Haaga-Helia
ammattikorkeakoulu Oy

Moderniin yritysverkkoon kohdistuvat kyberuhat ja niiltä suojautuminen

Arttu Talvio

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2021

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Arttu Talvio

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Moderniin yritysverkkoon kohdistuvat kyberuhat ja niiltä suojautuminen

Sivu- ja liitesivumäärä
32

Tämä opinnäytetyö käsittelee moderneja yrityskäytössä käytettäviä tietoverkkoja, niihin kohdistuvia kyberuhkia ja keinoja uhilta suojautumiseen. Opinnäytetyö antaa yleisen kuvan nykypäivän tietoverkkojen rakenteesta ja niihin kohdistuvista tavallisimmista hyökkäyksistä.

Tutkimuksessa on pyritty tuomaan esille tietoverkkojen kehitystä, ja sitä, miten niihin kohdistuvat uhat ovat kehittyneet samanaikaisesti. Tutkimuksessa käsitellyt kyberuhat keskittyvät pääosin tietoverkkotason uhkiin. Koska tutkittava aihe on hyvin laaja, tietyt aiheen osa-alueet on rajattu pois tai niitä on käsitelty vain suppeasti.

Opinnäytetyö keskittyy kyberuhkiin ja niiltä suojautumiseen, mutta tutkimuksen kannalta oli tarpeellista käsitellä myös tietoverkkojen toimintaa. Työn ensimmäiset kappaleet keskittyvät antamaan lukijalle yleiskuvan siitä, miten tietoverkot toimivat. Työn edetessä siirrytään käsittelemään tietoverkkoihin kohdistuvia uhkia ja lopulta suojautumiskeinoja uhkia vastaan.

Nykyisin tietoverkkoihin kohdistuvia uhkia on lukuisia, ja niiltä suojautumiseen tarvitaan erilaisia ratkaisuja. Luvussa 3 pyritään käsittelemään yritysverkkoihin kohdistuvia yleisimpiä uhkia. Tunnistettaessa mahdolliset tietoverkkoon kohdistuvat uhat, on niiltä suojautuminen helpompaa. Seuraava kappale käsittelee yleisimpiä suojautumiskeinoja luvussa 3 esitettyjä uhkia vastaan.

Opinnäytetyön loppupuolella on pyritty tuomaan tiivistetysti esiin myös tavallisimpia tietoturvauhkia, jotka eivät suoranaisesti liity tietoverkkoon tai sen rakenteeseen. Näitä uhkia ovat esimerkiksi heikot salasanat, ohjelmistopäivitykset ja tietojenkalastelu. Vaikka kyseiset uhat eivät ole suoraan sidoksissa tietoverkkoon, ovat uhat ja niiltä suojautuminen yritysten tietoturvan kannalta oleellisia.

Viimeinen kappale pyrkii ottamaan kantaa siihen, minkälaisilla suojautumiskeinoilla moderni yritysverkko voidaan pitää turvallisena. Opinnäytetyön tuloksesta voidaan todeta, että kyberuhkia on valtavasti ja että erilaiset kyberturvastrategiat ja -ratkaisut soveltuvat erilaisiin verkkoympäristöihin.

Asiasanat
Kyberturva, Tietoverkko, Kyberuhka, Tietoturva

Sisällys

1 Johdanto

Tietoverkot ja tietoturva ovat nykyään osa lähes jokaisen yrityksen ja ihmisen arkea. Tietotekniikasta tietämättömät ihmiset tuskin tulevat ajatelleeksi, miten tietoverkot toimivat esimerkiksi omalla työpaikallaan tai vaikka käytettäessä julkisia palveluita. Nykyään tietoverkot esimerkiksi yrityskäyttöön rakennetaan eri tavoin kuin vaikka kymmenen vuotta sitten. Lyhyessä ajassa tietoverkot ja niiden rakenne sekä toteutukset ovat muuttuneet huomattavalla tavalla. Miten tämä on vaikuttanut tietoverkkoihin kohdistuviin kyberuhkiin? Tietoverkkoteknologioiden muutos vuosien varrella on muuttanut myös kyberhyökkäysten toimintaperiaatteita. Kaksi vuosikymmentä sitten palomuuri, DMZ-verkko ja verkon segmentointi saattoi olla riittävä suoja yritysverkkoon kohdistuvia uhkia vastaan. Kolme vuosikymmentä sitten virukset eivät aiheuttaneet haittaa tai tavoitelleet taloudellista hyötyä, vaan niiden tarkoitus oli lähinnä tehdä kiusaa tai aiheuttaa hämmennystä. Nykyisin virukset ja haittaohjelmat useasti suunnitellaan taloudellista hyötyä tavoitellen ja ne voivat aiheuttaa merkittävää vahinkoa yritysten liiketoiminnalle.

Vaikka tietoverkkojen rakentaminen ja tekniikat niiden ympärillä ovat muuttuneet, taustalla toimivat kuitenkin samat vanhat protokollat. TCP/IP-protokollapino ja sen periaatteet toimivat edelleen tietoverkoissa, olipa sitten kyseessä pilvipalvelun avulla toteutettu palvelu tai fyysinen palvelin. Tietoverkkojen suunnittelussa ja rakentamisessa tärkeässä osassa on verkkoarkkitehtuurit ja verkkotopologiat. Verkkotopologialla tarkoitetaan tietoverkon rakennetta ja tapaa, miten laitteet verkossa on liitetty toisiinsa. Tietoverkon topologioista puhuttaessa voidaan tarkoittaa sekä fyysistä että loogista topologiaa.
Tämän opinnäytetyön tarkoituksena on kuvata tietoverkkojen toimintaa, tutkia niihin kohdistuvia uhkia ja hyökkäyksiä ja keinoja niiltä suojautumiseen. Tässä opinnäytetyössä ei käydä yksityiskohtaisesti läpi eri verkkotekniikoiden tai verkon aktiivilaitteiden toimintaa, vaan keskitytään tutkimaan tietoverkkojen toimintaperiaatteita ja niihin kohdistuvia kyberuhkia. Opinnäytetyö keskittyy pääasiassa tietoverkkoihin ja niihin kohdistuviin teknisiin uhkiin ja hyökkäyksiin, joten hallinnollinen tietoturva ja loppukäyttäjien koulutus uhkia vastaan on rajattu pois.

Tutkimuskysymyksinä tässä opinnäytetyössä ovat seuraavat kysymykset:

- Millaisia uhkia moderneihin yritysverkkoihin kohdistuu ja miten niiltä voidaan suojautua mahdollisimman tehokkaasti?
- Ovatko nykypäiväiset suojautumiskeinot tarpeeksi?
- Mitä eri suojautumiskeinoja tulisi erityyppisten yritysten ottaa käyttöön?

1.1 Termejä

APT
Advanced Persistent Threat eli kohdistettu haittaohjelmahyökkäys.

IDS
Intrusion Detection System eli tunkeutumisen havaitsemisjärjestelmä.

IPS
Intrusion Prevention System eli tunkeutumisen estojärjestelmä.

TCP/IP-pino
Usean eri tiedonsiirtoprotokollan yhdistelmä eli pino.

LAN
Local Area Network eli lähiverkko.

DoS
Denial of Service eli palvelunestohyökkäys.

DDoS
Distributed Denial of Service eli hajautettu palvelunestohyökkäys.

SMTP
Simple Mail Transfer Protocol on protokolla, jota käytetään viestien välittämiseen sähköpostipalvelimien välillä.

DNS
Domain Name System eli nimipalvelujärjestelmä muuntaa verkko-osoitteet IP-osoitteiksi.

IP-osoite
Internetiin kytkettyjen laitteiden osoittamiseen käytettävä numerosarja. IP-osoitteita on kahta eri muotoa riippuen protokollan versiosta (IPv4 ja IPv6).

TCP
Transmission Control Protocol on yleisin kuljetuskerroksen protokolla.

UDP

User Datagram Protocol on toinen yleisimmistä kuljetuskerroksen protokollista TCP:n jälkeen.

IoT

Internet of Things eli esineiden internet tarkoittaa laitteita, jotka ovat kytketty Internetiin. Laitteista voidaan lukea mittaustietoa ja niitä voidaan ohjata Internetin yli. Esimerkiksi lämpömittari, jonka lukeman voi tarkastaa etänä, tai uuni, jonka voi esilämmittää etäyhteydellä.

Haavoittuvuus

Heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Tietojärjestelmät, prosessit tai ihmisen toiminta voi sisältää haavoittuvuuksia.

MAC-osoite

MAC-osoite tai fyysinen osoite on verkkolaitteen yksilöivä osoite, joka on painettu verkkolaitteen verkkokorttiin.

SDN

Ohjelmisto-ohjattu tietoverkko on teknologia, jolla tietoverkkoja voidaan ohjata ja konfiguroida keskitetysti ohjelmistojen avulla.

API

Ohjelmointirajapinta, jonka avulla tietoa voidaan hakea kolmansien osapuolien sivustoilta, ja mahdollistaa tiedon siirtämisen eri ohjelmien välillä.

2 Tietoverkkojen toiminta ja periaatteet

Tietoverkko koostuu kahdesta tai useammasta toisiinsa liitetystä laitteesta, jotka kommunikoivat keskenään kaapeleiden tai radioaaltojen avulla (Davies 2019).
Paikallisverkko eli LAN (local area network), on ryhmä toisiinsa liitettyjä laitteita (yleensä tietokoneita), jotka rajoittuvat pienelle maantieteelliselle alueelle, yleensä yhteen rakennukseen. Paikallisverkkoa rakennettaessa tarvitaan tietokoneita, joista löytyvät verkkokortit, verkon aktiivilaitteita kuten kytkin sekä IP-osoitteita, jotta laitteet voivat tunnistaa toisensa. Paikallisverkkoa suurempi verkko on nimeltään laajaverkko eli WAN (wide area network). Laajaverkot yhdistävät paikallisverkkoja toisiinsa. (Panek 2019.)
Kahden edellä mainitun tietoverkkotyypin lisäksi on olemassa myös kaupunkiverkko eli MAN (metropolitan area network). Se on pienempi kuin WAN mutta suurempi kuin LAN. Kaupunkiverkko yhdistää laitteita metropolialueella, kuten suuressa kaupungissa, tai kaupungeissa, tai millä tahansa muulla laajalla alueella. Kaupunkiverkon ei kuitenkaan tarvitse olla kaupungissa, sillä nimitys viittaa verkon loogiseen kokoon fyysisen sijasta. (Cloudflare.)

Protokollien ja standardien avulla tietoverkot ja niihin yhdistetyt laitteet pystyvät toimimaan keskenään. Tietokoneet käyttävät erityyppisiä protokollia. Näiden protokollien muodostamaa joukkoa kutsutaan protokollapinoksi. TCP/IP on protokollapino, joka toteuttaa internetarkkitehtuurin, ja juontaa juurensa ARPANET:n viitekehyksestä ARM:stä. (Fall & Stevens 2011.)

2.1 TCP/IP

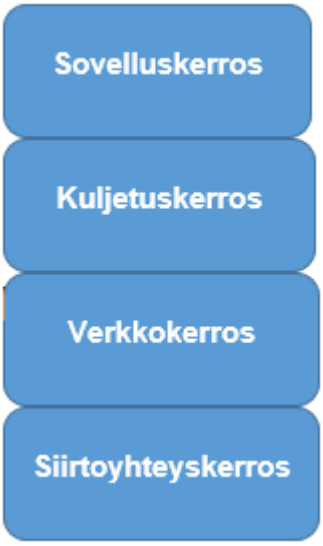
Internet on kasvanut valtavasti ja ylittänyt sen alkuperäisen koon moninkertaisesti. Alkuperäiset verkostot ja virastot, jotka kehittivät Internetiä, eivät enää edes osallistu sen ylläpitoon ja kehitykseen. Kaiken tämän valtavan muutoksen keskellä TCP/IP -protokollapino ei ole muuttunut, ja koko Internetin toiminta perustuu siihen. TCP/IP -protokollapinon suosion nopea kasvu ei perustunut ainoastaan sen olemassaoloon, tai siihen että se olisi ollut välttämätön. Protokollapino on nimetty sen kahden pääprotokollan TCP:n ja IP:n mukaan. TCP/IP -protokollapino ja sen tietyt ominaisuudet mahdollistivat globaalin data kommunikaation. (Hunt 2002.) Näitä ominaisuuksia ovat:

- Avoimet standardit, jotka ovat käytettävissä ja saatavilla vapaasti. Standardeja kehitetään laite- ja käyttöjärjestelmä riippumattomina. Protokollan ollessa niin suosittu,

se on myös ideaali yhdistettäessä laitteita toisiinsa, vaikka ne eivät kommunikoisikaan internetin välityksellä.

