista katkaista vain sulkemalla kyseinen virtuaalisovellus. (Hoppe & Seeling 2010, 294–295.)

Järjestelmänvalvojan oikeuksin käynnistetty virtuaaliohjelma saa automaattisesti vastaavat järjestelmänvalvojan oikeudet, jolloin mahdollinen hyökkääjä saattaa käyttää tietoturva-aukkoa ja saa myös järjestelmänvalvojan oikeudet. Tässä tapauksessa järjestelmänvalvojan oikeudet omaava hyökkääjä pystyy muuttamaan, luomaan ja jopa poistamaan tietoja kyseisestä koneesta. (Hoppe & Seeling 2010, 294–295.)

Sovellusvirtuaalisoinnin agentittomat ja agenttipohjaiset menetelmät eroavat toisistaan tietoturvassa. Agenttipohjaisen menetelmän suojaamiseksi on mekanismi, koska virtualisoidut sovellukset eivät käynnisty ilman tarvittavaa agenttiohjelmaa. Jos sovellusvirtualisointiohjelmisto on agenttipohjainen, kaikki sovellukset ovat suojattuja. Agenttipohjaisessa sovellusvirtuaalisoinnissa agenttiohjelma ja sovellusvirtualisoitu sovellus ovat erikseen, joten pelkällä sovellusvirtualisoidulla sovelluksella ei hyökkääjä yksinään tee vielä mitään. Agentittomat sovellukset sen sijaan ovat täysin siirrettävissä, joten ne ovat helposti kopioitavissa ja käytetettävissä missä tahansa

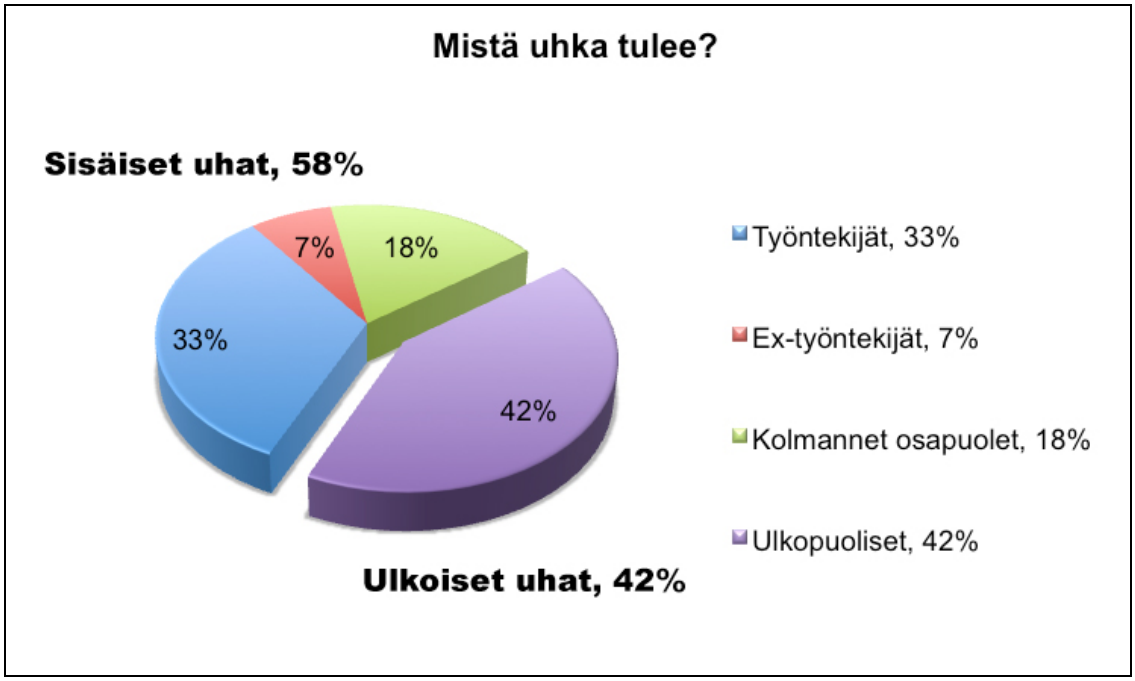
järjestelmässä. Sovelluksia on pyrittävä suojaamaan muillakin keinoin lisenssien leviämisen estämiseksi. (Ruest & Ruest 2009, 277–278.)

Virtualisoiduissakaan sovelluksissa ei kannata unohtaa tietoturvan merkitystä. Koska virtualisoitu sovellus on aina jollain tapaa vuorovaikutuksessa isäntäkoneeseen, on se haavoittuvainen tietoturvaongelmille. Virtualisoidussa sovelluksessa on siis omat riskinsä verrattuna sovelluksiin, jotka on asennettu työasemaan perinteisellä tavalla. Virtualisoitujen sovellusten määrän kasvaessa on erittäin tärkeää käyttää samoja yleisiä tietoturvatapoja ja -menetelmiä, joita ei pysty millään tavalla laiminlyömään tai ohittamaan. (Ruest & Ruest 2009, 294–295.)

4.1 Uhat

Tietoturvan kannalta järjestelmien suurin uhkatekijä on sen käyttäjät. Käyttäjille sattuvat inhimilliset virheet, vähäinen koulutus ja heikko tuntemus tietoturvasta altistavat järjestelmiä tietoturvariskeille. Clearswiftin (Clearswift, 2015.) teettämän tutkimuksen mukaan kolmannes organisaatioiden tietoturvauhista syntyy sen omista työntekijöistä.

Nykypäivänä haasteita tietoturvaan luovat uuden tyyppiset hyökkäykset. Hyökkäykset kohdennetaan organisaatioihin. Niiden motivaattorina toimii raha, jota tehdään hyökkäyksissä saaduilla tiedolla. Hyökkäykset kohdennetaan tietoturva-aukkoihin, joita syntyy kun käytetään vanhentuneita käyttöjärjestelmiä ja ohjelmistoja. Oman uhkakuvansa virtuaalisessa käyttöympäristössä luo hypervisorin haavoittuvuus. Kun hypervisor on haavoittuvainen, luo se pääsyn virtuaalipalvelimelle.



Kuva 3. Clearswiftin tutkimuksen tulos tietoturvauhista. (Clearswift 2015.)

