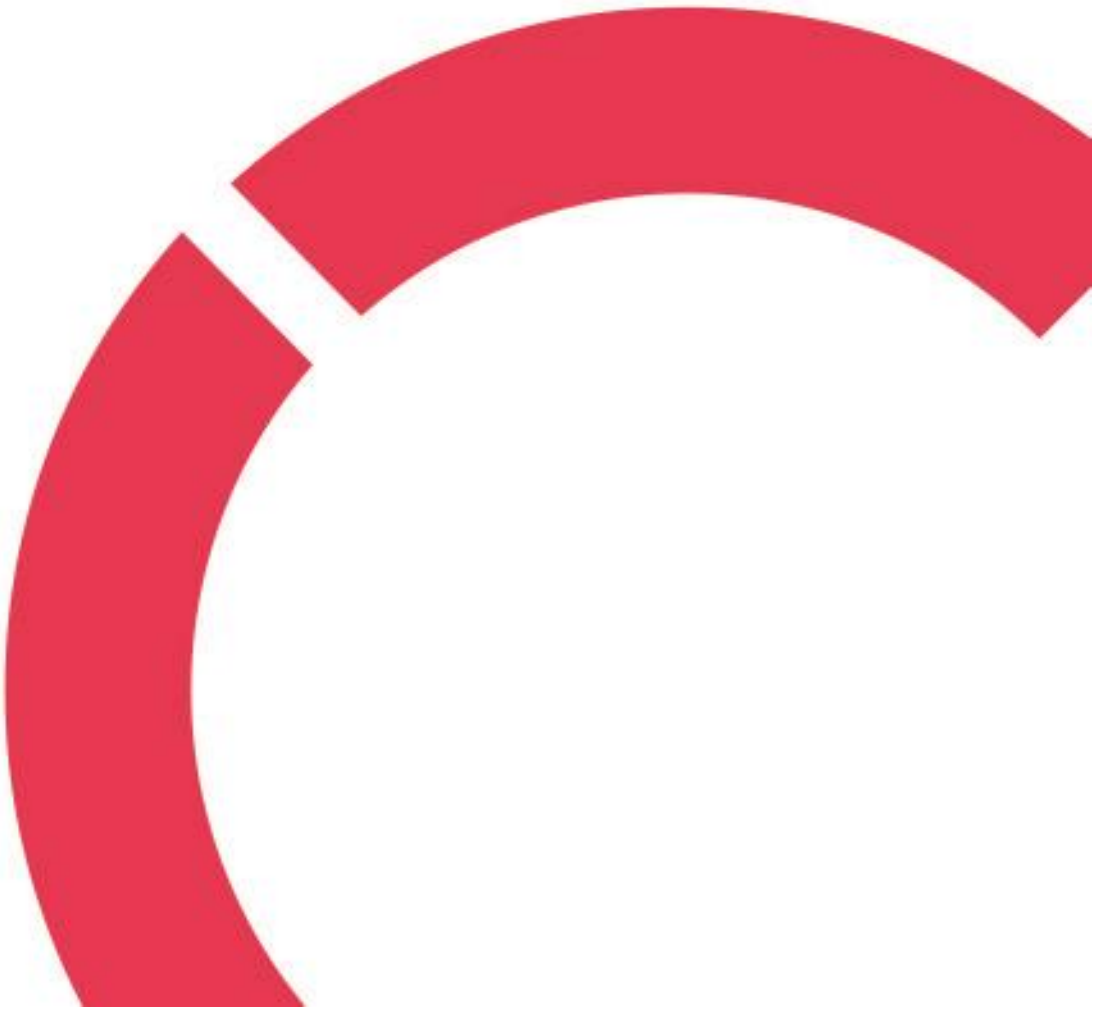
Barakas Stefanos, Kärppä Anttoni

KYBERTURVALLISUUS YRITYKSISSÄ

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Liiketalouden koulutus
Marraskuu 2022



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Marraskuu 2022	**Tekijä/tekijät** Stefanos Barakas, Anttoni Kärppä
Koulutus Tradenomi		☒ AMK ☐ YAMK
Työn nimi KYBERTURVALLISUUS YRITYKSISSÄ		
Työn ohjaaja Nina Östman-Tylli		**Sivumäärä** 27 + 1

Opinnäytetyössä perehdytään siihen, mitä kyberturvallisuus on miltä sen tulevaisuus näyttää ja miksi se on tärkeää. Opinnäytetyössä kerrotaan yleisimmät kyberriskit sekä keinot suojautua niitä vastaan. Työssä keskitytään erityisesti yritysten kyberturvallisuuteen. Tavoitteena on tehdä erityisesti yrityksien silmiä avaava tietopaketti kyberturvallisuudesta.

Aiheen luonteen vuoksi työssä on käytetty pelkästään internet lähteitä. Työ on kirjoitettu kokonaan tutkivalla menetelmällä pois lukien yrityksille tehty kyselytutkimus. Kyselytutkimus suoritettiin sähköpostin ja Google Formsin avulla.

Kyberuhkien tulevaisuutta on hyvin vaikea ennustaa koko ajan kehittyvän teknologian ja tekoälyn vuoksi. Jatkuvasti kehittyvät uhat vaativat jatkuvasti kehittyviä suojautumiskeinoja. Toimivin keino organisaatioiden kannalta voisi olla tekoälyn avulla toimiva automatisoitu kyberpuolustus, joka ei vaatisi organisaatioilta juurikaan resursseja toimiakseen.

Asiasanat
kyberhyökkäys, kyberturvallisuus, tietotekniikka

ABSTRACT

Centria University of Applied Sciences	**Date** November 2022	**Author** Stefanos Barakas, Anttoni Kärppä
Degree programme Bachelor of Business Administration		
Name of thesis CYBER SECURITY IN COMPANIES		
Centria supervisor Nina Östman-Tylli		**Pages** 27 + 1

The thesis explores what cybersecurity is, what its future looks like and why it is important. The thesis describes the most common cyber risks and how to protect against them. The thesis focuses in particular on cybersecurity in businesses. The aim is to make an eye-opening information package on cybersecurity especially for businesses.