- Riippumattomuus jostain tietystä verkkolaitteesta. Tämä mahdollistaa protokollan integraation useisiin erilaisiin verkkoihin. TCP/IP -protokollaa voidaan käyttää ethernetillä, DSL-yhteydellä, valokuidulla ja käytännössä jokaisella eri verkkoteknologialla.
- Yhteinen osoiteavaruus, joka mahdollistaa minkä tahansa TCP/IP-laitteen uniikin osoittamisen koko tietoverkossa, vaikka kyseessä olisikin valtavan kokoinen verkko kuten Internet
- Standardoidut korkeatasoiset protokollat, jotka mahdollistavat johdonmukaiset ja laajalti käytettävissä olevat käyttäjäpalvelut (Hunt 2002.)

Tietoverkoissa toimivat eri tiedonsiirtoprotokollat ja niiden yhdistelmät kuvataan usein kerroksien avulla (kuva 1). TCP/IP-protokollapinossa on neljä eri kerrosta, joissa jokaisessa toimii eri protokollat. Ylimmässä kerroksessa eli sovelluskerroksessa toimivia protokollia on esimerkiksi http-protokolla, joka mahdollistaa verkkosivujen toiminnan, SMTP-protokolla, joka toimii yhtenä sähköpostin mahdollistavista protokollista ja DNS-protokolla, joka kääntää IP-osoitteet numeroista tekstiksi. Kuljetuskerroksen protokollat vastaavat nimensä mukaisesti datan kuljettamisesta tietoverkoissa. Kuljetuskerroksessa toimivat pääasiassa TCP ja UDP-protokollat. Verkkokerroksessa datalle annetaan osoitteet, se pakataan ja reititetään eteenpäin. Verkkokerroksessa toimii esimerkiksi IP-protokolla, joka käyttää IP-osoitteita toimittaakseen dataa verkkolaitteiden välillä. Toinen merkittävä verkkokerroksessa toimiva protokolla on ICMP-protokolla, jonka avulla voidaan vastaanottaa ja lähettää verkon diagnostiikkaa käyttämällä ping-komentoa. Alimmassa kerroksessa eli siirtoyhteyskerroksessa toimii esimerkiksi Ethernet-protokolla. Siirtoyhteyskerros määrittelee tiedonsiirron fyysisen median, kuten sähkökaapelin tai valokuidun. (Lowe 2018.)



Kuva 1. TCP/IP-protokollapino

2.2 Palvelin ja asiakas

Useimmat verkossa toimivat sovellukset ovat suunniteltu palvelin/asiakas -mallia käyttäen. Yksinkertaisesti selitettynä palvelin/asiakas -mallissa asiakastietokone pyytää palvelintietokoneelta jotain tiedostoa tai palvelua, ja palvelintietokone vastaa asiakkaan pyyntöön. (Stevens & Fall 2011.)

Esimerkiksi kun vierailemme jollain verkkosivulla, päätelaitteemme toimii asiakkaana, ja pyytää web-palvelimelta haluamaamme verkkosivustoa. Jos kaikki toimii niin kuin kuuluukin, eikä palvelimella ole häiriöitä, tarjoaa palvelin meille pyytämämme verkkosivun.

Palvelintietokoneet ovat yleensä tavallista tehokkaampia kuin asiakastietokoneet, ja niissä on käytössä palvelinkäyttöjärjestelmä. Suosituimmat käytössä olevat palvelinkäyttöjärjestelmät ovat Windows-käyttöjärjestelmiä. Toinen paljon käytetty palvelinkäyttöjärjestelmä on Linux ja sen eri levityspaketit. Palvelinkäyttöjärjestelmät ovat suunniteltu nimenomaan palvelintarkoitukseen ja eroavat tavallisista työpöytäkäyttöjärjestelmistä. (Lowe 2018.)

2.3 Verkon aktiivilaitteet

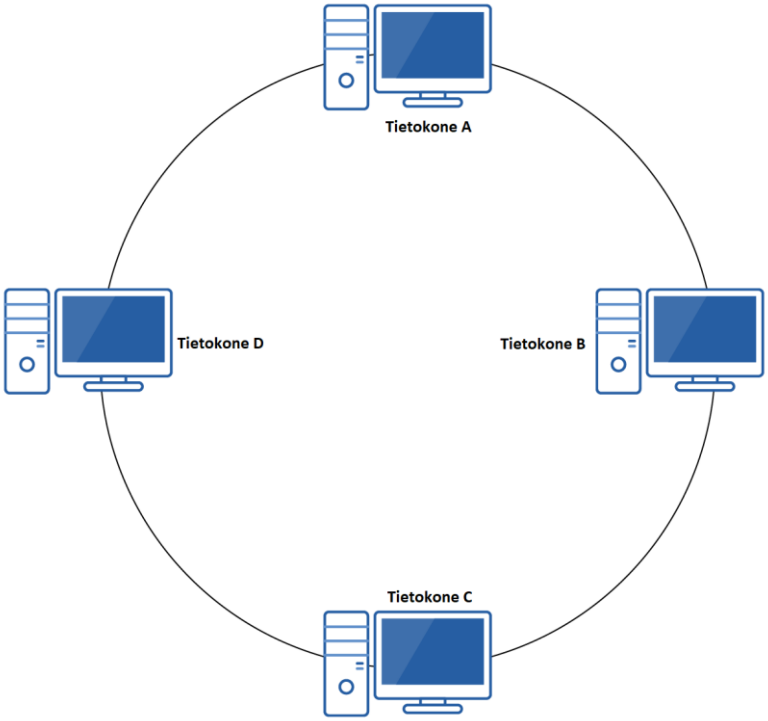
Verkon aktiivilaitteiksi lukeutuu muut laitteet kuin päätelaitteet esim. tietokoneet, puhelimet ja palvelimet. Lähiverkon aktiivilaitteita ovat kytkin, reititin ja keskitin. Keskitin on vanhanaikainen laite, jonka kytkin on korvannut lähes kokonaan. Keskitintä ei enää käytetä kuin ainoastaan harvoissa tapauksissa. Kytkimiä ja reitittimiä käytetään edelleen laajalti lähiverkoissa. (Davies 2019.)

Jokaisella lähiverkon laitteella on uniikki osoite, jota kutsutaan MAC-osoitteeksi tai fyysiseksi osoitteeksi. MAC-osoite on painettu verkkolaitteen fyysiseen verkkokorttiin, tästä nimitys fyysinen osoite. Kytkin oppii tunnistamaan lähiverkon laitteiden MAC-osoitteet, ja tallentaa osoitteet omaan muistiinsa. Tallennettujen osoitteiden avulla kytkin ohjaa datan oikeaan osoitteeseen lähiverkon sisällä. Lähiverkon päätelaitteet yhdistetään kytkimeen Ethernet-kaapelin avulla.

Reititin on toinen yleisin verkon aktiivilaite, ja sen tärkein tehtävä on yhdistää tietoverkkoja toisiinsa. Reititin käyttää IP-osoitteita ohjatakseen liikenteen verkkojen välillä, kun taas kytkin käyttää tiedonsiirrossa hyväkseen MAC-osoitteita. Reitittimen avulla lähiverkon liikenne on mahdollista ohjata ulos Internetiin. Ilman reititintä ei ole mahdollista ottaa yhteyttä Internetiin.

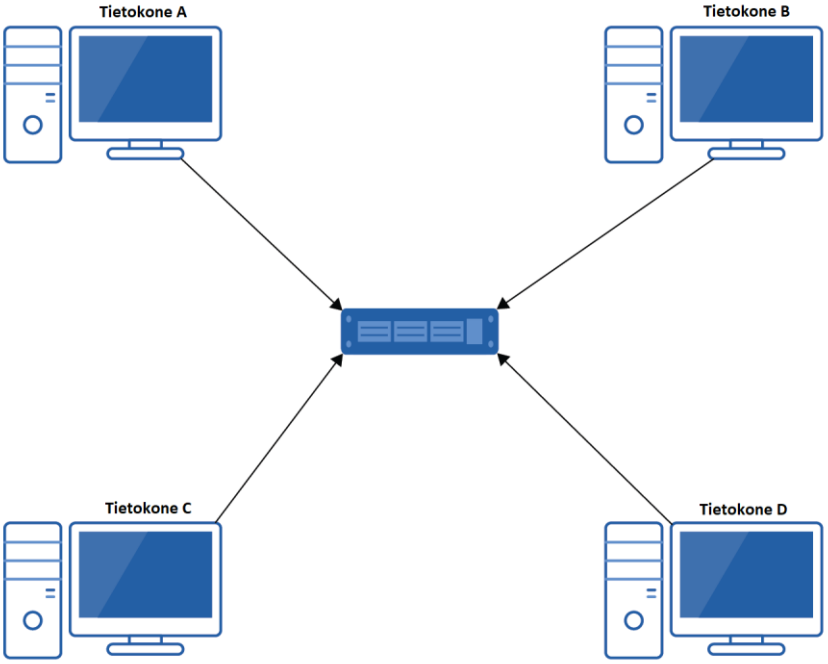
2.4 Topologia

Verkkotopologia voi viitata joko fyysiseen tai loogiseen topologiaan. Fyysisellä topologialla tarkoitetaan tapaa, jolla verkon laitteet ovat liitetty toisiinsa, kun taas looginen topologia kertoo, miten data liikkuu laitteiden välillä. Verkkotopologiat vaihtelevat yritysten koon ja tarpeiden mukaan, ja jokaisella topologialla on omat hyödyt ja haittansa. Topologioita ja niiden yhdistelmiä on useita, mutta käytetyimmät topologiat ovat rengas, tähti ja mesh. (Panek 2019.)



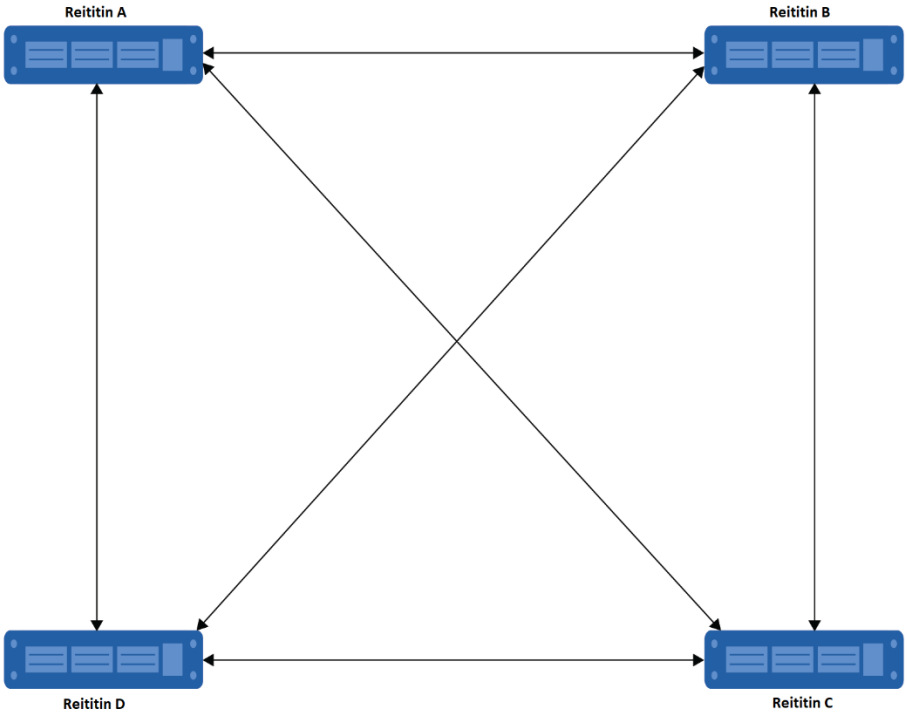
Kuva 2. Rengastopologia (Davies 2019)

Rengastopologiassa jokainen verkkolaite on yhdistetty kahteen laitteeseen ja data siirretään viereiselle laitteelle. Jos data ei ole tarkoitettu kyseiselle laitteelle, data lähetetään seuraavalle laitteelle, kunnes se saavuttaa oikean määränpään.