4.1.1 Tietomurrot

Ylläpitäjä voi vaikuttaa tietomurtoihin pitämällä palvelimien ohjelmistot päivitettyinä ja oikein säädettyinä. Palvelimen ylläpitäjän on hyvä suorittaa koehyökkäyksiä omaan ympäristöönsä, jotta mahdolliset aukot havaitaan ja korjataan. Isommat yritykset voivat myös kerätä tietoa mahdollisista riskeistä ulkopuolisten henkilöiden avulla. Tähän voidaan käyttää vaikka avoimia nettilomakkeita kotisivuilla tai käyttämällä www-hakukoneita yhdessä yrityksen nimen ja jonkin avainsanan kanssa. Avainsanoiksi voidaan mieltää jokin tietomurtoon tai hakkerointiin liittyvä sana. Tämän haun avulla voi mahdollisesti paljastua keskustelupalstoja tai muita sosiaalisia medioita, missä henkilöt ovat jakaneet tietoa aukoista. (Hacking Through Complexity verkkosivut 2013.)

Tietomurtojen mahdollisuus pysyy aina pienempänä, kunhan muistetaan pitää huoli ettei tietokoneissa ole haavoittuvuuksia, joita hyökkääjät voivat käyttää hyödykseen. Mahdollisiin tietovuotoihin on syytä reagoida nopeasti ja tarvittaessa muuttaa ja päivittää tietoturvaa. Pahimpia vahinkoja estämään riittävät ajan tasalla oleva palomuuri ja virustorjunta sekä koneiden

oikeaoppinen käyttö. Erilaisten tarkistuksien käyttäminen parantaa mahdollisten haittaohjelmien löytymistä, vaikka usean tarkistuksen yhtäaikainen käyttö ei ole suotavaa.

Käyttämällä salauksia ja säilyttämällä tietoja asianmukaisesti, tietomurtojen tekeminen vaikeutuu. Salaus ei kuitenkaan saisi olla liian yksinkertainen tai se murretaan nopeasti. Myös tarpeettomien, mutta arkaluonteisten tietojen poistaminen tietokoneelta tai verkkopalvelusta kannattaa tehdä pikimmiten.

4.1.2 Kaappaukset

Palomuureja, modeemeja, kytkimiä ja reitittimiä on mahdollista etäkonfiguroida. Tämä luo riskin, että hyökkääjä voi muokata käyttäjän laitteiston asetuksia haluamallaan tavalla ja esimerkiksi avata itselleen pääsyn sisäverkkoon internetin yli. Myös verkkoliikenteen seuranta ja tallennus voi onnistua kaapatulta verkkolaitteelta. Riskinä on, että hyökkääjä pääsee käsiksi verkossa liikkuvaan dataan.

4.1.3 Estohyökkäykset

Palvelunestohyökkäyksessä käyttäjän palvelu lamautetaan niin, että sen käyttö häiriintyy tai estyy kokonaan. Hyökkäyksessä lähetetään kohteeseen niin paljon dataa, ettei se pysty enää käsittelemään muita verkkopyyntöjä. Tämäntapaisia hyökkäyksiä käytetään yleensä verkkopalvelimia kohtaan tarkoituksena lamauttaa palvelimien sujuva toiminta. Hyökkäyksellä ei siis varsinaisesti pyritä varastamaan mitään.

Botnet-verkkojen avulla hyökkääjä voi tukkia sähköpostipalvelimen roskapostilla tai lähettää jollekin WWW-palvelimelle niin paljon sivunlatauspyyntöjä, että palvelin ei pysty vastaamaan kaikkiin pyyntöihin.

4.2 Edistävät vaikutukset

Paras tapa edistää tietoturvaa on ennaltaehkäisevä toiminta. Ennaltaehkäisevä toiminta kannattaa aloittaa luomalla tietoturvasuunnitelma. Suunnitelman tulisi sisältää ainakin tiedot siitä mitä, miten ja miksi suojataan. Suunnitelmaa tulisi myös päivittää tietyin väliajoin.

Arkaluonteisten materiaalien poistaminen työasemilta ja siirtäminen suojattuun sekä keskitettyyn palvelinjärjestelmään auttaa lisäämään tietoturvaa. Keskitetty palvelinjärjestelmä on helpompi suojata, eikä yhden työaseman saastuminen vaaranna tietoja.

Virtuaalikoneilla voidaan helposti tutkia haittaohjelmien käyttäytymistä ja kehittää parempia menetelmiä niiden torjumiseksi. Virtuaalikone voidaan testien jälkeen palauttaa jälleen lähtötilanteeseen. Virtuaalikoneen valvoja hallitsee kaikkia koneen käytössä olevia resursseja, näin virtuaalikoneen valvominen helpottuu.

Haittaohjelmilta suojautuminen toteutetaan yleensä virustorjuntaohjelmistoilla. Tämä ei kuitenkaan yksinään enää riitä, koska haittaohjelmat kehittyvät nopeasti ja niitä syntyy entistä tiheämpää tahtia.

Virtualisointiratkaisut tukevat tilan palauttamista aiempaan hetkeen, josta voi löytyä tallessa jo hävinneeksi luultuja tietoja. Samalla periaatteella on myös helpompi toipua tietomurroista, kun kone voidaan usein palauttaa murtoa edeltävään tilaan ja tehdä koneeseen tarvittavia muutoksia murron toistumisen estämiseksi.

4.2.1 Fyysinen turvallisuus

Vaikka järjestelmä olisi virtualisoitu, sijaitsee se aina jossain fyysisessä tilassa. Näiden tilojen suojaaminen luo pohjan kaikelle muulle suojautumiselle. Fyysisellä turvallisuudella pyritään estämään tärkeiden tietojen tuhoutuminen, vahingoittuminen tai joutuminen vääriin käsiin. Fyysiset tilat tulisi suojata ainakin seuraavilta uhkatekijöiltä:

- Varkaus
- Tulipalo ja lämpötilan liiallinen kohoaminen
- Vesivahinko ja kosteus
- Sähköhäiriö
- Pöly (Laaksonen 2006, 125-126.)

Ihmisten mukanaan kantamilla laitteilla on erityisen suuri riski joutua valtuuttamattoman tahon haltuun. Varkaudet kohdistuvat yhä enenevissä määrin myös laitteiden komponentteihin ja niiden sisällä olevaan tietoon. Tästä johtuen pääsy fyysisiin tiloihin tulisi rajata myös päiväsaikaan, jolloin osa kiinteistön hälytysjärjestelmästä voi olla kytketty pois päältä. (Laaksonen 2006, 126.)

Fyysinen tila olisi hyvä olla varustettu jonkinlaisella lämpötilojen valvontajärjestelmällä, joka hälyttää lämpötilan muuttuessa radikaalisti. Tämänlaisella valvontajärjestelmällä havaitaan nopeammin ilmastointilaitteiden rikkoutuminen tai mahdollinen tulipalo. Fyysiset tilat olisi syytä eristää muista tiloista niin, että mahdolliset tulipalot ja niistä syntyvä haitallinen savu tai vesivahingot eivät pääse leviämään laitteisiin. (Laaksonen 2006, 127.)

