Arto Hyytinen

Kybertoiminnallisuuden havainnointi Suomen Erillisverkot Oy:ssä

Kyberturvallisuuden pro gradu -tutkielma

18. tammikuuta 2018

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Arto Hyytinen

Yhteystiedot: arto.hyytinen@gmail.com

Ohjaajat: Ari Viinikainen ja Tapani Ristaniemi

Työn nimi: Kybertoiminnallisuuden havainnointi Suomen Erillisverkot Oy:ssä

Title in English: Information security awareness in State Security Networks Ltd.

Työ: Pro gradu -tutkielma

Suuntautumisvaihtoehto: Kyberturvallisuus

Sivumäärä: 60+8

Tiivistelmä: Valokuituverkko siirtyi Puolustusvoimilta Suomen Erillisverkot Oy konsernin hallintaan ja omistukseen liikkeenluovutuksen yhteydessä 1.3.2015. Tämä Pro Gradu tutkielma syntyi liikkeenluovutuksen tuoman turvallisuusnäkökulma-ajattelun vuoksi. Tutkielmassa käsitellään kyberturvallisuuden käsitteiden ja toimijoiden lisäksi Suomen Erillisverkot Oy konsernin työntekijöiden kyberturvallisuuden tietämystasoa Suomen Erillisverkot Oy konsernissa sekä CSIRT-toiminnallisuutta yleisesti. Tutkimuksessa selvitettiin yhtiön henkilöstön toimia ja termien tuntemusta kyberturvallisuuteen liittyen verkkokyselyn avulla. Kyselyn tuloksista voidaan havaita ajankohtaisten haittaohjelmien toimintamallien koulutuksen tarpeita sekä yhtiön käytännön toimien ohjeistamista USB-muistien suhteen. Kyselyn johtopäätöksenä voidaan todeta, että CSIRT-ryhmän pitää tuoda itseään selkeämmin esille organisaatiossa. Lisäksi tutkimuksesta käy ilmi uudenlainen tapa ajatella palomuuria, joka muodostuu ihmisistä.

Avainsanat: Kyberturvallisuus, CSIRT, kyberhyökkäykset, kybertoiminnallisuuden havainnointi, ihmisten muodostama palomuuri

Abstract: Ownership and control of Finland`s government optical fiber network was transferred from army to the State Security Networks Ltd. on 1.3.2015. This study was created in the middle of that process. In this study I research cybersecurity terms and CSIRT-function-

ality. A survey about cybersecurity terms and staff reactions in cybersecurity related situations was made. As a result one can observe the need of information update about ongoing cybersecurity threats and the organization`s USB-memory policy need to be announced for the staff. As a survey result CSIRT-group needs also announce themselves more in the organization. Human being firewall point of view is introduced in the study.

Keywords: Cyber security, CSIRT, cyber attacks, State Security Networks Ltd., cyber awareness, human being firewall

Esipuhe

Kaikki alkoi siitä, kun pääsin mukaan mobiilijärjestelmät koulutusohjelmaan yliopistossa. Tuossa vaiheessa olin osakkaana perheyrityksessä ja vahvasti isäni kanssa kiinni osakeyhtiön johtamisessa ja päivittäisessä työnteossa. Opiskelulle ei yksinkertaisesti jäänyt aikaa. Saatuani viran Puolustusvoimista vuonna 2011 ja osallistuttuani koulutuksiin ja kyberturvallisuuskursseille silloisen Puolustusvoimien Johtamisjärjestelmäkeskuksen turvallisuuspäällikön Mika Karjalaisen kanssa, innostuin kyberturvallisuudesta. Mikan haluan mainita sen vuoksi, että hänestä tarttui minuun oikeanlaista inspiraatiota ja sain Mikalta vinkkejä Pro Gradu tutkielman aiheeseen liittyen. Aihe oli vaativa niukan lähdeaineiston myötä, mutta mielenkiintoinen. Tutkielman teko ja tutkinnon suorittaminen on ollut haastavaa työn ja perheen ohessa. Aikatauluttaminen ja ajankäytön hallinta on ollut avainasemassa tutkintoa suorittaessa. Työelämän, opiskelun ja pienten lasten hoitamisen sovittaminen yhteen on ollut välillä haastavaa. Samalla voi todeta, että opiskelu on ollut erittäin palkitsevaa ja hyvää vaihtelua alati muuttuvan ja hektisen työelämän ohessa. Kouluttautuminen ja työympäristöstä palaaminen energisten ja avarakatseisten opiskelijoiden joukkoon on avannut silmiä tulevien osaajien osalta. Haluan kiittää perhettäni, joka on antanut muuta ajateltavaa suorittamisen ohella ja ollut tukenani suorittaessani tutkintoa työn ohessa. Lisäksi haluan kiittää työnantajiani Puolustusvoimia ja Suomen Erillisverkot Oy:tä ja esimiehiäni, joiden avulla tutkinnon suorittaminen oli mahdollista.

Jyväskylässä 1.12.2017

Arto Hyytinen

Termiluettelo

FIRMWARE	Laitteeseen kiinteästi asennettu ohjelma, joka huolehtii laitteen perustoiminnoista
CSIRT	Tietoturvapoikkeamaryhmä (Computer Security Incident Response Team)
CIRC	Tietoturvapoikkeamaryhmä (Computer Incident Response Capability)
CIRT	Tietoturvapoikkeamaryhmä (Computer Incident Response Team)
IRC	Tietoturvapoikkeamaryhmä (Incident Response Center or Incident Response Capability)
IRT	Tietoturvapoikkeamaryhmä (Incident Response Team)
SERT	Tietoturvapoikkeamaryhmä (Security Emergency Response Team)
SIRT	Tietoturvapoikkeamaryhmä (Security Incident Response Team)
JPCERT/CC	Japanin tietoturvapoikkeamaryhmien koordinointikeskus. (Japan Computer Emergency Response Team Coordination Center)
DOS	Palvelunestohyökkäys (Denial of Service)
ACERT/CC	Tietoturvapoikkeamaryhmä, joka palvelee USA:n maavoimia
AFCERT	Tietoturvapoikkeamaryhmä, joka palvelee USA:n ilmavoimia
NAVCIRT	Tietoturvapoikkeamaryhmä, joka palvelee USA:n merivoimia

Kuviot

Taulukot

Sisältö

1 Johdanto

Puolustusvoimilta siirtyi n. 140 henkilöä Suomen Erillisverkot Oy konsernin palvelukseen liikkeenluovutuksen yhteydessä 1.3.2015 alkaen. Tämän Pro Gradu tutkielman aihe syntyi liikkeenluovutuksen tuoman turvallisuusnäkökulma-ajattelun vuoksi. Tässä tutkielmassa käsitellään kyberturvallisuuden käsitteiden ja toimijoiden lisäksi Suomen Erillisverkot Oy konsernin työntekijöiden kyberturvallisuuden tietämystasoa Suomen Erillisverkot Oy konsernissa. Lisäksi tutkielmassa käydään läpi CSIRT-toiminnallisuutta. Opinnäytetyönä tehtiin ”Kybertoiminnallisuuden havainnointi Suomen Erillisverkot Oy:ssä” niminen tutkimus, jossa lähetettiin mm. Suomen Erillisverkot Oy:n työntekijöille kysely aiheeseen liittyen. Kyselylomakkeeseen saadut vastaukset luovutettiin kokonaisuutena Suomen Erillisverkot Oy konsernin ja sen koulutusryhmän käyttöön. CSIRT-toiminnasta ei ole aiemmin tehty tutkimusta Jyväskylän yliopistossa. Aiheesta ei myöskään ole tehty aiempia tutkimuksia Suomen Erillisverkot Oy konsernissa. Oletan tutkimustulosten kertovan, että työntekijöiden keskuudessa kyberturvallisuuteen liittyvät koulutukset kyberturvallisuuden termistön ja valveutuneisuuden suhteen ovat tarpeen. Lisäksi uskon tulosten kertovan, että yhtiön on syytä kiinnittää huomiota työntekijöiden ohjeistukseen poikkeavien tietoturvatilanteiden ja rikkeiden varalta. Tutkimustuloksissa uskon selviävän myös, että CSIRT-ryhmän toiminta täytyy tuoda selkeämmin esille ja havainnollistaa CSIRT-ryhmän sekä yksittäisen työntekijän toiminnot ja velvoitteet tietoturvarikkeiden varalta.

1.1 Tutkimuksen tarkoitus ja tavoite

Tutkimuksessa selvitetään Suomen Erillisverkot Oy konsernin työntekijöiden ja koko organisaation havainnointikykyä kyberturvallisuuden suhteen. Lisäksi tavoitteena on selvittää olemassa oleva työntekijöiden tietämys kyberturvallisuuden termistöön liittyen ja CSIRT-ryhmän toiminnallisuus. Tavoite on nostaa konsernin tietoturvatasoa tuomalla työntekijälle esille tietoturvallisuuteen liittyviä kysymyksiä ja lisätä samalla valveutuneisuutta asian suhteen. Tutkielman tavoite on saada myös yhtiön koulutusryhmälle tutkimustuloksia, -aineistoa ja näkemystä kyberkoulutusten tarpeesta yhtiön henkilöstölle.

1.2 Tutkimusaineisto

Tutkimusaineistona käytetään tieteellisiä lähteitä, jotka liittyvät tietoturvaan, kyberturvallisuuteen ja CSIRT-toiminnallisuuteen. Kyberturvallisuusympäristö muuttuu ja kehittyy erittäin nopealla vauhdilla, joten lähteitä täydennetään tarpeen mukaan myös tuoreimmilla internet-lähteillä. Lisää tutkimusaineistoa ja tuloksia saadaan konsernin työntekijöille tehtävän kuvailevan kyselyn perusteella. Tulokset käsitellään, taulukoidaan, analysoidaan ja niistä tehdään johtopäätökset. Kyselyn tulokset ja johtopäätökset ilmoitetaan yhtiön työntekijöille ja koulutusryhmälle jatkojalostusta varten.

1.3 Tutkimusongelma

Tutkimusongelma on Suomen Erillisverkot osakeyhtiön kyberturvallisuuteen liittyvän toiminnan tunnistaminen ja tason havainnollistaminen kyselyn avulla. CSIRT-toiminnasta löytyi kirjaston haulla 0 kappaletta tutkielmia Suomesta. Perehdyttävää kirjallisuutta CSIRT-toiminnasta löytyy, mutta julkaisut ovat englanninkielellä.

1.4 Tutkimusmenetelmä ja tutkimuksen eteneminen

Tutkimusmenetelmänä Suomen Erillisverkot Oy:n kybertoiminnallisuuden havainnoinnin suhteen käytetään kvantitatiivista tutkimusmenetelmää työntekijöiden kyberturvallisuuden tietämystason suhteen. Lisäksi teen katselmuksen julkaisuihin aiheeseen liittyen. Pyrin löytämään uusinta tietoa aiheesta, joten saatan joustaa hieman lähdekritiikin suhteen. Tutkimus etenee tietoturvan ja kyberturvallisuuden määrittelyn kautta CSIRT-toiminnallisuuden selvitykseen. Tämän jälkeen suoritetaan Suomen Erillisverkot Oy:n työntekijöille kuvaileva kysely. Kyselyn tulokset käsitellään ja jalostetaan esitettävään muotoon. Kyselyn tulosten käsittelyn ja analysoinnin jälkeen tehdään johtopäätökset tutkimuksesta ja koulutustarpeista yhtiössä sekä katsotaan kehityksen kohteet.

2 Tietoturva, kyberturvallisuus ja kyberavaruus

2.1 Tietoturvan määritelmä

Tietoturvalla tarkoitetaan tietojen, järjestelmien ja palveluiden suojaamista sekä normaalien että poikkeusoloissa lainsäädännön ja muiden toimenpiteiden avulla. Tietojen käytettävyyttä, luottamuksellisuutta ja eheyttä suojataan eri uhkia vastaan. [1]

Tietoturvan merkitys on noussut erittäin merkittävään rooliin laitteiden verkottumisen ja teollisen internetin myötä. Yhä useampi laite on verkossa ja se voidaan ottaa etähallintaan. Verkkoyhteys on jo olemassa esimerkiksi työpaikan kahviautomaatissa ja verkkoyhteyttä on suunniteltu niinkin arkiseen laitteeseen kuin jääkaappi. Tietoturvan pettäessä hyökkääjä voi päästä käsiksi kodin tai työpaikan laitteeseen ja tehdä ilkivaltaa muuttamalla esimerkiksi jääkapin lämpötilaa verkon välityksellä ikävin seurauksin. Näin ollen tavallisen käyttäjänkin tulee olla arjen keskellä yhä valveutuneempi verkon turvallisuuden suhteen.

Tietoturva tarkoittaa tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tietoturvallisuuden uhkina pidetään esimerkiksi erilaisia huijausyrityksiä, henkilökohtaisen yksityisyyden loukkauksia, roskapostia, teollisuusvakoilua, piratismia, tietokoneviruksia, verkkoterrorismia ja elektronista sodankäyntiä. Tietoturvauhkia ovat luvaton pääsy, tiedon luvaton käyttö, verkkotiedustelu, salaisen tiedon paljastuminen, salakuuntelu, tiedon sekaannus, tiedon muuntuminen, salaisen tiedon tutkituksi tuleminen, tiedon kopioituminen ja tiedon häviäminen. [2]

2.2 Tietoturvapoikkeama

Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmän (VAHTI) ohjesivustolla www.vahtiohje.fi on kuvattu tietoturvapoikkeama seuraavasti: ” *haitallinen tapahtuma, tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut*”. [3] Jokainen organisaatio tai yhtiö voi määritellä tietoturvapoikkeaman itse. Tietoturvapoikkeama voi olla esimerkiksi:

a) mikä tahansa todellinen tai epäilty haitta tietojärjestelmiin tai tietoverkkoihin.
b) teko joka rikkoo suoraan tai epäsuorasti organisaation turvallisuuspolitiikkaa
c) epäonnistunut tai onnistunut luvaton yritys päästä käsiksi järjestelmään tai yhtiön tietoihin
d) ei toivottu palvelujen häirintä tai palvelunestohyökkäys
e) tiedonkäsittelyn tai tiedon tallennuksen luvaton käyttö
f) järjestelmän laitteiston, laiteohjelmiston (firmware) tai ohjelmiston muuttaminen ilman omistajan tietoa, ohjeita tai suostumusta. [4]

2.3 Kyberturvallisuuden määritelmä

Ymmärtääkseen kyberturvallisuutta on aiheeseen perehtyvän syytä etsiä kyber-sanan historia ja tarkoitus. Useissa kyber-sanan historiaa käsittelevässä tieteellisessä artikkelissa, mm. Aalto yliopiston "Kyber rantautui Suomeen", Jarno Limnell 2014, lähdeviittauksena on Norbert Wienerin teos, Cybernetics: Or Control and Communication in the Animal and the Machine. Kyber-etuliite esiintyy kirjallisuudessa ensimmäisen kerran Norbert Wienerin esittelemänä. Teoksessa käytetään sanaa kybernetiikka, jolla kuvastetaan koneiden ja elävien olentojen välistä ohjausta ja kommunikointia. Sana kybernetiikka puolestaan muodostuu kreikkalaisesta sanasta kubernētēs, eli ohjata. [5] Computers & Security lehdessä vuonna 2013 (numerossa 38) julkaistussa tieteellisessä artikkelissa Johan van Niekerk ja Rossouw von Solms kuvailevat kyberturvallisuus-termiä käytettävän kirjallisuudessa kaiken sisältävänä terminä. Niekerk ja von Solms käyttävät esimerkkinä Merriam Websterin sanakirjaa, jossa kyberturvallisuutta kuvaillaan "tietokoneen tai tietokonejärjestelmän suojaamiseksi tehtäviksi toimenpiteiksi luvattoman pääsyn tai hyökkäyksen estämiseksi".[6] Kansainvälinen tietoliikenne liitto (The International Telecommunications Union), eli ITU, määrittelee kyberturvallisuuden seuraavasti: kyberturvallisuus on kokoelma työkaluja, käytäntöjä, turvallisuuskonsepteja, turvallisuuden suojatoimia, ohjeita, riskienhallinnan näkökulmia, toimintoja, harjoittelua, parhaita käytäntöjä, varmistamista ja teknologioita joita voidaan käyttää kyberturvallisuusympäristön suojaamiseen ja organisaation sekä käyttäjän tärkeää informaatio-omaisuutta. Organisaation ja käyttäjän informaatiovarat sisältävät yhdistetyt tietokonelaitteet, henkilöstön, infrastruktuurin, ohjelmistot, palvelut, tietoliikennejärjestelmät ja

siirretyn sekä tallennetun informaatiokokonaisuuden kyberympäristössä. Kyberturvallisuus pyrkii varmistamaan organisaation ja käyttäjän informaatiovarojen käytettävyyden ja ylläpidon turvallisuuden merkittäviä turvallisuusriskejä vastaan kyberympäristössä. Yleisiä turvallisuustavoitteita ovat informaation saavutettavuus, eheys ja luotettavuus. [7]

2.4 Tietoturvan ja kyberturvallisuuden erot

Kyberturvallisuus ja tietoturva on syytä erottaa toisistaan sekaannusten välttämiseksi. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa toiminta turvataan. Tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus.

Turvallisuus- ja puolustusasiain komitean sihteeristön vuonna 2013 julkaisemassa Suomen Kyberturvallisuusstrategiassa on tehty määrittelyjä lyhyesti ja selkeästi taulukkomuodossa, jonka liitän mukaan tutkielmaan termien selkeyttämisen vuoksi. [8]

Taulukko 1 Kyberturvallisuuden termistöä

Kyber-	Kyber-sanaa käytetään lähes poikkeuksetta yhdyssanan määriteosana eikä yksinään. Sanan merkityssisältö liittyy yleensä sähköisessä muodossa olevan informaation (tietojen) käsittelyyn: tietotekniikkaan, sähköiseen viestintään (tiedonsiirtoon), tieto- ja tietokonejärjestelmiin. Vasta koko yhdyssanalla (määriteosan ja perusosan yhdistelmällä) voidaan katsoa olevan oma merkityksensä. Sanan kyber voidaan katsoa tulevan alun perin kreikankielen sanasta “kybereo” - ohjata, opastaa, hallita.

Kyberriski	Kyberriskillä tarkoitetaan kybertoimintaympäristöön kohdistuvaa vahinkomahdollisuutta tai haavoittuvuutta, joka toteutuessaan tai jota hyväksi käyttäen kybertoimintaympäristön toiminnasta riippuvalle toiminnolle voi aiheutua vahinkoa, haittaa tai häiriötä.
Kybertoimintaympäristö	Kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö. Tarkennus 1 Ympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet. Tarkennus 2 Informaation (tietojen) käsittely tarkoittaa informaation (tietojen) keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä

	muita informaatioon (tietoihin) kohdistuvia toimenpiteitä.
Kyberturvallisuus	Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Tarkennus 1 Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle. Tarkennus 2 Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä (”yhteisöllinen tietoturva”). Menettelyjen avulla pystytään estämään tietoturvauhkien toteutuminen, ja niiden mahdollisesti toteutuessa estämään, lieventämään tai sietämään niiden vaikutuksia. Tarkennus 3 Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joi-

	den tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle.
Kyberuhka	Kyberuhkatarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon. Tarkennus Kybertoimintaympäristöön kohdistuvat uhkat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan.
Tietoturvallisuus	Tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus.