Kuva 3. Tähtitopologia (Davies 2019)

Tähtitopologiassa verkkolaitteet ovat kytketty keskuslaitteeseen kuten kytkimeen tai reitittimeen. Tähtitopologiassa tietoverkon kaikki liikenne kulkee keskuslaitteen kautta. Tähtitopologia eroaa rengastopologiasta siten, että rengastopologiassa laitteet ovat kytketty toisiinsa ilman keskuslaitetta. Tähtitopologiassa yhden laitteen menettäessä yhteyden keskuslaitteeseen, se ei vaikuta koko verkon toimintaan.



Kuva 4. Mesh-topologia (Davies 2019)

Mesh-topologiassa (kuva 4) laitteet ovat kytketty toisiinsa useilla yhteyksillä. Mesh-topologiassa laitteet voivat lähettää dataa monia eri reittejä. Yhden yhteyden katketessa laite pystyy lähettämään datan toista reittiä pitkin. Mesh-topologiassa kaapeleiden ja liittimien määrä kasvaa suureksi, eikä se skaalaudu hyvin pieniin lähiverkkoihin. Mesh-topologiaa käytetään usein MAN ja WAN-verkoissa. (Lowe 2018.)

2.5 Pilvipalvelut

Pilvipalveluilla tarkoitetaan tietojenkäsittelykapasiteetin tai -palvelun jakamista ja käyttämistä verkon yli. Näitä ovat esimerkiksi tallennustila, tietoverkkoratkaisut ja sovelluskehitysalustat. Pilvipalveluiden tuottamisessa käytetään jaettujen, skaalautuvien ja joustavien resurssien mallia. (Lowe 2018.)

Pilvipalveluita on saatavilla monenlaisia ja monia erilaisia käyttötarpeita varten. Yleensä pilvipalvelut jaetaan julkipilveen ja yksityiseen pilveen. Julkisella pilvellä tarkoitetaan kolmannen osapuolen tarjoamia resursseja yritysten tai yksityishenkilöiden käyttöön. Näihin resursseihin lukeutuu tietokoneiden ja tietoverkkojen käyttämät laitteet, tallennustila, rajapinnat ja lukuisat eri palvelut. Yksityinen pilvi koostuu samoista resursseista kuin julkinen pilvi, mutta on ainoastaan tietyn yrityksen, sen työntekijöiden, kumppanien ja asiakkaiden käytössä. Yritys voi rakentaa ja hallita yksityistä pilveä itse, tai jättää sen kolmansien osapuolien vastuulle. Julkisen pilven ja yksityisen pilven yhdistelmää kutsutaan hybridipilveksi. (Kirsch & Hurwitz 2020.)

Pilvipalvelut voidaan jakaa kolmeen yleisimpään palvelumalliin. Palvelumallit ovat infrastruktuuri palveluna (Infrastructure as a Service, IaaS), sovelluskehitysalusta palveluna (Platform as a Service, PaaS) ja sovellus palveluna (Software as a Service, SaaS). IaaS-mallissa palveluntarjoajalta vuokrataan palvelut sisältäen käyttöjärjestelmän, tallennustilan ja tietoverkkoratkaisut. Toisin sanoen IaaS-mallissa palveluntarjoaja vuokraa asiakkaan käyttöön virtuaalipalvelimen tämän valitsemalla käyttöjärjestelmällä varustettuna. PaaS-mallissa käyttöjärjestelmä ja sovelluskehitystyökalut ovat valmiina. PaaS-mallin avulla sovelluskehitys onnistuu pilvessä, eikä infrastruktuuriin tarvitse ottaa kantaa. SaaS-mallissa palveluntarjoaja tarjoaa sovelluksen kokonaisuudessaan, ja käyttäjillä on valmis palvelu käytössään. SaaS-palveluihin lukeutuvat esimerkiksi Microsoft Outlook, Netflix ja Facebook. (Kirsch & Hurwitz 2020; Kyberturvallisuuskeskus 2020.)

Pilvipalvelut vaativat toimiakseen pilvi-infrastruktuurin, johon kuuluu fyysinen laitteisto, virtualisointi, tallennustila ja verkkoympäristö. Pilvipalveluntarjoajilla on käytössään useita datakeskuksia eri puolilla maailmaa, joiden avulla pilvipalvelut toteutetaan. Fyysiseen laitteistoon kuuluu kytkimiä, reitittimiä, palomuureja, verkkolevyjä ja palvelimia.

Virtualisoinnin avulla fyysiset laitteistot on mahdollista jakaa pienempiin resursseihin, ja käyttäjät voivat muokata tarvitsemansa resurssit oikean kokoisiksi virtualisoinnin avulla. Esimerkiksi virtuaalipalvelimen laskentateho, keskusmuisti ja tallennustila voidaan muokata tarpeita vaativiksi. Verkkoympäristö on toteutettu datakeskuksissa kaapeleiden ja verkon aktiivilaitteiden avulla. Datakeskusten tietoverkko pilkotaan virtuaalisiin aliverkkoihin, ja asiakkaan käyttöön tarjotaan virtualisoitu verkkoympäristö. (Red Hat.)

2.6 SDN eli Software Defined Networking

Software Defined Networking tai suomeksi ohjelmisto-ohjattu tietoverkko on moderni teknologia, jonka avulla tietoliikenneverkkoja voidaan ohjata ohjelmistojen avulla keskitetysti. Perinteisesti verkkolaitteet kuten kytkimet ja reitittimet ovat konfiguroitu erikseen ja kiinteästi, ja niiden konfigurointia varten laitteisiin otetaan yhteys niiden hallintaliittymän kautta. Verkkolaitteiden konfigurointi tapahtuu yleensä yksitellen ja ylläpitäjän toimesta. SDN-ohjatut verkkolaitteet mahdollistavat niiden keskitetyn hallinnan, ja niille voidaan jakaa sääntöjä ohjelmallisesti. IT- ja verkkoympäristöt muodostuvat nykyään yhä useammasta laitteesta, ja jokainen laite vaatii konfigurointia, joka on verkon ylläpitäjien vastuulla. Reitittimissä tulee konfiguroida reititys, ja lisäksi palvelimia varten palomuuriin ja kuormantasaukseen liittyviä sääntöjä. Useiden laitteiden sääntöjen konfigurointi käy työlääksi suurissa verkkoympäristöissä. SDN-verkoissa verkon muutokset voidaan toteuttaa API-rajapinnan avulla ohjelmallisesti ilman, että ylläpitäjän tarvitsee konfiguroida jokainen laite erikseen. (Wallenius 2021.)

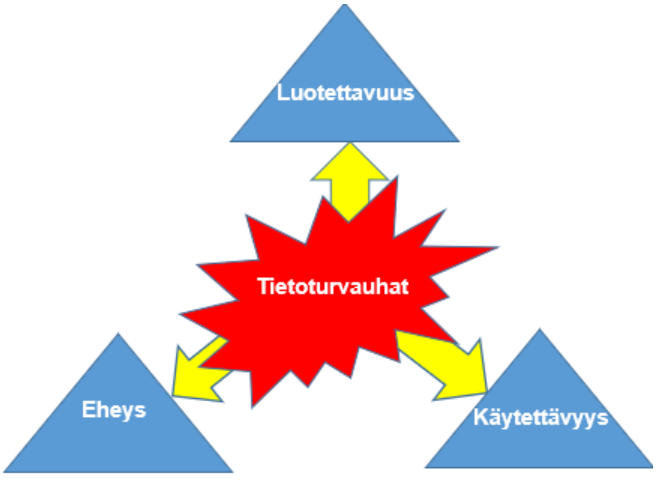
SDN-verkot soveltuvat varsinkin suurten verkkoympäristöjen hallinnointiin, ja SDN-teknologia on laajalti käytössä pilvipalveluiden toteutuksessa. Suurten pilvipalveluntarjoajien ympäristöjen hallinnointi kävisi mahdottomaksi, sillä näissä ympäristöissä verkkolaitteita on yleensä tuhansia. SDN-teknologian avulla asiakkaiden tarvitsemat verkot luodaan pilviympäristössä automaattisesti. Vaikka SDN-teknologia on laajalti käytössä pilviympäristöissä, käytetään sitä myös fyysisten verkkojen hallinnoinnissa. SDN-teknologian etuna on ketteryyden lisäksi myös parempi verkon tietoturva. SDN-verkkolaitteet eivät ole tietoisia muista laitteista, ja kuljettavat paketteja vain niille määrättyihin osoitteisiin. Koska SDN-verkkolaitteet eivät tiedä muista laitteista, niiden kautta ei ole myöskään mahdollista päästä muihin verkkoihin. (Wallenius 2021.)

3 Tietoverkkoihin kohdistuvat uhat

Tietoverkkojen muodostuessa jatkuvasti laajemmiksi ja monimutkaisemmiksi, niihin kohdistuvat uhat eivät muutu yksinkertaisemmiksi, tai katoa mihinkään. Moderniin ja nykypäiväiseen tietoverkkoon kohdistuvat uhat alkavat käydä monimutkaisemmiksi ja edistyneemmiksi. Uhkia tulee myös jatkuvasti uudenlaisia, ja yritysten täytyykin panostaa tietoturvaan entistä enemmän ja tehokkaammin. Useasti kuulee puhuttavan eräänlaisesta kilpajuoksusta, jossa tietoturvan ammattilaiset yrittävät keksiä keinoja torjua viimeisimmät uhat, kun samaan aikaan hyökkääjät ovat jo keksineet uusia keinoja murtaa suojaukset.

Viikoittain uutisoidaan uusista tietomurroista ja tietovuodoista, joiden kohteena ovat olleet ihmisten henkilötiedot, pankkitunnukset, potilastiedot, yritykset ja jopa eri maiden hallitukset. Hyökkäyksiä on nähty viimeisten vuosien aikana kohdistuvan moniin isoihin brändeihin kuten Target, Home Depot, JP Morgan Chase, Sony, Apple ja useisiin muihin isoihin toimijoihin. Hyökkääjien onnistuessa läpäisemään suurimpien ja tunnetuimpien yritysten puolustuksen, herää kysymys, onko pienemmillä yrityksillä ja kohteilla mahdollisuutta suojautua nykypäiväisistä hyökkäyksistä? (Williams, Aslam, Siegel & Donaldson 2015.)

Williams ym. mainitsee kirjassaan, että riippumatta kyberhyökkäyksen tekniikasta tai tavoitteesta, hyökkäykset vaikuttavat yleisesti kolmeen asiaan yrityksessä tai sen datassa. Kyberhyökkäykset vaarantavat tiedon luotettavuuden varastamalla datan, eheyden muokkaamalla dataa ja käytettävyyden estämällä pääsyn dataan tai niitä sisältäviin palveluihin.



Kuva 5. Tietoturvan kolme ulottuvuutta (Williams ym. 2015)

3.1 Tietoturva ja kyberturva

Termejä tietoturva ja kyberturva käytetään yleensä samaa tarkoittavina, vaikka ne tarkalleen ottaen tarkoittavatkin eri asioita. Termit liittyvät kuitenkin vahvasti toisiinsa. Tietoturvalla tarkoitetaan kaiken organisaatiossa olevan tiedon saatavuuden, eheyden ja luotettavuuden turvaamista, riippumatta siitä, onko tieto sähköistä tai paperilla. Yleisesti ottaen tietoturva käsittää myös fyysiset, ympäristölliset ja teknologiset valvontamenetelmät, kuten esimerkiksi lukolliset tiedostokaapit tai ovikoodilla suojatut ovet. (Calder 2020.) Tietoturva kuvataan monesti myös niin sanotulla CIA-kolmiolla (Kuva 5. Tietoturvan kolme ulottuvuutta (Williams ym. 2015 Kyberturva on tietoturvan osa, joka pyrkii suojaamaan samoja asioita kuin tietoturva, mutta keskittyy nimenomaan sähköiseen tietoon (Calder 2020).