4.2.2 Palomuuri

Palomuuri toimii eräänlaisena liikennepoliisina, joka ohjaa liikennettä laitteen ja internetin välillä. Palomuuri joko sallii tai estää liikenteen, riippuen

sen sisällöstä ja ohjaussäännöistä. Estetystä liikenteestä jää aina merkintä palomuurin lokiin. Palomuuria tarvitaan aina, se suojaa laitetta, käyttäjästä riippumattomista syistä, netistä saapuvalta toivomattomalta liikenteeltä. (Järvinen 2012, 189.)

Palomuurit toimivat yleensä siten, että se estää ulkoverkosta sisään pyrkivän liikenteen, jota ei ole sisäverkosta pyydetty. Yleensä sisältä ulkoverkkoon lähtevä liikenne päästetään aina palomuurista lävitse. Joissain tapauksissa myös sisältä ulos lähtevää liikennettä on rajoitettu, tällä pyritään estämään esimerkiksi työasemille päässeitä haittaohjelmia ottamasta yhteyttä isäntäänsä tai lähettämästä dataa ulos verkosta. (Järvinen 2012, 193-194.)

Palomuuri voi toimia myös erillisenä laitteena. Tällöin palomuurin toiminta on luotettavampi, koska sitä ei voi sulkea ohjelmallisesti. Laitepalomuurista puuttuu myös prosessit, joihin haittaohjelma voisi hyökätä. Ohjelma- ja laitepalomuuria voidaan käyttää myös yhdessä. Tällöin laitepalomuurista läpi päässyt haitallinen yhteyspyyntö pysähtyy koneen omaan palomuuriin. (Järvinen 2012, 190.)

4.2.3 Virustentorjuntaohjelmisto

Virukset, madot ja troijalaiset ovat luvattomien käyttäjien luomia ohjelmia, joilla pyritään vahingoittamaan tietoja tai laitteita. Virustentorjuntaohjelmisto pyrkii suojaamaan laitteita kyseisiltä haittaohjelmilta ja tarvittaessa poistamaan tai eristämään nämä laitteesta ennen kuin ne aiheuttavat vahinkoa. On tärkeää että virustentorjuntaohjelmisto pidetään automaattisesti päivittyvänä. Näin taataan päivittäin syntyvien uusien virusten ja niiden tietojen löytyminen virustentorjuntaohjelmiston virusluettelosta. (Microsoft 2015.)

4.2.4 Varmuuskopiointi

Tärkeät tiedot tulisi aina olla varmistettu tiedostojen varmuuskopioinnilla. Alkuperäinen tieto voi joko tuhoutua odottamattomasti, se voidaan varastaa tai pääsy tietoon estyy laiterikon tai haittaohjelman vuoksi. Varmuuskopioitu tieto löytyy vähintään kahdesta paikasta, jolloin tieto säilyy toisaalla vaikka toisen paikan tiedot menetettäisiin.

Varmuuskopiointi voidaan suorittaa paikallisesti, tällöin kopiot tallennetaan esimerkiksi ulkoiselle kovalevylle, optiselle levylle tai muistitikulle. Kopiointi voidaan suorittaa myös tähän tarkoitetulla ohjelmalla, jolloin kopiointi tapahtuu automaattisesti ja säännöllisesti. (PC Advisor, 2015.)

4.2.5 Salaus ja salasanat

Salausta käytetään muuttamaan luettava tieto muotoon, jota vain valtuutetut osapuolet pystyvät lukemaan. Salausjärjestelmä muuttaa tiedon salatekstiksi salausalgoritmia käyttäen. Salattua tietoa voi tämän jälkeen lukea vain purkamalla salauksen. Salatun tiedon voi purkaa käytännössä vain salausavaimella. (Surveillance Self-Defence, 2015.)

Tietokoneissa ja palveluissa käytetään pääsynvalvonta-mekanismina yleensä käyttäjätunnuksen ja salasanan yhdistelmää. Salasanan avulla käyttäjän henkilöllisyys todennetaan ja sen tarkoituksena on sallia tietolaitteiden, tietoverkkojen, sovellusten ja palveluiden sekä luottamuksellisen tiedon käyttö vain oikeutetuille henkilöille. Käyttäjätunnuksilla käyttäjille luodaan pääsy tiettyihin tietoihin.

4.2.6 Päivitykset

Tietolaitteiden ja sovellusten säännöllisellä päivittämisellä pienennetään huomattavasti haittaohjelmien hyväksikäyttämien haavoittuvuuksien määrää. Haittaohjelmat pyrkivät läpi käyttöjärjestelmien ja ohjelmistojen haa-

voittuvuuksista eli tietoturva-aukoista, saastuttaakseen laitteen. Haittaohjelmat keskittyvät yleensä suosituimpiin ja laajasti käytössä oleviin järjestelmiin, kuten Adoben sovelluksiin ja Windowsin käyttöjärjestelmiin. Haavoittuvuuksista johtuen ohjelmisto-kehittäjät etsivät taukoamatta sovellusten haavoittuvuuksia, korjatakseen ne ennen kuin haittaohjelmat löytävät ne. Käyttäjille julkaistavien päivitysten tavoitteena ovat yleensä:

- Tietoturva-aukkojen korjaaminen
- Käyttöjärjestelmän resurssien optimointi
- Uudempien ja turvallisempien ominaisuuksien lisääminen
- Vanhojen ja haavoittuvien ominaisuuksien poisto
- Ohjelmiston tehokkuuden lisäys ajureita päivittämällä (Goodrich, Ryan 2015)

Turva-aukkojen määrä on suoraan verrannollinen laitteessa olevien sovellusten määrään. Onkin suositeltavaa, että ylimääräiset ja käyttämättömät sovellukset poistetaan laitteesta. Sovelluksen poistamisen yhteydessä poistuu myös sen mahdolliset tietoturva-aukot. Ennen poistamista on kuitenkin syytä ottaa varmuuskopiot tärkeistä tiedoista ja varmistua ettei kyseisen sovelluksen poistaminen aiheuta toimimattomuutta muussa järjestelmässä. (US-Cert, 2015.)

On suositeltavaa käyttää sovelluksen automaattista päivitysten tarkistusta. Tällöin saat välittömästi tiedon, kun uusi päivitys on saatavilla. Käyttöjärjestelmien tietoturvapäivitykset kannattaa asettaa päivittymään automaattisesti. Kaikki tietoturvapäivitykset tulisi aina ladata ja asentaa viivyttelemättä, jotta mahdolliset tietoturva-aukot suljettaisiin ennen hyökkäystä. (Expert Reviews, 2015.)