2.5 Kyberavaruus

Kyberavaruus on virtuaalinen välikappale, joka on vähemmän konkreettinen kuin vesi, ilma tai avaruus. Yksi yleinen tapa ymmärtää kyberavaruutta ja kyberhyökkäyksiä on nähdä kyberavaruuden koostuvan kolmesta kerroksesta: fyysinen, synteettinen ja semanttinen kerros. Fyysinen kerros on ensimmäinen kerros, synteettinen kerros on fyysisen kerroksen yläpuolella ja semanttinen kerros ylimpänä. Kaikki informaatiojärjestelmät toimivat fyysisellä tasolla, koostuen ohjainlaatikoista ja yleensä johdoista. Poistaessasi fyysisen kerroksen, myös järjestelmä katoaa. Tietojärjestelmään on mahdollista hyökätä kineettisillä tavoilla, mutta

sen kaltaisia fyysisiä hyökkäyksiä ei ole tarpeen käydä tässä tarkemmin lävitse. Riittää todeta, että tietokonetta ei voi huijata tuhoamalla sen komponentteja. Huijaaminen voidaan toki tehdä vaihtamalla komponentti toiseen. Synteettinen taso sisältää ohjeet ja protokollat, jotka suunnittelijat ja käyttäjät antavat koneelle. Näiden ohjeiden ja protokollien kautta koneet ovat vuorovaikutuksessa toisten koneiden kanssa. Esimerkkinä voidaan mainita:

- laitteen tunnistus
- pakettien kehystys
- osoitteiden määritys
- reititys
- asiakirjojen formaatit
- tietokannan käsittelyt

Jotkut kommunikointi-infrastruktuurit sisältävät paksumman synteettisen kerroksen kuin toiset, mutta jokaisella vähänkin kahta tyhjää jogurttipurkkia ja niiden välistä johtoa kehittyneemmällä järjestelmällä täytyy olla sellainen. Tämä on se taso, jolla hakkeroinnilla on tapana tapahtua, kun ulkopuoliset ihmiset asettavat toimivaltansa suunnittelijoiden ja käyttäjien toimivallan ulkopuolelle. Ylin, eli semanttinen kerros, pitää sisällään tietoa jota koneessa on. Tässä tiedossa on mainittu muun muassa perustelut, jonka vuoksi kone on olemassa. Osa tiedosta on tarkoitettu järjestelmän manipulointiin, kuten osoitteen etsintä taulukot tai tulostinten ohjauskoodit. Tämä tieto on semanttisessa muodossa, mutta tarkoituksella syntaktisia. Muu tieto, kuten prosessinohjaus, on tarkoitettu tietokoneavusteiseen teollisuuteen. Loput järjestelmän tiedosta on merkityksellistä vain ihmisille, koska se on muunnettu luonnolliselle kielelle. Tiedon ja ohjeiden erottaminen voi olla vaikeaa. Moni murtautumisen toimenpide suoritetaan laittamalla muokattua sisältöä valeasuun tavallisen sisällön sekaan. Esimerkkinä voidaan mainita viruksia sisältävä sähköpostin liitetiedosto ja nettisivut muokatulla koodilla. Tietokoneisiin voidaan hyökätä semanttisen kerroksen kautta syöttämällä sinne virheellistä tietoa, kuten sytyttämällä tulitikun lämmityspatterin termostaatin viilentääksesi huonetta tai luomalla valheellisen uutislähteen. Yleensä vain tietokoneet, joiden tietoja on peukaloitu synteettisellä tasolla hyväksyvät virheellisen tiedon. Tämän tyyppisestä toiminnasta paras esimerkki on tietokone, joka on ohjattu väärälle www-sivulle, käyttäjän uskoessa olevan oikealla verkkosivulla. [9]

2.6 Järjestelmän ulkoiset uhkat

Kyberhyökkäykset voidaan laukaista verkon ulkopuolelta hakkereiden avulla tai sisäpuolelta käyttäen agentteja tai haitallisia komponentteja. Ulkoinen hakkerointi on yleisin tapa, jonka esimerkiksi valtio valitsee siviilikohteiden osalta. Armeijat ja tiedustelutoimistot eivät voi kuitenkaan kokonaan ohittaa sisäpiirin hyökkäyksiä. Synteettinen taso, eli kyberavaruus, on viranomaisten valvonnan alla. Ihminen, joka omistaa tietokoneen voi normaalisti tehdä sillä mitä haluaa. Suurimman osan ajasta käyttäjä uskoo hallitsevansa tietokonetta, vaikka se on verkossa. Tietokoneet organisaatioiden sisällä ovat yleensä järjestelmähallinnan piirissä, jolloin niiden osat ovat käyttäjän ulottumattomissa. Tällaisessa hakkerointitapauksessa joudutaan rikkomaan tietohallinnon asettamia säädöksiä. Hakkeri voi lähettää roska-postin liitetiedostolla tai ohjata käyttäjän virheelliselle sivustolle, josta haittaohjelma ladataan koneelle. Toiset haittaohjelmat varastavat tietoa koneesta, kun taas toiset auttavat hakkeria ajamaan komentoja koneessa ja saamaan koneen haltuun. Hakkerit voivat myös hämätä organisaation järjestelmää naamioimalla itsensä normaaliksi käyttäjäksi käyttäjän pääsyoikeuksilla. Joissain tapauksissa hakkerit menevät pidemmälle ja onnistuvat saamaan järjestelmähallintaoikeudet. Järjestelmänhallintaoikeuksilla hakkerit voivat muuttaa lähes kaiken järjestelmässä. Saatuaan pääsyn järjestelmään hakkerit voivat tehdä monenlaista ilkivaltaa. Yleisin hakkeroinnin päämäärä on varastaa tietoa. Kun kyseessä on toiselta valtiolta varastaminen, sitä kutsutaan tietokoneverkon hyväksikäytöksi. Yhtiöt saattavat myös varastaa tekijänoikeudella suojattua tietoa toisilta yhtiöiltä. Myös yksilöt varastavat yhä useammin tietoa toiselta yksilöltä. Useasti tämä toiminta liittyy identiteettivarkauteen. Jokainen voi varastaa toiselta. Koska tiedon varastaminen ei estä käyttäjiä nauttimasta oman järjestelmän käytöstä, on olemassa muutama asia, josta voi huomata käyttäjän olevan hakkeroinnin kohteena. Tunkeutumisen havainnointi on mahdollista, jos käyttäjä huomaa datapakettien kautta luvattoman tiedon siirtämisen koneesta. Keskivertokäyttäjä ei tätä usein huomaa, koska kaikenlaista odottamatonta, mutta kuitenkin normaalia liikennettä tapahtuu jatkuvasti. Luvaton pääsy voi johtaa inhottaviin häiriöihin ja tietokorruptioon. Häiriöt tapahtuvat, kun järjestelmät ovat huijattu suorittamaan operaatioita, jotka laittavat järjestelmät sulkeutumaan, ylikuormittumaan, suorittamaan tahallisia virheitä tai sekaantumaan toisten järjestelmien kanssa suoritettaviin

toimintoihin. On harvinaista, että hakkerit voisivat rikkoa fyysisiä kohteita. Yksi laboratoriossa tehty esitys näytti, että väärän ohjelmistokoodin avulla voidaan aiheuttaa turbiinin tuhoutuminen. Tietokorruptio tapahtuu yleensä, kun data ja algoritmit ovat muutettu luvattomilla tavoilla. Yleensä muutos on vahingoksi järjestelmän oikealle toiminnalle. On hyvä erottaa korruptio ja häiriö toisistaan. Häiriön vaikutukset ovat välittömiä, rajuja ja ilmeisiä, kun taas korruption vaikutukset ovat hienovaraisia ja ne voivat uusiutua. On helppo sanoa, että järjestelmä ei toimi. Vaikeampaa on erottaa se, että tekeekö toimiva kone väärä informaatiota vai huonoja ratkaisuja. Hakkerit jättävät usein haittaohjelman järjestelmään myöhempää käyttöä varten. Nämä ”implantit” ovat usein lepotilassa ja voidaan aktivoida joko saastutetun koneen toiminnolla tai hakkerin komennon toimesta. Koneen toiminnan esimerkkinä voidaan mainita esim. uuden informaation ilmestyminen koneelle, josta hakkeri on kiinnostunut. Joissain tapauksissa ”implantit” toimivat itsenäisesti, etsimällä verkosta tietokoneita, joissa implantteja ei vielä ole. Riippumatta siitä, mitä hakkeri aikoo tehdä varastetulla tiedolla, ensimmäinen ja vaikein vaihe on päästä sisään järjestelmään. Pääsy järjestelmään onnistuu käyttäjätunnusten tai järjestelmähallitsijan tunnusten selvittämisellä. Tästä syystä ensimmäiset vaiheet tietoverkkoihin soluttautumisessa näyttää hyvin samalta kuin tietoverkkohyökkäyksen ensimmäiset vaiheet. Tästä seuraa se, että ne joilla on parhain kyky päästä sisään toiseen järjestelmään, ovat myöskin pätevimpiä suorittamaan tietoverkkohyökkäyksen. [9]

Synteettisen kerroksen levätessä fyysisen kerroksen päällä, voidaan todeta, ettei kyberavaruuteen ole varmaa tietä. Mikäli hakkeri on päässyt järjestelmään ulkopuolelta, se johtuu siitä, että hakkeri on ohjannut järjestelmän tekemään jotain, mitä käyttäjät eivät halunneet tehdä ja hakkeri on tehnyt sen, mitä järjestelmän suunnittelijat ovat pyrkineet estämään. Joka tapauksessa, tietokonesuunnittelun ja käyttöohjeen taistellessa ohjelmistoa vastaan, ohjelmisto vie aina voiton. Kuka tahansa järjestelmään pyrkii sisään, pääsy järjestelmään tapahtuu ohjelmiston luvan avulla. Ohjelmistossa voi olla puutteita tai ohjelmisto voi olla väärin konfiguroitu. Väärin konfiguroinnista voidaan mainita pääkäyttäjän asettamat oikeudet, jotka eroavat siitä mitä pääkäyttäjä luuli asettavansa. Järjestelmä on juuri sitä, miten se on konfiguroitu, ei välttämättä sitä, mitä sen halutaan olla. Tämän tyyppinen eroavaisuus on turvallisuusuhka ja se tekee järjestelmästä haavoittuvan. Hakkerin käyttämää manuaalista tai

automaattista metodia, joka hyödyntää haavoittuvuuksia saadakseen pääsyn järjestelmään tai syöttääkseen järjestelmään vääristettyjä ohjeita, kutsutaan hyväksikäytöksi. Järjestelmän eheys määrittää sen, kuinka pahasti järjestelmää voidaan vahingoittaa hyökkäyksillä kyberavaruudesta. Voidaan sanoa, että järjestelmän eheys on tärkeämpi, kuin hyökkääjien hyökkäysten laatu. Yhteenvetona voidaan sanoa, että jos ei ole haavoittuvuuksia, niin ei tapahdu järjestelmän hyväksi käyttöä tai kyberhyökkäyksiä. Kuitenkin teoriassa kaikki tietokoneisiin kohdistuvat ilkityöt ovat lopulta järjestelmän omistajan vika. Jos kyseessä ei ole tietokoneen väärä käyttötapa tai väärä konfigurointi, niin vikana on järjestelmän käyttö tietoturva-aukoista huolimatta. Käytännössä kaikki tietokonejärjestelmät ovat alttiita virheille. Suunnittelun ja koodin välinen ero johtuu ohjelmistojärjestelmien monimutkaisuudesta ja mahdollisesta inhimillisestä virheestä. Mitä kompleksisempi järjestelmä on, sitä enemmän on paikkoja, jossa virhe voi piileskellä. Jokaisessa järjestelmässä on haavoittuvuuksia, toisissa järjestelmissä ne ovat pahempia kuin toisissa. Ohjelmistojen tuottajat löytävät itse ison osan haavoittuvuuksista ja julkaisevat korjauspäivityksiä, jotka käyttäjien on sitten tarkoitus asentaa. Toiset valmistajat tekevät korjaukset nopeammin ja paremmin kuin toiset valmistajat. Hakkerit löytävät haavoittuvuuksia ja kiirehtivät hyödyntämään tietoturva-aukot käyttäjiin, jotka ovat muuten tehneet kaiken oikein. Tuhansia aukkoja on ympärillämme koko ajan. Useimmat hyödynnettävät aukot, jotka päätyvät uutisiin, eivät toimi ajan tasalla olevissa järjestelmissä. Kyberhyökkäykset nojaavat tavallaan petokseen. Kyberhyökkäys pyrkii johdattelemaan järjestelmät tekemään sitä, mitä suunnittelijat eivät halua niiden tekevän. Löydetty tietoturva-aukko osoittaa järjestelmänhallitsijoille, että jokin ei ole kunnossa. Hyvillä lokitiedostoilla järjestelmänhallitsijat voivat pystyä päättelemään, jos jotain poikkeavaa on tapahtunut hakkerin ja järjestelmän kanssakäymisen välillä. Tiedostomuutokset datassa tai ohjeissa tai järjestelmään kuulumattoman tiedoston löytäminen voi paljastaa hakkerin. Prosessi on tuskin täydellinen, joten on mahdollista huomata haavoittuvuus, mutta olla huomaamatta laajempaa suunnitteluvirhettä, josta kyseinen haavoittuvuus on vain osa. Yksittäisellä järjestelmänhallitsijalla on tuskin koskaan suoraa näkyvyyttä ohjelmistopaketteihin eikä hän voi korjata haavoittuvuuksia, joista ohjelmiston tuottaja ei ole itsekään tietoinen. Jokainen järjestelmänhallitsija voi kuitenkin hyödyntää kansainvälisiä tietoturvayhteisöjä, joilla on yhteinen intressi löytää ja korjata merkittävät haavoittuvuudet. [9]

Järjestelmän rajaus voi olla helpompi hahmottaa kyberavaruuden kautta tarkasteltuna. Järjestelmään voidaan laskea mukaan käyttäjän laitteet, eli laitteet joiden toiminnot ja parametrit ovat käyttäjän asettamia. Nämä järjestelmän reuna-alueet ilman eristystä tai määriteltyä salausta ovat usein toistuvasti haavoittuvia, koska käyttäjät ovat harvoin koulutettuja tai keskittyneitä informaatioturvallisuuteen. Käyttäjän järjestelmät ja oikeudet voidaan ottaa haltuun salasana hakkeroinnin, tietojen kalastelun, käyttäjän manipuloinnin, saastutettujen www-sivujen latauksien tai esimerkiksi saastuneen median käytön (.zip tiedosto tai usb-muistin) ynnä muun vastaavan toiminnan kautta. Valitettavasti järjestelmäalueen kokonaisturvallisuus ei useinkaan ole parempi, kuin kaikkein huolimattomimman käyttäjän turvallisuus. Ydin, eli valvonta, reitittimet, hallinnointilaitteet, koneisto ja tietokannat, on se jota järjestelmänhallitsija hallinnoi. Järjestelmänvalvojat pitäisi olla koulutettu ja ajan tasalla turvallisuusasioihin liittyen. He myös määrittävät termit, joilla käyttäjät ja heidän järjestelmät kommunikoivat ytimen kanssa. Henkilöstö on hyvä altistaa turvallisuuskysymyksille ja on käytännöllistä turvallisuuden kannalta ajatella, että käyttäjät eivät aina ole varuillaan turvallisuuden suhteen. Ydin on mahdollista suojata turvallisuuden suhteen epävarmoilta käyttäjiltä. Ei ole täysin selvää, voivatko verkot toimia, kun käyttäjän järjestelmät ovat tarpeeksi pahasti vaarantuneet, vaikka verkonhallinta on järjestelmänhallinnan osa. Yleisesti ottaen on vaikeaa vaarantaa ydintä kahdesti täsmälleen samalla tavalla, mutta muut järjestelmän alueet ovat aina vaarassa. [9]

2.7 Järjestelmän sisäiset uhkat

Valtiotasolla tarkasteltaessa hyökkäävällä valtioilla on käytännössä vain kaksi tapaa päästä käsiksi suljettuihin järjestelmiin. Toinen on rekrytoida talon sisältä henkilö. Tämän metodin toimivuutta on vaikea ennustaa. Talon sisältä rekrytoitu henkilö voi syöttää väärää informaatiota järjestelmiin. Tämä on erityisen tehokasta silloin, jos rekrytoidut henkilöt ovat itse järjestelmänhallitsijoita. Toinen tapa on vaikuttaa tuotantoketjuun niin, että kohdejärjestelmät sisältävät komponentteja, jotka näyttävät normaaleilta, mutta sisältävät koodia, joka reagoi valtion käskystä tai toimii asetettujen ohjeiden mukaan. Talon sisältä rekrytoidun henkilöiden ja komponenttien metodit ovat valtion tiedustelupalvelujen vaikutusten piirissä, joten ne ovat korkeasti suojattu. Näin ollen on vaikea tietää, kuinka hyvin ne ovat toimineet. Tässä

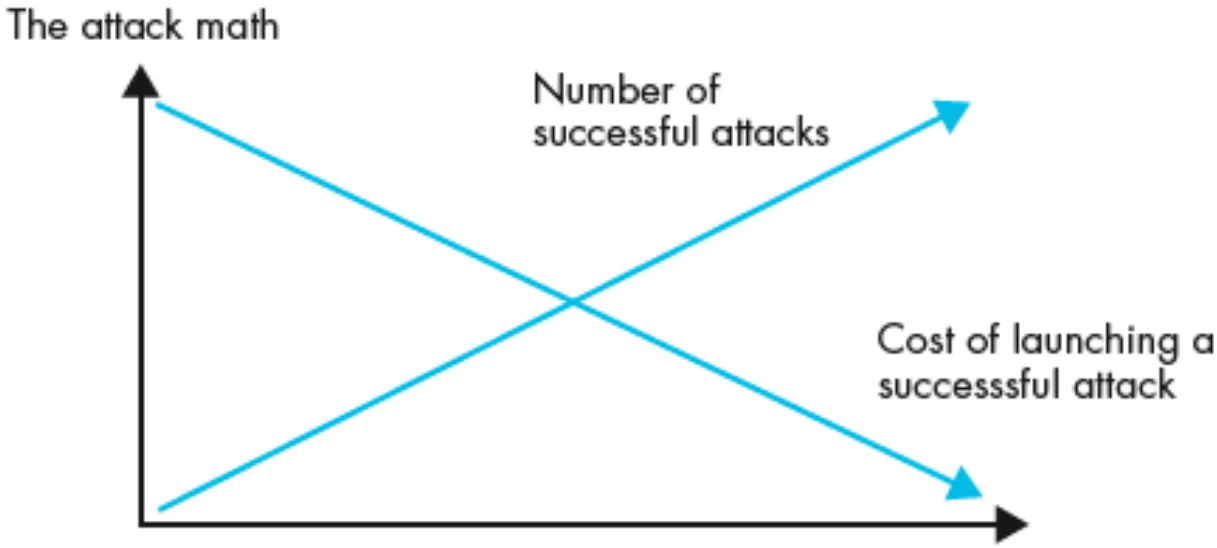
on selvä ero tietokoneen hakkerointiin verrattuna, jonka tekniikoita julkistetaan verkossa ja lehdissä. Toisin kuin hakkereita sisältävän internetiin yhteydessä olevan järjestelmän käsittelyssä, sisältäpäin haittaa tekevää ilkivaltaa suorittaessa, toiminnalla on tapana rikkoa tietoturvasäädöksiä. Tällaisen toimintaan kykenevän järjestelmäoperaattorin täytyy mennä todella kattavien turvallisuusprosessien läpi, saavuttaakseen vaadittavan tietoturvatason ja välttääkseen sisäisen uhkan hälytykset. Sisäinen uhka on aina ollut osa tietokoneturvallisuutta. Parhaiten hallitut järjestelmät tekevät vahingonteon vaikeaksi haittaa tekevälle työntekijälle, joissakin tapauksissa rajoitetaan pääsyoikeuksilla materiaaliin lukuoikeuksia. Yleisenä periaatteena vahingollinen työntekijä esiintyy samanlaisena riskinä, kuin varomaton käyttäjä avoimen järjestelmän ympäristössä. Vahingolliset järjestelmänhallitsijat ovat huomattavasti pahempi ongelma. Talon sisältä rekrytoitu henkilö voi tehdä tarkkoja paikallisia iskuja, mutta tällainen tapaus harvemmin vaikuttaa valtakunnallisesti. Tämän tyyppistä hyökkäystä ei voi toistaa kovin helposti, toisin kuin tietoturva-aukkoa. Yhtiön sisäisen haitantekijän löytäminen voi johtaa tutkimuksiin, jotka voivat vaikuttaa koko rekrytointiverkostoon. [9]

2.8 Kyberuhkien torjuminen ja talous

Isojen yhtiöiden ja valtion virastojen tietomurroista aiheutuneet viimeaikaiset median otsikot ovat arkipäivää. Tämä herättää kysymyksiä mm. miksi ja loppuvatko hyökkäykset koskaan? Nämä tietomurrot vaarantavat meidän digitaalisen elämäntyylin. Jatkuvasti lisääntyvä ymmärrys tietomurtojen määrän kasvuun lisää huomiota ja investointeja yritysmaailman sekä hallituksen toimesta ympäri maailman. Digitaalisuuden myötä yhä useampi todellinen ja konkreettinen asia on nyt koneiden generoima, joka esiintyy vain bittien ja tavujen muodossa. Konkreettisena esimerkkinä voidaan ajatella vaikka pankkitiliäsi ja konkreettisen rahan käsittelyn poistumista. Luotat siihen, että varasi ovat olemassa, koska näet ne kirjautuessasi verkkopankkiin. Toisena esimerkkinä voidaan mainita satatuhatta lentokonetta, jotka lentävät päivittäin keskiverto päivänä toistensa ohi turvalliselta etäisyydeltä ja nousevat sekä laskeutuvat oikeilla aikaväleillä. Kuvittele, jos tätä luottamusta ei voisi enää pitää itsestään selvyytenä. Minkälainen totaalinen kaaos siitä syntyisi? Luotamme päivä päivältä enemmän, että digitaalinen maailma vain toimii. Kaikki se tehokkuus ja tuottavuus, jonka digitaalinen

aika on tuonut, antaa helposti valheellisen kuvan. Nojautuminen digitaalisiin järjestelmiin on syy siihen, että huoli kyberhyökkäyksiin nousee kiivaasti. Hallituksen johtajat, koulujen johtajat, yritysten johtajat ja puolustusvoimien johtajat tietävät, että sujuvasti toimivan rakennetun digitaalisen yhteiskunnan ja kaoottisen yhteiskunnan romahduksen välinen raja on hiuksen hieno. [10]

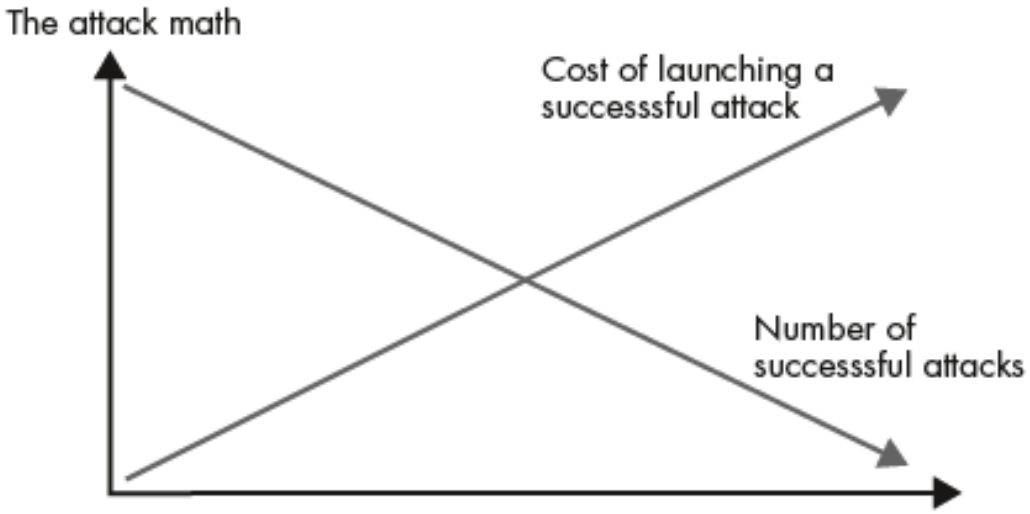
Tietokoneiden ja laitteiden jatkuva laskentatehon hinnanlasku mahdollistaa kyberrikollisten tehdä lukuisia ja pitkälle kehittyneempiä hyökkäyksiä yhä halvemmilla kustannuksilla kts. kuva 1.