3.2 Palvelunestohyökkäys

Distributed Denial of Service (DDoS) eli hajautettu palvelunestohyökkäys vaikuttaa tiedon saatavuuteen estämällä pääsyn siihen. Palvelunestohyökkäyksiä voi olla vaikea tunnistaa etenkin, jos järjestelmät ja niiden toiminta, joihin se kohdistuu, hidastuu mutta ei lamauta niitä kokonaan. Palvelunestohyökkäyksen tarkoituksena on lamauttaa uhrin käyttämät palvelut. Palvelunestohyökkäykset ovat yleisiä, ja voivat kaataa suurenkin osan uhrin käyttämistä palveluista, ennen kuin hyökkäystä voidaan lievittää tai hyökkääjä lopettaa hyökkäyksen. (Williams ym. 2015.)

Palvelunestohyökkäyksessä hyökkääjä lähettää valtavan määrän dataa uhrin palvelimille, jolloin palvelimet ylikuormittuvat, joka johtaa niiden kaatumiseen tai palveluiden hidastumiseen. Palvelinten ylikuormittamiseen tai palveluiden hidastamiseen tarvittava verkkoliikenteen määrä on niin suuri, ettei sitä voi toteuttaa yhdellä tai edes kymmenellä tietokoneella. Yleensä palvelunestohyökkäykset toteutetaankin käyttämällä valtavaa joukkoa haittaohjelmalla saastuneita tietokoneita eli bottiverkkoa. Bottiverkkoja on myös mahdollista vuokrata omaan käyttöön, ja kohdistaa palvelunestohyökkäys haluttuun kohteeseen. Bottiverkkojen vuokraamiseksi ja tätä kautta palvelunestohyökkäyksen laukaisemiseksi, ei vaadita teknisiä taitoja, ja käytännössä kuka vain voi laukaista palvelunestohyökkäyksen vuokraamalla siihen tarkoitetun bottiverkon käyttöönsä.

3.3 Bottiverkot

Bottiverkko koostuu valtavasta määrästä saastuneita päätelaitteita, jotka vastaanottavat käskyjä hyökkääjältä ja toimii niiden perusteella. Saastuneita päätelaitteita kutsutaan ”zombeiksi” tai ”boteiksi”. Botit ovat internetiin yhdistettyjä laitteita, jotka ovat hyökkääjän

hallussa. Hyökkääjä käyttää botteja laukaistakseen kyberhyökkäyksiä, ja koska hyökkäykset ovat lähtöisin muilta kuin hyökkääjän omilta laitteilta, on hyökkäystä vaikeaa jäljittää ja yhdistää itse hyökkääjään. Botit hyväksikäyttävät haavoittuvuuksia ja kopioivat itseään automaattisesti. Bottiverkkoja käytetään esimerkiksi palvelunestohyökkäyksissä, roskapostin lähettämisessä tai arkaluontoisen tiedon keräämisessä. Bottiverkot koostuvat tyypillisesti sadoista tuhansista tai jopa miljoonista boteista. (Irwin & Wu 2016.)

Viime vuosikymmenen aikana eniten huomiota saanut bottiverkko on nimeltään Mirai. Mirai koostuu pääsääntöisesti IoT-laitteista, ja hyödyntää levitäkseen niiden heikkoja oletussalasanoja. Mirai haittaohjelmalla on avoin lähdekoodi, ja se on luettavissa julkisesti verkossa.

Mirai-haittaohjelman saastuttamien laitteiden bottiverkkoa käytettiin vuoden 2016 lopussa laukaisemaan poikkeuksellisen tehokkaita palvelunestohyökkäyksiä, joihin arvellaan osallistuneen yli 600 000 saastunutta laitetta. Hyökkäykset kohdistuivat merkittäviin toimijoihin, joista yksi oli tietoturvablogia ylläpitävä Krebs on Security. Hyökkäyksessä lähetetyn datan määrän mitattiin olevan yli 600Gbit/s, joka tekee siitä yhden suurimmista mitatuista palvelunestohyökkäyksistä. (Antonakakis 2017.)

3.4 Haittaohjelmat

Haittaohjelmia on olemassa erityyppisiä ja ne ovat kehittyneet vuosien varrella yhä monimutkaisemmiksi. Haittaohjelmat ovat tietokoneohjelmia, jotka tarkoituksellisesti aiheuttavat tietojärjestelmän tai laitteen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Haittaohjelmien kirjoittajien tarkoituksena on rikkoa tiedon luotettavuus, käytettävyys ja/tai eheys. (Rains 2020.) Haittaohjelmat pyrkivät naamioitumaan osaksi jotain hyödyllistä ohjelmaa, viestiä, dokumenttia tai dataa, ja käyttää hyväkseen järjestelmässä olevia haavoittuvuuksia saavuttaakseen tavoitteensa. Nykyään haittaohjelmilla on useita ominaisuuksia ja niissä yhdistyvät useat eri haittaohjelmatyypit. Tällä hetkellä tyypillinen haittaohjelma koostuu troijalaisesta, rootkit-haittaohjelmasta, viruksesta, madosta ja bottiverkosta. (Irwin & Wu 2016.)

3.4.1 Madot

Madot ovat tietokoneohjelmia, jotka levittävät kopioita itsestään muihin verkkoon kytkettyihin laitteisiin. Madot ovat suunniteltu levittämään itseään ja saastuttamaan mahdollisimman monta laitetta. Laajalle levinneet madot voivat aiheuttaa merkittävää haittaa verkkoliikenteeseen. Pahimmassa tapauksessa, jossa liian monta laitetta lähettää kopioita madosta, saattaa koko tietoverkko lamaantua. Tietoverkko saattaa pysyä lamaantuneena, kunnes madon saastuttamat laitteet puhdistetaan tai kytketään pois verkosta.
Madot käyttävät useita erilaisia leviämismekanismeja levittääkseen ja kopioidakseen itseään tietoverkossa. Matojen leviämismekanismeja ovat esimerkiksi P2P ja IRC pikaviestintä protokollat, SQL injektio, web-sivut, puskurin ylivuoto, sähköposti ja tiedostojen jako. Sosiaalisen median yleistyessä, palveluita kuten Facebook ja Twitter on käytetty levittämään matoja. Tapauksissa, joissa mato on levinnyt sosiaalisen median alustoilla, madon tarkoituksena on ollut ottaa haltuun käyttäjän tili päätelaitteen sijasta. Monimutkaisin tällä hetkellä tunnettu mato on Stuxnet-mato, joka löydettiin vuonna 2011. Stuxnet-mato turvautuu 0-päivä haavoittuvuuten ja leviää sitä hyväksikäyttämällä USB-tikuista sisäverkkoihin. (Irwin & Wu 2016; F-secure.)

3.4.2 Troijalaiset

Troijalaiset ovat käytännöllisiä ohjelmistoja kuten pelejä tai ohjelmistopäivityksiä, joihin on piilotettu haittaohjelma. Tämä haittaohjelmatyyppi tekee jotain haitallista tai kiellettyä, antaa hyökkääjälle pääsyn rajoitettuihin resursseihin, levittää virusta/matoa tai asentaa kohdejärjestelmään takaoven. Takaovella tarkoitetaan piilotettua sisäänkäyntiä järjestelmään, joka kiertää järjestelmässä olevat turvamekanismit. Takaovi mahdollistaa järjestelmään pääsyn niiltä, joilla ei normaalisti olisi tarvittavia valtuuksia. (Irwin & Wu 2016.)

3.4.3 Rootkit-haittaohjelma

Rootkit-haittaohjelman ominaispiirre on pysyä piilossa. Rootkit-haittaohjelma kaivautuu syvälle käyttöjärjestelmään, ja muokkaa sitä tavoin, jolla se onnistuu pitämään itsensä ja muut haittaohjelmat piilossa, jotta niitä ei ole mahdollista poistaa käyttöjärjestelmästä. Rootkit-haittaohjelmat pystyvät piilottamaan itsensä jopa virustentorjuntaohjelmistoilta. (Irwin & Wu 2016.)
Rootkit-haittaohjelmat muokkaavat myös käyttöjärjestelmän oikeuksia siten, että haittaohjelmalla on täydet valtuudet sen sisällä. Täysiä valtuuksia kutsutaan joissain käyttöjärjestelmissä nimellä root, tämän vuoksi haittaohjelmatyyppiä kutsutaan nimellä rootkit. (Williams ym. 2015.)

3.4.4 Virukset

Virukset kiinnittyvät muihin käyttöjärjestelmän ohjelmiin voidakseen suorittaa haittakoodin ja levittää itseään. Virukset eivät pysty suorittamaan niissä olevaa haittakoodia tai levittämään itseään ilman toista ohjelmaa. (Williams 2015.)
Samalla tavoin kuin biologiset virukset, tietokonevirukset sisältävät ohjeet sen leviämistä varten. Suoritettaessa viruksen sisältämä haittakoodi, se kykenee toteuttamaan siihen kirjoitettuja käskyjä kuten lataamaan tiedostoja tai käynnistämään muita ohjelmia. (Irwin & Wu 2016.)

3.4.5 Kiristyshaittaohjelmat

Viime vuosien aikana on uutisoitu yrityksistä, jotka ovat joutuneet keskeyttämään tai jopa lopettamaan toimintansa kokonaan kiristyshaittaohjelmien lamauttaessa yrityksen IT-infrastruktuurin.
Kiristyshaittaohjelmat saastuttavat uhrin tietokoneen ja salaavat niissä olevan datan, jonka jälkeen haittaohjelma pyytää lunnaita salausavainta vastaan. Kiristyshaittaohjelmat voivat olla kallis kiusa yksittäisille käyttäjille, mutta yrityksiin kohdistuessa lamauttaa ne täysin. (Williams ym. 2015.)
Kiristyshaittaohjelmat tulivat näkyvästi julkisuuteen kesällä 2017, kun haittaohjelmat WannaCry ja NotPetya kylvivät tuhoa ympäri maailmaa. Näiden tapausten jälkeen on raportoitu valtava määrä yrityksiin ja palveluihin kohdistuvista kiristyshaittaohjelmahyökkäyksistä. WannaCry-kiristyshaittaohjelma levisi pandemian omaisesti toukokuussa 2017. WannaCry levisi tietokoneissa, jotka käyttivät käyttöjärjestelmänään Microsoft Windowsia ja pääasiassa Windows XP:tä. Uhriksi joutuneiden tietokoneiden data salattiin, ja uhreilta vaadittiin lunnaita tiedostojen salauksen purkamista vastaan. Tämä hyökkäys levisi laajalle, sillä uhrien tietokoneisiin ei ollut asennettu viimeisimpiä ohjelmistopäivityksiä. Kyberhyökkäyksestä vastuussa olevat rikolliset käyttivät Windows-käyttöjärjestelmissä ollutta haavoittuvuutta, käyttämällä oletettavasti Yhdysvaltain tiedustelupalvelu NSA:n kehittämää hyökkäysmenetelmää. Hyökkäysmenetelmä nimeltään EternalBlue vuodettiin julkisuuteen hakkeriryhmän ”Shadow Brokers” toimesta. Microsoft julkaisi päivityksen, joka suojasi tietokoneita EternalBlue-hyökkäysmenetelmältä kaksi kuukautta ennen WannaCry:n leviämistä. Monien yksittäisten käyttäjien ja yritysten laiminlyödessä ohjelmistojen päivitykset WannaCry levisi hallitsemattomasti ympäri maailmaa. WannaCry saastutti maailmanlaajuisesti noin 230 000 tietokonetta. Ensimmäisten uhrien joukossa oli espanjalainen teleoperaattori Telefónica. Kyberhyökkäyksen kriittisimpänä uhrina voidaan kuitenkin pitää Iso-Britannian julkista terveydenhuoltoa. Tuhannet julkisen terveydenhuollon sairaalat ja niissä tehdyt leikkaukset sekä operaatiot kärsivät kiristyshaittaohjelman aiheuttamista vahingoista. Kolmasosa koko Iso-Britannian julkisen terveydenhuollon sairaaloista

joutuivat iskun uhriksi. Hyökkäys vaikutti jopa ambulanssien reitteihin, ja on raportoitu ihmisistä, jotka jäivät ilman kiireellistä apua sitä tarvitessaan. Iso-Britannian julkisen terveydenhuollon on arvioitu kärsivän jopa 92 miljoonan punnan tappiot, sillä jopa 19 000 ajanvarausta jouduttiin perumaan kyberhyökkäyksen aiheuttamien vahinkojen vuoksi. WannaCry:n levitessä ympäri Eurooppaa, tietokonejärjestelmät 150 eri maassa lamaantuivat hyökkäyksen takia. WannaCry:n on arvioitu aiheuttaneen 4 miljardin dollarin edestä taloudellista vahinkoa maailmanlaajuisesti. (Kaspersky 2020.)