5 VMWARE-VIRTUAALIYMPÄRISTÖN TURVAAMINEN

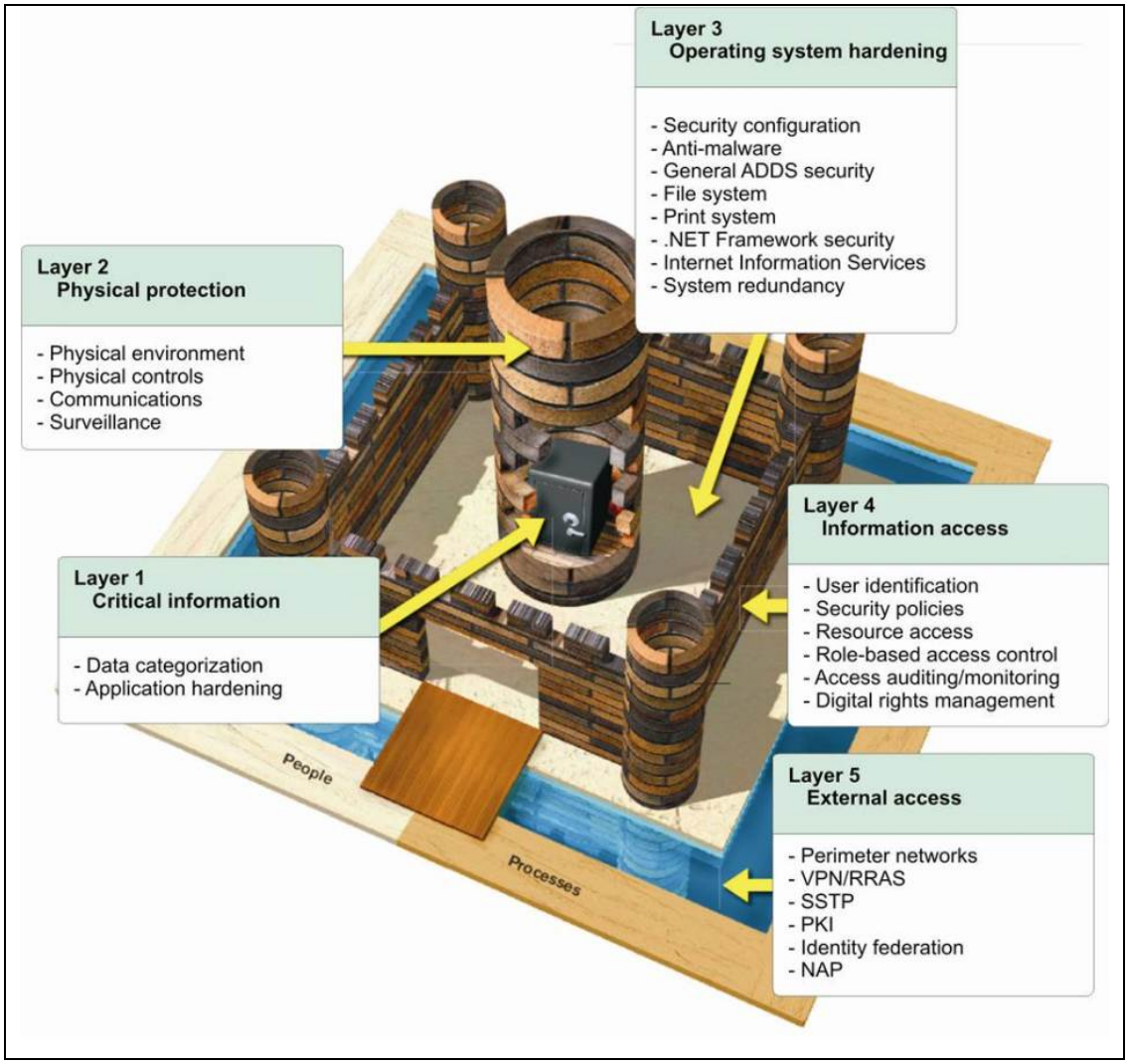
Mikään järjestelmä ei turvaa täydellisesti virtuaaliympäristöä erilaisilta uhkatekijöiltä. Mitä useampaa suojaustasoa käytetään, sitä varmemmin vältytään riskiltä hävittää dataa ja parannetaan käytettävyyttä. On syytä valmistella järjestelmä toipumaan mahdollisista ongelmista. Järjestelmän elvyttäminen ei koskaan ole helppo tehtävä. Vaikka järjestelmä olisi miten monitasoisesti suojattu, niin organisaatiolla tulisi aina olla yksityiskohtainen palautussuunnitelma, jota seurata. Kuten kaikki muutkin virtuaalisen ympäristön operaatiot, myös palauttaminen pitää olla suunniteltua. (Ruest & Ruest 2009, 356.)

Jokaisella järjestelmällä pitäisi olla palautusstrategia suojaamassa sen koneita. Virtuaaliympäristössä tämä tarkoittaa saman strategian käyttämistä resurssivarannoissa ja virtuaalikoneissa. Tärkeää on olla suunnitelma erityyppisiä tilanteita varten. Tämän vuoksi on tärkeää arvioida mahdollisia riskejä. (Ruest & Ruest 2009, 357.)

5.1 Castle Defence System (CDS)

Virtualisoitu VMware ympäristö tulisi turvata samoin kuin turvataan fyysisiä verkkoympäristöjä. Yleensä IT-järjestelmien suojaus jaetaan viiteen tasoon, joiden voidaan ajatella muodostavan linnakkeen. Tätä kutsutaan nimellä Castle Defense System (CDS). Tullakseen valmiiksi turvallisuusmenettelyksi, kuuluu menettelyyn vielä kaksi osaa: ihmiset ja prosessit. Nämä kaksi osaa ympäröivät linnaketta ja täydentävät turvallisuusmenettelyn, joka kuvataan Kuvassa 4. (Ruest & Ruest 2009, 315, 316.)

- Taso 1: Kriittinen informaatio – Järjestelmän sydämessä on se tieto, jota olet suojaamassa, kuin kuvitteellinen holvi linnakkeesi keskiössä.
- Taso 2: Fyysinen suojaus – Suojaustoimenpiteet pitäisi aloittaa tietojärjestelmien fyysisellä suojauksella. Tämä taso on kuin torni holvin ympärillä.
- Taso 3: Käyttöjärjestelmän karkaisu – Kun fyysiset suojaukset on asetettu, pitäisi jokaisen tietokoneen käyttöjärjestelmän turhia osia karsia. Karsimisella pyritään vähentämään mahdollisuutta hyökkäyksille niin paljon kuin mahdollista. Tämä taso kuvaa sisäpihaa.
- Taso 4: Information Access – Kun annetaan pääsy dataan, tulisi varmistua siitä, että jokainen on tunnistettu, valtuutettu sekä tarkastettu. Taso on kuin linnan muuri ja ovet, jotka sallivat tunnistettujen pääsyn sisään.
- Taso 5: External Access – Suojauksen viimeinen kerros työskentelee ulkomaailman kanssa. Se sisältää demilitarisoidun alueen, jolla yhdistetään järjestelmä ulkomaailmaan, aivan kuin linnakkeen vallihauta.