Kuva 1. Onnistuneiden hyökkäysten määrä suhteessa hyökkäysten kuluihin [10]

Kyberturvallisuuden hyvien ja pahojen välinen taistelu on myös siis matemaattinen. Pahat ja ilkeämieliset toimijat voivat käyttää olemassa olevia haittaohjelmia tai tietoturva-aukkoja, jotka ovat nykypäivänä ilmaisia tai todella edullisia pitää verkossa. Kansallisvaltiot, rikollisorganisaatiot ja kehittyneet hakkerit voivat käyttää laajasti saatavilla olevia työkaluja tunkeutuakseen järjestelmiin ja peittääkseen identiteettinsä. Tämä on johtanut siihen, että onnistuneiden hyökkäyksien määrä on selkeästi kasvanut ja onnistuneiden hyökkäysten kustannukset ovat selkeästi laskeneet. [10]

Yhä edistyneempien ja määrällisesti kasvavien hyökkäysten puristuksissa puolustautuja yleensä tukeutuu vuosikymmeniä vanhaan turvallisuustekniikkaan ja monitasoisiin tuotteisiin, jotka eivät ole suunniteltu kommunikoimaan keskenään. Tämä johtaa siihen, ettei tietoturvapoikkeamaan ole selkeää näkymää ja poikkeamaan reagointi on manuaalista. Automaatiolla ja turvallisuusalustan päivittämisellä hyökkäysten kulut saadaan kasvamaan ja onnistuneiden hyökkäysten määrä laskemaan. Kts. kuva 2.



Kuva 2. Automaatiolla ja turvallisuusalustan päivittämisellä saadaan hyökkäysten kulut nousemaan ja onnistuneiden hyökkäysten määrä laskemaan. [10]

Hyökkäysten määrä ei ole laskusuunnassa, joten hyökkäysalustojen ja potentiaalisten kohteiden määrä jatka kasvuaan. Eri laitteiden internet-yhteydet tulevat vain lisääntymään. Voidaan ymmärrettävästi olettaa, että hyökkäysten estäminen ei ole mahdollista. Meidän täytyy yksinkertaisesti vain tunnistaa kaikki hyökkäykset ja reagoida niihin. Ilman merkittävää ennaltaehkäisyä mikään teknologian, prosessin tai ihmisten yhdistelmä ei pysty priorisoimaan ja reagoimaan jokaiseen tunkeutumiseen, joka voi merkittävästi vaikuttaa verkkoon ja niihin jotka sitä käyttävät. Matemaattinen ongelma on ylitsepääsemätön. Kaikessa yksinkertaisuudessaan tunnistaminen ja reagointi pitäisi olla ennaltaehkäisyn rinnalla täydennyksenä vaihtoehdon sijaan. [10]

3 CSIRT

3.1 Mikä on CSIRT?

A Computer Security Incident Response Team (CSIRT) vapaa suomennos tarkoittaa tietoturvatapahtuman reagointiryhmää. CSIRT-ryhmä tuottaa palveluita käyttäjälle, yhtiölle tai organisaatiolle. Computer Security Incident Response Team toimii yhden luukun periaatteella. CSIRT tarjoaa luotettavaa yhteydenottopistettä tietoturvauhkien raportoimiseen. CSIRT-ryhmä tuottaa keinot tapahtumien raportointiin ja jakaa vaaratilannetta koskevaa tietoutta. On olemassa runsaasti organisaatioita, jotka eivät ole ottaneet turvallisuusuhkia riittävästi huomioon päivittäisessä toiminnassa. CSIRT-ryhmä tekee työtä nostaakseen valveutuneisuutta asiakkaidensa keskuudessa tietokoneen tietoturvauhkiin liittyen ja tuottaa informaatiota suojatakseen kriittistä it-infrastruktuuria ja laitteistoa mahdollisia organisoituja kyberhyökkäyksiä vastaan. CSIRT-ryhmän täytyy vähintään valistaa toimialueensa käyttäjiä, että käyttäjät tietävät mihin raportoida poikkeavista tapahtumista. Isossa ja valtiollisessa organisaatiossa ryhmän täytyy jakaa tehdyt suojaustoimenpiteet muiden vastaavien ryhmien kanssa, jotta eri CSIRT-ryhmien välinen koordinointi on mahdollista toteuttaa. Tärkeä ja kriittinen osa infrastruktuurin suojausta on tiedon kerääminen kaikista lähteistä. Verkottuminen suojatussa ympäristössä ja tapahtumien tiedon sekä tunnistus- ja vastatoimien tekniikoiden jakaminen voivat olla suuressa merkityksessä heikkouksien tunnistamisessa ja korjaamisessa. [11] & [12]

Kyseessä on palveluryhmä, joka on vastuussa vastaanottamaan tietokoneiden tietoturvapoikkeamat ja niiden ilmoitukset. CSIRT-palveluryhmän tehtävä on arvioida poikkeamat ja reagoida niihin. CSIRT-palvelut toteutetaan yleensä määriteltynä kokoonpanona, joka voi olla yritys, valtiollinen tai opetuksellinen toimija. CSIRT voi olla pysyvä ryhmä tai tilanteen mukaan paikalle kutsuttava ryhmä. Pysyvä ryhmä suorittaa tietoturvapoikkeamiin reagointia päätyönään. Tilanteen mukaan paikalle kutsuttava ryhmä kokoontuu työskentelemään, kun tietoturvapoikkeama on havaittu ja tarve ryhmän toiminnalle on olemassa. [11]

3.2 CSIRT-ryhmän tehtävät

CSIRT-ryhmää voidaan verrata palolaitokseen. Palolaitoksella on hätänumero, johon voidaan soittaa, kun epäillään tulipaloa. Palolaitos lähtee sammuttamaan paloa, kun siitä on saatu havainto. Vastaavasti CSIRT-ryhmällä on numero ja sähköpostiosoite, joihin voidaan ottaa yhteyttä epäillessäsi tietoturvarikettä tai – uhkaa. CSIRT-ryhmä ei välttämättä ilmesty ovellesi, kuten palolaitoksen väki, vaan vuorovaikutus tapahtuu puhelimen tai sähköpostin välityksellä. Toinen hyvä konkreettinen vertaus palolaitokseen tulee ennaltaehkäisyn kautta. Palolaitos pyrkii ennaltaehkäisemään paloja lisäämällä tuliturvallisuustietoisuutta ja havainnointia. CSIRT-ryhmä tarjoaa teknisiä dokumentteja, koulutusta ja harjoittelua ennaltaehkäisyn kannalta. Lisäksi CSIRT-ryhmä voi järjestää kyberhyökkäysten torjumisen ja tunkeutumisen havainnoimisen suhteen harjoituksia tai jopa kyberohjelmiston kehitystä. Nämä ennaltaehkäisevät tietoturvatapahtumia sekä vähentävät reagointiaikaa tapahtuman sattuessa. Kehityksen saralla palolaitokset vaikuttavat myös lainsäädäntöön lisätäkseen paloturvallisuutta ja paloturvallisia tuotteita. Kehitystyössä samankaltaiset CSIRT-ryhmät osallistuvat foorumeihin parantaakseen ja kehittääkseen turvallisuusstandardeja. [6] Toiminnot ja vuorovaikutus tietoturvarikkeen tapahtuessa CSIRT-ryhmän ja sen palveleman yhteisön välillä edellyttää, että yhteisö tuntee CSIRT-ryhmän toimintatavat ja – mallit. Monet reagointiryhmät ovat tekemisissä tapahtumien käsittelyn kanssa, joten on tärkeää, että yhteisö ymmärtää CSIRT-ryhmän suhteen muihin ryhmiin. [13]

CSIRT-ryhmä auttaa organisaatiota hallitsemaan riskejä ja toipumaan tietoturvarikkeistä ja – uhkista. Lukijalle herää todennäköisesti kysymys, että minkälaisia konkreettisia palveluja CSIRT-ryhmä tuottaa? CSIRT voi suorittaa sekä reagoivia, että ennakoivia toimintoja auttaakseen suojaamaan ja turvaamaan organisaation kriittistä omaisuutta. Ei ole olemassa standardisoituja funktioita tai palveluja, joita CSIRT tuottaa. Jokainen ryhmä valitsee omat palvelunsa toimialueensa mukaan. CSIRT-toiminnan päätähtäin on syytä kohdistaa yhtiön liiketoiminnan tai emoyhtiön kannalta tärkeisiin palveluihin, mitä tahansa palveluja se tuottaakaan. Kriittisen omaisuuden suojaaminen on avainasemassa organisaation ja CSIRT-ryhmän menestymiseen. CSIRT-ryhmän täytyy tehdä ja tukea liiketoiminnan kannalta kriittisiä prosesseja ja järjestelmiä toimialueellaan. Prosessi, jonka avulla CSIRT-ryhmä toimii, on ni-

meltään tapahtumahallinta. Tapahtumanhallintaprosessi sisältää kolme toiminnallisuutta: tapahtuman raportointi, tapahtuman analysointi ja tapahtumaan reagointi. Tapahtuman raportointi tarjoaa CSIRT-ryhmän keskitetyn kontaktipisteen paikallisten ongelmien raportointiin. Keskitetty piste tarjoaa yhden paikan, johon kerätään kaikki raportit ja toiminnallisuus. [12]

3.3 CSIRT-ryhmän tunnettavuus

Jokaisen käyttäjän pitäisi tietää mahdollisimman paljon CSIRT-ryhmän palveluista ja toiminnoista jo paljon aikaisemmin, ennen kuin hän niitä todella tarvitsee. Selkeät tiedotukset CSIRT-ryhmän toimintamalleista auttavat käyttäjiä ymmärtämään, kuinka raportoida tietoturvarikkeistä ja minkälaista tukea on tarjolla. Selkeät rajaukset CSIRT-ryhmän palveluihin tekevät CSIRT:n toimimisen todelliseksi ja tehokkaaksi. Ryhmän pitäisi kertoa sen toimintamallit ja palvelut sopivassa muodossa toimivaltansa alueelle. On tärkeä ymmärtää, että kaikki toimintamallit ja toimenpiteet ei tarvitse olla julkisesti saatavilla. Esimerkkinä voidaan todeta, ettei ole tarpeellista ymmärtää ryhmän sisäistä toimintaa toimiakseen heidän kanssaan. CSIRT voi ohjeistaa rikkeen raportoinnissa, järjestelmän analysoinnissa tai turvaamisessa ilman asiakkaan CSIRT-ryhmän sisäisen toiminnan tuntemista. Aikaisemmin jotkin ryhmät tuottivat eräänlaiset toiminnalliset puitteet, toiset tuottivat usein kysyttyjen kysymyksien lista (U.K.K), kun taas toiset kirjoittivat levitettäviä papereita käyttäjien kokouksiin tai lähettivät uutiskirjeitä. Nevil Brownlee & Erik Guttman suosittelee jokaisen CSIRT-ryhmän julkaisevan omat toimintamallinsa ja menettelytapansa heidän omalla palvelimella, esim. www-palvelimella. Oma www-serveri mahdollistaa kyseisen CSIRT-ryhmän asiakkaiden helpon pääsyn tiedon lähteelle. Ongelmana on se, että miten CSIRT-palvelun tarvitsija löytää oman oikean ryhmänsä. CSIRT-toimivallan alla olevien asiakkaiden täytyy löytää helposti oma CSIRT-ryhmänsä, jota tulisi käyttää. CSIRT-ryhmien tiedot tulee olla löydettävissä hakukoneilla, joka auttaa jakamaan tietoa eri CSIRT-ryhmien olemassaolosta ja heidän perustiedoistaan. On hyödyllistä olla keskitetty säilytyspaikka, joka sisältää kaikkien olemassa olevien CSIRT-ryhmien tiedot. Käyttäjän pitää pystyä tarkistamaan tiedon luotettavuus huolimatta siitä, mistä lähteestä tieto tulee. On suositeltavaa, että tärkeät

dokumentit pitää olla suojattu digitaalisella allekirjoituksella. Tämä auttaa käyttäjä todentamaan, että tieto on alun perin CSIRT-ryhmän julkaisemaan ja että sitä ei ole päässeet sivulliset muuttamaan. [13]

3.4 CSIRT-ryhmän toiminta ja palvelut

CSIRT-ryhmän toimintaa vaativa tapahtuma voi olla esimerkiksi verkon tai palvelimen toiminta, joka uhkaa tietojärjestelmien turvallisuutta. Organisaatio tarvitsee CSIRT-ryhmän järjestelmään murtautujia ja muita tahallisia haitantekoja varten. Tietoturvarikkeen tapahtuessa yhtiöllä on tärkeää olla tehokas ja nopea tapa selvittää tapahtuma. Tarvitaan ryhmä, joka tekee selvityksen mahdollisimman pian. Tietoturvarikkeen aiheuttamat vahingot ja kustannukset organisaatiossa mitataan tapahtuman tunnistamisen, analysoinnin ja reagointinopeuden perusteella. Järjestelmän palauttamisen kulut ja toiminnan palauttaminen rikettä edeltävälle tasolle riippuvat reagointinopeudesta. CSIRT-ryhmä toimii paikan päällä ja kykenee muodostamaan nopean vastauksen tietoturvarikkeeseen ja auttaa toipumaan siitä. Ryhmällä voi olla myös kokemusta järjestelmistä, joihin on tunkeuduttu. Näin heillä on valmiuksia koordinoida järjestelmän puhdistamista ja palauttamista normaaliin tilaan sekä ehdottaa toimintatapoja. CSIRT-ryhmän suhteet muihin tietoturvajärjestöihin auttavat tuottamaan ja jakamaan toimintamalleja ja hälytyksiä potentiaalisiin ongelmiin. Ryhmä toimii myös organisaation muiden osastojen kanssa yhteistyössä varmistaakseen uusien järjestelmien kehityksen tietoturvallisesta näkökulmasta. CSIRT-ryhmä auttaa tunnistamaan organisaation haavoittuvuuksia ja suorittaa haavoittuvuuksien tunnistamista ja hallintaa. Lisäksi ryhmä voi suorittaa ennakoivaa analyysiä ja yhteistyötä muiden vastaavien CSIRT-ryhmien kanssa tulevaisuuden uhkia varten. [4]

Nevil Brownlee & Erik Guttman:in parhaiden käytäntöjen mukaan CSIRT-ryhmän palvelut voidaan jakaa karkeasti kahteen kategoriaan. Tosiaikaiset toiminnot, jotka liittyvät suoraan tapahtumanhallinnan reagointiin ja muut toiminnot, jotka tukevat tapahtumanhallinnan tapahtuman käsittelyä. Muut toiminnot ja osa reaaliaikaisista toiminnoista koostuvat palveluista, jotka ovat valinnaisia. Valinnaisiksi niitä voidaan sanoa siksi, koska kaikki CSIRT-ryhmät eivät niitä tarjoa. Palvelut voidaan jaotella seuraavasti:

- Tapahtuman reagointi, joka sisältää yleensä raporttien arvioinnin tapahtumista ja yhteydenpidon muiden CSIRT-ryhmien kanssa. Yhteydenpito sisältää mm. raporttien vertailun, yhteydenpidon yhteyksiä tarjoavien operaattoreiden kanssa ja tapahtumien koordinoinnin.

- Ennakoiva toiminta, joka sisältää mm tiedontarjontapalvelua. Tiedontarjontapalvelun sisältönä voidaan mainita tunnettujen haavoittuvuuksien arkisto, korjauspäivityksiä ja raportoitujen ongelmien ratkaisuja. Lisäksi ennakoiva toiminta sisältää turvallisuuteen liittyviä työkaluja, koulutusta ja harjoituksia, tuotteen arvioimista ja auditointia sekä konsultointia. [13]

3.5 Yleisimmät CSIRT-ryhmät

Alla on mainittu muutamia yleisiä kategorioita tietoturvatapahtuman reagointiryhmille:

- sisäiset tietoturvatapahtuman reagointiryhmät tuottavat tapahtumanhallintapalveluita heidän organisaatiolle. Esimerkkinä voidaan mainita oma CSIRT-ryhmä pankille, tuotteita valmistavalle yhtiölle, yliopistolle tai virastolle.

- kansalliset tietoturvatapahtuman reagointiryhmät tuottavat tapahtumanhallintapalveluita koko maalle. Esimerkkinä on Singaporen tietokone hätätilanne reagointiryhmä (SingCERT)

- koordinaatiokeskus koordinoi ja helpottaa tapahtumien käsittelyä eri tietoturvatapahtuman reagointiryhmien välillä. Esimerkkinä toimii CERT- koordinaatiokeskus tai Yhdysvaltojen tietokone hätätilanne valmiusryhmä (US-CERT)

- analyysikeskus keskittyy yhdistämään tietoa eri lähteistä määritelläkseen tapahtumien toistuvuutta ja samankaltaisuutta. Tätä tietoa voidaan käyttää apuna ennustettaessa tulevaa toimintaa tai tuotettaessa aikaisia varoituksia, kun toiminta täsmää aikaisemmin havaittuun vastaavaan käyttäytymiseen

- toimittajaryhmä (vendor team) käsittelee ohjelmisto- tai laitteistotuotteiden haavoittuvuuksien raportit. Ryhmä voi työskennellä organisaation sisällä määritelläkseen, ovatko organisaation tuotteet haavoittuvia ja kehittääkseen palautumis- tai ehkäisystrategioita haavoittuvuuksien varalle. Toimittajaryhmä voi myös olla sisäinen tietoturvatapahtuman reagointiryhmä toimittajaorganisaatiolle (vendor organization).