3.5 APT eli kohdistettu haittaohjelmahyökkäys

Advanced Persistent Threat (APT) tai suomeksi, kohdistettu haittaohjelmahyökkäys on tietoverkkohyökkäys, jonka takana ovat yleensä valtiolliset toimijat. Kohdistettujen haittaohjelmahyökkäysten operoijista puhutaan yleensä APT-ryhminä. Esimerkki toimialalla tunnetusta APT-ryhmästä on APT38 tai Lazarus Group, jolla on vahvat kytkökset Pohjois-Koreaan. APT38-ryhmää pidetään syyllisenä kiristyshaittaohjelma WannaCry:n levittämiseen kesällä 2017. Kyberturvayhteisö seuraa näiden ryhmien toimintaa, ja yhdistelee niiden käyttämiä tunkeutumistaktiikoita sekä kampanjoita, ja sitä kautta nimeävät ryhmiä (MITRE 2021).

Nämä uudenlaiset hyökkäykset poikkeavat tavanomaisista kyberhyökkäyksistä, eikä ainoastaan sen vuoksi että ne ovat erityisen edistyneitä. Kohdistetut haittaohjelmahyökkäykset tuovat esiin sen faktan, että nykypäivän kyberhyökkäykset ovat laajalti ammattimaisempia ja järjestäytyneitä kuin koskaan aikaisemmin. Kohdistetun haittaohjelmahyökkäyksen operoija tai operoijat ovat hyvin taitavia hakkereita, ja hyväksikäyttävät useita teknologioita ja haavoittuvuuksia tunkeutuakseen kohteen suojausten läpi systemaattisesti. Kohdistettu haittaohjelmahyökkäys eroaa tavanomaisesta haittaohjelmasta siten, että se on kohdistettu tiettyyn toimijaan kuten yritykseen tai valtioon, ja uhka on pysyvä (persistent), kunnes hyökkäyksen toteuttajat ovat saavuttaneet tavoitteensa. Kohdistetut haittaohjelmahyökkäykset ovat keskittyneitä tiettyyn kohteeseen, ja yleensä niiden operoijat toimivat jonkun ulkovaltion toimesta. Hyökkäyksen tavoitteena voi olla varastaa yrityssalaisuuksia, tai jopa valtiotason asiakirjoja. Vaikka kyseessä olisi suuri ja hyvin suojattu yrityksen tai valtionhallinnon tietojärjestelmä, hyökkääjät eivät luovuta törmätessään esteisiin. Vaikka kyseessä olisikin kuinka edistynyt ja vaikeasti läpäistävä kyberturvainfrastruktuuri, kohdistetun haittaohjelmahyökkäyksen operoijat usein onnistuvat murtamaan sen lopulta. (Williams ym. 2015.)

3.6 Tietomurrot

Tietomurroissa tiedon luotettavuus vaarantuu. Nykyään suuri osa tietoturvaloukkauksista, joista uutisoidaan, on tietomurtoja, ja tästä hyvänä esimerkkinä voidaan pitää psykoterapiakeskus vastaamon tapausta, joka kuohutti mediassa vuoden 2020 lopussa. Tietomurtojen kohteeksi joutuneen datan tyyppi vaihtelee, mutta yleisiä vuodettuja tietoja ovat esimerkiksi sosiaaliturvatunnukset, pankkikorttien numerot, terveystiedot, yrityssalaisuudet ja yritysten johtoportaan kirjeenvaihto. Varastettu data myydään eteenpäin siitä eniten maksavalle. Tietomurrot keskittyvät murtautumaan paikkaan, jossa dataa säilytetään. Data voi olla varastoituna esimerkiksi tietokantaan, varmuuskopioihin tai sovelluspalvelimiin. Yksi lähestymistapa voi olla myös varastaa tietojärjestelmän ylläpitäjän käyttäjätunnukset. (Williams ym. 2015.)
Psykoterapiakeskus vastaamon tapauksessa hyökkääjä pääsi oletettavasti käsiksi tietokantaan, joka sisälsi potilaskertomuksia ja henkilötietoja mukaan lukien sosiaaliturvatunnukset.

3.7 Haavoittuvuudet

Haavoittuvuudella tarkoitetaan vikaa ohjelmakoodissa tai laitteistossa, jota hyväksikäyttämällä hyökkääjän on mahdollista murtautua tietojärjestelmään, ja suorittaa haitallista koodia. Osa haavoittuvuuksista on mahdollista korjata ohjelmistopäivityksillä, mutta kriittisimmät haavoittuvuudet voivat vaatia koko järjestelmän uudelleen suunnittelua tai teknologian korvaamista uudella. (Williams ym. 2015.)

Nollapäivähaavoittuvuudella tarkoitetaan haavoittuvuutta, joka on julkaistu ennen kuin haavoittuvuudesta vastuussa oleva taho, on julkaissut haavoittuvuuden korjaavan päivityksen. Useissa tapauksissa vastuussa oleva taho ei ole tietoinen haavoittuvuudesta, jolloin suojauspäivitystäkään ei ole julkaistu. Tämä tilanne mahdollistaa hyökkääjän hyväksikäyttävän haavoittuvuutta. Nollapäivähaavoittuvuudet ovat arvokkaita, joista hyökkääjät ja valtiot ovat valmiita maksamaan jopa miljoona dollaria. (Rains 2020.)

4 Uhilta suojautuminen

Tietoverkkoihin kohdistuvilta uhilta on pyritty suojautumaan niin kauan kuin niitä on ollut olemassa. Suojautumiskeinoja on vuosien varrella kehitetty monenlaisia, ja yrityksillä on ollut käytössä paljon erilaisia suojautumiskeinoja. Yleisin ja ehkä myös vanhin näistä yksittäisistä suojautumiskeinoista on palomuuri. Ajan saatossa uhat ja hyökkääjät ovat kuitenkin kehittyneet, eikä pelkkä palomuuri yksinään ole enää riittävä keino suojaamaan nykyaikaista tietoverkkoa.

4.1 Palomuuri

Palomuurin tarkoitus on valvoa verkkoliikennettä, joka tulee julkisesta Internetistä sisäiseen verkkoon. Palomuuri toimii esteenä oletettavasti turvallisen ja luotettavan sisäverkon ja uhkia täynnä olevan julkisen Internetin välillä. (Irwin & Wu 2016.)
Yksinkertainen kuvaus palomuurin toiminnasta on joko sallia tai estää saapuva tai lähtevä tietoliikenne perustuen ennalta määriteltyihin kriteereihin. Nämä kriteerit voivat olla palomuurin käyttämiä oletussääntöjä, käyttäjän itse luomia sääntöjä tai näiden yhdistelmiä. (Davies 2019.)

Ilman palomuuria tietoverkon tietoturva jää jokaisen yksittäisen käyttäjän vastuulle, eikä tämä lähestymistapa ole hallittavissa suurissa, eikä edes pienissä tietoverkoissa (Irwin & Wu 2016).

Kyberuhat ovat ajansaatossa siirtyneet alemmilta verkkokerroksilta ylemmäs sovellustasolle, joka on heikentänyt palomuurien tehokkuutta yleisellä tasolla kyberuhkien torjunnassa. Palomuureja tarvitaan kuitenkin edelleen torjumaan merkittävät uhat, jotka toimivat alemmilla verkkokerroksilla. (Irwin & Wu 2016.)

4.2 IDS ja IPS

IDS eli tunkeutumisen havaitsemisjärjestelmä on laite tai tietokoneohjelmisto, joka monitoroi tietoverkkoa tai -järjestelmiä tunnistaen vihamielistä toimintaa. Tunkeutumisen havaitsemisjärjestelmä voidaan jakaa kahteen eri tyyppiin. Konekohtainen järjestelmä eli Host IDS ja verkkopohjainen järjestelmä eli Network IDS. Konekohtainen järjestelmä antaa paremman näkyvyyden yksittäisen päätelaitteen käyttäytymisestä ja siinä suoritettavista sovelluksista. Verkkopohjainen järjestelmä on usein sijoitettu palomuurin tai reitittimen taakse, joka suojaa yrityksen sisäverkkoa Internetistä tulevalta liikenteeltä, ja pystyy suojaamaan useita päätelaitteita. (Irwin & Wu 2016.)

IPS eli tunkeutumisen estojärjestelmä on edistyneempi versio tunkeutumisen havaitsemisjärjestelmästä, sillä IPS kykenee havaitsemisen lisäksi myös estämään haitallisen liikenteen tai verkkoon kohdistetun hyökkäyksen. Järjestelmiä käytetään usein myös rinnakkain, ja silloin niistä puhutaan lyhenteellä IDPS (intrusion detection and prevention system). Tunkeutumisen estojärjestelmä käyttää useita taktiikoita tunnistaakseen ja estääkseen haitallisen toiminnan sekä verkkoliikenteen. Sääntöpohjainen havaitseminen sekä tilastollinen havaitseminen ovat taktiikoista suosituimmat. (Palo Alto Networks.)

Sääntöpohjaista havaitsemista käytetään tunnistamaan tiettyjä tunnettuja haavoittuvuuksia ja niiden hyväksikäyttömenetelmiä. Hyväksikäyttömenetelmät voivat olla esimerkiksi tietyn tyyppistä ohjelmakoodia, skriptejä tai puskurinylivuotoja. Hyväksikäyttömenetelmistä kerätään tiettyjä tunnusmerkkejä esimerkiksi koodirivi, ja tämän avulla merkitään se haitalliseksi, jotta se voidaan tunnistaa ja estää tulevaisuudessa. Sääntöpohjaisen havaitsemisen haasteena on sääntötietokannan koko, ja liikenteen vertaaminen sitä vasten.
Tämä voi hidastaa tunnistusprosessia ja tehdä tunkeutumisen estojärjestelmän haavoittuvaksi palvelunestohyökkäykselle.

Tilastollisessa havaitsemisessa tietoverkon tai päätelaitteen käyttäytymistä seurataan ja tarkkaillaan tietoliikennettä, jonka avulla luodaan profiili. Tämä profiili perustuu useisiin metriikoihin kuten liikenteen määrään, pakettien lukumäärään kussakin protokollassa, yhteyksien määrään ja eri IP-osoitteiden määrään. Näiden metriikoiden avulla luodaan profiili, joka vastaa tavallisen käyttäjän toimintaa tietoverkossa. Tunkeutumisen estojärjestelmän havaitessa epäilyttävää liikennettä tai toimintaa, verrataan sitä profiiliin, joka on luotu tavallisen käyttäjän käyttäytymisen perusteella. Jos epäilyttävä liikenne poikkeaa tavallisen käyttäjän liikenteestä ja toiminnasta, antaa tunkeutumisen estojärjestelmä ilmoituksen. (Irwin & Wu 2016.)

4.3 DMZ

DMZ:lla eli demilitarisoidulla alueella tarkoitetaan erillistä fyysistä tai loogista aliverkkoa, joka on eristetty yrityksen muusta verkosta. Demilitarisoidun alueen tarkoitus on tarjota tietyt palvelut internetiin mahdollisimman turvallisesti. DMZ-verkossa voidaan ylläpitää esimerkiksi web- tai DNS-palvelinta. Näiden palveluiden ollessa auki internetin suuntaan, voi niihin kohdistua hyökkäyksiä. Hyökkääjän onnistuessa murtautumaan DMZ-verkkoon, yrityksen sisäiset palvelut ja tietokoneet ovat paremmin suojassa, sillä ne sijaitsevat eri verkossa. (Irwin & Wu 2016.)

Perinteinen tapa jaotella tietoverkot on ollut jakaa ne kahteen osaan. Palvelut, jotka ovat auki Internetiin on sijoitettu DMZ-verkkoon. Kaikki muut palvelut sijoittuvat ”luotettuun ja turvalliseen” sisäverkkoon. Perinteinen tapa ei ole kuitenkaan osoittautunut toimivaksi. Hyökkääjän päästessä murtautumaan sisäverkkoon, esimerkiksi käyttäjän varastetuilla tunnuksilla, on koko sisäverkko ja sen sisältämät palvelut helposti murrettavissa. (Williams ym. 2015.)