Due to the nature of the topic, the work has been based solely on internet sources. The work has been written entirely using the investigative method, excluding the questionnaire survey of businesses. The survey was conducted using email and Google Forms.

The future of cyber threats is very difficult to predict due to the ever-evolving technology and artificial intelligence. Constantly evolving threats require constantly evolving defenses. The most effective way for organizations could be an AI-powered automated cyber defense that would require little or no resources for organizations to operate.

Key words
cyber-attack, cyber security, information technology

KÄSITTEIDEN MÄÄRITTELY

RANSOMWARE

Eräänlainen haittaohjelma, joka estää laillisten käyttäjien pääsyn omaan järjestelmään vaatien maksun tai lunnaita antaakseen pääsyn takaisin.

MALWARE AS A SERVICE

Hakkereita, joita palkataan suorittamaan lunnasohjelmahyökkäyksiä kolmannen osapuolen toimesta.

DOS/DDOS

Kohdennettu palvelunestohyökkäys.

MAN IN THE MIDDLE

Man in the middle (MITM) -hyökkäys on kyberhyökkäys, jossa pahantahtoinen toimija salakuuntelee verkon käyttäjän ja verkkosovelluksen välistä keskustelua.

CROSS SITE SRCIPTING

Cross Site Scripting (XSS) on koodin lisäyshyökkäys, jossa hakkeri lisää haitallista koodia lailliseen verkkosivustoon.

DNS-TUNNELOINTI

DNS-tunnelointi on kyberhyökkäys, joka hyödyntää DNS-kyselyitä ja -vastauksia ohittaakseen perinteiset turvatoimenpiteet ja siirtääkseen dataa ja koodia verkossa.

DRIVE BY HYÖKKÄYS

Drive by hyökkäys on kehittynyt muoto haittaohjelmahyökkäyksestä, joka hyödyntää useiden verkkoselaimien, lisäosien tai sovellusten heikkoja kohtia hyökkäyksen käynnistämiseksi.

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

KUVIOT

KUVAT

TAULUKOT

1 JOHDANTO

Opinnäytetyön ensimmäinen tavoite on selvittää lukijalle mitä kyberturvallisuus oikein on. Käsite on varmasti kaikille tuttu terminä, mutta sen avaaminen lukijalle heti työn alussa oli mielestämme tärkeää. Siksipä työn ensimmäinen kappale keskittyy pelkästään siihen. Niin tässä, kuin muissakin työn kysymyksissä, käytimme oikeastaan vain internetlähteitä, sillä aiheen luonne vaatii ajantasaisen tiedon käyttämistä ollakseen relevanttia. Uusien, ajan tasalla olevien kirjojen löytäminen mahdotonta. Työn kirjoittaminen oli pääsääntöisesti hyvin tutkivaa.

Seuraavaksi keskityimme siihen, minkä vuoksi termi kyberturvallisuus on oikeastaan edes olemassa, eli kyberhyökkäyksiin ja haittaohjelmiin. Mitä kyberhyökkäykset ja haittaohjelmat ovat? Minkälaisissa muodoissa niitä esiintyy? Päätimme käydä läpi yleisimmät kyberhyökkäysten ja haittaohjelmien muodot hieman tarkemmin, jotta voisimme antaa lukijalle jonkinlaisen käytännön käsityksen siitä, mitä nämä arkimaailmassa tarkoittavat ja samalla ehkä antaa ymmärrystä siitä, miksi kyberturvallisuus on nykyään oikeasti tärkeää.

Ennen kuin siirrymme keskittymään kyberturvallisuuteen yritysmaailmassa, ajattelimme, että kyberhyökkäyksistä ja haittaohjelmista on luontevinta siirtyä seuraavaksi siihen, miten niitä vastaan voi yksinkertaisimmillaan puolustautua. Käymme läpi kaikille tuttuja asioita, mutta pureudumme niihin vähän syvemmin.

Kun kyberturvallisuus ja sen eri aihepiirit alkoivat olla pääpiirteittäin tuttuja, aloimme keskittyä siihen, mikä niiden rooli on yritysmaailmassa. Selvitimme yleisimmät kyberriskit yrityksille. Käymme läpi eri keinoja, joilla yritykset voivat ennaltaehkäistä tai ainakin minimoida riskin joutua kyberhyökkäyksen kohteeksi. Pohdimme myös, olisiko kybervakuutus varteenotettava vaihtoehto yrityksille.

Viimeisenä päätimme tehdä yrityksille kyselytutkimuksen, jossa käymme läpi erityisesti viime kappaleessa mainittuja asioita. Tutkimuksen tekeminen osoittautui melko hankalaksi, sillä yritykset eivät olleet kovin kiinnostuneita vastaamaan sähköpostin kautta lähetettyyn kyselyyn. Parin sadan sähköpostin lähetettyämme vastausprosentiksi osoittautui noin 6. Kyselyn toteuttamiseen käytimme Google Formsia.

2 MITÄ KYBERTURVALLISUUS ON?

Kyberturvallisuus on laajalti käytetty käsite, jolla on hyvin vaihtelevia määritelmiä. Lyhyen ja selkeästi ymmärrettävän kyberturvallisuuden moniulotteisuutta kuvaavan määritelmän puuttuminen haittaa teknologista ja tieteellistä kehitystä, joiden tulisi toimia yhdessä ratkaistakseen monimutkaisia kyberturvallisuushaasteita. Lyhyen, kattavan, merkityksellisen ja yhdistävän määritelmän muotoileminen mahdollistaa tehostetun keskittymisen eri tieteidenvälisiin kyberturvallisuus tutkimuksiin ja vaikuttaa siten akateemisen, teollisen sekä valtion ja kansalaisjärjestöjen lähestymistapoihin kyberturvallisuuden haasteisiin. (Craigen, Diakun-Thibault ja Purse 2014).