- tapahtumanvastinetuottajat tarjoavat tapahtumanhallintapalvelua, maksua vastaan tyyppisenä palveluna, toisille organisaatioille

Tapahtumahallintaryhmille on olemassa laaja kirjo kirjainlyhenteitä ympäri maailmaa. Yleisimmät kirjainlyhenteet ovat:

- CSIRT = Computer Security Incident Response Team
- CIRC = Computer Incident Response Capability
- CIRT = Computer Incident Response Team
- IRC = Incident Response Center or Incident Response Capability
- IRT = Incident Response Team
- SERT = Security Emergency Response Team
- SIRT = Security Incident Response Team
  [4]

3.5.1 JPCERT/CC

On olemassa erimuotoisia ja laajuisia tietoturvatapahtuman reagointiryhmiä, jotka palvelevat eri yhteisöjä. Japanissa on koko maanlaajuinen CSIRT-ryhmä, jonka nimi on JPCERT/CC (Japan Computer Emergency Response Team Coordination Center). AusCERT

puolestaan tuottaa CSIRT-palveluja koko Aasian ja Tyynenmeren alueelle. Alueen sisällä voi silti olla erillisiä toimijoita, jotka tuottavat palveluita yliopistolle tai kaupalliselle organisaatiolle. On olemassa myös yritysryhmiä, jotka tuottavat CSIRT-palveluja asiakkailleen ilmaiseksi. [4]

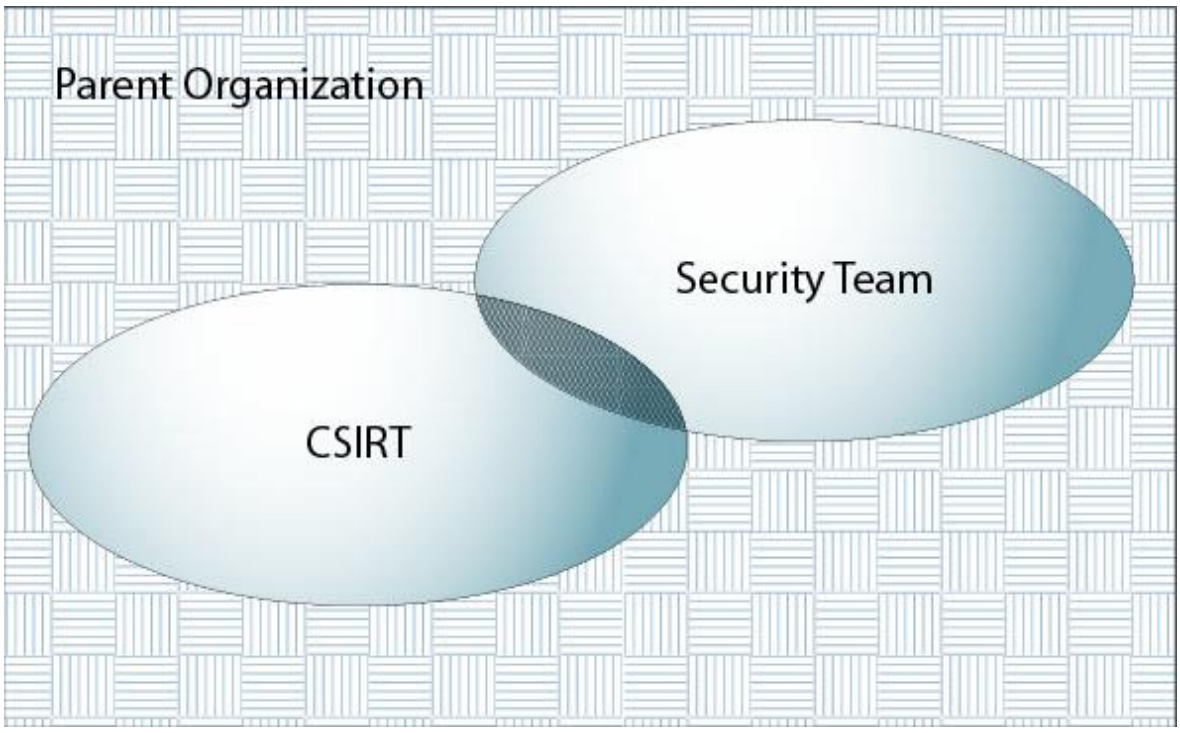
3.5.2 The Software Engineering Institute (SEI)

The Software Engineering Institute (lyhennettynä SEI) on voittoa tuottamaton Yhdysvaltain liittovaltion rahoittama tutkimus- ja kehityskeskus. SEI toimii Carnegie Mellon yliopistossa ja se on Yhdysvaltain puolustusministeriön perustama ja ohjaama. SEI:n toimiala on ohjelmistot ja kyberturvallisuus. The Software Engineering Institute hoitaa Yhdysvaltojen puolustusministeriön tehtäviä, joita yksityisen sektorin tutkimus ja kehityskeskukset eivät pysty suorittamaan. SEI on tasapuolinen, puolueeton ja rehellinen toimija, jossa on töissä parhaita ohjelmisto- ja kyberturvallisuusosaajat ja se tarjoaa keskitetyn paikan ohjelmistosuunnittelun ja kyberturvallisuuden tiedoille. SEI kehittää sekä ylläpitää ydinosaamista Yhdysvaltain puolustusministeriön kriittisille alueille. SEI auttaa hallinto- ja teollisuusorganisaatioita kehittämään pitkällä tähtäimellä integroituja ratkaisuja ja järjestelmiä, jotka ovat turvallisempia, käytettävimpiä ja luotettavampia. "CERT" ja "CERT Coordination Center" ovat The Software Engineering Institute:n rekisteröityjä tavaramerkkejä ja Yhdysvaltain patentteja. CERT-nimen käyttö vaatii organisaatiolta yhteydenottoa ja luvan pyytämistä SEI:ltä. [14]

3.6 CSIRT-ryhmän sijainti organisaatiossa

CSIRT-ryhmän paikka organisaatiossa kulkee käsi kädessä heille määritellyn tehtävän ja heille määrätyn toimialueen mukaan. CSIRT- ryhmän organisaatiokaavan sijainnille ei ole olemassa ennalta määrättyä ja hyväksyi todettua paikkaa, joten ryhmän täytyy itse määritellä mitä heidän on tarkoitus tehdä ja kenen kanssa. Tämä määrittely asettaa CSIRT-ryhmän sijainnin organisaatiossa. Esimerkiksi ryhmän sijoittaminen yhtiön järjestelmähallintaosastolle olisi virhe ja on todettu, että kyseinen rakenne ei toimi. Välttääksemme tämän kaltaisia virheitä, tässä osassa tekstiä on tarkoitus tuoda näkökulmia CSIRT-ryhmän sijaintiin yhtiön organisaatiokaaviossa. CSIRT voi olla itsessään organisaation turvallisuusryhmä tai se voi

olla kokonaan erillään organisaation tietoturvaryhmästä. Organisaatiolla ei myöskään tarvitse olla erillistä CSIRT-ryhmää, tätä roolia voidaan hoitaa organisaation tietoturvaryhmän toimesta. Toteutustavasta riippumatta tapahtumanhallintapalvelun toimintamallit ovat tärkeimmässä asemassa. CSIRT-ryhmää käsitellään tässä yhteydessä yleisimmässä ja yksinkertaisimmassa muodossaan, eli osana isompaa tietoturvaryhmää yhtiön sisällä. Mihin tahansa CSIRT -ryhmä on sijoitettu, niin on elintärkeää että sillä on johdon tuki ja CSIRT-ryhmä saa tarvittavan auktoriteetin tehdäkseen päivittäisen työnsä. Kts. Kuva 3. [11]



Kuva 3 kuvaus CSIRT-ryhmän sijoittamisesta ja tehtävästä organisaation sisällä, josta näkyy osittainen päällekkäisyys turvallisuusryhmän kanssa [11]

CSIRT-ryhmän täytyy olla yritysympäristössä hyvin sulautettu organisaation rakenteeseen. CSIRT-ryhmän toiminta voi olla osittain päällekkäin tietoturvaryhmän kanssa. Yhden emoyhtiön sisällä saattaa olla myös useampia tapahtumanhallinnan käsittely yksiköitä. Kyseinen

tilanne voi esiintyä palveluntuottajaorganisaation ja verkkopalveluntuottajan omien erillisten ryhmien kautta. Yksi käsittelee tapahtumia yhtiön oman tietoverkon sisällä ja toinen käsittelee tapahtumia tuottaessaan palveluita asiakkailleen. Palveluntuottajaorganisaatiot voivat tuottaa myös lisäpalveluita, esimerkkinä turvallisuusaukkojen käsittely tuotteissa. Päällekkäisyyttä saattaa esiintyä organisaation sisällä, mutta se ei näy palvelun tuottamisessa organisaation ulkopuolisille tahoille. Yhtiö voi jakaa ryhmät esimerkiksi haittaohjelmien aiheuttamien tapahtumien hallintaryhmään ja verkkohyökkäyksien sekä verkkotunkeutujien tapahtumahallintaryhmään. Riskienhallinnan kannalta katsottuna on tärkeää määrittää CSIRT-ryhmän rooli organisaatiossa, jota ryhmä toteuttaa. Ennen roolin määrittelyä CSIRT-ryhmä ei voi rajata toimenkuvaansa. Ryhmän rooli vaihtelee riippuen emoyhtiön mallista ja ryhmän piirissä olevan toiminnan luonteesta. Minkälaiseksi tahansa CSIRT-ryhmän rooli määritelläänkään, on välttämätöntä, että ryhmän toimintaan tuetaan johdon osalta ja että kaikki mukana olevat ymmärtävät CSIRT-ryhmän roolin. [11]

Tietojenkäsittelyä, verkkoja ja viestintävälineitä ylläpitävät osat organisaatiosta voidaan määritellä kantavan teknisen riskin. Liiketoimintariskiä kantaa mukanaan moni eri osa organisaatiosta. On tärkeää ymmärtää kenellä on vastuu riskienhallinnasta ja miten jokainen osa organisaatiosta vuorovaikuttaa toisiinsa ja mitkä ovat heidän vastuut. Kaupallisessa organisaatiossa voi eri ryhmillä saman organisaation sisällä olla sama vastuu riskienhallinnan kannalta katsottuna. Esimerkiksi verkko-operaatio ryhmä vastaa verkon turvallisuustapahtumista, järjestelmänhallintaryhmä vastaa palveluiden turvallisuustapahtumista, fyysisen turvallisuuden ryhmä vastaa kulkemisesta organisaation eri rakennuksiin ja toimipisteisiin, CSIRT-ryhmä on vastuussa tietokoneisiin liittyvien tapahtumaraporttien reagoinnin koordinoinnista ja yhtiön turvallisuusryhmä on vastuussa yhtiönlaajuisten toimintamallien ja ohjeiden asettamisesta mukaan lukien kaikki muut turvallisuusryhmät ja henkilöstö. Riippumatta tarkasta roolistaan riskienhallinnassa, jokaisen ryhmän täytyy ymmärtää vastuunsa suhteessa muihin organisaation komponentteihin ja ymmärtää kuinka toimia muitten ryhmien kanssa, ettei yksi ryhmä toimi eristyksissä tai muiden ryhmien toimivallan alueella. Jokaisella ryhmällä täytyy olla selkeä kuvaus velvollisuuksistaan, yhteydenpitomalleista ja vastuistaan. Samanaikaisesti organisaatiosta saatetaan ottaa yhteyttä ulkopuoliseen CSIRT-

ryhmään, jonka vastuut ja velvollisuudet täytyy olla hyvin sisällytetty ja hyvin kuvattu organisaation riskienhallintakaaviossa päällekkäisyyksien välttämiseksi. [11]

3.7 CSIRT-ryhmän suhde muihin ryhmiin

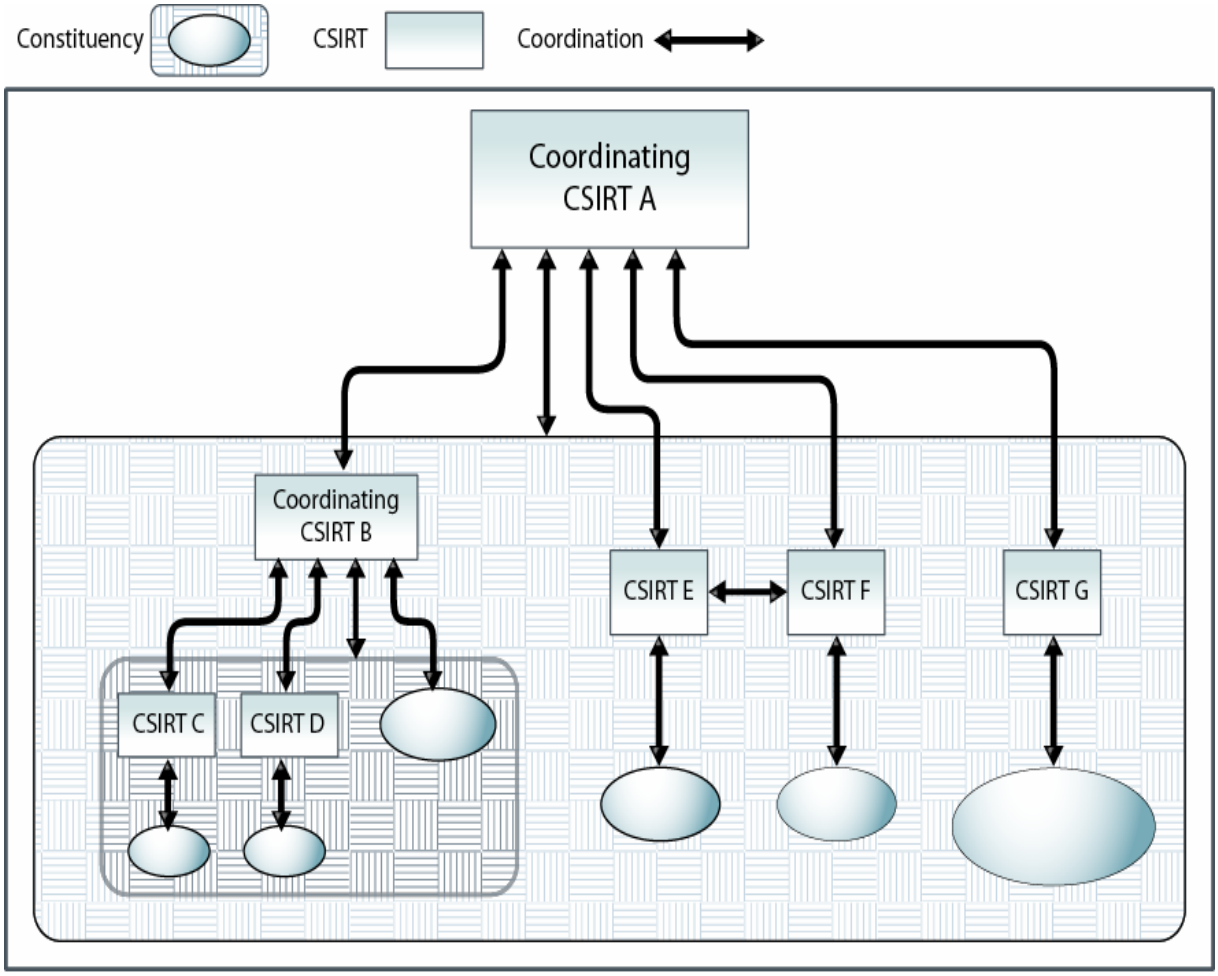
CSIRT-ryhmän toiminta-alue on internet, eli maailmanlaajuinen. Yhä useampi järjestö ja organisaatio ovat CSIRT:n palvelemia. CSIRT-ryhmien täytyy tehdä yhteistyötä yli rajojen, jotta ryhmän työ tulee tehdyksi. Tämän tyyppinen yhteistyö ja koordinointi on CSIRT:n rakenteen ydin. Pelkkä tehtävänkuvaus, toiminta-alueen määrittely ja CSIRT:n paikan määrittäminen organisaatiossa ei ole tehokasta, ellei koordinointia ole sovittu ja määritelty oikein. CSIRT nykymallien mukaan on olemassa hierarkkisia rakenteita, joita voidaan havaita erityyppisten ryhmien välillä. On olemassa tiimejä, jotka palvelevat selkeästi rajattua toimialuetta, sekä tiimejä, jotka toteuttavat koordinaattorin roolia ristiin eri CSIRT:n ryhmien välillä. Tällainen rakenne kuitenkaan ei ole todellista hierarkiaa ja useimmissa tapauksissa rakenne on sekä informatiivinen että vapaaehtoinen. Informatiivinen rakenne nähdään hyötynä, koska se mahdollistaa tiimien joustavan, nopean ja tehokkaan tiedonjaon toisten luotettavien CSIRT-ryhmien kanssa. [11]

On olemassa joitain jaoteltuja hierarkioita, kuten Amerikan Yhdysvaltojen puolustusvoimien sisällä olevat:

- ACERT/CC, joka palvelee USA:n maavoimia
- AFCERT, joka palvelee USA:n ilmavoimia
- NAVCIRT, joka palvelee USA:n merivoimia.

Amerikan Yhdysvaltojen puolustusministeriö DOD-CERT koordinoi kaikkia USA:n puolustusvoimien ryhmiä. Moni tiimi toimii kuitenkin suoraan muiden vertaisten tiimien kanssa, eikä koordinoivan CSIRT:n kanssa. Tämä tapahtuu yleensä, kun tiimit arvioivat ettei koordinoivan CSIRT:n tarvitse osallistua käsiteltävän ongelman käsittelyyn. Koordinoiva CSIRT usein pyytää, että heitä informoidaan kaikesta toiminnasta. Näin koordinoiva CSIRT pystyy saamaan oman toimialueensa aktiivisuustason kokonaiskuvan ja hälyttämään muita tiimejä valvomaan samankaltaista toimintaa. Kuvassa 2. on kuvattu eri mahdollisuuksia tietoturva-

poikkeamaryhmien vertaissuhteisiin. Ryhmä voi olla koordinoiva CSIRT, jos se toimii koordinoivassa roolissa muiden CSIRT-ryhmien joukossa. Kuvassa 2. CSIRT A ja CSIRT B toimivat koordinoivina ryhminä. CSIRT C ja CSIRT D ryhmien koordinoinnin lisäksi CSIRT B:lla on ohjattavana muu ryhmä C:n ja D:n rinnalla, joka näkyy kuvassa tyhjänä soikiona CSIRT C ja CSIRT D-ryhmän rinnalla. E- ja F-ryhmän välillä on suoraa yhteydenpitoa, joten A-ryhmän hierarkia ei ole kovin tiukka eikä se puutu tähän liikenteeseen. Yhteysmalleja, joita on kuvattu tässä osassa, voidaan käyttää kuvaamaan mitä tahansa tietoturvapoikkeamaryhmää riippumatta sen tarkoituksesta. [11]



Kuva 4. CSIRT-jäsenten suhteet [11]

4 Aiheeseen liittyvät tieteelliset tutkimukset

4.1 Tieteelliset haut tutkielman aiheeseen liittyen

Kybertoiminnallisuuden havainnoinnista ja CSIRT-toiminnasta löytyi kirjaston haulla 0 kappaletta tutkielmia Suomesta. Kyberturvallisuuden havainnointi hakusanalla aiheeseen liittyviä tutkimuksia löytyi Suomesta 0 kappaletta. Englanninkielisillä yhdistetyillä hakusanoilla ”cyber” ja ”survey” kyberturvallisuustutkimuksia ja niistä julkaistuja tuloksia löytyi DART-Europe E-theses Portal tietokannasta 6 kappaletta. Lisäksi googlen tieteellisellä haulla löytyi tutkimuksia, joita on vertailtu seuraavissa alaotsikoissa.

4.2 “Users Really Do Plug in USB Drives They Find” -tutkimus

Hyvä aiheeseen liittyvä tutkimus löytyi USB-muisteihin liittyen Matthew Tischerin, Zakir Durumericzin, Sam Fosterin, Sunny Duanyn, Alec Morin, Elie Burszteinin ja Michael Baileyn Illinoisin yliopiston, Michiganin yliopiston ja Google, Inc:n yhteistyössä tekemässä tutkimuksessa nimeltä ”Users Really Do Plug in USB Drives They Find”. Tässä tutkimuksessa tutkittiin uskomusta, että käyttäjät ottavat löytämänsä USB-muistin ja laittavat sen kiinni tietokoneeseen. Tutkimuksessa pudotettiin 297 kappaletta USB-muistitikkuja yliopiston alueelle 27 – 29. huhtikuuta 2015. Tutkimustulokset osoittivat, että onnistumisprosentti on 45 - 98 prosenttia. Kahdeksan oppilaan ryhmä pudottelivat tikkuja, esim. samalla kun solmivat kengän nauhojaan ja katsoivat samalla ympärilleen, ettei kukaan huomannut USB-muistitikun jättämistä siihen paikkaan. Pudotettuaan muistitikun, tutkijat merkitsivät USB-muistitikun sijainnin älypuhelimeen. Päivän mittaan tutkijat pystyivät katsomaan oliko USB-muistitikkua siirretty. Tarkkailujakson aikana 98 % (290 kpl) muistitikuista siirtyi alkuperäisestä paikastaan ja 45 % (135 kpl) muistitikuista kytkettiin tietokoneeseen ja sieltä avattiin tiedosto. Tutkimuksessa jää epäselväksi 155 kpl USB-muistitikun kohtalo. Nämä 155 kpl muistitikkua saatettiin kytkeä tietokoneeseen avaamatta tiedostoa. Oletettu odotusaika on vähemmän kuin 6 minuuttia, siitä kun ensimmäinen tiputetuista USB-muistitikuista on kytketty tietokoneeseen. Tutkimuksessa todettiin, että ne jotka kytkivät USB-muistitikun tietokoneeseen, he olivat epäitsekkäästi etsimässä USB-muistitikun omistajaa. Nämä yksilöt eivät ole

teknisesti osaamattomia, mutta he ovat enemmänkin yhteisön jäseniä, joilla on tapana ottaa vapaa-ajalla enemmän riskejä kuin muut heidän ikäisensä. [15]

4.3 ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi”

”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” niminen tutkimus löytyi valtioneuvoston selvitys ja tutkimustoiminnan teettämänä. Tutkimuksen tekijänä ovat olleet Martti Lehto, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi ja Mirva Salminen. Tässä tutkimuksessa on haastateltu yhteensä 31 yksityisten yrityksien ja julkisten organisaatioiden tieto/kyberturvallisuudesta vastaavaa henkilöä. Tästä tutkimuksesta löytyy kappale 3.5.3 Havainnointikyky. Tutkimuksessa kerrotaan haastatteluista, että: *”yksityisten yritysten haastattelujen teemat käsittelivät yritysten kyberturvallisuuden vahvuuksia, heikkouksia, uhkia ja mahdollisuuksia. Lisäksi haastattelussa kartoitettiin laajemmin kunkin toimialan kyberturvallisuuden tilaa ja kehittämistarpeita. Haastattelut toteutettiin puolistrukturoituina teemahaastatteluina ja haastateltaville luvattiin täysi anonymiteetti”.*[16] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi- tutkimuksessa havainnointikyky mainittiin haastatteluissa keskeiseksi haasteeksi kyberturvallisuuden parantamisessa.

Tutkimusta tehdessä en saanut yhtiöltämme juuri tietoa CSIRT-toiminnasta tai CSIRT-ryhmän yhteistoiminnasta muiden vastaavien ryhmien kanssa. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi- tutkimuksessa todetaan *” yksityisen sektorin, erityisesti kriittisten yritysten osalta, ilmoitusvelvollisuudessa ja tiedon jakamisessa koetaan olevan tehostamisen mahdollisuuksia. Tarvittaessa tulee lainsäädännön keinoin lisätä ilmoitusvelvollisuutta. Keinoina tehostamiseen mainittiin myös julkinen-yksityinen-yhteistyön kehittäminen”.* [16] Tässäkin tutkimuksessa on korostettu usean eri lähteen kautta yhteistyön ja nopean tiedon välittämisen merkitystä. Julkinen-yksityinen-yhteistyö kyberhavainnoinnin osalta olisi merkittävä parannus havainnointikykyyn ja nopeaan reagointiin.