4.4 Verkon segmentointi

Verkon segmentoinnilla tarkoitetaan tietoverkon jakamista erillisiin aliverkkoihin. Verkon segmentoinnilla pyritään parantamaan tietoverkon tietoturvaa ja suorituskykyä. Kun tietoverkko on jaettu pienempiin kokonaisuuksiin, on siinä liikkuvaa tietoliikennettä helpompi seurata ja hallita. (Mukherjee 2020.)

Perinteinen tietoturvastrategia keskittyi suojaamaan tietoverkon reunaa palomuurien ja tunkeutumisen havaitsemisjärjestelmien avulla. Perinteisessä tietoturvastrategiassa sisäverkkoa ja sen käyttäjiä pidettiin turvallisena, eikä sisäverkon tietoturvaan kiinnitetty erityisesti huomiota. Viimeisimmissä suurissa tietomurroissa luottamus sisäverkon käyttäjiin on kuitenkin kyseenalaistettu, sillä käyttäjät sisäverkossa voivat olla tietomurtojen lähde. Lisäksi hyökkääjien läpäistessä tietoverkon reunan suojausmenetelmät, ovat hyökkääjät vapaita liikkumaan sivuttain verkon sisällä, ja näin pääsevät käsiksi luottamukselliseen dataan. Sisäverkon jakaminen erillisiin aliverkkoihin vaikeuttaa hyökkääjien pääsyä liikkumaan verkon sisällä. Sivuttain liikkumisella tietoverkossa tarkoitetaan hyökkääjän murtautumista muihin samassa verkossa sijaitseviin laitteisiin tai tietoihin. (Palo Alto Networks.)

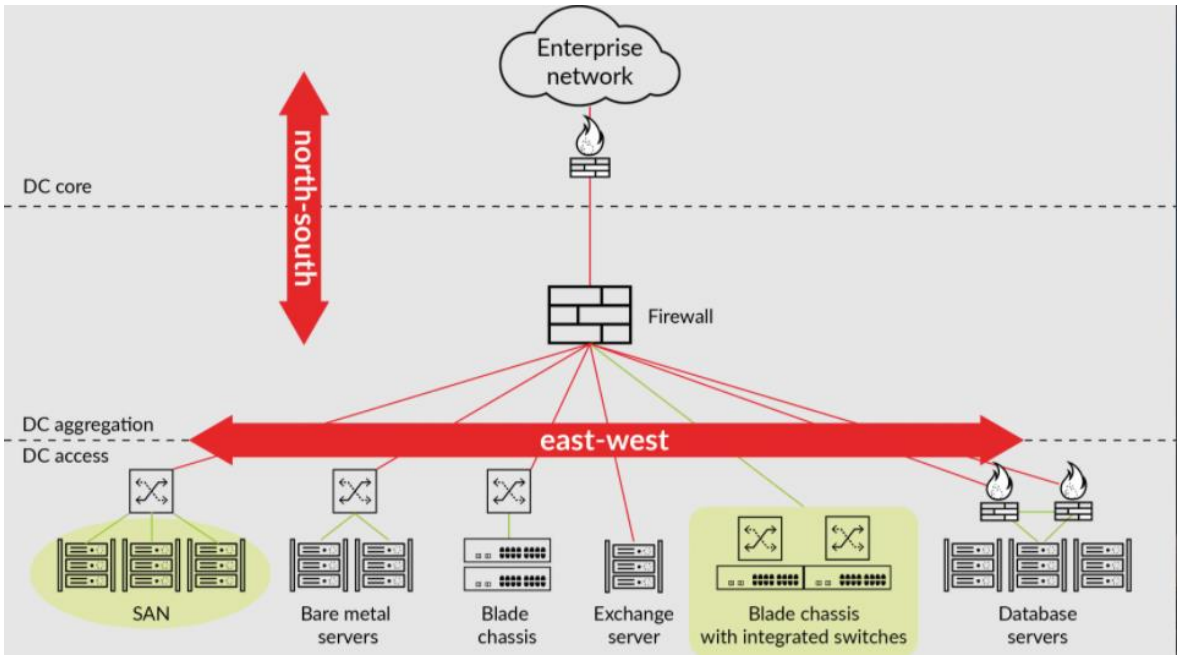
Käyttäjiin luottamisen noustessa puheenaiheeksi monessa tietomurrossa, yritykset ovat alkaneet omaksumaan uudenlaisen Zero Trust-tietoturvastrategian, jota käydään läpi myöhemmin tässä kappaleessa. Zero Trustin perusperiaatteena onkin olla luottamatta kehenkään, edes käyttäjiin, jotka ovat jo verkon sisällä. Verkon segmentoinnin ja Zero Trust-mallin yhdistäminen tuottaa hyökkääjille vaikeuksia. Hyökkääjän päästessä tunkeutumaan ulkoverkosta sisäverkkoon, se ei ole enää riittävä keino päästä käsiksi arkaluontoiseen dataan. Aliverkot, jotka on eristetty toisistaan, pitävät datan turvassa hyökkääjiltä. (Palo Alto Networks.)

4.4.1 Mikrosegmentointi

Perinteinen verkon segmentointimalli jakaa tietoverkon pienempiin aliverkkoihin. Ongelmaksi tietoturvan näkökulmasta kuitenkin nousee käyttäjien suuri määrä aliverkoissa. Vaikka tietoverkko on jaoteltu pienempiin osiin, aliverkkojen käyttäjämäärät voivat nousta

suuriksi. Hyökkääjän onnistuessa murtautumaan yhteen näistä aliverkoista, hyökkääjän on silti mahdollista liikkua aliverkossa sivuttain, ja ottaa haltuun muita käyttäjätilejä sekä päätelaitteita.

Perinteinen verkon segmentointimalli toimii parhaiten tietoverkossa, jossa tietoliikenne kulkee pääasiassa pohjois-etelä -suunnassa eli asiakkaan ja palvelimen välillä. Nykyisin useat hybridipilvi arkkitehtuurit ovat erilaisia, ja tietoliikenne kulkee länsi-itä-suunnassa eli palvelimelta palvelimelle tai sivuttain (kuva 6). Virtuaalipalvelimien käyttö hybridipilviympäristössä on tavallista, ja yksi palvelin voi ylläpitää jopa satoja eri palveluita. Palveluita voi olla esimerkiksi toiset virtuaalikoneet, tietokannat ja sovellukset. Mikrosegmentoinnilla pyritään estämään sivuttaissiirtymää näiden palveluiden välillä hyökkääjän päästessä sisään järjestelmään. (Palo Alto Networks.)



Kuva 6. Tietoliikenteen kulkusuunta (Palo Alto Networks)

4.5 Perimeter Security / perinteinen tietoturvastrategia

Perinteisen tietoturvastrategian periaatteena on suojata tietoverkkoa jakamalla se osiin, ja näin estää hyökkääjien tunkeutuminen verkon kriittisimpiin osiin. Tietoverkko, joka on rakennettu käyttäen perinteistä tietoturvastrategiaa, kuvataan usein niin, että sillä on kova ulkokuori mutta pehmeä sisus. Kuvausta käytetään, sillä kun tietoverkkoon murtaudutaan, mikään ei estä hyökkääjiä liikkumasta verkon sisällä vapaasti, tai pysymään sen sisällä ikuisesti. Strategia keskittyy pitämään hyökkääjät loitolla panostamalla verkon suojausteknologioihin kuten palomuureihin, DMZ-verkkoihin, proxypalvelimiin ja segmentaatioon. 2000-luvun alkupuolella lähes jokainen kyberhyökkäys toteutettiin hyväksikäyttämällä tie-

toverkkojen haavoittuvuuksia. Tämän vuoksi tietoverkkoammattilaiset käyttivät osaamistaan parantamaan nimenomaan tietoverkkojen tietoturvaa. Monet yritykset laajensivatkin tietoverkkotiimejään vahvistamaan tietoverkkojen tietoturvaa ja panostivat DMZ-verkkoihin sekä palomuurien hallinnointiin. Asiantuntijoita, jotka tuntevat teknologiat kuten TCP/IP, reitittimet, kytkimet ja palomuurit on paljon verrattuna toisten tietoturvateknologioiden kuten sovellusten tietoturvan tai haittaohjelmien analysoinnin asiantuntijoihin. Koska perinteinen tietoturvastrategia on suhteellisen vanha, ja se on ollut käytössä vuosia, sen ympärillä on edelleen paljon palveluntarjoajia. Tämän vuoksi monille yrityksille on luonnollista edelleen turvautua tuttuun ja perinteiseen tietoturvastrategiaan. (Rains 2020.)

Perinteisellä tietoturvastrategialla, aivan kuten kaikilla muillakin eri strategioilla on huonot puolensa. Tarkastellessa aikaa 15-20 vuoden takaa, historia on todistanut tämän strategian kehnoksi. Jokaisessa merkittävässä tietomurrossa, joka on päätynyt otsikoihin, on ollut käytössä perinteinen tietoturvastrategia. Syy minkä vuoksi perinteinen tietoturvastrategia on epäonnistunut suojaamaan yritysten tietoverkkoja, piilee strategian perustana toimivassa olettamuksessa. Perinteisen tietoturvastrategian olettamus on, ettei sitä soveltaviin yrityksiin ole mahdollista tunkeutua, sillä ne pystyvät suojaamaan itsensä täydellisesti. Tämä olettamus on kuitenkin kovin optimistinen. (Rains 2020.)

4.6 Zero Trust

Zero Trust -suojausmallin periaate on, ettei mihinkään resurssiin, edes niihin, jotka ovat yritysverkon sisällä, tulisi luottaa. Zero Trust -suojausmalli auttaa torjumaan tietomurtoja poistamalla luottamuksen yrityksen tietoverkkoarkkitehtuurista. Zero Trust -suojausmallin motto onkin ”älä koskaan luota vaan tarkista aina”. Zero Trust on suunniteltu suojaamaan moderneja yritysverkkoja käyttämällä verkon mikrosegmentointia, jolla pyritään estämään sivuttaissiirtymä hyökkääjän päästessä murtautumaan verkkoon. Zero Trust kehitettiin, kun tajuttiin että perinteiset suojausmallit toimivat sillä periaatteella, että kaikkeen mikä on yritysverkon sisällä, voidaan luottaa. Perinteiset suojausmallit siis luottivat siihen, ettei käyttäjien identiteetti ole vaarantunut ja että kaikki käyttäjät toimivat luotettavasti verkon sisällä. Zero Trust tunnistaa luottamuksen haavoittuvuutena. Verkon sisällä ollessa, niin käyttäjät kuin hyökkääjätkin ovat vapaita liikkumaan verkon sisällä ja pääsevät käsiksi kaikkeen dataan, joihin heillä on pääsyoikeudet. (Palo Alto Networks.)

Zero Trust -suojausmallin kolmena pääperiaatteena voidaan pitää käyttäjän tai sovelluksen todentamista, päätelaitteen todentamista, ja luottamusta. Päätelaitteiden todentaminen ja valtuuttaminen on yhtä tärkeää kuin käyttäjien ja sovellustenkin. Todentaminen pyritään suorittamaan kaiken saatavilla olevan datan kuten käyttäjätietojen, laitetietojen, sijainnin ja mahdollisten poikkeavuuksien avulla. Todentamisen lisäksi tärkeässä roolissa

on vähimpien oikeuksien periaate. Käyttöoikeudet Zero Trust-verkossa pyritään rajoittamaan siten, ettei käyttäjillä ole kuin ainoastaan tarvittavat käyttöoikeudet. Tällä pyritään estämään sivuttaissiirtymä verkossa. (Gilman & Barth 2017; Microsoft.)
Digitalisaation ja ennennäkemättömien tapahtumien kuten COVID-19 pandemian myötä, yritysten on täytynyt muuttaa työskentelytapojaan. Yhä useammat yritykset sallivat työntekijöiden käyttää työskentelyssään omia laitteitaan (BYOD). Työntekijöiden käyttäessä omia laitteitaan yrityksillä ei ole enää mahdollisuutta kontrolloida yritysverkkoa ja siihen kytkettyjä päätelaitteita. Zero Trust -suojausmalli perustuu käyttäjien ja niiden laitteiden todentamiseen, ja näiden toimien myötä antaa pääsyn yrityksen resursseihin. Zero Trust -suojausmallissa luottamus ei siis määrity sen perusteella, onko käyttäjä tai laite yrityksen sisäverkossa. (Mukherjee 2020.)