Kuva 4. Kuvassa esitellään viisitasoinen IT-järjestelmien suojaus. (Ruest & Ruest 2009, 316.)

5.1.1 Kriittinen informaatio

Kriittisellä informaatiolla tarkoitetaan kahdentasoista dataa, jotka tulisi suojata. Nämä tasot ovat virtuaaliset levyasemat ja tietokantojen sisältämät tiedot. Virtuaaliset levyasemat pitävät sisällään muun muassa käyvät ja sammutetut virtuaalikoneet, virtuaalikoneiden levykuvat ja mallit sekä kaiken muun, mitä virtuaalikoneet pitävät sisällään. Tietokannat puolestaan pitävät sisällään asetustiedostoja, isäntäkoneen konfigurointiasetuksia ja paljon muuta. Nämä kaikki tarvitsevat erityistä suojausta. (Ruest & Ruest 2009, 327.)

Virtuaalisten levyasemien suojaaminen tarkoittaa paljon muutakin kuin pelkkien virtuaalikoneen asennustiedostojen suojaamista. Asetustiedostot, tilannekuvat, lokitiedostot ja kaikenlaiset muut tiedot, joilla virtuaalikone muodostuu verkkoon sijaitsevat levyasemalla. Aina, kun kone tehdään virtuaalisesti, on se myös siirrettävissä. Tämän lisäksi virtuaalikoneet ovat itsenäisiä ja sisältävät usein arkaluonteista materiaalia, kuten salasanoja ja pääsyoikeuksia. Tästä syystä tulisi aina varmistua siitä, että ylläpitohenkilökunta on täysin luotettava. On mahdollista, että joku varastaa virtuaalikoneen kaikkine salaisine tietoineen, kenenkään huomaamatta. (Ruest & Ruest 2009, 328, 329.)

Jokainen hypervisorin hallintajärjestelmä sijaitsee tietokannoissa. Olisikin syytä varmistua siitä, että vain tarkoituksenmukaisilla henkilöillä on pääsy näihin tietoihin. Tietokantajärjestelmän asennus tulisi aina varmistaa parannetulla suojauksella. Olivatpa tiedot arkistoissa tai keskustietokannassa, ne tulee aina olla suojattuna. (Ruest & Ruest 2009, 329.)

5.1.2 Fyysinen suojaus

Toinen taso on tietojärjestelmien fyysinen suojaus. Järjestelmiä ei koskaan tulisi sijoittaa julkiselle paikalle siten, että kenellä tahansa on niihin vapaa

pääsy. Usein yritykset siirtyvät virtuaaliseen infrastruktuuriin jo olemassa olevasta fyysisestä, joten fyysisen suojauksen perusteet ovat valmiiksi olemassa. (Ruest & Ruest 2009, 330.)

Tietojärjestelmät olisi syytä sijoittaa tiloihin, joissa järjestelmällä on hyvin pieni mahdollisuus altistua ulkomaailman tapahtumille. Vaaratekijöitä ovat ainakin luonnonilmiöt, kuten vesivahinko ja tulipalo. On syytä huomioida, että tilat voivat altistua myös epäsuoralle vahingolle. Esimerkiksi liian lähellä tietä sijaitsevat tilat voivat vahingoittua liikenneonnettomuudessa. (Ruest & Ruest 2009, 330.)

Yrityksen henkilökuntaa on syytä kouluttaa tietoturvauhkien varalle ja luoda toimintamalleja, joilla estetään laitteiston jääminen suojaamattomaksi tai käyttäjätunnusten joutuminen vääriin käsiin. Tiloissa kulku tulisi olla vartioitua ja vieraat tunnistaa jokaisessa tilassa. Jokainen asennus tulisi dokumentoida, minkä lisäksi turvasuunnitelmasta tulisi kertoa henkilökunnalle heidän asemastaan riippuen tietyt asiat. (Ruest & Ruest 2009, 330, 331.)

5.1.3 Käyttöjärjestelmän karkaisu

Käyttöjärjestelmän karkaisun tavoitteena on minimoida mahdollisille hyökkäyksille alttiiden pintojen määrää. Järjestelmästä tulisi poistaa kaikki ylimääräinen ja tarpeeton. Kun jokin ohjelmisto jää tarpeettomaksi, olisi se hyvä poistaa järjestelmästä viipymättä. Myös kaikki vanhentunut mutta arkaluonteinen materiaali on syytä tuhota järjestelmästä. (Ruest & Ruest 2009, 332.)

Järjestelmän turvallisuusasetusten säädöllä yhdistetään turvaparametrit laitteeseen sen asennusvaiheessa. Kun konetta asennetaan, varsinkin palvelinta, pitää suorittaa muutamia muutoksia oletusasetuksiin, jotta varmistutaan siitä, että kone on asianmukaisesti suojattu. VMwarella tämän tekeminen vaatii ainoastaan sen, että asettaa suojauksen tasolle ”Korkea”. (Ruest & Ruest 2009, 332.)

5.1.4 Information Access

Neljänteen tasoon kuuluvat käyttäjän ja käyttöoikeuksien tunnistaminen. Paras tapa hallita todennusta, valtuutusta ja tilien tarkistusta on käyttää aktiivihakemiston ryhmäkäytäntöjä. Esimerkiksi pääsynvalvonta voidaan toteuttaa ryhmäkäytäntöobjektilla (Group Policy object). Oletusobjektia voidaan muokata apuohjelmalla, mutta paras ja helpoin tapa olisi luoda kokonaan uusi ryhmäkäytäntöobjekti. Kaikki luodut ryhmäkäytäntöobjektit tulee dokumentoida ja jokainen muutos lisätä huolellisesti. (Ruest & Ruest 2009, 343.)

5.1.5 External Access

Viidennellä tasolla keskitytään ympärysverkkoon sekä sisäverkon suojaamiseen ulkopuolisilta vaikutuksilta. Nykypäivänä on lähes mahdotonta luoda toimivaa sisäverkkoa ilman minkäänlaista kosketusta ulkomaailmaan. Tästä syystä sisäverkkoa tulisi suojata niin paljon kuin mahdollista luomalla esteitä, jotka täytyy selvittää, ennen kuin kukaan pääsee sisään. Näitä esteitä voi olla useassa eri muodossa. Tätä ympäristöä kutsutaan usein demilitarisoiduksi alueeksi, eli aliverkoksi jolla yhdistetään organisaation oma järjestelmä turvattomampaan alueeseen, kuten internetiin. Ympärysverkko voi sisältää minkä tahansa määrän komponentteja, mutta kun käytössä on resurssivarantoja, ne voidaan rajoittaa sarjalla palomuureja, jotka suojelevat sisäverkkoa. (Ruest & Ruest 2009, 346.)