Martti Lehdon, Jarno Limnéllin, Eeva Innolan, Jouni Pöyhösen, Tarja Rusin ja Mirva Salmisen tekemässä tutkimuksessa löytyy mielenkiintoinen 3.5.7 Kyberosaamisen ja -ymmärryksen parantaminen niminen otsikko. Tämän tutkimuksen alussa on todettu, tutkimuksen tavoitteeksi muun muassa nostaa konsernin tietoturvatasoa tuomalla työntekijälle esille tietoturvallisuuteen liittyviä kysymyksiä ja lisätä samalla valveutuneisuutta asian suhteen. *''Strategian tavoitteena oli, että parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä. Sen mukaan yhteiskunnan toimijoiden jatkuvan osaamisen ja tietämyksen kehittämisen tukena panostetaan yhteisten kyberturvallisuuden ja tietoturvallisuuden ohjeistojen kehittämiseen, hyödyntämiseen ja kouluttamiseen. Yhteiskunnan kokonaisvaltaisen valmiuden kehittämiseksi harjoitustoimintaan otetaan mukaan myös yhteiskunnan elintärkeiden toimintojen kannalta tärkeät yritykset ja kansalaisjärjestöt''*.[16] Harjoitustoimintaa on ollut havaittavissa keväisin Jyväskylän ammattikorkeakoulun (JAMK) järjestämillä yhteistoimintaharjoituksen muodossa. Tässä harjoituksessa eri viranomaisten valittu joukko ovat harjoitelleet yhdessä kyberpuolustusta ja – hyökkäystä. Suomen Erillisverkot Oy voisi harkita koko yhtiön laajuisia sisäisiä harjoituspäiviä, jolloin tehtäisiin vastaavanlainen harjoitus kuin JAMK järjestää. Näin yhtiö saisi kokemusta omasta toimintakyvyn palauttamisesta hyökkäyksen tapahtuessa. Käytännön kokemus yhtiön laajuisesti olisi haittaohjelmasta toipumisessa tai muun vastaavan hyökkäyksen tapahtuessa elintärkeää.

Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi tutkimuksesta on otsikko 6.2.10 Yleinen tietous. Tämän otsikon alla on todettu: *''Kyberturvallisuus, kuten turvallisuus, on aina myös kulttuurinen asia. Hyvään turvallisuuskulttuuriin liittyy ymmärrys riskeistä, vastuun kokeminen turvallisuuden kehittämisestä ja mahdollisuudesta vaikuttaa turvallisuuden parantamiseen. Kulttuurin muutos vie aikaa ja turvallisuuskulttuuri on vasta hiljalleen vakiintumassa ihmisten toimintaan ja käyttäytymiseen kybertoimintaympäristössä''*.[16] TUVE-verkon siirryttyä Suomen Erillisverkot Oy:n hallintaan 1.3.2015 voidaan toimintaamme pitää uutena, jolloin on ymmärrettävää että kyberturvallisuuskulttuurin ja esimerkiksi CSIRT-toiminnan rakentaminen vie oman aikansa. Teettämästäni kyselystä saa kuitenkin havainnollistavaa materiaalia henkilöstön koulutusta ja valveutuneisuuden nostoa varten. Henkilöstön koulutuksista tuli yhtiössä toistuva tapa toteutuneen kyselyn ja tutkielman teon jälkeen.

4.4 Kyberturvallisuusriskien muodostuminen ihmisten käyttäytymiseen ja tietämättömyyteen liittyen

4.4.1 ComptTIA:n tutkimus 1200 työntekijälle ihmisten käyttäytymisestä

CompTIA:an kuuluva The Blackstone Group on tehnyt tutkimuksen kyselynä 1200 työntekijälle, jotka työskentelevät kokopäiväisinä Yhdysvalloissa tietokoneilla. Kysely on suoritettu lokakuun 10. - lokakuun 16. välisenä aikana verkkokyselynä. Kyselyssä käytettiin kiintiöitä iän, sukupuolen ja yhtiön koon mukaan, tulosten varmistamiseksi. The Blackstone Group on osa The Computing Technology Industry Association:ia eli CompTIA:a. CompTIA koostuu kahdesta tuhannesta yhtiöstä ja kolmesta tuhannesta akateemisesta ja koulutuskumppanista sekä melkein kahdesta miljoonasta IT-sertifikaatista. CompTIA on sitoutunut edistämään alan kasvua koulutusohjelmien, markkinatutkimusten, verkostoitumisen, ammatillisten sertifikaattien ja yleisten käytäntöjen edistämisen kautta. [17] Tutkimuksessa todetaan yhtiöiden tehneen ison työn suojautuakseen sisäisiltä ja ulkoisilta uhkilta tietoverkkorikollisuuden osalta. Teknologian innovaatioiden tahdin kasvaessa uhkat ovat vain monimutkaistuneet. Laitteiden suojaaminen ja verkossa olevan datan suojaaminen on jatkuvaa taistelua hyökkääjiä vastaan. Vuonna 2015 syyskuun puolessa välissä oli raportoitu 606 kappaletta tietovarkauksia, vaarantaen yli 175 miljoonaa tietuetta vuoden 2015 osalta. [18] Tutkimuksessa todetaan työntekijän kyberturvallisuustietämyksen ja kyberturvallisuuskäyttäytymisen laahaavan perässä. Vaikka osa tapahtumista johtuu järjestelmästä ja sen puutteellisesta suunnittelusta, pääosassa syyllisenä on yhtiön yksittäinen työntekijä ja hänen tekemät virheet tietokoneella. [19] IT-alan parhaiden käytäntöjen tunteminen ei riitä. Kyberturvallisuus heijastuu useista työntekijän tekemistä ratkaisuista teknologian kanssa, esimerkiksi vaihtaako työntekijä kirjautumistunnuksiaan tarpeeksi usein välttääkseen salasanan murtamisen ja estääkseen tietojen kalastelu yritykset. Vuonna 2014 Internet Crime Complaint Center vastaanotti 269 422 valitusta, joissa puhutaan yhteensä yli 800 miljoonan dollarin menetyksistä. Vaikka käyttäjät ovat enemmän valveutuneita kuin aiemmin, huolimaton käyttäytyminen jatkuu. [20]

4.4.2 The Blackstone Group:in teettämän kyselyn ja tutkimuksen vertailu

1200 työntekijä koskevan tutkimuksen ja kyselyn tärkeimmät havainnot olivat:

- 63 % työntekijöistä käyttää heidän työpuhelimiaan henkilökohtaisiin aktiviteetteihin
- 49 % työntekijöistä on ainakin 10 tunnusta, mutta vain 34 % sisältää 10 erilaista tunnusta
- 94 % työntekijöistä yhdistää kannettavan tietokoneensa / puhelimensa julkisiin wifi-verkkoihin
- 45 % työntekijöistä eivät saa kyberturvallisuusharjoitusta tai -koulutusta työnantajiltaan

CompTIA:n tutkimukseen osallistuneista 1200 työntekijästä 45 % jää tutkimuksen perusteella ilman kyberturvallisuusharjoitusta tai -koulutusta. Suomen Erillisverkot Oy:ssä työntekijöiden koulutus on ollut konsernissamme teettämäni kyberturvallisuuskyselyn jälkeen vähintään kvartaalin välein, joten konsernimme työntekijöistä käytännössä 0 % on jäänyt vuoden 2017 loppuun mennessä ilman kyberturvallisuuskoulutusta.

4.4.3 Ihmisten toiminta USB-muistin löytyessä

Vuonna 2015 elokuusta lokakuuhun CompTIA teetti sosiaalisen kokeen tarkkaillakseen ihmisten kyberturvallisuuskäyttäytymistapoja löytäessään USB-muistitikun. Tutkimusryhmä asetti hypoteesin niin, että toistuvien ja hyvin esille tuotujen kyberhyökkäyksistä ja tietomurroista huolimatta, moni käyttäjä käyttäytyy tietoturvan suhteen huonosti ja asettaa laitteensa ja tietonsa riskialttiiksi. 200 merkitöntä USB-muistitikkua pudotettiin vilkkaille julkisille paikoille, kuten lentokentälle, kahvilaan, julkiselle aukiolle ja kauppakeskukseen. USB-muistitikut olivat esiohjelmoitu tekstitiedostoilla, joissa oli ohjeistettu löytäjä lähettämään sähköpostia määriteltyyn osoitteeseen tai painamaan linkkiä. Muutaman viikon sisällä 17 % ihmisistä ottivat löytämänsä USB-muistitikun ja yhdistivät muistin heidän laitteeseensa, avasivat tekstitiedoston ja painoivat linkkiä tai lähettävät sähköpostia pyydettyyn osoitteeseen. Huomioitavaa oli, että ihmisen teknologiaosaaminen ei ollut ratkaiseva tekijä siihen, että otettiinko löydetty USB-muistitikku mukaan vai ei. Esimerkiksi San Franciscon kansainvälisellä lentokentällä joukko IT-alalla työskenteleviä ihmisiä löysivät kyseisiä

USB-muistitikkuja ja yhdistivät ne laitteisiinsa. Itseasiassa turvallisuustoimiston henkilöstö, joka sijaitsi monikansallisen yhtiön rakennuksessa, löysivät ja yhdistivät laitteeseensa levitetyn USB-muistitikun, koska myös he lähettivät postia annettuun osoitteeseen. [21]

Suomen Erillisverkot Oy:ssä tekemässäni kyselyssä kysymys nro 8. ”Jos löydän USB-muistitikun yhtiömme tiloista, miten toimin?” oli annettu kolme vaihtoehtoa:

- a) Laitan muistitikun koneeseen ja tutkin sen tiedostot, jotta löydän sen omistajan
- b) Laitan tikun tietokoneeseeni ja tarkistan sen heti F-Securen virustorjuntaohjelmistolla
- c) Toimitan löytämäni usb-tikun suoraan tietohallintoon

Näistä vaihtoehdoista 94 % 25 – 35 vuotiaista miehistä, 93 % 36 – 45 vuotiaista miehistä ja 97 % 46 - ja siitä vanhemmat valitsi oikein toimittamalla USB-muistin tietohallintoon. Kyselyyn osallistuneista naisista jokainen olisi toiminut oikein ja toimittanut USB-muistin oikeaoppisesti tietohallintoon. CompTIA:n tutkimuksessa 17 % oli kytkenyt USB-muistin koneeseen, joten yhtiöstämme n. 6 % miehistä ja 0 % naisista olisi kyselyn perusteella tehnyt saman.

Moni sähköpostin lähettäjistä kyseli, oliko heidän löytämissään USB-muisteissa virus. Tämä osoittaa sen, että lähettäjät olivat valmiita vaarantamaan laitteensa vaikka he ymmärsivät riskit. Luottaminen löydettyihin USB-muisteihin, suojaamattomiin WIFI-verkkoihin tai tunnistamattomiin sähköposteihin asettaa yksilön ja laitteet riskialttiiksi. Havainnot osoittavat, että kokeneet ja oppineet IT-käyttäjät saattavat tehdä huonoja päätöksiä kohdatessaan epäilyttävää teknologiaa ja miten haastavaa on sisäistää hyviä kyberturvallisuuskäytänteitä, vaikka tieto olisi jo sisäistetty.[21]

Viruksen tai hakkerin iskiessä suurin osa työntekijöistä aloittavat omat toimet tai ottavat yhteyttä heidän IT-tukeensa. Vähintään joka kolmas (35 %) kyselyyn osallistunut työntekijä vaihtaisi kaikki laitteiden ja tilien tunnukset tietoturvarikkeen tapahtuessa. Tämä on loogi-nen toimenpide, koska moni työntekijä käyttää samaa salasanaa useissa eri palveluissa. To-

sin yksi viidestä työntekijästä (20 %) vaihtaisi tunnukset vain tiliin, johon tietomurto vaikutti. Yksi kolmasosa (33 %) työntekijöistä ottaisi yhteyttä IT-tukeensa selvittääkseen tilanteen.[21]

5 Sosiaalinen hakkerointi

Sosiaalinen hakkerointi (social engineering) aiheuttaa vuosittain miljoonien dollareiden tappiot ihmisille. Huijaukset perustuvat hyökkääjän eli rikollisen taitoon hyväksikäyttää ihmiseen sisäänrakennettua ominaisuutta; taipumusta luottaa. Tällainen hyökkäys on vaikea tunnistaa ja pysäyttää. Sosiaalisessa hakkeroinnissa huijaaja manipuloi onnistuneesti uhrin tekemään tietynlaisia toimia, kuten lähettää rahaa verkon yli tai luottamuksellisia tietoja huijaajan esittäessä luotettavaa lähdettä. Sosiaaliset hakkerit käyttävät lukuisia eri taktiikoita hankkiakseen tietoa, joka auttaa heitä saamaan uhriensa luottamuksen. Huijaaja käyttää pitkälle kehitettyjä lähestymistapoja eli tietojen kalastelua tai toimivaksi todettuja keinoja, kuten roska-astioiden tutkiminen, huijauspuheluiden tai esittämällä yhteistyökumppanin työntekijää tai kollegaa. Huijarin saadessa haltuun tarvittavan informaation esiintyäkseen luotettavasti, hän voi ottaa yhteyttä uhrinsa ja aloittaa huijausoperaation. Jokainen voi joutua sosiaalisen hakkeroinnin uhriksi, mutta viime vuosina erityisesti liiketoiminnan parissa tämän tyyppiset huijaukset ovat nousussa. Mark Lowers, joka toimii Lowers Risk Group yhtiön toimitusjohtajana Purcellville:ssä Amerikan Yhdysvalloissa, kertoo yhtiönsä käsitelleen tuhansia huijaustapauksia hyvin hoidetuissa yhtiöissä. Sosiaalisen hakkeroinin onnistumisten kautta on siirretty satoja tuhansia rahaa. Rahoja ei saatu takaisin, koska rahat olivat siirretty jo useisiin eri pankkeihin huijauksen tultua ilmi. Vuonna 2014 McAfee-tietoturvayhtiön tekemässä tutkimuksessa todetaan sähköpostin tarjoavan varsin tuottoisa mahdollisuuden sosiaalisille hakkereille. 97 % ihmisistä maailmanlaajuisesti eivät pystyneet tunnistamaan tietojenkalastelusähköposteja. Federal Bureau of Investigation (FBI) puolestaan raportoi Amerikan Yhdysvalloissa olleen yli 7000 uhria ja aiheuttaen 747 miljoonan Yhdysvaltain dollarin rahalliset tappiot liiketoiminnan sähköpostihuijausten tyyppisissä sosiaalisessa hakkeroinnissa sitten vuoden 2013. [22]

22 biljoonan edestä rahaa käsittelevän Webster Bank:in huijaus- ja tappioryhmän vetäjä Kim Syrop kertoo, että liiketoiminnan sähköpostihuijauksissa huijarit hyökkäävät usein sellaisiin toimijoihin, jotka työskentelevät ulkoimaisten palvelun- tai tavarantoimittajien kanssa tai toimijoihin, jotka suorittavat pankkisiirtoja tai muita maksuja verkon yli. Vastaanottajalle huijauslaskut ja huijausmaksupyynnöt näyttävät tulevan luotettavalta toimijalta, jonka vuoksi moni työntekijä on saatu suorittamaan onnistuneesti rahansiirto väärään paikkaan.

Muissa tapauksissa huijarit esittävät yhtiön toimitusjohtajaa luomalla naamioituja sähköpostiosoitteita tai hakkeroimalla olemassa olevia sähköpostitilejä. Näiltä tileiltä huijarit ottavat yhteyttä yleensä alemman tason työntekijään pyytämällä rahansiirtoa painottaen asian luottamuksellisuutta. Näissä tapauksissa työntekijä haluaa täyttää esimiehensä toiveet nopeasti ja tehokkaasti, johon huijari perustaa toimintansa.[22]

5.1 Ihmisten muodostama palomuuri

Sosiaalisen hakkeroinnin ollessa vahvasti läsnä joka puolella, pankeilla on koko ajan tärkeämpää olla järjestelmät ja ohjeet tunnistaakseen ja estääkseen tämän tyyppiset huijaukset. Ihmisen ollessa heikoin lenkki turvallisuusketjussa, Mark Lowers (Lower Risk Group Ltd.) painottaa vahvasti koko konsernia koskevaa koulutusta vahvaa puolustusta rakentaessa. Lowersin mukaan pelkät ohjeet ja toimintamallit eivät riitä, vaan henkilöstöä on koulutettava kuinka tunnistaa tämän tyyppiset huijaukset; ihmisistä täytyy muodostua palomuuri. Tätä ihmisten palomuuria on jatkuvasti testattava ja päivitettävä, kun uusia uhkia muodostuu. Wester Bank:in Syrop varmistaa, että koko yhtiö tunnistaa tämän hetken huijaukset ja huomaa varoittavat merkit. Pankki huolehtii siitä, että kaikki liiketoimintalinjan johtajat ovat ajan tasalla näissä asioissa ja että he osaavat kouluttaa heidän alaiset ja asiakkaat. Lowers ja Syrop ovat molemmat sitä mieltä, että vahva huijauksenestokulttuuri lähtee pankin johtajatasolta. Havainnointi, koulutus ja kulttuuri ovat avaintekijöitä, Lowers kertoo. [22]

5.2 Kokemuksia tilien kaappauksista

Sosiaalisen hakkeroinnin ja ihmisten muodostaman palomuurin myötä kyberturvallisuuden kannalta tärkein tekijä on yksittäinen henkilö ja hänen toiminta. Eri järjestelmien tilien kaappaaminen on yleistynyt rajusti, koska elämämme on siirtynyt yhä enemmän digitaaliselle puolelle, eli ns. kybermaailmaan. Shay, Richard, Ion, Iulia, W. Reeder, Robert ja Consolvo, Sunny ovat tehneet tutkimuksen liittyen tilien kaappaamisiin. Tutkimukseen osallistui 294 henkilöä ja näistä 30 % tileistä oli tunkeuduttu ilman lupaa tuntemattomien toimesta. Kyselyn tuloksena voitiin poimia viisi teemaa:

1. tilit, joihin tunkeuduttiin, olivat arvokkaita uhreille

2. hyökkääjät ovat usein tuntemattomia, mutta joskus tuttuja uhrille
3. käyttäjät omaavat jonkin verran vastuullisuutta pitääkseen heidän tilinsä suojattuna
4. käyttäjien ymmärrys tärkeitä turvallisuustoimenpiteitä kohtaan on puutteellinen
5. haitta tilin kaappauksesta on uhrille emotionaalinen ja konkreettinen [23]

”Yhden tunnin aikaikkunassa minun koko digitaalinen elämä oli tuhottu“, kirjoitti kirjailija ja toimittaja Mat Honan Wired magazine – lehdelle.[24] Vuonna 2012 paljon luetussa kertomuksessa Honan kuvailee, kuinka hän menetti pääsyn Googlen, Twitterin ja AppleID-tileihin. Lisäksi hän menetti valokuvia, dokumentteja ja sähköposteja monien vuosien osalta sekä hänen Twitter-syötteeseen laitettiin rasistisia viestejä. Loppuen lopuksi Honan sai palautettua pääsyn tileilleen vaivan, merkittävien kustannusten ja ajan käytön jälkeen. Tietoa oli hävinnyt paljon. [25] Yhden hyökkääjistä ottaessa yhteyttä, Honan pääsi kysymään, miksi hyökkääjä oli tehnyt tämän hänelle. Syy oli Honanin kolmikirjaiminen Twitter-nimi ”mat”. Tiedon tuhoaminen oli vain sivullista vahinkoa. [23]

Honanin artikkeli hänen kokemuksistaan on hyvä varoittava tarina. Meidän maine, kontaktit ja tiedot ovat helposti hukattavissa ja niihin pääsy saattaa estyä. Korkeassa asemassa olevien ihmisten ja heidän läheisten tileihin tunkeutuminen on lisääntynyt. Esimerkkeinä voidaan poimia seuraavat tapaukset. Amerikan Yhdysvaltojen varapresidenttikandidaatin Sarah Palinin sähköpostitili oli hakkeroitu vuonna 2008 [26], Twitter-johtajan vaimon henkilökohtainen sähköpostitili oli hakkeroitu vuonna 2009 [27], Anonymous hakkeriryhmä murtautui turvallisuusyhtiön johtajien tileille vuonna 2011 [28] ja hyökkääjät murtautuivat lukuisten mediatalojen Twitter-tileille, mukaan lukien Associated Press [29], the Financial Times [30], the Guardian [31] ja the Onion vuonna 2013 [32].

6 Henkilöstön kybertoiminnallisuuden havainnointi

Yhtiön tai organisaation yksittäisen työntekijän valveutuneisuus on avainasemassa kybertoiminnallisuuden havainnoinnin ja poikkeavuuksien suhteen. Organisaation CSIRT-ryhmä ei kykene havaitsemaan kaikkea ja yksittäinen työntekijä voi inhimillisen virheen myötä rikkoa vahingossa tietoturvapolitiikkaa. Tässä tutkimuksessa selvitettiin Suomen Erillisverkot Oy:n työntekijöiden tietämys- ja valveutuneisuustasoa kybertoiminnallisuuden suhteen. Kyselylomake toimitettiin kaikille Suomen Erillisverkot Oy:n työntekijöille verkkokyselynä. Kysely on tutkielman liitteenä (LIITE 1).