4.7 Päätelaitteiden tietoturva

Yritysverkko rakentuu monista osista kuten pilvipalvelimista, verkon aktiivilaitteista ja niitä suojaavista laitteista ja sovelluksista. Oleellisena osana yritysverkkoa ovat myös päätelaitteet, jotka tulee myös suojata niihin kohdistuvilta hyökkäyksiltä. Digitalisaation ja lisääntyneen etätyön vuoksi yhä useammat yritykset ovat siirtyneet BYOD-malliin, jolla tarkoitetaan työntekijöiden käyttävän omia henkilökohtaisia laitteitaan työntekoon. Bring Your Own Device eli BYOD-mallin yleistyessä yrityksillä ei ole enää yhtä tarkkaa kuvaa verkossa olevista laitteista kuin ennen.

Päätelaitteet ovat nykyään suhteellisen hyvin suojattuja, ja esimerkiksi viimeisimpien Windows-käyttöjärjestelmien mukana toimitetaan virustentorjuntaohjelmisto sekä palomuuri. Päätelaitteiden suojaukseen keskittyneitä palveluntarjoajia löytyy markkinoilta suuri määrä. Nykyaikainen yksityiskäyttäjälle tarkoitettu virustentorjuntaohjelmisto koostuu useista eri suojausmenetelmistä. Perinteisen haittaohjelmaskannauksen lisäksi ohjelmistoista löytyy esimerkiksi haitallisten verkkosivustojen suodatusta ja pankkitoimintojen suojausta. Myös VPN-ratkaisut ovat tavallisia päätelaitteiden suojauksessa, ja se saattaa sisältyä joissain tapauksissa virustentorjuntaohjelmistoon.

Päätelaitteiden suojaukseen keskittyneet ohjelmistot tarjoavat jatkuvasti uusia ja kehittyneempiä teknologioita suojatakseen päätelaitteet entistä tehokkaammin. Näihin teknologioihin lukeutuu esimerkiksi haavoittuvuuksien hallintaa, virustentorjuntaa, tiedostojen eheyden monitorointia, päätelaitteiden palomuureja, luotettujen sovellusten listaamista, selainten suojausta, mobiililaitteiden hallintaa ja monia muita. Useat näistä teknologioista löytyy nykyisin sisäänrakennettuna Windows ja Linux käyttöjärjestelmistä, mutta se ei ole estänyt palveluntarjoajia kehittämään palveluistaan entistä parempia. Pelkkä päätelaitteiden

suojaus yritysverkon suojaamiseksi ei kuitenkaan ole tarpeeksi, mutta se on tärkeä osa yrityksen tietoturvastrategiaa. (Rains 2020.)

4.8 Intrusion Kill Chain

Uhrin näkökulmasta on hyödyllistä ymmärtää miten tietomurrot ja kyberhyökkäykset, joissa hakkerit ovat päässeet käsiksi tietokoneisiin ja käyttäjätileihin yrityksen sisällä ovat toteutettu. Yritykset, jotka ymmärtävät miten kyberhyökkäys heitä vastaan on toteutettu, pystyvät vastaisuudessa havaitsemaan ja hidastamaan mahdollisia hyökkäyksiä. Jokainen yksittäinen vaihe hyökkäyksessä tarjoaa mahdollisuuden puolustautumiseen. (Williams ym. 2015.)

Vuonna 2011 useat Lockheed Martinin tutkijat julkaisivat tutkimuksen, jossa tutkittiin APT hyökkäyskampanjoita, ja havaitsivat tietyn järjestyksen toistuvan jokaisessa hyökkäyksessä. Tutkimalla tätä hyökkäysketjua ja eri askeleita hyökkäyksessä, voidaan hyökkäys yrittää pysäyttää. (Williams ym. 2015.)

Kuva 7. Lockheed Martin Kill Chain (Williams ym. 2015)

Kuvassa 7 on havainnollistettu kohdistetun haittaohjelmahyökkäyksen (APT) seitsemän eri vaihetta. Jokaista vaihetta varten on mahdollista suunnitella suojautumiskeinoja.

Selitteet eri vaiheille:

1. **Tiedustelu**: Ensimmäisessä vaiheessa hyökkääjät etsivät uhristaan tietoja Internetistä esimerkiksi sähköpostiosoitteita tai sosiaalisen median tilejä.
2. **Aseistaminen**: Yhdistetään haittaohjelma johonkin toimitettavaan tiedostoon esimerkiksi PDF tai Microsoft Office -tiedostoon.
3. **Toimitus**: Toimitetaan haittaohjelma uhrin ympäristöön. Kolme käytetyintä taktiikkaa ovat sähköpostin liitetiedostot, nettisivut ja USB-tikut.
4. **Hyväksikäyttö**: Kun haittaohjelma on toimitettu, se hyväksikäyttää jotain käyttöjärjestelmän haavoittuvuutta ja ajaa hyökkääjän koodia uhrin ympäristössä.
5. **Asennus**: Haittaohjelma asentaa troijalaisen tai takaoven uhrin järjestelmään, jotta hyökkääjä saa pysyvän pääsyn järjestelmään.

6. **Command & Control (C&C)**: Haittaohjelman saastuttamat järjestelmät ottavat yhteyttä hyökkääjään palvelimille, jonka kautta hyökkääjät antavat käskyjä ja kontrolloivat saastuneita laitteita.
7. **Toiminnot**: Viimeiseen vaiheeseen päästyään hyökkääjä alkaa suorittamaan alkuperäisiä toimintoja murretussa järjestelmässä. Tyypillisesti nämä toiminnot keskittyvät datan varastamiseen uhrin ympäristöstä. Hyökkääjät voivat myös saastuttaa muitakin järjestelmiä uhrin ympäristössä ja liikkua tietoverkossa sivuttain.

Lockheed Martinin hyökkäysketjun lisäksi on olemassa toinen hyökkäyskeskeinen viitehys, jota tietoturvan ammattilaiset käyttävät. Tämä viitekehys on MITRE:n kehittämä kokonaisuus erilaisista hyökkäystaktiikoista, ja on nimeltään MITRE ATT&CK. MITRE ATT&CK:n on tarkoitus täydentää Lockheed Martinin hyökkäysketjua, eikä korvata sitä.

4.9 DDoS hyökkäykseltä suojautuminen

DDoS eli hajautettu palvelunestohyökkäys aiheuttaa uhrilleen merkittävää haittaa, ja voi pahimmassa tapauksessa lamauttaa koko yrityksen liiketoiminnan. Hajautettu palvelunestohyökkäys on pysyvä uhka yrityksille, ja yritysten tulisikin olla tietoisia suojauskeinoista. Hyökkäysten lieventämiseksi tai kokonaan torjumiseksi on oleellista tuntea tietoverkko ja siinä kulkeva tietoliikenne. Tunnistettaessa tietoliikenteen tavanomainen määrä, on helpompi tunnistaa myös tietoverkkoon kohdistuva epätavallinen liikenne, jolloin kyseessä voi olla hajautettu palvelunestohyökkäys.

Perinteinen suojausmenetelmä koostui fyysisistä laitteista, jotka suodattivat haitallisen liikenteen normaalin liikenteen seasta. Perinteinen menetelmä oli kallis hankkia ja ylläpitää. Lisäksi perinteinen menetelmä vaati toimiakseen tarpeeksi suuren verkon, jotta se kykeni ottamaan hyökkäyksen vastaan. Hyökkäyksen ollessa voimakkuudeltaan tarpeeksi suuri, se saattoi kaataa verkon ja ylikuormittaa sitä ylläpitäneet laitteet. Nykyisin hyökkäyksiä voidaan lieventää useiden palveluntarjoajien tarjoamilla pilvipohjaisilla ratkaisuilla. (Cloudflare.)

Cloudflare käy artikkelissaan läpi neljä eri vaihetta, jotka ovat käytössä pilvipohjaisessa hajautetun palvelunestohyökkäyksen lieventämisessä:

1. Havaitseminen – hyökkäyksen torjumiseksi on tärkeää tunnistaa haitallinen liikenne tavallisesta liikenteestä. Yllättäen kohonnut verkkoliikenteen määrä ei vält-

tämättä tarkoita hyökkäystä, sillä kyseessä voi olla esimerkiksi suuri määrä tavallisia käyttäjiä, jotka ovat lataamassa uutta päivitystä samanaikaisesti. Havaitsemisessa auttavat lähde IP-osoitteiden tarkistus, tunnistettavissa olevat hyökkäysmallit sekä aikaisemmista hyökkäyksistä kerätty data.

2. Vastatoimet – kun hyökkäys ja siinä käytetyt menetelmät on tunnistettu, DDoS suojauspalvelu estää osan haitallisesta liikenteestä ja ohjaa osan suojauspalvelun käyttämään verkkoon. Lisäksi käytössä on erikoistuneita suojausmenetelmiä kuten sovellustason palomuuri ja muita suodatusmenetelmiä, joiden avulla hyökkäystä voidaan lieventää.
3. Reititys – jäljellä oleva haitallinen liikenne paloitellaan pienemmiksi osiksi ja reititetään siten, että palvelu pystyy vastaanottamaan kuorman kaatumatta ja hidastumatta.
4. Mukautuminen – hyökkäykseen mukautuminen auttaa vastaamaan hyökkäyksiin tulevaisuudessa. Verkkoliikenteen analysoinnin avulla voidaan kerätä tietoa hyökkääjän käyttämistä IP-osoitteista, hyökkäyksen maantieteellisestä sijainnista ja tietyistä hyökkäyksessä käytetyistä protokollista. (Cloudflare.)

4.10 Yleiset ratkaisut tietoturvallisuuden parantamiseksi

Yleistä tietoturvaa on myös mahdollista vahvistaa ja parantaa yksinkertaisilla keinoilla, jotka eivät vaadi teknistä osaamista kyberturvan alalta, tai aiheuta edes välttämättä lisäkustannuksia. Yritykset voivat edistää työntekijöidensä tietoturvallista käyttäytymistä esimerkiksi ohjeistusten tai koulutusten avulla. Nykyään yhä useammilla yritysten työntekijöillä on omat tietokoneensa, ja on hyvin tärkeää, että työntekijä tuntee tietoturvan perusasiat. Pienilläkin asioilla voi olla hyvin suuri merkitys tietoturvapoikkeamien ehkäisemisessä.

4.10.1 Salasanat

Digitalisaation myötä ihmisten on muistettava useita eri salasanoja, sillä erilaisten sähköisten palveluiden ja tietojärjestelmien määrä on valtava. Useiden eri salasanojen muistaminen käy hankalaksi, ja käyttäjät saattavat käyttää samoja salasanoja eri palveluissa, tai kirjoittaa salasanojaan esimerkiksi muistilapulle. Myös heikkojen ja liian lyhyiden salasanojen käyttö on yleistä. Tällainen toimintatapa on kuitenkin tietoturvan näkökulmasta hälyttävä. Yhden salasanan vuotaessa vääriin käsiin, ovat kaikki tilit vaarassa, joissa on käytetty samaa vuodettua salasanaa. Tästä syystä jokaisessa eri palvelussa ja järjestelmässä tulisi käyttää eri salasanoja. Nykyisin salasanojen muistamisen helpottamiseksi useat eri palveluntarjoajat ovat tuoneet markkinoille salasanan hallintaohjelmia, joihin voi-

daan tallentaa useita käyttäjätunnuksia ja salasanoja. Salasanan hallintaohjelmistojen lisäksi kaksivaiheinen tunnistus lisää käyttäjätilien tietoturvallisuutta. Kaksivaiheinen tunnistus vaatii oikean salasana lisäksi koodin, joka lähetetään esimerkiksi käyttäjän puhelimeen. Näin ollen vuodettua salasanaa ei voida väärinkäyttää, ellei hyökkääjällä ole pääsyä käyttäjän puhelimeen, jota voidaan pitää epätodennäköisenä.

4.10.2 Päivitykset

Päivitykset kuuluvat lähes jokaiseen tekniseen laitteeseen ja ohjelmistoon. Päivityksillä pyritään korjaamaan ohjelmista löytyneitä virheitä, ja näin tekemään niistä turvallisempia. Korjausten lisäksi päivitykset saattavat tuoda myös ohjelmistoihin hyödyllisiä lisäominaisuuksia. (Järvinen & Rousku 2017.)