Kyberturvallisuus-termin purkaminen auttaa kohdistamaan pohdinnan sekä "kyber”- että "turvallisuus" -alueille ja paljastaa joitain perinnöllisiä ongelmia. "Kyber" on etuliite, joka viittaa kyberavaruuteen ja viittaa sähköisiin viestintäverkkoihin ja virtuaalitodellisuuteen. Termi "kyberavaruus" tuli suosituksi William Gibsonin vuoden 1984 romaanissa Neuromancer, jossa hän kuvaa näkemystään puhtaan tiedon kolmiulotteisesta tilasta, joka liikkuu tietokoneryhmien välillä, jossa ihmiset ovat tiedon tuottajia ja käyttäjiä. Se, minkä nykyään tunnemme kyberavaruutena, on tarkoitettu ja suunniteltu tietoympäristöksi ja kyberavaruuden arvostus on nykyään laajentunut. Se on maailmanlaajuinen yhteiskunta, jossa ihmiset ovat yhteydessä toisiinsa ideoiden, palveluiden ja ystävyyden vuoksi.

Mitä tulee termiin "turvallisuus", tarkastelemassamme kirjallisuudessa ei näyttänyt olevan laajalti hyväksyttyä käsitettä, ja termiä on ollut tunnetusti vaikea määritellä yleisessä merkityksessä. Keskeinen turvallisuuden periaate on olla vapaa vaarasta tai uhista. Lisäksi, vaikka olemme osoittaneet, että turvallisuus on kiistanalainen aihe.

Eli tiivistettynä, kyberturvallisuus on datan, omaisuuden, palveluiden ja arvojärjestelmien suojaamista, jolla voidaan vähentää niiden katoamisen, vahingoittumisen, vaarantumisen tai väärinkäytön todennäköisyyttä sellaiselle tasolle, joka on oikeassa suhteessa määritettyyn arvoon.

3 KYBERHYÖKKÄYKSET

Miksi kyberhyökkäykset ovat niin yleisiä? Tämä johtuu siitä, että kyberhyökkäykset ovat halvempia, helpompia ja vähemmän riskialttiita kuin fyysiset hyökkäykset. Verkkorikolliset tarvitsevat vain muutamia asioita tietokoneen ja Internet-yhteyden lisäksi. Heitä ei rajoita maantiede tai etäisyys. Heidät on vaikea tunnistaa ja asettaa syytteeseen Internetin anonyymin luonteen vuoksi. Koska tietotekniikkajärjestelmiä vastaan tehdyt hyökkäykset ovat erittäin houkuttelevia, kyberhyökkäysten määrän ja kehittyneisyyden odotetaan kasvavan jatkuvasti. (Jang-Jaccard ja Nepal 2014). Seuraavaksi käymme läpi yleisimpiä haittaohjelmia ja kyberhyökkäysten muotoja.

3.1 Ramsomware

Ransomware on eräänlainen haittaohjelma, joka estää laillisten käyttäjien pääsyn omaan järjestelmään vaatien maksun tai lunnaita antaakseen pääsyn takaisin. Hyökkäys on suunniteltu hyödyntämään järjestelmän heikkouksia ja tunkeutumaan verkkoon. Kun järjestelmä on saanut tartunnan, lunnasohjelma antaa hakkereille mahdollisuuden joko estää pääsyn kiintolevylle tai salata tiedostoja. Hyökkääjät vaativat yleensä maksua jäljittämättömän kryptovaluutan kautta. Valitettavasti monissa kiristysohjelmien hyökkäystapauksissa oikea käyttäjä ei saa takaisin pääsyä laitteisiinsa edes lunnaiden maksamisen jälkeen. (Baker 2021).

3.2 Maas-malli

Malware as a Service eli MaaS-malli. MaaS-mallissa hakkereita palkataan suorittamaan lunnasohjelmahyökkäyksiä kolmannen osapuolen toimesta. Tällä tavalla periaatteessa kuka tahansa, joka haluaa suorittaa kyberhyökkäyksen, voi sen tehdä, vaikka ei omaisi juurikaan teknisiä taitoja. (Baker 2021).

3.3 Palvelunestohyökkäys

Palvelunestohyökkäys (DoS) on kohdennettu hyökkäys, joka puskee verkkoon vääriä pyyntöjä liiketoiminnan häiritsemiseksi. DoS-hyökkäyksessä käyttäjät eivät pysty suorittamaan perustehtäviä, kuten pääsyä sähköpostiin, verkkosivustoille, online-tileille tai muihin resursseihin, joita hyökkäyksen koh-

teena oleva tietokone tai verkko käyttää. Vaikka useimmat DoS-hyökkäykset eivät johda tietojen katoamiseen ja ne ratkaistaan yleensä ilman lunnaita, ne maksavat organisaatiolle aikaa, rahaa ja muita resursseja kriittisen liiketoiminnan palauttamiseksi. DoS- ja DDoS (Distributed Denial of Service) -hyökkäysten välinen ero liittyy hyökkäyksen alkuperään. DoS-hyökkäykset ovat peräisin vain yhdestä järjestelmästä, kun taas DDoS-hyökkäykset käynnistetään useista järjestelmistä. DDoS-hyökkäykset ovat vaikeampia estää kuin DOS-hyökkäykset, koska useat järjestelmät on tunnistettava hyökkäyksen pysäyttämiseksi. (Baker 2021).

3.4 Tietojenkalastelu

Tietojenkalastelu on eräänlainen kyberhyökkäys, joka käyttää sähköpostia, tekstiviestejä, puhelinta ja sosiaalista mediaa houkutellakseen uhrin jakamaan arkaluontoisia tietoja, kuten salasanoja tai tilinumeroita. Tietojenkalastelussa uhri voidaan myös houkutella lataamaan tiedoston, joka asentaa viruksia hänen laitteeseensa. COVID-19 lisäsi dramaattisesti kaikenlaisia kyberhyökkäyksiä, mukaan lukien tietojenkalasteluhyökkäyksiä. Tämä johtuu puhtaasti siitä, että karanteenin aikana ihmiset viettävät enemmän aikaa verkossa. (Baker 2021).