6.1 Kysymykset ja niiden asettelu

Etsin tutkielmani kysymyksiä varten vastaavia sähköpostin kautta suoritettuja tietoturvakyselyitä tutkimuksiin liittyen. Ensimmäiset kysymykset tulivat vastaan tammikuussa 2006 Risto Kaukon ja Mikko Salkinojan Tampereen yliopistolle tehdyssä tutkimuksessa ”Sähköinen yhteys” – laadullinen tutkimus Sähköisen reissuvihkon soveltuvuudesta kodin ja koulun väliseen yhteydenpitoon. Tutkielman liitteessä 3 on aseteltu kysymykset seuraavasti:

1.a) Onko mahdollista, että laitteistosi saa virustartunnan e-reissuvihkoa käytettäessä?

b) Mikäli vastasit "kyllä", miten virus voisi tarttua? Mikäli vastasit ei, niin miksi ei?

2. Onko (olettamuksesi perusteella) teoriassa mahdollista, että asiaankuulumaton osapuoli pääsee tarkastelemaan e-reissuvihkolla lähetettyjä luottamuksellisia tietoja? Jos on, niin kuinka tämä olisi mahdollista?

3. Mikäli välittäisit e-reissuvihkolla epähuomiossa luottamuksellista tietoa väärään osoitteeseen (väärälle henkilölle).

a) kuinka toimisit?

b) kuinka vastaanottajan tulisi mielestäsi toimia?

c) voiko tästä aiheutunut toiminta olla mielestäsi lainvastaista? [33]

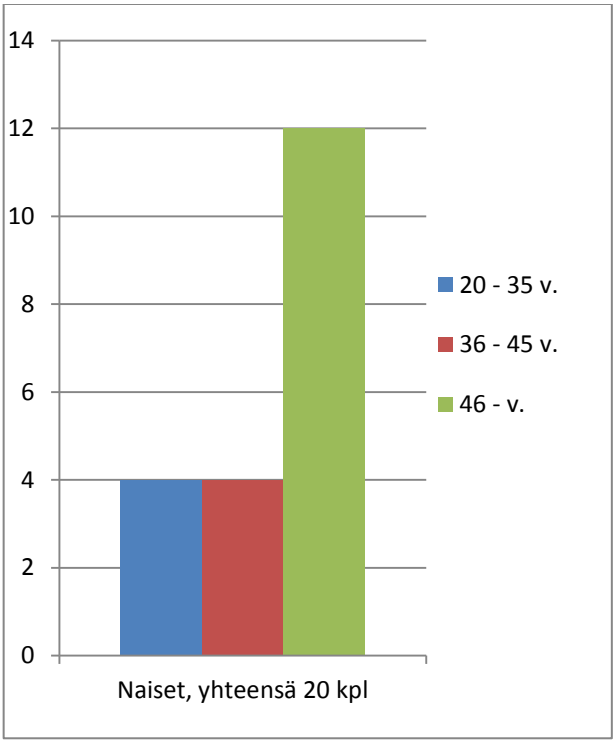
Näistä kysymyksistä en saanut tukea omiin kysymyksiini, mutta 2006 vuoden kysymyksistä tuli hyvä esimerkki muuttuneesta tietoturva- ja kyberturvallisuusympäristöstä. Kysymysten asettelusta huomaa, että lähteen kirjoitusvuotena (2006) tietoturva ja voimakkaan verkottumisen myötä tietoturvallisuus ja kyberturvallisuus ovat olleet luonnollisesti eri tasolla kuin vuonna 2017.

Tähän tutkimukseen soveltuvia valmiita vastaavia kyselypohjia ja vastauksia ei löytynyt, joten päätin laatia ja toteuttaa yhtiön henkilöstölle esitettävät kysymykset itse. Kysymyksiin valittiin vuonna 2016 tunnettuja ja mediassa esiintyneitä haittaohjelmia, kyberturvallisuudessa yleisesti tunnettuja hyökkäysmetodeja sekä CSIRT-toimintaan ja termeihin liittyviä kysymyksiä. Lisäksi kysymyksiin valittiin tietohallinnon yleisten käytäntöjen mukaisia oikeita toimintatapoja muun muassa löydettyihin USB-muistitikkuihin liittyen.

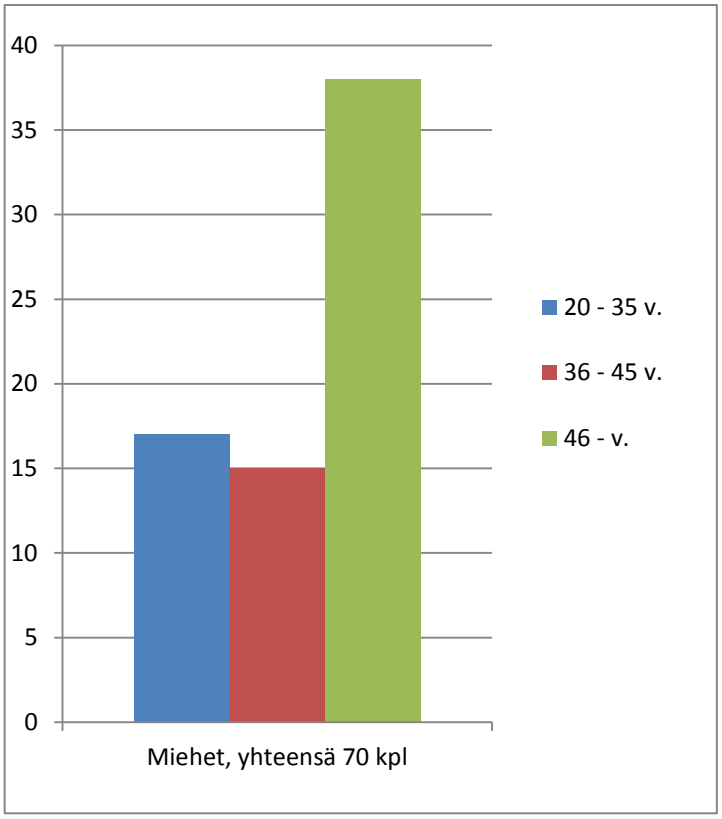
6.2 Kyselyn tulokset

Linkki selainpohjaiseen verkkokyselyyn lähetettiin sähköpostitse koko Suomen Erillisverkot konsernin henkilöstölle. Vastaanottajia oli 331 kappaletta. Vastauksia saatiin neljässä päivässä yhteensä 90 kappaletta. 20 kappaletta vastauksista tuli naisilta ja 70 kappaletta miehiltä. Pidän henkilöstön vastausprosenttia 27,2 % melko hyvänä, koska vastaamiseen oli aikaa vain neljä päivää. Vertailuarvoksi voidaan ottaa Antti Tiittasen, Terveysalan opiskelijoiden käsitykset tietoturvasta ensimmäisen opiskeluvuoden jälkeen, Kymenlaakson ammattikoreakoulussa tekemä, tammikuussa 2013 valmistunut, kvantitatiivinen tutkimus joka on tehty verkkokyselynä 164 opiskelijalle. Tutkimuksen vastausprosentti oli ollut 36 %. Kyselyyn oli vastannut hyväksytysti siis 59 opiskelijaa. [34] Suomen Erillisverkot Oy:ssä täytyy huomioida myös henkilöstön työasioiden kuormitus, jolloin kyselyyn vastaamiseen ei välttämättä jää aikaa, eikä se ole välttämättä ajan käytön priorisoinnissa korkeimmalla tasolla. Kyselyyn vastanneiden naisten ikäjakauma on nähtävissä taulukossa 1 ja kyselyyn vastanneiden miesten ikäjakauma on nähtävissä taulukossa 2. Vastaukset luokiteltiin prosentuaalisesti kysymysten vastauksien vaihtoehtojen mukaan.

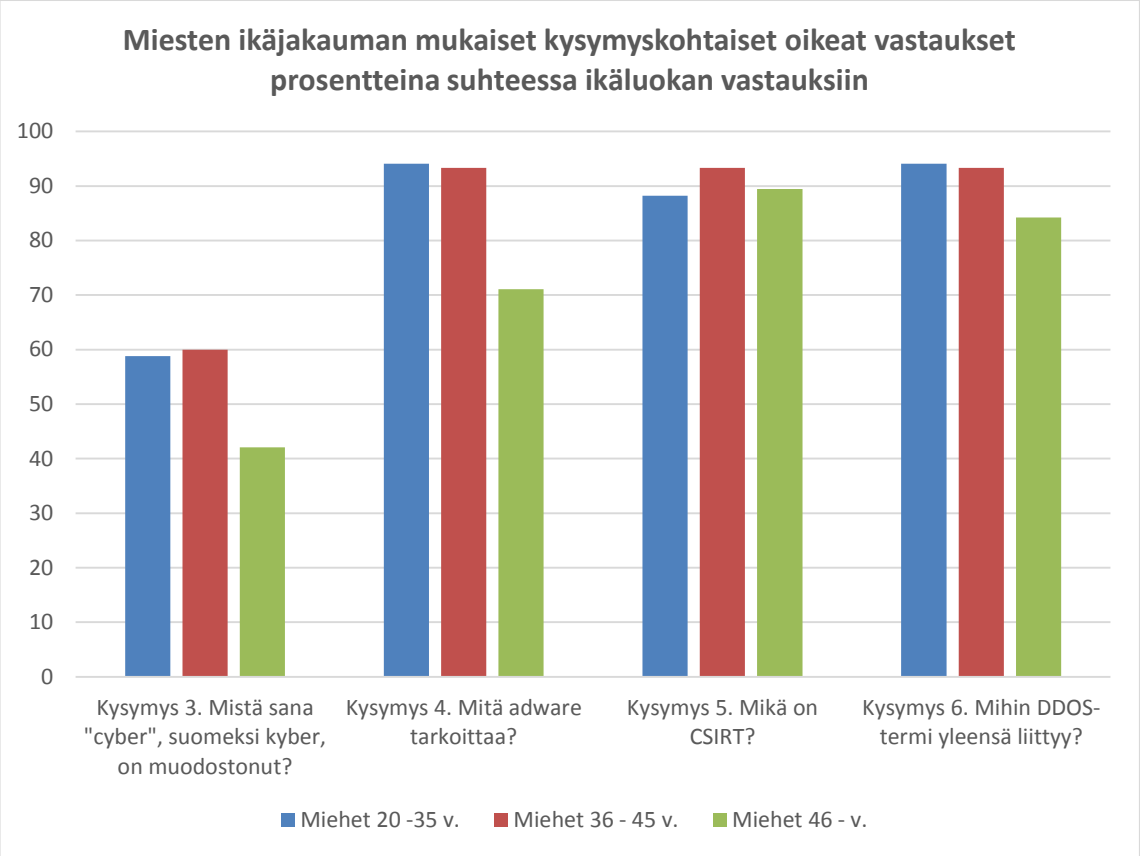
Taulukko 2. Kyselyyn vastanneiden naisten ikäjakauma:



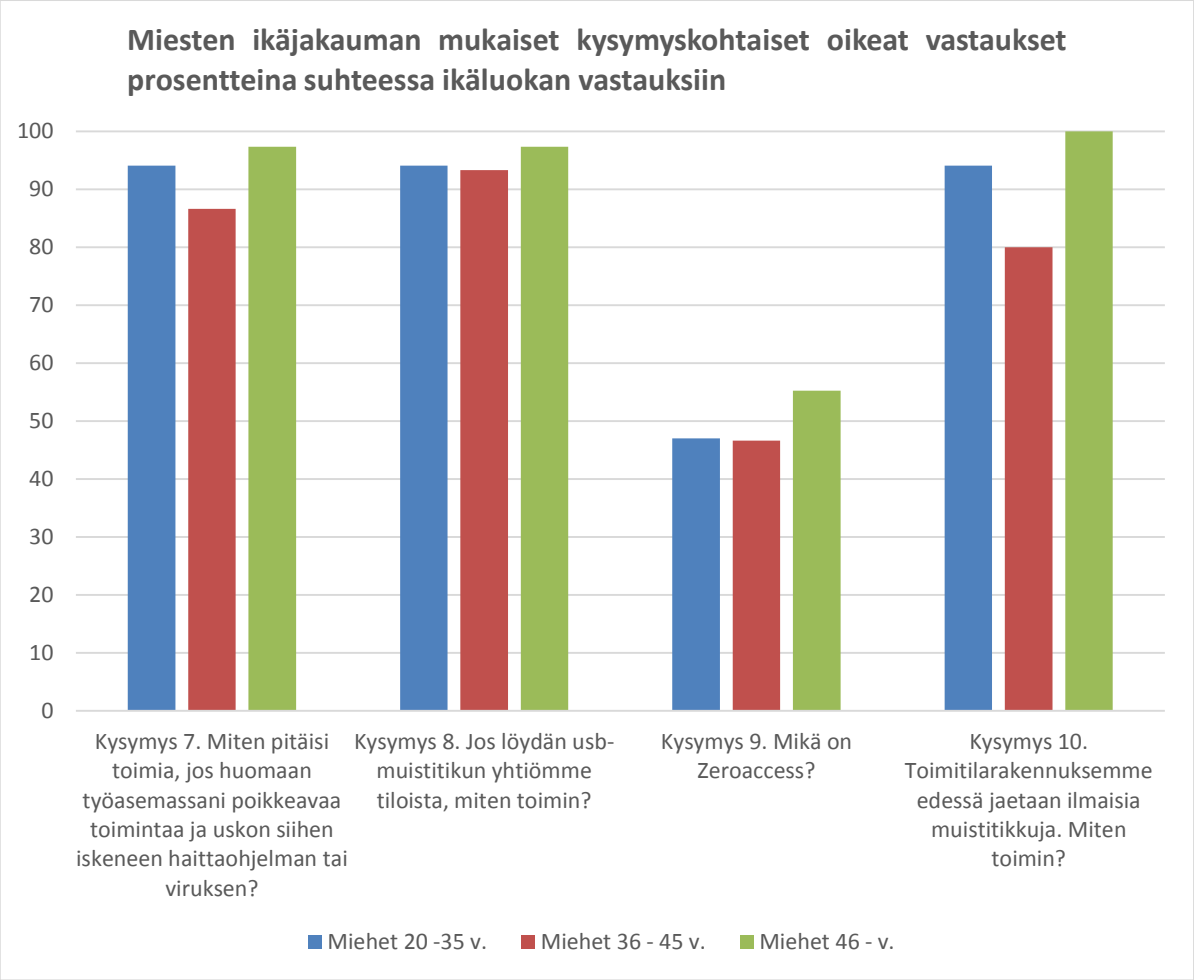
Taulukko 3. Kyselyyn vastanneiden miesten ikäjakauma:


40
35
30
25
20
15
10
5
0
20 - 35 v.
36 - 45 v.
46 - v.
Miehet, yhteensä 70 kpl

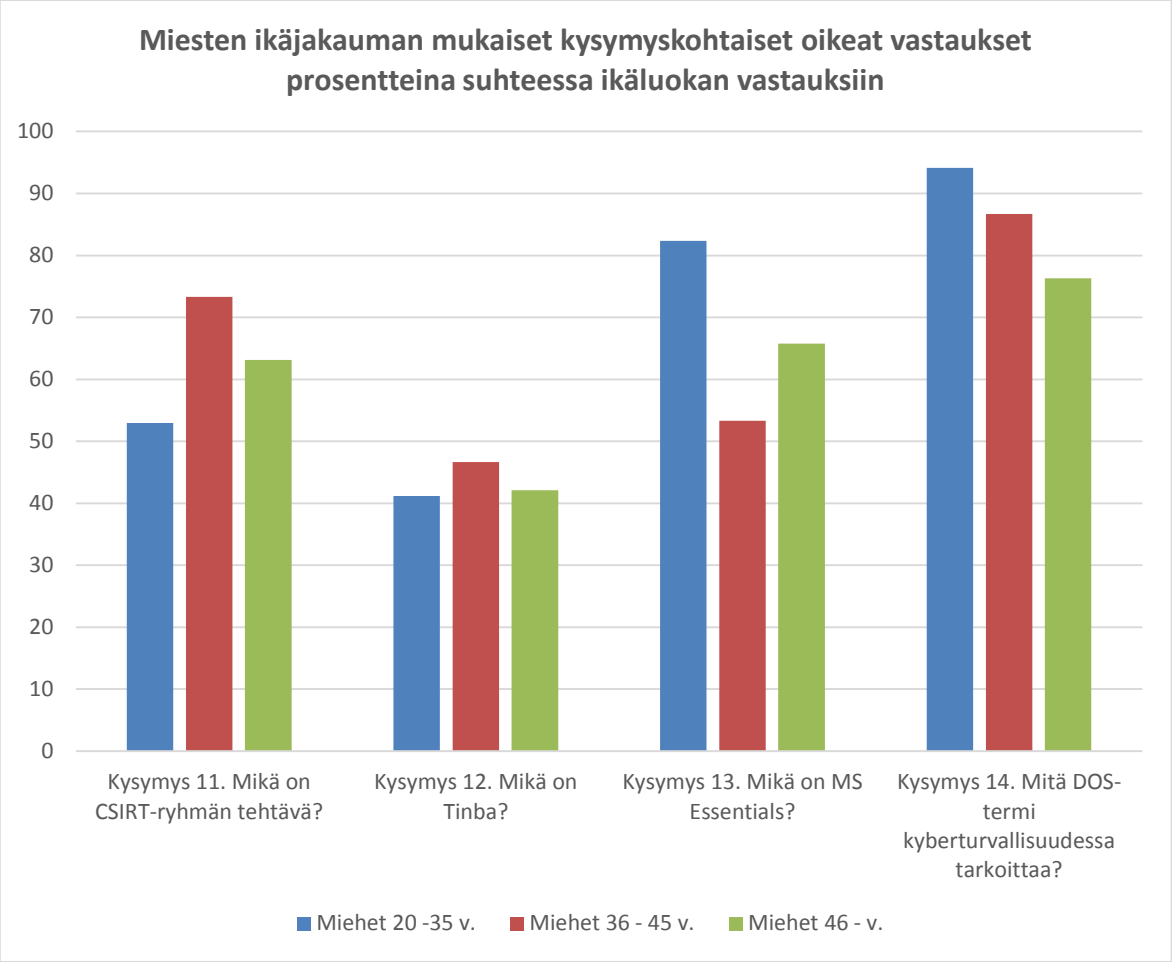
Taulukko 4. Miesten vastaukset kysymyksiin 3 – 6.



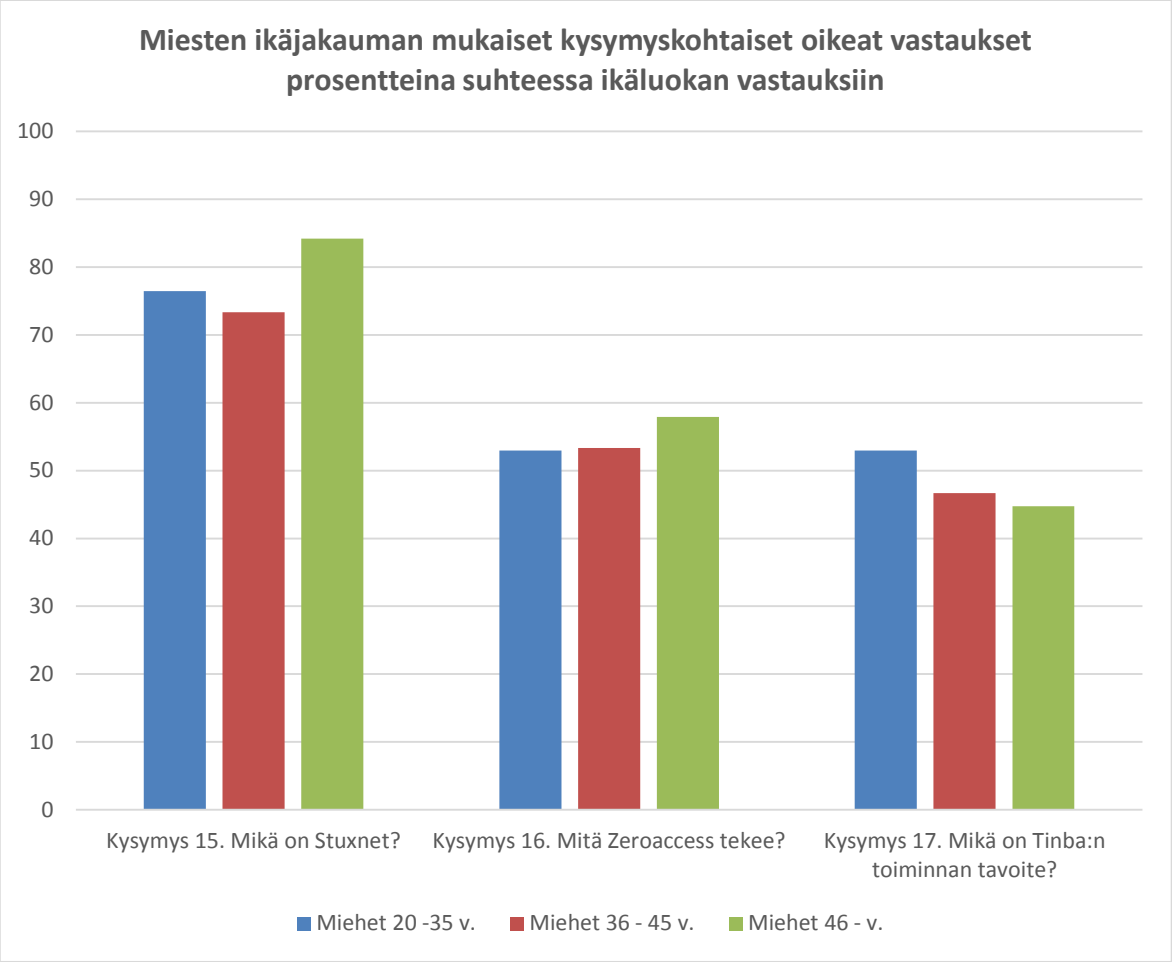
Taulukko 5. Miesten vastaukset kysymyksiin 7 – 10.