Hallinnollisten työasemien ja isäntäpalvelimien välinen viestintä tulisi aina olla salattua riippumatta siitä, sijaitsevatko ne verkon ulko- vai sisäpuolella. Suojauksen parantamiseksi parasta olisi luoda oma virtuaalinen lähiverkko, jonne sijoitetaan kaikki isäntä- ja hallinnolliset koneet. Näin rajoitetaan muiden käyttäjien tai palveluiden kanssakäymistä kyseisten laitteiden kanssa. Virtuaalisesta lähiverkosta huolimatta kaikki viestintä tulee edelleen olla salattua. (Ruest & Ruest 2009, 348.)

5.1.6 Turvallisuusmenettelyn täydentäminen

Castle Defence System tarjoaa hyvän turvallisuuspolitiikan, mutta se ei pysty yksin suojaamaan kriittisiä resursseja. Se tarvitsee rinnalleen reagoivia ja ennakoivia puolustusmenetelmiä. Tämä tarkoittaa lisäpuolustusta useilla tasoilla. (Ruest & Ruest 2009, 352.)

On olemassa käynnin aikaisia operaatioita, joita tulisi suorittaa säännöllisin väliajoin, jotta järjestelmän suojausta pystytään seuraamaan. Näin varmistutaan myös siitä, että vastavaikutussuunnitelmat toimivat halutulla tavalla. Hyvää harjoitusta on itse simuloida tilanteita, jolloin nähdään, miten torjutaan ja onko torjuntasuunnitelma riittävä. Suurin tekijä hyvään torjuntaan on se, että jokainen organisaatiossa tietää oman työtehtävän ja roolinsa suunnitelmassa. Lopuksi, jotta turvallisuuspolitiikka tuetaan täysin, on syytä rajoittaa ylläpitäjille ja toimijoille annettavia oikeuksia. (Ruest & Ruest 2009, 353.)

5.2 Integroidut kumppaniratkaisut

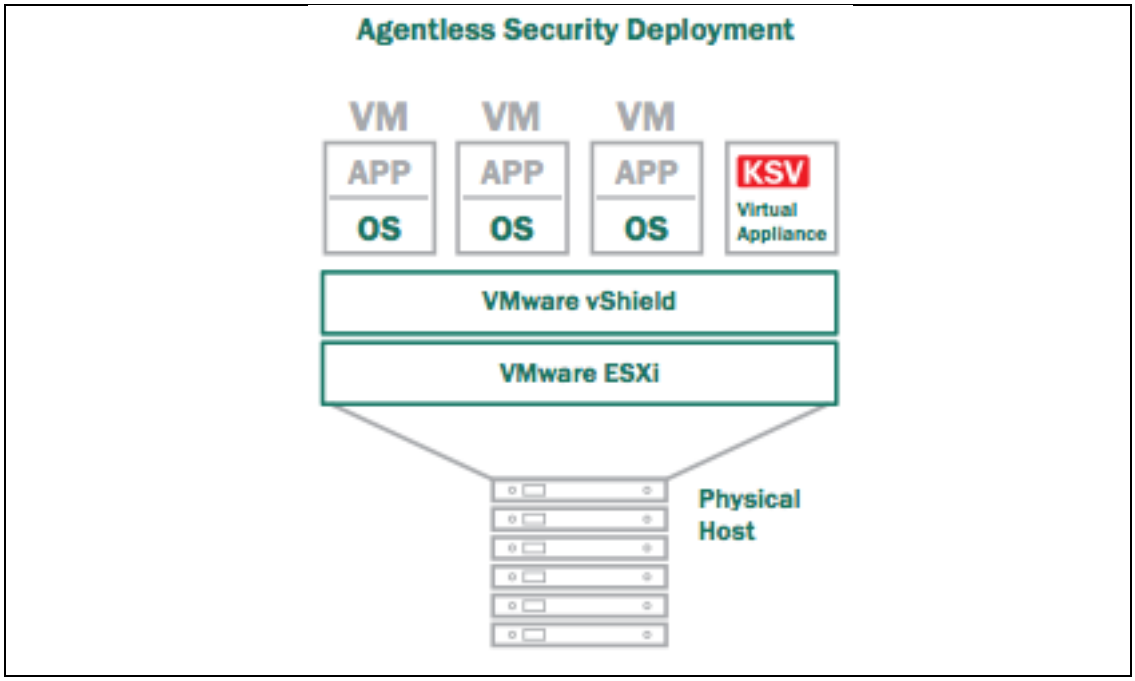
VMwarella on pitkä lista kumppaneita, joiden ratkaisuja on integroitu toimimaan heidän tuotteidensa kanssa. Tämä mahdollistaa kumppaniratkaisuille pääsyn tietovirtoihin niin sisään kuin ulospäin, ilman suurempia ohjelmistomuutoksia. Kumppaniratkaisut ovat pääsääntöisesti agentittomia. Näin mahdollistuu ratkaisujen toimiminen ilman, että jokaiselle laitteelle asennetaan erillinen agenttiohjelma.

5.2.1 Kaspersky Security for Virtualization

Kaspersky tarjoaa erityisesti VMwaren tuotteisiin suunniteltua ja integroitua ratkaisua suojautumaan haittaohjelmilta ja suojaamaan verkkoa. Agentittomana toteutuksena sillä pystytään suojaamaan kaikki virtuaalisen ympä-

ristön laitteet, kuten tietokoneet, palvelimet ja datakeskukset, entistä tehokkaammin. Agentittomuus mahdollistaa erilaisten turvallisuusasetusten luomisen eri ryhmille laitteita. Ohjelmisto on avoin, joustava ja se sisältää kehittyneet hallintatyökalut yksinkertaistamaan turvallisuustehtäviä kaikilla alustoilla. (Kaspersky 2015.)

Kasperskyn virtualisointiin suunniteltu ratkaisu pitää sisällään eilaisia piirteitä. Kuten tiedostotason haittaohjelmilta suojaavan järjestelmän, jolla voidaan suojata jokainen laite. Pilvipalveluihin pohjautuvan järjestelmän, joka havaitsee uudet uhat jopa 0.02 sekunnissa. Verkkosuojauksen, joka sisältää erityistä teknologiaa suojaamaan virtuaalikoneita verkkouhilta. Jaetun välimuistin ansiosta tiedostoa, joka sijaitsee samalla palvelimella, ei tarvitse erikseen skannata jokaiselta virtuaalikoneelta. Ratkaisuun kuuluu myös hallinta paneeli, jolla pystytään hallitsemaan kaikkia Kasperskyn tekniikalla turvattuja laitteita. (Kaspersky 2015.)