3.5 Man in the middle

Man in the middle (MITM) -hyökkäys on kyberhyökkäys, jossa pahantahtoinen toimija salakuuntelee verkon käyttäjän ja verkkosovelluksen välistä keskustelua. MITM-hyökkäyksen tavoitteena on kerätä esimerkiksi henkilötietoja, salasanoja tai pankkitietoja. Vaikka MITM-hyökkäykset kohdistuvat usein yksilöihin, se on merkittävä uhka myös yrityksille ja suurille organisaatioille. Yksi yleinen pääsykeino hakkereille on ohjelmistopalveluina myytävät sovellukset. Kyberhyökkääjä voi käyttää näitä sovelluksia sisäänpääsynä organisaation verkkoon ja mahdollisesti vaarantaa minkä tahansa datan, mukaan lukien asiakastiedot, IP-osoitteet tai organisaation ja sen työntekijöiden omia tietoja. (Baker 2021).

3.6 Cross Site Scripting

Cross Site Scripting (XSS) on koodin lisäyshyökkäys, jossa hakkeri lisää haitallista koodia lailliseen verkkosivustoon. Koodi käynnistyy komentosarjana käyttäjän verkkoselaimessa, jolloin hyökkääjä voi varastaa arkaluonteisia tietoja tai esiintyä käyttäjänä. Verkkofoorumit, ilmoitustaulut, blogit ja muut verkkosivustot, joiden avulla käyttäjät voivat lähettää omaa sisältöään, ovat kaikkein herkimpiä XSS-hyökkäyksille. Vaikka XSS-hyökkäys kohdistuu yksittäisiin verkkosovelluksien vierailijoihin, haavoit-

tuvuudet ovat sovelluksessa tai verkkosivustossa. Organisaatiot, jotka tarvitsivat etätyövoiman käyttöönottoa, ovat saattaneet vahingossa altistua tämän tyyppisille hyökkäyksille asettamalla sisäiset sovellukset saataville verkon kautta tai ottamalla käyttöön pilvipohjaisia palveluita. (Baker 2021).

3.7 DNS-tunnelointi

DNS-tunnelointi on kyberhyökkäys, joka hyödyntää DNS-kyselyitä ja -vastauksia ohittaakseen perinteiset turvatoimenpiteet ja siirtääkseen dataa ja koodia verkossa. Kun hakkeri on saanut levitettyä ”tartunnan” hän voi vapaasti osallistua komento- ja valvontatoimintoihin. Tämä antaa hakkereille reitin päästää haittaohjelmat leviämään ja antaa mahdollisuuden poimia tietoja, IP-osoitetta tai muuta arkaluonteista tietoa. DNS-tunnelointihyökkäykset ovat lisääntyneet viime vuosina osittain siksi, että ne ovat suhteellisen helppo ottaa käyttöön. Tunnelointityökalut ja -oppaat ovat jopa helposti saatavilla verkossa yleisten sivustojen kautta. (Baker 2021).

3.8 Drive by hyökkäys

Drive by hyökkäys on kehittynyt muoto haittaohjelmahyökkäyksestä, joka hyödyntää useiden verkkoselaimien, lisäosien tai sovellusten heikkoja kohtia hyökkäyksen käynnistämiseksi. Drive by hyökkäyksen aloittaminen ei vaadi ihmisen toimintaa. Kun hyökkäys on käynnissä, hakkeri voi kaapata laitteen, vakoilla käyttäjän toimintaa ja varastaa tietoja. (Baker 2021).

4 YLEISIMMÄT SUOJAUTUMISKEINOT

Yleisimmät suojautumiskeinot ovat suurimmalle osalle internetin käyttäjälle hyvin itsestään selviä, mutta uskomme, että niiden tärkeyttä on silti syytä korostaa. Ensimmäinen keino omien tietojen suojaamiseen on tietysti hyvä ja vahva salasana. Vahvan salasanan käyttäminen jokaisella käyttämälläsi tilillä on tärkein ja helpoin keino tietojesi suojaamiseen. Suurin osa sivustoista, pankeista ja muista sovelluksista tarjoaa nykyään myös mahdollisuuden käyttää kaksi vaiheista tunnistusta. Jos vain mahdollista, on sen käyttäminen enemmän kuin suositeltavaa. Kolmas helppo tapa suojata omia tietoja on jonkin antivirus eli virustentorjunta ohjelman käyttäminen. Näihin kolmeen suojautumiskeinoon keskitymme lisää seuraavissa kappaleissa.

4.1 Salasana

Hyvä salasana koostuu oikeastaan kolmesta eri tekijästä. Mitä pidempi salasana, sitä vaikeampi se on murtaa. Salasanan pituus on tärkein tekijä. Käytä aina merkkien, numeroiden ja erikoismerkkien yhdistelmää. Erilaisten merkkien käyttäminen tekee salasanan arvaamisesta vaikeampaa. Käytä erilaisia salasanoja. Tunnistetieto hyökkääjät käyttävät botteja testatakseen, käytetäänkö yhdeltä verkkotililtä varastettuja salasanoja myös muilla tileillä. Esimerkiksi tietomurto pienessä yrityksessä voi vaarantaa jopa pankkitilin, jos siinä käytetään samoja tunnistetietoja. Käytä pitkää, satunnaista ja ainutlaatuista salasanaa kaikissa tileissäsi. Salasanojen murtamiseen on olemassa monia eri työkaluja, joita hakkerit käyttävät. Tästä syystä vahva salasana on erittäin tärkeää, sillä et suojaudu ainoastaan ihmiseltä, joka yrittää arvata salasanasi, vaan mahdollisesti myös ohjelmalta, joka pystyy arvailemaan salasanaasi jopa 2000 kertaa minuutissa. (Poston 2020).