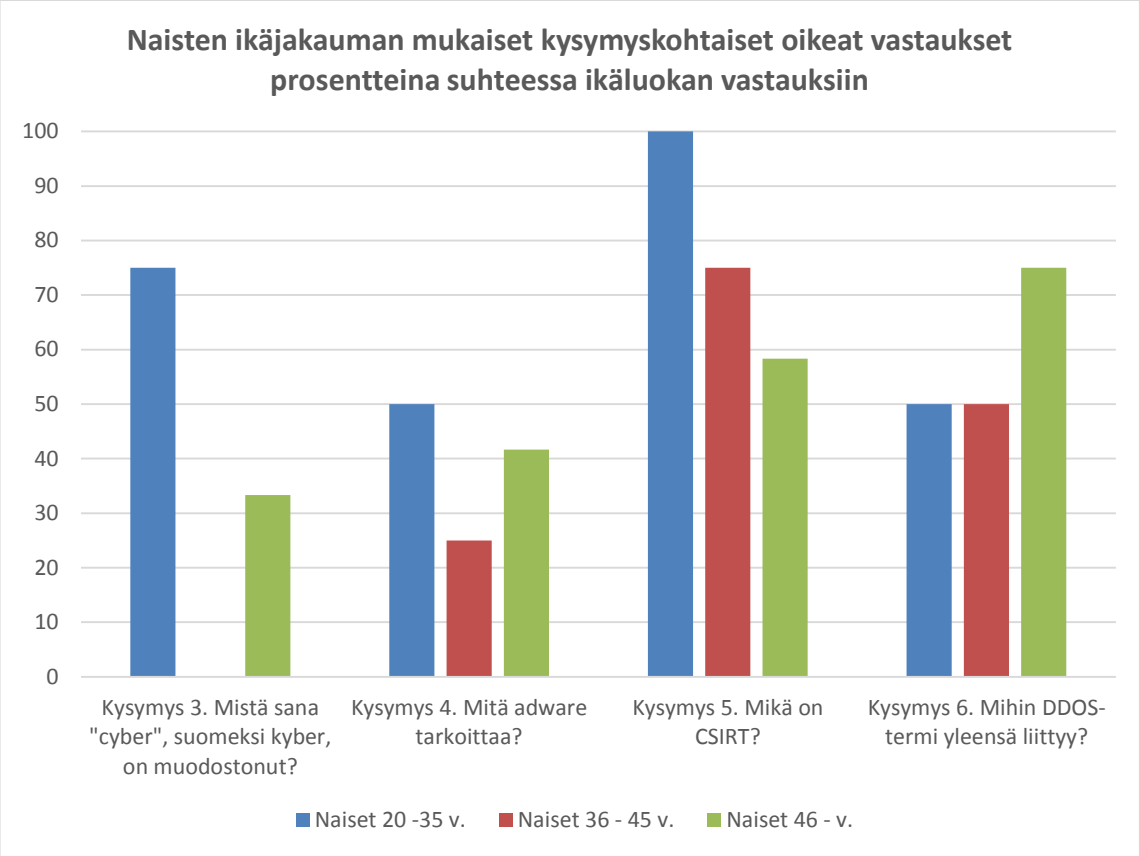
Taulukko 6. Miesten vastaukset kysymyksiin 11 – 14.



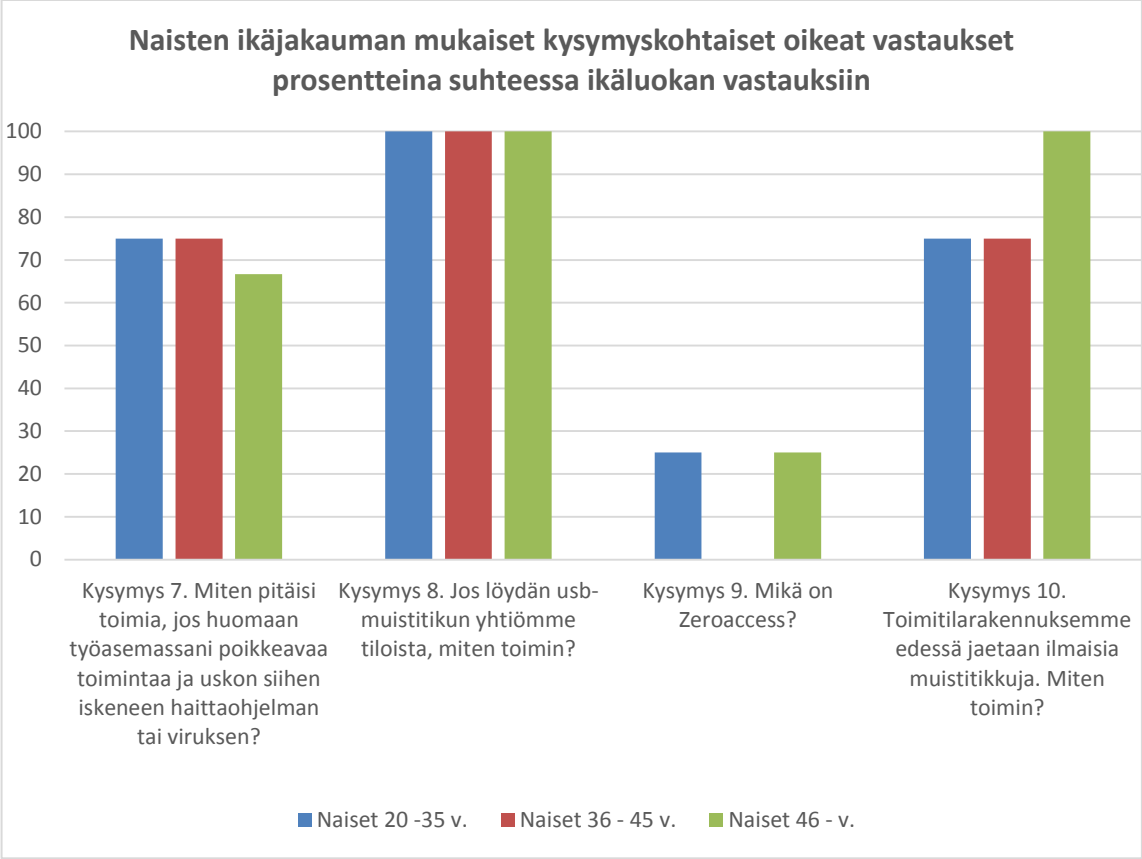
Taulukko 7. Miesten vastaukset kysymyksiin 15 – 17.



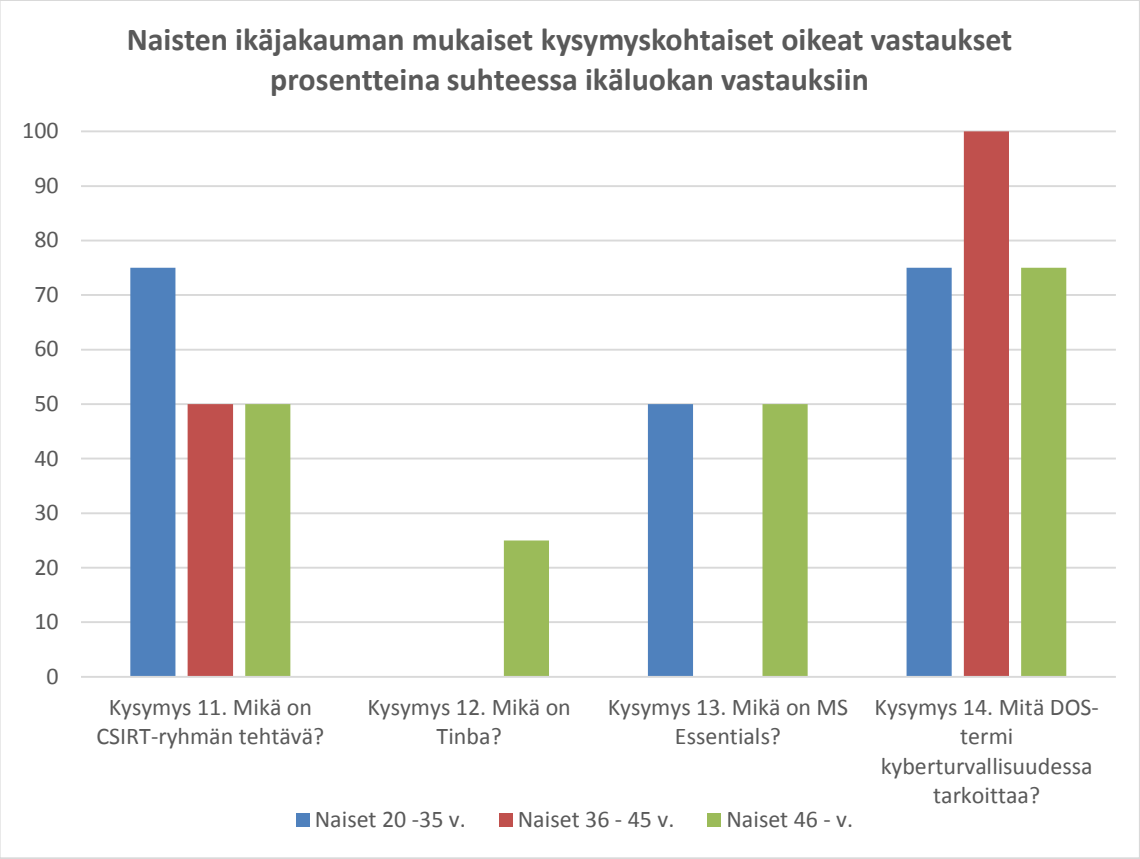
Taulukko 8. Naisten vastaukset kysymyksiin 3 – 6.



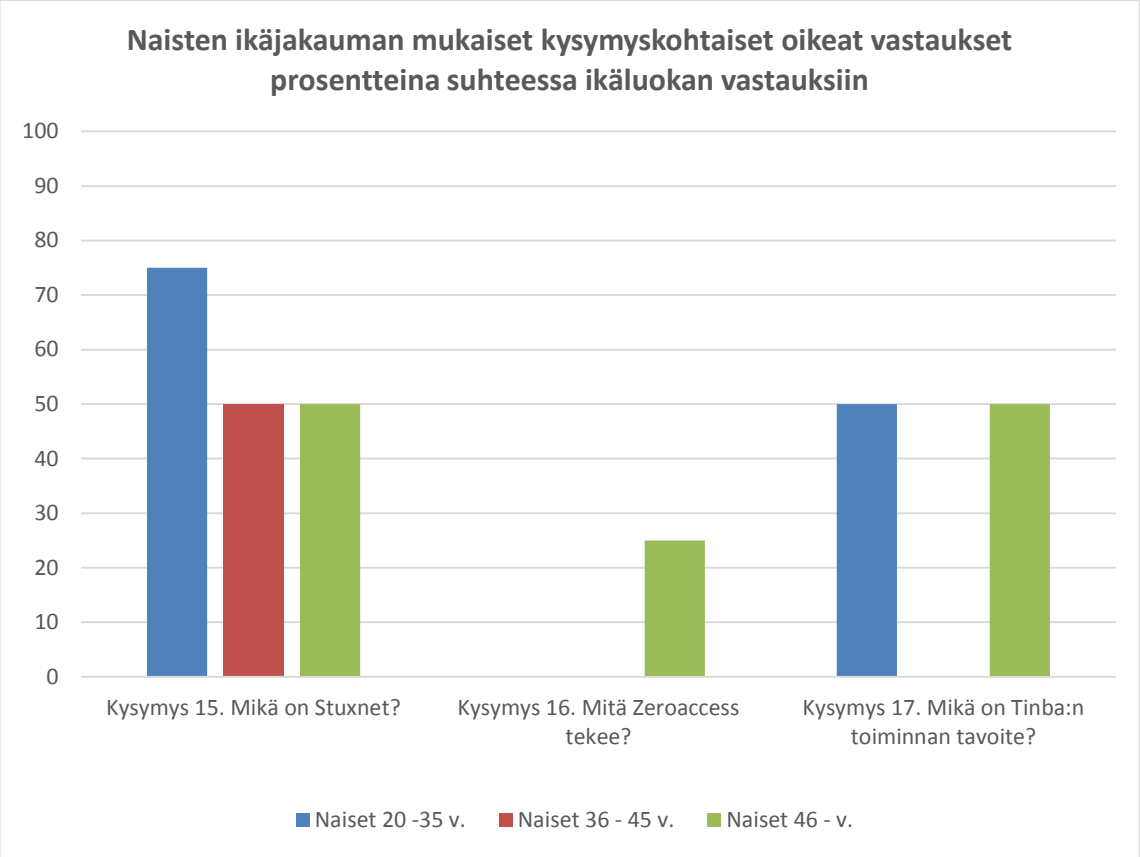
Taulukko 9. Naisten vastaukset kysymyksiin 7 – 10.



Taulukko 10. Naisten vastaukset kysymyksiin 11 – 14.



Taulukko 11. Naisten vastaukset kysymyksiin 15 – 17.



6.3 Kyselyn johtopäätökset ja vertailu vastaaviin tutkimuksiin

Yhtiön kyberturvallisuustiedotuksessa oli havaittavissa selkeä aktiivisuustason nosto, kun esitin kysymykset ja lupaa niiden kysymiseen henkilöstöltä. Esittämäni kyberturvallisuus-kyselyn jälkeen konsernin kolme eri kyberturvallisuushenkilöä innostuivat pitämään esityksiä yhtiön tiedotustilaisuuksissa. Pro Gradu tutkielman otsikon mukainen kybertoiminnallisuuden havainnointi ja valveutuneisuus Suomen Erillisverkot Oy:ssä parani siis jo pelkästään yhtiössä teettämäni kyselyn perusteella.

Kyselyn tulokset ovat jaettu miesten ja naisten sekä ikäluokkien kesken. Havainnot ja johtopäätökset tehdään tarkemmalla tasolla jaottelun mukaisesti. Ensimmäisenä havaintona on

virusten ja haittaohjelmien nimien tuntemuksen puute. Vuonna 2016 esillä olleiden haittaohjelmien ja virusten nimituntemus, mm. Zeroaccess ja Tinba, ei ole riittävällä tasolla. Konsernin kyberturvallisuusyksikön olisi syytä järjestää henkilöstölle ajankohtaistiedotteita pinnalla olevista haittaohjelmista, jolloin henkilöstön tietämys tunnettuihin ja kyseisellä hetkellä eniten vaikuttaviin haittaohjelmiin ja niiden toimintamalleihin lisääntyisi. Otsikossa 5.1 mainittu ”ihmisten muodostama palomuuri” on erinomainen näkökulma ja viittaa juuri tähän. Kyberturvallisuuteen ja yksittäisen työntekijän havainnointikyky ja valveutuneisuus on tutkimuksen edetessä vahvistunut tutkielman tekijän silmissä yhä tärkeämmäksi. Esimerkiksi yhtiön intranetin sivuilla voisi julkaista ajankohtaisia tiedotteita aiheeseen liittyen.

CSIRT-ryhmän tehtävä on n. 30 - 40 % kyselyyn vastanneille vielä epäselvä. Kuten tutkimuksessa on todettu, CSIRT-ryhmän pitää tuoda itsensä selkeästi esille organisaatiossa. Organisaation pitää tietää ja tuntea CSIRT-ryhmä ja sen ohjeet. Tulin itse liikkeenluovutuksen seurauksena Suomen Erillisverkot Oy konserniin ja CSIRT-ryhmä sekä toimintamallit tietoturvapoikkeaman havaitessa oli kyselyyni asti epäselvät. Lisäksi toimintaohjeita poikkeavuuksia havaittaessa ei ollut tullut eteeni ainuttakaan kertaa. Perehdytys on tältä osin jäänyt vajaaksi ja perehdytyksessä onkin yhtiössä parantamisen varaa, kuten varmasti monessa muussakin yhtiössä.

Henkilöstön toiminta USB-muistitikkujen kanssa on kyselyn perusteella yhtiössä hyvällä tasolla, mutta parantamisen varaakin löytyy. Ilahduttavaa oli huomata kysymys numero 8:n oikein vastanneiden määrä. USB-muistitikun löytäminen yhtiön tiloista ja toimittaminen oikeaan paikkaan on tärkeä tiedostaa. Muutama vastaaja oli kuitenkin laittamassa löytämäänsä tuntematonta USB-muistitikkua työasemaansa kiinni, joten yhtiön tietoturvapolitiikkaa USB-muistitikkujen suhteen on syytä terävöittää. Kysymyksessä nro 10 kysyttiin toimia ilmaisen USB-muistitikun suhteen. 36 – 45 vuotiaille miehille on syytä kertoa ilmaisten muistitikkujen vaaroista, koska 80 % vastasi kysymykseen oikein. Kääntäen voidaan sanoa, että joka viides vastasi väärin. Yhtiön 20 – 45 vuotiaille naisille on myös syytä terävöittää toimintaa USB-muistien kanssa, koska 75 % oli vastannut oikein, eli joka neljäs väärin. Kaiken kaikkiaan konsernin henkilöstöä on syytä tiedottaa USB-muistitikkujen käytöstä ja tuntemattomien tikkujen vaaroista.

53 prosenttia vastanneista 20 – 35 vuotiaista miehistä tiesi CSIRT-ryhmän tehtävän, kun taas 36 – 45 v. miehistä sen tiesi 73 prosenttia. 45 vuotiaat ja sitä vanhemmista miehistä CSIRT-ryhmän tehtävän tiesi 63 prosenttia. Naisista puolestaan 75 prosenttia 20 – 35 vuotiaista ja 50 prosenttia 36 ja sitä vanhemmista tiesi CSIRT-ryhmän tehtävän. Näiden tulosten perusteella voidaan todeta CSIRT-ryhmän ja sen tehtävän julkistaminen koko konsernille olisi hyvä asia. Kuten tutkielman alkupäässä on lähteidenkin perusteella todettu, kaikkien konsernissa työskentelevien pitäisi tuntea CSIRT-ryhmä ja sen toimintamallit, jo ennen kuin todellinen tarve yhteydenottoon tulee.

"Users Really Do Plug in USB Drives They Find" tutkimuksen USB-muisteista 45 % kytkettiin tietokoneeseen ja sieltä avattiin tiedosto. Suomen Erillisverkot Oy:ssä toteuttamani kyselyn kysymys numero 8., eli "Jos löydän USB-muistitikun yhtiömme tiloista, miten toimin?" on vertailukelpoinen Illinoisin yliopiston, Michiganin yliopiston ja Google, Inc:n yhteistyössä tekemässä tutkimuksen kanssa. Teettämässäni kyselyssä 93 – 9 7 % miehistä eivät kytkisi USB-muistia koneeseen, tutkiakseen sen sisältöä tai omistajaa, vaan toimittaisi sen oikea oppisesti tietohallintoon. Naisista 100 % ei kytkisi USB-muistia koneeseen katsoakseen sen sisällön tai omistajan, vaan toimittaisi sen oikeaoppisesti tietohallintoon. Näiltä osin USB-muistien suhteen toimiminen verrattuna CompTIA:a tutkimukseen on Suomen Erillisverkot Oy:ssä erinomaisella tasolla. [15]

"Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi" tutkimuksessa on todettu seuraavasti: *"Suomessa on edellytyksiä ennaltaehkäisyyn ja parempaan havainnointikykyyn uhkien torjumiseksi. Haastatteluissa ei pääosin osattu antaa arviota havainnointikyvystä koko yhteiskunnan osalta. Kattavia arvioita hallinnonalakohtaisestikin oli vaikea antaa, koska vakaviin tilanteisiin ei ole jouduttu"*.[16] Tästä voidaan todeta havainnointikyvyn olevan vaikeasti mitattavissa. Toteuttamassani kyselyssä havainnointikykyä voidaan mitata termistön tuntemuksen ja käytännön toimien perusteella. Termi "ihmisten muodostama palomuuri" on hyvä sisäistää. Martti Lehdon, Jarno Limnéllin, Eeva Innolan, Jouni Pöyhösen, Tarja Rusin ja Mirva Salmisen tekemässä tutkimuksessa todettiin yleisesti, että *"kansallinen kyberturvallisuustapahtumien havainnointikyky on puutteellinen toimivaltuuksien puutteiden vuoksi. Siksi tilannetietoisuus on heikko*

ja edellytykset estää, rajoittaa ja toipua vakavista kyberhyökkäyksistä on rajallinen. Yrityksillä on entistä vaikeampi havaita kehittyneitä kyberhyökkäyksiä (APT). Tällä hetkellä yritysvakoiluun tähtääviä APT-hyökkäyksiä toteuttavat rikollisorganisaatioiden lisäksi valtiolliset tiedusteluorganisaatiot". [16] Suomen Erillisverkot Oy:ssä havainnointi ei ole puutteellista toimivaltuuksien puutteiden vuoksi. Lisäksi havainnointikyky lähtee yksittäisestä työntekijästä, joiden kouluttamisella ja tietoisuuden lisäämisellä päästään jo selkeään kybertuvallisuuden havainnointitason nostoon. Pienen yhtiön johdon on helppo hyväksyttää ja valtuuttaa esimerkiksi CSIRT-ryhmälle täydet valtuudet, toisin kuin valtion tasoisessa isossa organisaatiossa. Näin ollen Suomen Erillisverkot Oy:ssä tilannetietoisuus yhtiön sisällä pitää olla vahva ja toipuminen kyberhyökkäyksestä nopeaa.