Päivittämättä jätetyissä laitteissa ja tietojärjestelmissä saattaa piillä kriittisiä tietoturva-aukkoja, joita hyväksikäyttämällä hyökkääjät voivat levittää haittaohjelmaa tai tunkeutua järjestelmään. Kappaleessa 3.4.5 käsitellään vuoden 2017 kiristyshaittaohjelma aaltoa, joka pääsi osin leviämään päivittämättömien Windows-tietokoneiden avulla. Päivityksiä, ja etenkin tietoturvapäivityksiä voidaan pitää tärkeänä osana yleisen tietoturvallisuuden parantamista.

4.10.3 Tietojenkalastelu

Tietojenkalastelu (phishing) on merkittävä uhka yritysten tietoturvallisuudelle. Sähköposti on hyvin yleinen viestintäväline yritysten sisäiseen ja ulkoiseen viestintään. Suurin osa tietojenkalastelusta tapahtuukin juuri sähköpostin välityksellä. Sähköpostin välityksellä tapahtuvassa tietojenkalastelussa hyökkääjän tarkoituksena on saada uhri klikkaamaan haitallista linkkiä. Yleensä tämä toteutetaan väärennetyn sähköpostiviestin avulla, joka on luotu vaikuttamaan oikealta sähköpostilta. Hyökkääjä voi esimerkiksi käyttää väärennettyä pankin sähköpostiviestiä, jossa uhria pyydetään kirjautumaan sisään tililleen, jotta tämä voi tarkastaa epäilyttävät tilitapahtumat. Todellisuudessa sähköpostiviesti ja siinä olevat linkit ovat väärennöksiä, jotka ohjaavat uhrin väärennetylle verkkosivulle. Jos uhri erehtyy syöttämään tietonsa väärennetylle verkkosivustolle, hyökkääjä saa haltuunsa uhrin salasanan. Pahimmassa tapauksessa hyökkääjä pystyy kirjautumaan yrityksen järjestelmiin kaappaamallaan salasanalla.

5 Miten tietoverkkoihin kohdistuvilta uhilta voidaan suojautua?

Tutkiessa moderneja tietoverkkoja ja niihin kohdistuvia kyberuhkia huomattiin tietoverkkoihin kohdistuvan huomattavan paljon erilaisia hyökkäyksiä ja uhkia. Koskaan ei kuitenkaan voi olla varma minkälainen hyökkäys kohdistuu juuri oman yrityksen verkkoon. Tämän seikan vuoksi oikeiden suojausmekanismien valitseminen saattaa olla hankalaa. Tämän tutkimuksen tarkoituksena on antaa osviittaa siitä, minkälaisia uhkia nykypäivän tietoverkkoihin kohdistuu, ja minkälaiset suojausmekanismit ovat riittäviä, tai ovatko ne ylipäätään riittäviä.

Alan kirjallisuutta lukiessa käy ilmi, että kyberturvastrategioita on useita, ja että ne ovat muuttuneet vuosien varrella. Lähdemateriaalia tutkiessa kaksi strategiaa nousee esiin ylitse muiden. Monet teokset käsittelevät niin kutsuttua perinteistä tietoturvastrategiaa, joka keskittyy suojaamaan yrityksen sisäverkon ja Internetin välisen alueen. Toinen näistä strategioista on Zero Trust. Molempia strategioita käsitellään luvussa neljä. Perinteinen tietoturvastrategia ei enää riitä suojautumaan moderneilta kyberhyökkäyksiltä, mutta strategia on silti käytössä useilla yrityksillä. On yllättävää, että monet yritykset luottavat edelleen vanhoihin kyberturvastrategioihin, vaikka on paljon näyttöä niiden toimimattomuudesta nykypäivän moderneja kyberuhkia vastaan.

Rains (2020) käy läpi kirjassaan useita erilaisia yritysten käytössä olevia kyberturvastrategioita. Perinteinen strategia keskittyy palomuureihin, DMZ-verkkoon, proxypalvelimiin ja verkon segmentaatioon, ja sitä voidaan pitää vanhahtavana. Pilvipalveluiden yleistyessä yrityskäytössä hyvin nopeasti, tietoturvastrategia tulisi muuttaa pilviympäristöön sopivaksi. Pilviympäristöön hyvin soveltuva Zero Trust vaikuttaisi olevan tehokas strategia suojata moderni yritysverkko kyberuhilta. Tietoverkkojen moderni hallinnointi esimerkiksi SDN-teknologian avulla voi myös parantaa yritysten tietoturvaa. Yritysten tulisi seurata tietoverkkoteknologioiden ja tietoturvaratkaisujen kehitystä, ja etsiä juuri omaan liiketoimintaan soveltuva ratkaisu. Vaikka Zero Trust-malli näyttää yleistyvän, se ei välttämättä ole kuitenkaan sopivin ratkaisu kaikille yrityksille.

Kappaleessa neljä käytiin läpi yleisimmät uhat, joita nykyaikaiseen tietoverkkoon ja yrityksiin kohdistuu. Kappaleessa viisi on kuvattu yleisimpiä suojausmenetelmiä, joita yhdistelemällä ja käyttöön ottamalla voidaan uhriksi joutumisen todennäköisyyttä pienentää.

Kohdistetut haittaohjelmahyökkäykset, joiden takana on useasti valtion tukema toimija, saattavat olla lähes mahdottomia torjua. Päätelaitteiden tietoturvaohjelmistot ovat hyödylli-

siä ja suojaavat päätelaitteita tunnetuilta haittaohjelmilta, mutta ovat harvoin tarpeeksi torjuakseen kohdistetun haittaohjelmahyökkäyksen. Sosiaalista manipulointia ja tietojenkalastelua vastaan on myös haastavaa suojautua. Vaikka yrityksellä olisi käytössään kuinka monimutkaiset ja tehokkaat tekniset suojautumisratkaisut, ihminen on kuitenkin useasti suojauksen heikoin lenkki. Yritysten työntekijät johtohenkilöstöä myöten tulisikin kouluttaa tunnistamaan sosiaalinen manipulointi ja tietojenkalasteluyritykset. Myös yleiset tietoturvakoulutukset auttavat ennaltaehkäisemään tietomurtoja ja parantavat yritysten tietoturvallisuuden tasoa. Yritysten tulisi huomioida tämä strategiassaan, ja kouluttaa työntekijät työtehtävästä riippumatta.

Erilaisten ja jatkuvasti kehittyvien haittaohjelmien lisäksi hajautetut palvelunestohyökkäykset ovat uhka yritysten liiketoiminnalle ja sen jatkuvuudelle. Teknologian ja tietoliikenneyhteyksien kehittyessä huimaa vauhtia, palvelunestohyökkäykset käyvät vuosi vuodelta haitallisemmiksi. Yritysten tulisi huomioida palvelunestohyökkäyksen uhka kyberturvastrategiassaan. Markkinoilla on useita eri palveluntarjoajia, jotka tarjoavat suojaa hajautettua palvelunestohyökkäystä vastaan.

6 Oma oppiminen opinnäytetyöprosessissa

Opinnäytetyöprosessi on ollut yksi laajimmista itsenäisesti tehdyistä projekteistani, ja pelkästään projektin laajuus on opettanut paljon. Projektin aikana opin eniten ajankäytönhallinnasta ja tieteellisestä kirjoittamisesta. Opinnäytetyön kirjoittaminen ja tietoperustan laatiminen oli hyvin mielenkiintoista, sillä lähdemateriaaliksi sain valita juuri itseäni kiinnostavat aineistot. Projektin laajuudesta huolimatta opinnäytetyöprosessi onnistui mielestäni hyvin ja opinnäytetyö valmistui aikataulussa.

Opinnäytetyön aihe oli itseäni kiinnostava ja tämä teki aiheeseen perehtymisestä ja työn kirjoittamisesta helpompaa. Vaikka osa opinnäytetyön asioista oli minulle entuudestaan tuttua opintojen ja työelämän kautta, opin kuitenkin paljon uutta lähdekirjallisuutta lukiessani. Suuri osa opinnäytetyössäni käyttämästä lähdemateriaalista oli englanninkielistä, ja joidenkin englanninkielisten termien kääntäminen suomeksi aiheutti haasteita. Aihealueen ja tutkittavan ilmiön ollessa kovin laaja, joidenkin asioiden rajaus oli myös haasteellista. Myös tietoperustaa laatiessa ja sopivaa lähdekirjallisuutta etsiessä sopivan kirjallisuuden rajaaminen ja oikean aineiston valitseminen osoittautui hankalaksi, sillä aiheesta löytyi hyvin paljon kirjallisuutta. Vaikka kirjallisuuden suuri määrä tuotti pieniä haasteita opinnäytetyöprosessissa, en kuitenkaan pidä sitä ongelmana, sillä tietoisuutta tästä tärkeästä aiheesta on hyvä olla laajasti tarjolla yrityksille sekä yksityishenkilöille.

Lähteet

Aditya Mukherjee 2020. Network Security Strategies. Packt Publishing. Birmingham.

Alan Calder 2020. Cyber Security: Essential Principles to Secure Your Organisation. IT Governance Publishing. Cambridge.

Chris K. Williams; Abdul Aslam; Stanley G. Siegel; Scott E. Donaldson. 2015. Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. Apress. New York City.

Cloudflare. What is a metropolitan area network (MAN)? Luettavissa: https://www.cloudflare.com/learning/network-layer/what-is-a-metropolitan-area-network. Luettu: 3.2.2021

Cloudflare. What is DDoS mitigation? Luettavissa: https://www.cloudflare.com/learning/ddos/ddos-mitigation/. Luettu 3.3.2021

Craig Hunt 2002. TCP/IP Network Administration, 3rd Edition. O'Reilly Media, Inc. Sebastopol.

Crystal Panek 2019. Networking Fundamentals. Sybex. Hoboken.

Daniel Kirsch & Judith S. Hurwitz 2020. Cloud Computing For Dummies, 2nd Edition. Wiley. Hoboken.

Doug Lowe 2018. Networking All-in-one For Dummies, 7th Edition. Wiley. Hoboken.

Evan Gilman & Doug Barth 2017. Zero Trust Networks. O'Reilly Media, Inc. Sebastopol.

F-secure. Worm. Luettavissa: https://www.f-secure.com/v-descs/articles/worm.shtml. Luettu 3.3.2021

Gordon Davies 2019. Networking Fundamentals. Packt Publishing. Birmingham.

J. David Irwin & Chwan-Hwa Wu 2016. Introduction to Computer Networks and Cybersecurity. CRC Press. Boca Raton.

Järvinen, P & Rousku, K. 2017. Työpaikan tietoturvaopas: tunnista uhat, hallitse riskit. Alma Talent. Helsinki.

Kaspersky 2020. What is WannaCry ransomware? Luettavissa: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. Luettu: 9.2.2021

Kevin R. Fall & W. Richard Stevens 2011. TCP/IP Illustrated, Volume 1: The Protocols. Addison-Wesley Professional. Boston.

Kyberturvallisuuskeskus 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf. Luettu 17.3.2021

Niklas Wallenius. Mikä on software defined networking (SDN) ja mitä hyötyä siitä on? Luettavissa: https://niklaswallenius.fi/sdn-mita-hyotya/. Luettu 10.4.2021.

Manos Antonakakis ym. 2017. Understanding the Mirai Botnet. Luettavissa: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. Luettu 13.2.2021.

Microsoft. Zero Trust. Luettavissa: https://www.microsoft.com/fi-fi/security/business/zero-trust. Luettu 11.3.2021

MITRE 2021. MITRE ATT&CK. Luettavissa: https://attack.mitre.org/groups/. Luettu: 9.2.2021

Palo Alto Networks. What is a Zero Trust Architecture? Luettavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture. Luettu 19.2.2021

Palo Alto Networks. What is and intrusion prevention system? Luettavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips**.** Luettu 24.2.2021

Palo Alto Networks. What is Microsegmentation? Luettavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation. Luettu 4.3.2021

Palo Alto Networks. What is network segmentation? Luettavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation. Luettu 23.2.2021

Red Hat. What is cloud infrastructure? Luettavissa: https://www.redhat.com/en/topics/cloud-computing/what-is-cloud-infrastructure. Luettu 17.3.2021

Tim Rains 2020. Cybersecurity Threats, Malware Trends, and Strategies. Packt Publishing. Birmingham.