4.2 Kaksivaiheinen tunnistautuminen

Vaikka käyttäisitkin hyvää ja vahvaa salasanaa, voidaan se silti saada selville. Tästä syystä on kannattavaa ottaa käyttöön kaksivaiheinen tunnistautuminen aina kun se on mahdollista. Sitä käytettäessä hakkeri ei pääse suoraan tilillesi käsiksi, vaikka saisikin selville salasanasi. Esimerkiksi kun kirjaudut jollekin sosiaalisen median alustalle normaalisti käyttäjätunnuksella ja salasanalla et pääse vielä suo-

raan sisään. Tässä vaiheessa aktivoituu kaksivaiheinen tunnistus. Saat joko sähköpostina tai tekstiviestinä vahvistuslinkin, jota klikkaamalla pääset kirjautumaan, tai koodin, joka pitää vielä syöttää kirjautumissivulla päästäksesi sisään.

4.3 Virustentorjunta ohjelmisto

Virustentorjunta ohjelmistoa käytetään estämään, tarkistamaan, havaitsemaan ja poistamaan viruksia tietokoneelta. Asennuksen jälkeen useimmat virustorjuntaohjelmistot toimivat automaattisesti taustalla tarjotakseen reaaliaikaisen suojan virushyökkäyksiä vastaan. Kattavat virustorjuntaohjelmat auttavat suojaamaan tiedostosi ja laitteistosi haittaohjelmilta, kuten niin kutsutuilta madoilta, troijalaisilta ja vakoiluohjelmilta. Ne voivat myös tarjota lisäsuojaa, kuten mukautettavat palomuurit ja verkkosivustojen estot. (Verizon 2022).

5 KYBERYTURVALLISUUDEN MERKITYS YRITYSMAAILMASSA

Teknologia kehittyy nopeasti. Uusia laitemuotoja kehittyy lyhyin väliajoin. Teknologiat, kuten pilvipalvelut ja laitteet, joissa on internet kehittyvät aggressiivisesti. Kaikki nämä uudet teknologiat ja laitteet on suojattava tietoverkkorikollisilta nykyisten teknologioiden suojaamisen lisäksi. Näitten syitten takia jokainen yritys tarvitsee vahvan kerroksen kyberturvallisuustoimenpiteitä, joiden avulla se voi puolustautua kyberhyökkäyksen ja sen seurausten kasvavilta huolenaiheilta. Yritykset voivat ryhtyä erilaisiin toimenpiteisiin suojautuakseen näiltä kriittisiltä uhkilta. Tietoverkkorikollisuuden uhka kohdistuu kaikenlaisiin ja kaikenkokoisiin yrityksiin. Internetin ansiosta yritykset käyttävät digitaalitekniikkaa kaikissa toimenpiteissään, kuten sähköpostien lähettämisessä ja vastaanottamisessa, rahaliikenteessä, verkostoitumisessa ja yhteistyössä sekä reaaliaikaisessa työskentelyssä. Kun nämä viestintälinjat menevät poikki, voi sillä olla katastrofaalinen vaikutus koko yrityksen toimintaan. Mikä tahansa verkkohyökkäys voi pilata yrityksen maineen, koska sen asiakkaiden arkaluonteiset tiedot saattavat kadota. (iED Team, 2021).

5.1 Yleisimmät riskit yritykselle

Suurin riskitekijä yrityksille on tietoisuuden puute. Yritysten on toimittava ennakoivasti kyberturvallisuudessa tai kyberuhan torjunnassa. Meneillään oleva pandemia on pakottanut yritykset etääntymään, ja siten se on lisännyt digitaalisten palvelujen käyttöönottoa kaikkialla maailmassa. On kasvava huolenaihe, jos heillä ei ole oikeaa näkemystä tai tietoa. Tietoisuus on avainasemassa, koska verkkorikolliset ovat yhä älykkäämpiä ja käyttävät yhä useammin monimutkaisia, kehittyneitä työkaluja työnsä hoitamiseen. Digitaalisen tietoturvatietoisuuden puute johtaa siihen, että asiakkaat ovat mukana vaarantamassa yrityksen turvallisuutta tai yksilön yksityisyyttä. Jos se on lopetettava, yritysten on puututtava asiaan tekemällä säännöllisiä tiedotuskampanjoita ja pitämällä työntekijät ajan tasalla niistä tavoista ja menetelmistä, joita hakkerit käyttävät hyökkäyksiinsä. Tietoturvakurssi tarjoaa työntekijöille laajaa koulutusta erilaisista työkaluista. (iED Team, 2021).

5.1.1 Hakkerit

Hakkerit voivat lähettää laillisen näköisiä sähköpostiviestejä, jotka saattavat suostutella sinut antamaan arkaluonteiset tunnistetietosi tai käyttää ponnahdusikkunoita, jotka houkuttelevat sinut napsauttamaan.

Tai käyttävät sähköposteja kehottaakseen sinua lataamaan työssäsi hyödyllisiä liitetiedostoja. He hankkivat valtakirjasi vastaavalla tavalla ja käyttävät niitä liikesähköpostien lähettämiseen, rahaliikenteen suorittamiseen, arkaluontoisten tietojen varastamiseen ja piiloutumiseen järjestelmään pitkäksi aikaa. (iED Team, 2021).