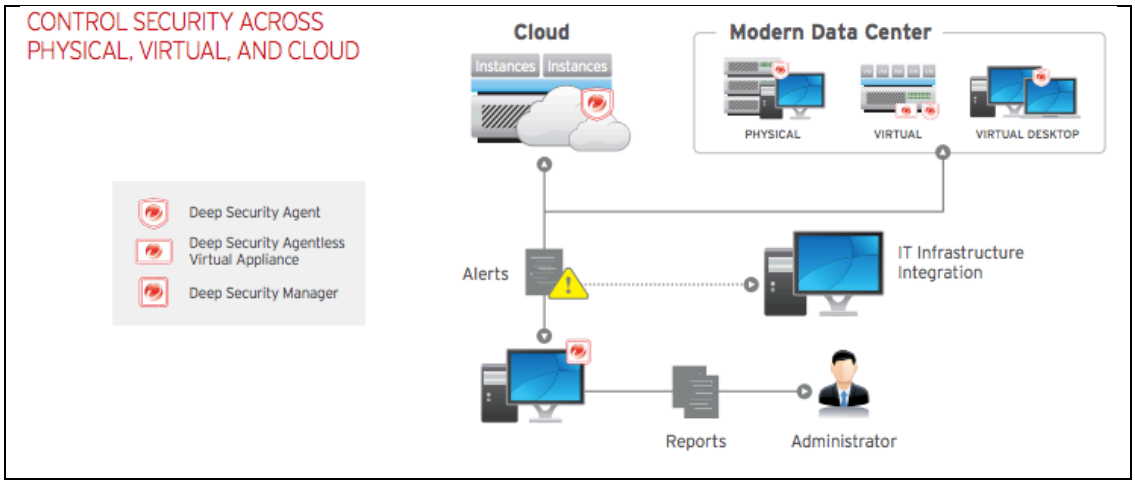


Kuva 5. Kaspersku Security for Virtualization tarjoaa agentitonta virustentorjuntaa VMwaren tuotteille. (Kaspersky 2015.)

5.2.2 Trend Micro Deep Security

Trend Micron tarjoama Deep Security ratkaisu integroituu VMwaren ohjelmointirajapinnan kanssa tarjoamaan virtualikoneille agentitonta haittaohjelmilta suojautumista. Deep Securityn virtualisoinnin turvallisuus ohjelmisto suojaa virtualityöpöytiä ja –palvelimia 0-päivä haavoittuvuuksilta, samalla minimoiden operoinnin vaikutuksia resurssien käyttöön ja hätäpaikkauksia. Ratkaisu mahdollistaa organisaatioiden siirtää turvallisuuspolitiikkansa työtaakkaa pilvipalveluihin. (Deep Security esite 2014.)

Deep Securityn järjestelmään kuuluu viisi erilaista moduulia. Yksi moduuleista on agentti, joka suojaa haittaohjelmilta. Agentti laajentaa fyysisten, virtuaalisten ja pilvipalvelinten tietoturvaa VMware ympäristössä. Tunkeutumisen torjunta seuraa kaikkea saapuvaa ja lähtevää tietoliikennettä protokollan poikkeamilta, politiikkojen rikkomuksilta ja sisällöltä, joka enteilee hyökkäyksiä. Se suojaa automaattisesti tiedettyjä, mutta paikkaamattomia haavoittuvuuksia. Kaksisuuntainen isäntäpohjainen palomuuri vähentää hyökättävää pintaa fyysisissä, virtuaalisissa ja pilvipalvelimissa. Monitoroinnilla Deep Security tarkistelee jatkuvasti kriittisiä käyttöjärjestelmiä ja ohjelmatiedostoja, sekä hakemistoja, rekisteröinti avaimia ja arvoja, jotta se huomaa ja voi raportoida odottamattomat muutokset reaaliaikaisesti. Lokien tarkastus kerää ja analysoi käyttöjärjestelmien ja ohjelmistojen lokeja. Tunnistaakseen epäilyttävää käytöstä, turvallisuustapahtumia ja hallinnollisia tapahtumia datakeskuksessa. (Deep Security esite 2014.)



Kuva 6. Trend Micron Deep Securityllä toteutetun järjestelmän turvallisuusohjaus fyysisen, virtuaalisen ja pilvessä toimivien järjestelmien kesken. (Deep Security esite 2014.)

6 YHTEENVETO

Tässä opinnäytetyössä käsittelin VMwarella virtualisoidun toimintaympäristön tietoturvaa. Aihe on mielenkiintoinen ja ajankohtainen, koska virtualisointi yleistyy ja kehittyy vuosi vuodelta. Aivan samanaiheisia opinnäytetöitä ei käsitykseni mukaan ole tehty, mikä lisäsi mielenkiintoani. Aihevalinta osoittautui työn edetessä varsin haastavaksi, mutta samalla hyvin opettavaiseksi. Lähteeni painottuivat pääasiassa englanninkielisiin, koska aiheen tuoreudesta johtuen suomenkielistä kirjallisuutta oli selvästi vähemmän. Lähteistäni johtuen englanninkielinen termistö tuli minulle työn aikana tutuksi, mistä on varmasti tulevaisuudessa hyötyä. Alati kehittyvän tekniikan johdosta, myös osa kirjallisuudesta sisälsi vanhentunutta tietoa.

Virtualisointi on nykyajan, mutta selvästi myös tulevaisuuden tekniikkaa. Virtualisointi on viimevuosina ottanut huimia harppauksia niin suosiossa kuin kehityksessä. Nämä tekijät yhdessä alati kehittyvien uhkakuvien kanssa luovat organisaatioille jatkuvan paineen kehittää ja luoda uusia turvallisuusmenettelyjä. Uusien virtualisointitekniikoiden jatkuva syntyminen pakottaa myös VMwarea jatkuvasti kehittämään tuotteitaan, jos se haluaa pysyä markkinoiden johtavana palveluntarjoajana.