Erona muihin vastaaviin tutkimuksiin oli tässä tutkimuksessa käytetty ihmisten tietämystason ja tietojen mittaaminen. Aiemmissa tutkimuksissa ihmisen termistön tietämystä ei ole mitattu, vaan lähinnä käyttäytymistä esimerkiksi löydetyn USB-muistin kanssa. CSIRT-termin ja -toiminnan tuntemista ei aiemmissa tutkimuksissa ollut työntekijöiltä kysytty. CSIRT ja sen tehtävä sekä ohjeet pitäisi kuitenkin jokaisella organisaation työntekijällä olla tiedossa.

6.4 Koulutustarve

Tutkimuksen tulosten perusteella tehdyt johtopäätökset osoittavat selkeitä kyberturvallisuuteen liittyviä koulutustarpeita yhtiössä. Ajankohtaisista kyberuhkista ja haittaohjelmista on tarvetta tiedottaa paremmin, jotta tämän hetken vaarat ja haittaohjelmien toimintamallit tiedostetaan paremmin. Otsikossa 5.1 mainittu ”ihmisten muodostama palomuuri” saadaan näin ollen päivitettyä. USB-muistitikkujen käyttöpolitiikasta on myös syytä järjestää tiedotusta. Yhtiön kyberturvallisuuskyselyyn vastanneista useampi vastaaja oli yhdistämässä tuntematonta USB-muistitikkua työasemaansa. Yksikin haittaohjelman sisältävä USB-muistitikku voi tehdä isoja tuhoja yhtiössä. Koko konsernissa on siis syytä terävöittää, että työasemissa käytetään vain tietohallinnon kautta saapuneita hyväksyttyjä USB-muistitikkuja. Erityisesti konsernissa työskenteleville naisille olisi hyvä järjestää lyhyitä ja ytimekkäitä katsauksia pinnalla oleviin haittaohjelmiin, jolloin ajankohtainen tieto olisi paremmin hallussa. Tämä tuo kyberturvallisuutta ja kyberajattelua myös työntekijöiden kotiin. Otsikon 5.4.3 alla

on todettu käytännön tapojen olevan vaikea muuttaa, vaikka kyberturvallisuustieto olisikin jo sisäistetty.

Martti Lehdon, Jarno Limnéllin, Eeva Innolan, Jouni Pöyhösen, Tarja Rusin ja Mirva Salmisen ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” tutkimuksessa todetaan: *”Kyberturvallisuuden osaaminen tulisi olla kansalaistaito ja ulottua koko koulutusalaan. Turvallisuusviranomaisten koulutuksessa tarvitaan yleinen kyberturvallisuuskoulutus koko henkilöstölle ja lisäksi syväosaamiseen tähtäävää koulutusta alan erityisosaajille. Tutkimuksessa ja osaamisessa tulee kasvattaa osaajien kriittistä massaa, jotta kansallinen osaamisen ja tutkimuskyvykkyyden kansallinen omavaraisuus säilyy”*.[16] Tekemäni tutkimuksen jälkeen yhtiössämme alkoi vapaaehtoiset esitykset ja valveutuneisuuden nostot kyberturvallisuuteen ja ilmiöihin liittyen. Yhtiömme toiminta liittyy vahvasti turvallisuuteen ja kriittiseen viestintään, joten pitäisin näitä koulutuksia koko henkilöstölle pakollisena. Tähän asti kyberasiat ovat olleet vapaaehtoisia.

7 Yhteenveto

Tutkimuksen alkuperäinen tavoite oli lähteä tutkimaan yhtiömme CSIRT-toiminnallisuutta. Lähtiessäni selvittämään ja kyselemään yhtiömme CSIRT-toiminnasta, en saanut juuri tietoa asiasta. Tietoa ei haluttu antaa, edes yhtiön omille työntekijöille. Asiasta ei haluta tietoa julkisuuteen. Asian lisäselvitysten jälkeen selvisi, ettei yhtiössä jossa työskentelen, ollut omaa CSIRT-ryhmää vielä toiminnassa. Tämän myötä tutkimuksen aihe muuttui tutkielman edetessä pelkästä CSIRT-toiminnasta laajemmaksi ja henkilöstön havainnointikykyä sekä koulutusta käsitteleväksi. Ihmisten kyberturvallisuuskäyttäytymisen näkökulman tuominen mukaan tutkielmaan oli hyvä asia. Yksittäisen ihmisen rooli ja ratkaisut kyberturvallisuuteen liittyen konsernitasolla on erittäin iso tekijä kokonaisuuden kannalta, ellei jopa isoin. The Blackstone Group:in teettämässä kyselyssä todettu työntekijöiden työnantajan kyberturvallisuuteen liittyvän koulutuksen puuttuminen 45 % työntekijöistä (otsikko 5.4.2) on mielenkiintoinen tulos. Havainnointi, kulttuuri ja koulutus ovat avaintekijöitä. Mielestäni tärkein näistä on koulutus. Suomen Erillisverkot Oy:ssä alkaneet kyberturvallisuuskoulutukset ovat johtaneet korkeampaan turvallisuus- ja kyberturvallisuusriskein havainnointikulttuuriin niin työntekijöiden kotipuolessa, kuin työpaikalla.

Kyberturvallisuus on hyvin laaja käsite. Kyberturvallisuuteen liittyy vahvasti kokonaisturvallisuus, jonka yksi osa-alue kyberturvallisuus on. Kyselyssä esille tullut ilmaisten USB-muistitikkujen jakaminen ja niiden kulkeutuminen yhtiön sisälle on myös fyysistä kokonaisturvallisuutta, kun taas muistitikun sisältö bittimuodossa on enemmän pelkästään kyberturvallisuuteen liittyvää. Tutkimuksen toteuttaminen yhtiössä nosti selkeästi yhtiön sekä työntekijöiden valveutuneisuutta kybertoiminnallisuuden sekä kokonaisturvallisuuden suhteen. Kysyin suullisesti palautetta kyselystä, jolloin vastauksena usealta työntekijältä tuli herääminen turvallisuusajattelun suhteen. Yhtiössä järjestettiin kyselyn jälkeen useita koulutuksia ja esityksiä kyberturvallisuuteen liittyen. Lisäksi USB-muistitikkujen käyttöpolitiikan suhteen tuli tiedote ja niiden vaaroihin kiinnitettiin enemmän huomiota. Yhtiön kokonaisturvallisuus ja valveutuneisuus kybertoiminnallisuuden suhteen parani kyselyn myötä ja yhtiö sai arvokasta tietoa työntekijöiden vastauksista. Tutkimuksen tavoite oli kybertoiminnallisuuden havainnointikyvyn tutkiminen ja sen lisääminen yhtiössä. Otsikon 5.1 mukainen ”Ihmisten muodostama palomuuri” sai yhtiössä selkeän päivityksen teettämäni tutkielman

myötä. Termistön tuntemus ja tietämys lisääntyi yhtiön työntekijöiden joukossa merkittävästi sekä koulutusten määrä lisääntyi. Tutkimuksen konsernille asetettu tavoite saavutettiin.

Lähteet

[1] HETKY Tietoturvakerho. (1997), Suomen Atk - kustannus

[2] Legal Information Institute, Cornell Law School, 477 Myron Taylor Hall, Ithaca, NY 14853. Viitattu 21.12.2015. Saatavilla verkossa os. https://www.law.cornell.edu/uscode/text/44/3542

[3] Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmä, VAHTI 8/2008, Valtiovarainministeriö. Viitattu 17.5.2017. Saatavilla verkossa https://www.vahtiohje.fi/web/guest/maaritelmat-t

[4] Carnegie Mellon University, Carnegie Mellon Institute, Software Engineering Institute, Pittsburg, U.S.A. Viitattu 21.12.2015. Saatavilla verkossa http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm

[5] Norbert Wiener (1948), Cybernetics: Or Control and Communication in the Animal and the Machine.

[6] Johan van Niekerk & Rossouw von Solms. (2013), Computers & Security magazine, nro 38

[7] International Telecommunications Union (ITU). (2008), ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity

[8] Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013, Turvallisuuskomitean taustamuistio Taitto: Tiina Takala / Puolustusministeriö. Paino: Forssa print, 2013 ISBN: 978-951-25-2433-4 nid. ISBN: 978-951-25-2434-1 pdf

[9] Libicki, Martin C. (2009) Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND

[10] Caxton Business & Legal, Inc. (2015), Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, ISBN: 978-0-9964982-0-3

[11] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle. (2003), Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd Edition. Carnegie Mellon Institute, Software Engineering Institute, Pittsburgh, U.S.A

[12] Simon Martinez, CSIRT, 2871 Hop Scotch Ct, Waldorf, MD 20603, viitattu , 23.3.2016 Saatavilla verkossa os. https://www.csirt.org/

[13] Nevil Brownlee & Erik Guttman (1998) Best Current Practice, RFC 2350 Expectations for Computer Security Incident Response. The University of Auckland. Viitattu 26.5.2016 Saatavilla verkossa os. https://tools.ietf.org/html/rfc2350

[14] Carnegie Mellon University, The Software Engineering Institute, Pittsburgh, U.S.A Viitattu 26.5.2016 Saatavilla verkossa os. http://www.sci.cmu.edu/about/organization/index.cfm

[15] Matthew Tischer, Zakir Durumericz, Sam Foster, Sunny Duany, Alec Mori, Elie Bursztein ja Michael Bailey (2017) Users Really Do Plug in USB Drives They Find. University of Illinois, Urbana Champaign, University of Michigan, Google, Inc. Saatavilla verkossa os. https://zakird.com/papers/usb.pdf

[16] Martti Lehto, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi ja Mirva Salminen (2017), Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 30/2017, ISSN 2342-6799 (pdf), ISBN 978-952-287-368-2 (pdf) 18.5.2017

[17] CompTIA UK, 15th floor, City Point, 1 Ropemaker Street, London. Viitattu 21.8.2017 Saatavilla verkossa os. https://www.comptia.org/about-us,

[18] IDT911, “Data Breach Reports,” Identity Theft Resource Center. Viitattu 21.8.2017. Saatavilla verkossa os. http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

[19] CompTIA,“Trends in IT Security” (2015). Viitattu 21.8.2017. Saatavilla verkossa os. https://www.comptia.org/resources/trends-in-information-security-study

[22] Federal Bureau of Investigation (2015), “2014 Internet Crime Report”. Viitattu 21.8.2017. Saatavilla verkossa os. https://www.fbi.gov/news/news_blog/2014-ic3-annual-report

[21] Cyber Secure: A Look at Employee Cybersecurity Habits in the Workplace (2015). Viitattu 22.8.2017. Saatavilla verkossa os. https://www.comptia.org/resources/cyber-secure-a-look-at-employee-cybersecurity-habits-in-the-workplace

[22] Meinert, Monica C. (2016). SOCIAL ENGINEERING: The Art of Human Hacking, American Bankers Association. ABA Banking Journal; 108.3: 49, New York

[23] Shay, Richard & Ion, Iulia & W. Reeder, Robert & Consolvo, Sunny (2014). "My religious aunt asked why i was trying to sell her viagra": Experiences with account hijacking. Teoksessa: CHI '14 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, s 2657 - 2666, Toronto, Ontario, Canada

[24] Honan, M. (2012). “How Apple and Amazon Security Flaws Led to my Epic Hacking,”. Wired. Viitattu 20.9.2017 Saatavilla verkossa os. https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

[25] Honan, M. (2012), “Mat Honan: How I Resurrected My Digital Life After an Epic Hacking”. Wired. Viitattu 20.9.2017 Saatavilla verkossa os. https://www.wired.com/2012/08/mat-honan-data-recovery/

[26] Bridis, T. (2008), “Hacker impersonated Palin, stole e-mail password” Associated Press. Viitattu 20.9.2017. Saatavilla verkossa os. http://6abc.com/archive/6398817/

[27] Schonfeld, E. (2009), “Twitter's @Ev Confirms Hacker Targeted Personal Accounts; Attack Was 'Highly Distressing”. Viitattu 20.9.2017. Saatavilla verkossa os. https://techcrunch.com/2009/07/14/twitters-ev-confirms-hacker-targeted-personal-accounts-attack-was-highly-distressing/

[28] Bright, P. (2011), “Anonymous speaks: the inside story of the HBGary hack”. Viitattu 20.9.2017. Saatavilla verkossa os. https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

[29] Perlroth, N. & Shear, M.D. (2013). “In Hacking, A.P. Twitter Feed Sends False Report of Explosions” The New York Times: The Caucus (Apr 23, 2013)

[30] O'Mahony, J. (2013). “Financial Times hacked by Syrian Electronic Army”. Viitattu 20.9.2017. Saatavilla verkossa os. http://www.telegraph.co.uk/technology/twitter/10064184/Financial-Times-hacked-by-Syrian-Electronic-Army.html

[31] The Associated Press (20138. “Twitter feeds of UK's Guardian newspaper hacked”. Viitattu 21.9.2017. Saatavilla verkossa os. https://phys.org/news/2013-04-uk-guardian-newspaper-twitter-hacked.html

[32] Onion Inc.'s Tech Team (2013). “How the Syrian Electronic Army Hacked The Onion”. Viitattu 20.9.2017. Saatavilla verkossa os. http://theonion.github.io/blog/2013/05/08/how-the-syrian-electronic-army-hacked-the-onion/

[33] Risto Kauko ja Mikko Salkinoja (2006) ”Sähköinen yhteys” – laadullinen tutkimus Sähköisen reissuvihkon soveltuvuudesta kodin ja koulun väliseen yhteydenpitoon. Tampereen yliopisto.

[34] Antti Tiittanen (2013), Terveysalan opiskelijoiden käsitykset tietoturvasta ensimmäisen opiskeluvuoden jälkeen. Kymenlaakson ammattikorkeakoulu

Liitteet

A Kybertoiminnallisuuden havainnointi Suomen Erillisverkot Oy:ssä, kysely

B Kybertoiminnallisuuden havainnointi Suomen Erillisverkot Oy:ssä, kyselyn oikeat vastaukset

LIITE A

Kybertoiminnallisuuden havainnointi Suomen Erillisverkot Oy:ssä, kysely

1. Sukupuoli:

a) mies

b) nainen

2. Ikä:

a) 0 - 20 v.

b) 20 - 35 v.

c) 36 - 45 v.

d) 46 - 75 v.

3. Mistä sana "cyber", suomeksi kyber, on muodostonut?

a) avaruuden laajuutta kuvaavasta termistä

b) sanasta cybernetics, joka pohjautuu kreikkalaiseen sanaan kubernētēs (ohjata)

c) sanoista computer virus attackers

4. Mitä adware tarkoittaa?

a) adware on ohjelma, joka näyttää mainoksia tietokoneellasi

b) adware on lisähohjelmisto windowsiin

c) adware on Microsoft Officen lisäosa

5. Mikä on CSIRT?

a) Computer Service IRQ Team, eli IT-palvelu ryhmä

b) Computer Social Investigating Request Team, eli sosiaalisen median seurantaryhmä

c) Computer Security Incident Response Team, eli tietoturvapoikkeamaryhmä, jolle ilmoitetaan kaikki tietoturvarikkeet ja -poikkeamat

6. Mihin DDOS -termi yleensä liittyy?

a) Disk Operating System, eli IBM-yhteensopivien tietokoneiden käyttöjärjestelmäperhe

b) Distributed Denial of Service, useista lähteistä tapahtuva palvelunestohyökkäys

c) Dynamic Destroyer of System, virus

7. Miten pitäisi toimia, jos huomaan työasemassani poikkeavaa toimintaa ja uskon siihen iskeneen haittaohjelman tai viruksen?

a) Sammuttaa tietokone ja tehdä ilmoitus asiasta

b) Jättää tietokone päälle, mutta irrottaa verkkopiuha ja tehdä ilmoitus asiasta

c) Ottaa heti kaikki johdot irti tietokoneesta ja tehdä ilmoitus asiasta

8. Jos löydän usb-muistitikun yhtiömme tiloista, miten toimin?

a) Laitan muistitikun koneeseen ja tutkin sen tiedostot, jotta löydän sen omistajan

b) Laitan tikun tietokoneeseeni ja tarkistan sen heti F-Securen virustorjuntaohjelmistolla

c) Toimitan löytämäni usb-tikun suoraan tietohallintoon

9. Mikä on Zeroaccess?

a) Yleisin Windows - haittaohjelma Suomessa toukokuussa 2016

b) Android - käyttöjärjestelmä

c) Palomuuriohjelmisto

10. Toimitilarakennuksemme edessä jaetaan ilmaisia muistitikkuja. Miten toimin?

a) Otan luonnollisesti ilmaisen muistitikun käyttööni ja teen heti työasemani varmuuskopiot tikulle

b) Kieltäydyn kohteliaasti ilmaisesta muistitikusta ja kehotan myös työkavereitani kieltäytymään

c) Mainostan yhtiössämme mahdollisuutta säästää rahaa ja kehotan myös muita hakemaan tikkuja kiireesti käyttöön.

11. Mikä on CSIRT-ryhmän tehtävä

a) Suojella tietokonetta uhkilta

b) Ryhmän tehtävä on suorittaa tietoturvapoikkeamiin reagointia päätyönään

c) Central Security Impact Request Team, eli keskusturvallisuuden suojaus

12. Mikä on Tinba?

a) 3DVR valmistaja (3D Virtual Reality)

b) Suomen yleisimpiä haittaohjelmia keväällä 2016

c) Hakkeriryhmä

13. Mikä on MS Essentials?

a) Microsoftin tarjoama ilmainen haittaohjelmien torjuntasovellus Windows-koneisiin

b) Microsoft Officen maksullinen lisäpaketti

c) Lotus Notesin kirjoitusohjelma

14. Mitä DOS-termi kyberturvallisuudessa tarkoittaa?

a) Vanhaan Microsoftin luomaan käyttöjärjestelmään

b) Denial of Service, eli palvelunestohyökkäys

c) Die OS, käyttöjärjestelmän tuhoamisvirus

15. Mikä on Stuxnet?

a) Internetissä toimiva eristetty verkko

b) Virustorjuntaohjelmisto

c) Haittaohjelma, jolla viivästytettiin Iranin ydinaseen kehittelyä

16. Mitä Zeroaccess tekee?

a) Asentaa itsensä piiloon, lataa lisää haittaohjelmia koneeseen ja avaa takaportin saastuneeseen koneeseen

b) Formatoi tietokoneen kovalevyn

c) Yrittää ylikuumentaa prosessorin ja virtalähteen

17. Mikä on Tinba:n toiminnan tavoite?

a) Tehdä tietokoneesi toimintakyvyttömäksi

b) Tyhjentää tietokoneesi kovalevy

c) Päästä käsiksi pankkitunnuksiisi ja salasanoihisi

LIITE B

Kybertoiminnallisuuden havainnointi Suomen Erillisverkot Oy:ssä, kyselyn oikeat vastaukset

3. Mistä sana "cyber", suomeksi kyber, on muodostonut?

b) sanasta cybernetics, joka pohjautuu kreikkalaiseen sanaan kubernētēs (ohjata)

4. Mitä adware tarkoittaa?

a) adware on ohjelma, joka näyttää mainoksia tietokoneellasi

5. Mikä on CSIRT?

c) Computer Security Incident Response Team, eli tietoturvapoikkeamaryhmä, jolle ilmoitetaan kaikki tietoturvarikkeet ja -poikkeamat

6. Mihin DDOS -termi yleensä liittyy?

b) Distributed Denial of Service, useista lähteistä tapahtuva palvelunestohyökkäys

7. Miten pitäisi toimia, jos huomaan työasemassani poikkeavaa toimintaa ja uskon siihen iskeneen haittaohjelman tai viruksen?

b) Jättää tietokone päälle, mutta irrottaa verkkopiuha ja tehdä ilmoitus asiasta

8. Jos löydän usb-muistitikun yhtiömme tiloista, miten toimin?

b) Laitan tikun tietokoneeseeni ja tarkistan sen heti F-Securen virustorjuntaohjelmistolla

9. Mikä on Zeroaccess?

a) Yleisin Windows - haittaohjelma Suomessa toukokuussa 2016

10. Toimitilarakennuksemme edessä jaetaan ilmaisia muistitikkuja. Miten toimin?

b) Kieltäydyn kohteliaasti ilmaisesta muistitikusta ja kehotan myös työkavereitani kieltäytymään

11. Mikä on CSIRT-ryhmän tehtävä

b) Ryhmän tehtävä on suorittaa tietoturvapoikkeamiin reagointia päätyönään

12. Mikä on Tinba?

b) Suomen yleisimpiä haittaohjelmia keväällä 2016

13. Mikä on MS Essentials?

a) Microsoftin tarjoama ilmainen haittaohjelmien torjuntasovellus Windows-koneisiin

14. Mitä DOS-termi kyberturvallisuudessa tarkoittaa?

b) Denial of Service, eli palvelunestohyökkäys

15. Mikä on Stuxnet?

c) Haittaohjelma, jolla viivästytettiin Iranin ydinaseen kehittelyä

16. Mitä Zeroaccess tekee?

a) Asentaa itsensä piiloon, lataa lisää haittaohjelmia koneeseen ja avaa takaportin saastuneeseen koneeseen

17. Mikä on Tinba:n toiminnan tavoite?

c) Päästä käsiksi pankkitunnuksiisi ja salasanoihisi