5.1.2 Tietovuodot

Tietovuodon suojaaminen on toinen huolenaihe, jolla varmistetaan asiakkaiden yksityisyys ja turvallisuus. Yritykset tai yritykset tallentavat kaikki tietonsa aina asiakastiedoista, liiketoimintatiedoista ja muista arkaluonteisista tiedoista, jotka voivat olla potentiaalisessa varkausvaarassa, jos hakkerit pääsevät käsiksi mihin tahansa tärkeisiin työntekijän tunnistetietoihin. Yksi monista suositelluista tavoista suojata tietoja vuotamiselta on käyttää poltettavia sähköposteja. Nämä polttosähköpostit eivät ole mitään muuta kuin organisaatioiden valesähköposteja, joita he käyttävät kirjautuakseen verkkosivustoille, joille he eivät mielellään anna koko valtakirjaansa. Voit myös käyttää monia työkaluja, joiden avulla voit varmistaa tietojesi maksimaalisen turvallisuuden. (iED Team, 2021).

5.1.3 Sosiaalinen manipulointi

Sosiaalisen manipuloinnin hyökkäykset lisääntyvät sosiaalisen median käytön lisääntyessä. Hakkerit tekevät ”social engineering” hyökkäyksiä saamalla valtakirjat käyttöönsä sosiaalisen median kautta. Sosiaalisen suunnittelun hyökkäyksiä tapahtuu päivittäin monenlaisia. Monien nykytekniikoiden lisääntyessä on monia uusia menetelmiä valtakirjojen hankkimiseksi sosiaalisen median kautta. Hakkerit suorittavat huijauksia eri tavoin. On suositeltavaa olla avaamatta mitään sähköpostia, joka näyttää ensisilmäyksellä epäilyttävältä. Eikä kenenkään pidä ladata mitään tiedostoa, jos lähettäjä näyttää epäilyttävältä, eikä koskaan syöttää tietojasi tarkistamatta asianmukaisesti lähettäjän laillisuutta. (iED Team, 2021).

6 ENNALTAEHKÄISEMINEN JA SUOJAUTUMISKEINOT

Yrityksissä on hallituksella vastuu tehdä kyberturvallisuuden kannalta oikeita päätöksiä. Pieni perehtyminen teknologiaan auttaa hallituksen jäseniä pienentämään uhkia. Pelkkä perustason kyberturvallisuus organisaatiossa auttaa jo torjumaan useimmat tavanomaisista hyökkäyksistä. Kyberturvallisuuden perustason toimenpiteitä voidaan määritellä esimerkiksi NIST:n (National Institute of Standards and Technology) kyberturvallisuuskehyksellä. (NIST 2022).

6.1 Perehdytys

Työntekijöille olisi annettava koulutusta kyberturvallisuudesta koska tietoturvauhkaa ei voida välttää, jos sitä ei tunnisteta. Yleisin uhka aiheutuu inhimillisestä erehdyksestä, ja se on tärkein syy kyberkoulutuksen olemassaoloon. Me kaikki teemme virheitä ja meistä lähes jokainen on ollut tekemisissä jonkinlaisen hakkerointiyrityksen kanssa. (Cybint Author 2021).

Kun työnantajat asettavat tietoisuutta kyberturvallisuudesta koskevan koulutuksen etusijalle, he auttavat ehkäisemään suuria menetyksiä yrityksessä. Tietoisuuskoulutuksessa käsitellään kuitenkin harvoin taitoja ja tietojen soveltamista. Työntekijöiden riskikäyttäytymisen muuttaminen on se, mikä todella auttaa tukahduttamaan verkkohyökkäyksen. Pelkkä tietoturvatietämys ei riitä, vaan on otettava käyttöön koko työuran kestävä koulutusstrategia, joka auttaa kitkemään tietoverkkorikollisuuden kokonaan. Kyberturvallisuuteen kohdistuu jatkuvasti uusia uhkia, joten jatkuva koulutus on välttämätöntä, ja sen pitäisi olla nykyään osa yleistä työkoulutusprosessia alusta alkaen. Jotkut luulevat, että pienet yritykset voivat välttää suuret hakkeroinnit ja tietoturvaloukkaukset, mutta tämä ei yksinkertaisesti pidä paikkaansa. Koska inhimillinen erehdys on suurin kohtaamamme ongelma, se tarkoittaa, että kaikki ovat vaarassa. Työntekijät on pidettävä ajan tasalla kaikista uusimmista tiedoista. (Cybint Author 2021).

Kyberturvallisuus on kovassa kasvussa ja uusia uhkia ilmaantuu koko ajan, joten koulutuksen on oltava jatkuvaa. Maailma on täynnä teknologiaa, ja se tekee elämästämme helpompaa, mutta on ratkaisevan tärkeää, että osaamme hallita sitä ja että pidämme kyberturvallisuuden aina näköpiirissämme. Koska uusia kyberuhkia ilmaantuu päivittäin, koulutuksen pitäisi olla elinikäinen prosessi, ja työnteki-

jöiden on testattava oppimaansa. Jos näin ei toimita, sillä voi olla pitkäkestoisia liiketoimintaan liittyviä seurauksia. Kun etsit työntekijöille kyberturvallisuuskoulutusta, paras vaihtoehto on ohjelma, joka menee kyberturvallisuustietoisuutta pidemmälle ja keskittyy taitoihin ja toteutukseen. (Australian Goverment 2021).

6.2 Varmuuskopiointi

Yrityksen tietojen ja verkkosivuston varmuuskopioiminen auttaa palauttamaan menetetyt tiedot, jos kohtaat verkkovahingon tai tietokoneongelman. On tärkeää, että varmuuskopioit tärkeimmät tietosi säännöllisesti. Onneksi varmuuskopiointi ei yleensä maksa paljon ja se on helppo tehdä. Tärkeiden tiedostojesi turvallisuuden varmistamiseksi kannattaa käyttää useita varmuuskopiointimenetelmiä. Hyvä varmuuskopiointijärjestelmä voisi olla esimerkiksi seuraavanlainen: päivittäiset varmuuskopiot kannettavalle laitteelle ja/tai pilvitallennukseen, palvelimen varmuuskopiot viikon lopussa, neljännesvuosittaiset palvelimen varmuuskopiot, vuosittaiset palvelimen varmuuskopiot, sekä säännöllinen tarkistaminen että tietojen palauttaminen varmuuskopiosta toimii. On hyvä myös ottaa tavaksi varmuuskopioida tiedot ulkoiselle asemalle tai kannettavalle laitteelle, kuten USB-tikulle. Säilytä kannettavat laitteet erikseen muualla kuin toimipisteessä, jolloin yrityksellläsi on varasuunnitelma b, jos toimipiste ryöstetään tai se vahingoittuu. Älä jätä laitteita kytkettyinä tietokoneeseen, sillä ne voivat joutua kyberhyökkäyksen kohteeksi. (Australian Government 2021).