Virtualisointi on iso osa nykypäivän liiketoimintaa, enkä usko roolin ainakaan pienenevän tulevaisuudessa. Toimiva ja tehokas virtuaaliympäristön turvaaminen koostuu useasta eri osa-alueesta. Osa näistä alueista on tuttua perinteisten ympäristöjen turvaamisesta. Tietoturvan kannalta suurin yksittäinen vaikuttaja on järjestelmien käyttäjät. Virtualisointi kuitenkin vaatii organisaatioita pohtimaan uudelleen rajat henkilöstön työtehtäville, koska perinteisen ympäristön mukaan määritellyt työtehtävät eivät täysin päde virtuaalimaailmassa. Virtualisointi on myös muuttanut tavan, jolla IT-palveluita toimitetaan. Aiemmin uuden palvelun hankkiminen vaati fyysisen laitteen ostamista, jonka toimittaminen saattoi kuitenkin kestää useita viikkoja. Nykyään virtuaaliympäristön mahdollistamana samaisia palveluita pystytään toimittamaan minuuteissa.

Virtualisoinnilla organisaatiot pyrkivät joustavuuteen ja hallintaa sekä kustannussäästöihin. Säästöjä syntyy kun fyysisiä laitteita tarvitaan vähemmän. Tämä heijastuu suoraan kuluihin, joita aiheutuu järjestelmien ylläpidosta. Esimerkiksi ilmastoinnin tarve pienemmälle määrälle fyysisiä laitteita on pienempi, joka taas tarkoittaa sähkönkulutuksen laskua. Myös järjestelmien elinkaari kasvaa virtualisoinnin myötä. Palvelimien elinkaari on yleisesti pidempi kuin työasemien. Vanhojen työasemienkin käyttöikä kasvaa, kun laitteistojen kapasiteetti ja prosessointi siirtyy palvelinpäähän. Ohjelmistojen päivittäminen on helpompaa ja nopeampaa, koska sen tarvitsee tehdä vain yhdessä paikassa. Sama koskee tietoturvaa.
Virtualisointi ei itsessään poista tietoturva-aukkoja, vaan haavoittuvuudet ovat hyödynnettävissä samalla tavalla kuin perinteisissäkin ratkaisuissa. Tietoturvan kannalta järjestelmien suurin uhkakuva on sen käyttäjien toiminta. Nykypäivän tietoturvahaasteita luovat uudenlaiset hyökkäykset, joilla pyritään anastamaan rahan arvoista tietoa.

Tietomurtoja voidaan ennaltaehkäistä monella tapaa. Tärkeimpiin toimenpiteisiin kuuluu ohjelmistojen pitäminen päivitettyinä sekä oikein säädettyinä. Omiin palveluihin on mahdollista suorittaa koehyökkäyksiä, joilla selvitetään mahdollisia tietoturvan aukkoja ja puutteita. Tietoturvaa voidaan parantaa erillisillä järjestelmillä. Palomuuri ja virustorjunta pystyvät estämään pahimpia vahinkoja. Organisaatioiden on hyvä kouluttaa säännöllisesti myös henkilökuntaansa, sekä luoda ja päivittää tietoturvasuunnitelma. Suunnitelmalla selvitetään mitä, miten ja miksi organisaatiossa suojataan.

VMwarella on useita erilaisia virtualisointiin liittyviä ratkaisuja, joilla se on saavuttanut johtavan aseman virtualisointi- ja pilvipalvelumarkkinoilla. VMwarella on pitkä lista kumppaneita, joiden ratkaisuja on integroitu heidän tuotteisiinsa. Nämä kumppaniratkaisut ovat yleensä agentittomia, millä mahdollistuu ratkaisujen toimiminen ilman kaikkialle erikseen asennettavaa agenttiohjelmistoa.

LÄHTEET

Clearswift, 2015. Viitattu 10.02.2015. Saatavissa: http://www.clearswift.com/blog/2013/05/02/enemy-within-emerging-threat

CommVerge, 2015. Viitattu 10.02.2015. Saatavissa: http://www.commverge.com/Solutions/DataCenterSolutions/Virtualization/tabid/192/Default.aspx

Deep Security esite, 2014. Viitattu 06.05.2015. Saatavissa: http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_deep-security.pdf

Gartner, 2010. Viitattu 06.05.2015. Saatavissa: http://www.gartner.com/newsroom/id/1322414

Goodrich, Ryan, 2015. Viitattu 06.02.2015. Saatavissa: http://anti-virus-software-review.toptenreviews.com/pc-security-and-the-importance-of-patch-updates.html

Expert Reviews, 2015. Viitattu 06.02.2015. Saatavissa: http://www.expertreviews.co.uk/software/1304965/when-windows-xp-support-ends-this-is-how-you-secure-your-pc-and-save-all-updates

Hacking Trough Complexity, 2013. Viitattu 13.11.2013. Saatavissa: http://www.hackingthroughcomplexity.fi/2011/11/miten-havaita-tietomurrot.html

Järvinen, Petteri, 2012. Arjen tietoturva: Vinkit & ratkaisut. Espoo: Docendo.

Laaksonen & Nevasalo & Tomula, 2006. Yrityksen tietoturvakäsikirja. Edita Publishing Oy.

Kaspersky, 2015. Viitattu 06.05.2015. Saatavissa: http://www.kaspersky.fi/business-security/virtualization/agentless

Microsoft, 2015. Viitattu 06.02.2015. Saatavissa: http://windows.microsoft.com/fi-fi/windows/understanding-security-safe-computing#1TC=windows-7

PC Advisor, 2015. Viitattu 06.02.2015. Saatavissa: http://www.pcadvisor.co.uk/how-to/software/3356160/how-back-up-your-pc-laptop/

Ruest, D. & Ruest, N. 2009. Virtuaalization: Beginner's guide. New York, Chicago: McCraw-Hill.

Surveillance Self- Defence, 2015. Viitattu 06.02.2015. Saatavissa: https://ssd.eff.org/en/module/what-encryption

TechTarget 2013a. Viitattu 13.11.2013. Saatavissa: http://searchvmware.techtarget.com/What-is-VMware-vSphere-4

TechTarget 2013b. Viitattu 13.11.2013. Saatavissa: http://searchvmware.techtarget.com/definition/VMware-Workstation

Tietoviikko 2013a. Viitattu 13.11.2013. Saatavissa: http://www.tietoviikko.fi/kaikki_uutiset/article390893.ece

Tietoviikko 2013b. Viitattu 13.11.2013. Saatavissa: http://www.tietoviikko.fi/kaikki_uutiset/article384906.ece

US-Cert, 2015. Viitattu 06.02.2015. Saatavissa: https://www.us-cert.gov/sites/default/files/publications/ TenWaystoImproveNewComputerSecurity.pdf

VMware verkkosivut 2013. Viitattu: 13.11.2013. Saatavissa: http://www.vmware.com

VMware haku 2013. Viitattu: 13.11.2013. Saatavissa: http://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp?topic=/ com.vmware.vsphere.vmadmin.doc_41/vsp_vm_guide/about_vms_in_vsp_da tacenter/c_virtual_machine_components.html

Williams, D. & Garcia, J. 2007. Virtuaalization with XEN. Syngress