6.3 Ohjelmistojen pitäminen ajan tasalla

Varmista, että päivität ohjelmistosi ja että ohjelmoit käyttöjärjestelmäsi ja tietoturvaohjelmistosi päivittymään automaattisesti. Päivitykset voivat sisältää tärkeitä tietoturvapäivityksiä viimeaikaisten virusten ja hyökkäysten varalta. Useimmissa päivityksissä voit ajoittaa päivitykset työajan jälkeen tai muuna sopivampana ajankohtana. Päivityksillä korjataan vakavia tietoturva-aukkoja, joten päivityskehotuksia ei saa koskaan jättää huomiotta. (Australian Government 2021).

6.4 Palomuuri

Palomuurin käyttäminen. Palomuuri on ohjelmisto tai laitteisto, joka on tietokoneen ja internetin välissä. Se toimii portinvartijana kaikelle saapuvalle ja lähtevälle liikenteelle. Palomuurin käyttöönotto

suojaa yrityksesi sisäisiä verkkoja, mutta niitä on korjattava säännöllisesti, jotta ne voivat hoitaa tehtävänsä. Muista asentaa palomuuri kaikkiin yrityksen kannettaviin laitteisiin. (Australian Government 2021).

6.5 Suodatus

Käytä roskapostisuodattimia vähentääksesi yrityksesi saamien roskaposti- ja phishing-sähköpostiviestien määrää. Roskaposti- ja phishing-sähköpostiviestejä voidaan käyttää virusten tai haittaohjelmien levittämiseen tietokoneellesi tai luottamuksellisten tietojen varastamiseen. Jos saat roskaposti- tai phishing-sähköposteja, paras tapa on poistaa ne. Roskapostisuodattimen käyttäminen auttaa vähentämään sitä, että sinä tai työntekijäsi avaatte roskapostin tai epärehellisen sähköpostin vahingossa. (Australian Government 2021).

6.6 Turvallinen verkko

Varmista, että otat verkon salauksen käyttöön ja salaa tiedot, kun niitä tallennetaan tai lähetetään verkossa. Salaus muuttaa tietosi salaiseksi koodiksi, ennen kuin lähetät ne internetin kautta. Tämä vähentää varkauden, tuhoutumisen tai peukaloinnin riskiä. Voit ottaa verkon salauksen käyttöön reitittimen asetusten kautta tai asentamalla laitteeseesi VPN-ratkaisun (Virtual Private Network), kun käytät julkista verkkoa. (Australian Government 2021).

6.7 Salasanat

Välttääksesi tietoverkkorikollisen pääsyn tietokoneeseesi tai verkkoosi, vaihda kaikki oletussalasanat uusiin salasanoihin, joita ei voi helposti arvata. Rajoita sellaisten tilien käyttöä, joilla on hallinnolliset oikeudet. Rajoita pääsyä tileihin, joilla on järjestelmänvalvojan oikeudet tai harkitse järjestelmänvalvojan käyttöoikeuksien poistamista kokonaan käytöstä. Hallinnointioikeudet mahdollistavat sen, että joku voi suorittaa normaalia korkeampia tai arkaluontoisempia tehtäviä, kuten asentaa ohjelmia tai luoda muita tilejä. Nämä ovat hyvin erilaisia kuin tavalliset oikeudet tai vieraskäyttäjän oikeudet. Rikolliset hakevat usein näitä oikeuksia, jotta he saisivat paremman pääsyn ja hallinnan yrityksessäsi. Voit vähentää tätä riskiä luomalla vakiokäyttäjätilin, jolla on vahva salasana, jota voit käyttää päivittäin. Käytä hallinnollisilla oikeuksilla varustettuja tilejä vain tarvittaessa, rajoita käyttöoikeuksia käyttävien

henkilöiden määrää, äläkä koskaan lue sähköposteja tai käytä internetiä käyttäessäsi hallinnollisilla oikeuksilla varustettua tiliä. (Australian Government 2021).

6.8 Yleinen laajakuva

Pidä kirjaa kaikista yrityksesi käyttämistä tietokonelaitteista ja ohjelmistoista. Varmista, että ne on suojattu kielletyn käytön estämiseksi. Muistuta työntekijöitäsi olemaan varovaisia: missä ja miten he säilyttävät laitteitaan ja mihin verkkoihin he liittävät laitteensa. USB-muistitikkujen tai kannettavien kiintolevyjen käytössä myös oltava huolellinen sillä tuntemattomat virukset ja muut uhat voivat siirtyä niiden kautta kotoa yritykseesi. Poista kaikki ohjelmistot ja laitteet, joita et enää tarvitse, ja varmista, että niissä ei ole arkaluonteisia tietoja ennen poistamista. Jos vanhat ja käyttämättömät ohjelmistot tai laitteet jäävät osaksi yritysverkkoasi, niitä ei todennäköisesti päivitetä ja niistä voi tulla takaovi, jonka kautta rikolliset voivat hyökätä yritykseesi. Aiempien työntekijöiden luvaton pääsy järjestelmiin on yleinen tietoturvaongelma yrityksissä. Poista välittömästi käyttöoikeudet henkilöiltä, jotka eivät enää työskentele yrityksessäsi, tai jos he vaihtavat roolia eivätkä enää tarvitse käyttöoikeuksia. (Australian Government 2021).

7 VAKUUTUKSET

Tarvitseeko yritys tietoturvavakuutusta? Tähän kysymykseen vastasi Ville Stolpe opsec.fi:n verkkoartikkelissa seuraavalla tavalla: “Moni vakuutusyhtiö on tuonut viime aikoina markkinoille tietoturva- ja kyberturvallisuusvakuutuksia. Organisaatioiden miettiessä, onko tällaiselle vakuutukselle tarvetta, kannattaa heidän aloittaa tarvekartoitus liiketoiminnan riskien arvioimisesta. Silloin, kun riskiarvioinnin kautta nousee esille sellaisia suuria riskejä, jotka liittyvät tietojärjestelmissä tapahtuvaan tietojenkäsittelyyn, kannattaa harkita yhtenä kontrollina riskin siirtämistä vakuutusyhtiölle. Tällaiset riskit uhkaavat yleensä koko liiketoiminnan jatkuvuutta, joten vakuutus saattaa olla tarpeellinen”. (opsec, Mika Lindberg 2022).

7.1 Kartoitus

Kybervakuutuksen sopivaa kattavuutta ei ole välttämättä itse osattava päätellä. Vakuutuksia myyvät yhtiöt tarjoavat myös vakuutusmeklarin palveluita, joiden kanssa käydään läpi liiketoiminnan riskit ja etsitään paras kybervaakutusturva asiakkaan tarpeisiin nähden. (Howden, 2022).

7.2 Vaihtoehdot

Alta löytyvistä vertailutaulukoista voit nähdä eri vakuutusyhtiöiden tietoturva- ja kyberturvallisuusvakuutusten verkosta löytyviä yleisiä ehtoja. Vertailutaulukoista löytyy, mitä eri vakuutukset yritykselle korvaavat ja mitä velvoitteita ne asettavat vakuutettavalle organisaatiolle. (OPSEC, Mika Lindberg 2022).

Mitä korvataan?	LähiTapiola	OP	IF	Fennia
Toiselle aiheutuneet vahingot (vastuuvahingot)	Kyllä	Kyllä	Kyllä	Kyllä
Itselle aiheutunut keskeytysvahinko ja tiedostojen palautus	Kyllä	Kyllä	Kyllä	Kyllä
Vakuutetulle syntyvät ja vakuutusyhtiön ennalta hyväksymät kustannukset, jotka aiheutuvat välttämättömistä kriisinhallintatoimenpiteistä, kuten vahinkotapahtuman selvittämisestä ja torjumisesta, lainsäädännön edellyttämästä tiedottamisesta, lakimiesavun käytöstä sekä viestinnästä	Kyllä	Kyllä	Kyllä	Kyllä
Vakuutuksesta korvataan taloudellinen vahinko (mukaan lukien puolustuskulut)	Kyllä	Kyllä	Kyllä	Kyllä
Kyberkiristys (lunnaat)	-	-	-	Kyllä
Maineriskit (PR-kulut)	Kyllä	Kyllä	Kyllä	Kyllä
Tietovarkaus ja tietoväärennös	Kyllä	-	-	-
Tietoturvallisuuden pettäminen - korvausvastuu	-	-	-	Kyllä
Digitaalinen media - korvausvastuu	-	-	-	Kyllä
Kyberrikosturva (anastettu rahasumma)	-	-	-	Kyllä
Maksukortteja koskevat tietoturvastandardit (PCI-DSS)	-	-	-	-
Rkkoutuneiden IT-laitteiden korjaamisesta tai vaihtamisesta	-	-	Kyllä	-
Ilmoittamisesta aiheutuvat kulut	Kyllä	Kyllä	Kyllä	Kyllä
Tietosuojaloukkaus	Kyllä	Kyllä	Kyllä	Kyllä
Palvelunestohyökkäys	Kyllä	Kyllä	Kyllä	Kyllä
IT-forensiikka (tarvittaessa)	Kyllä	-	-	-

KUVA 1. Mitä tietoturvavakuutus korvaa (OPSEC, Mika Lindberg 2022).

Velvoitteet	LähiTapiola	OP	IF	Fennia
Vakuutuksenottajan on nimettävä henkilö, jonka tehtävänä on vastata tietoturvallisuudesta.	Kyllä	Kyllä	-	-
Salasanavaatimukset	Kyllä	Kyllä	Kyllä	-
Tietolaitteet on varustettava virustorjuntaohjelmistolla ja palomuurilla, jotka on päivitettävä säännöllisesti	Kyllä	Kyllä	Kyllä	Kyllä
Tiedostojen varmuuskopiointi on tehtävä säännöllisesti	Kyllä	Kyllä	Kyllä	Kyllä
Tietoaineiston ja laitteiden turvallinen säilyttäminen	Kyllä	-	-	Kyllä
Velvollisuus tehdä vakuutusyhtiön vaatimuksesta tutkintapyyntö poliisille	Kyllä	-	-	-
Kadonneesta tietolaitteesta on ilmoitettava tietoturvallisuudesta vastaavalle henkilölle välittömästi	Kyllä	-	-	-
Varmuuskopioitavissa olevat ohjelmistot on varmuuskopioitava ennen tietojärjestelmään asentamista ja aina muutosten yhteydessä.	-	-	-	Kyllä
Varmuuskopiot, alkuperäistuotteet ja asentamiseen oikeuttavat tunnukset on säilytettävä siten, etteivät ne voi tuhoutua samassa vahingossa tietojärjestelmään asennettujen tiedostojen ja ohjelmiston kanssa	-	-	-	Kyllä
Tietojärjestelmän ja tietoverkkojen on oltava suojattu tietoturvapoikkeamilta	-	-	-	Kyllä
Salasanoja ja käyttäjätietoja säilytetään turvallisesti	-	-	Kyllä	-
Ohjelmistot ja järjestelmät tulee päivittää viimeisimpien tietoturvapäivitysten mukaisesti.	-	-	Kyllä	-
Tietoturvapolitiikan kehittäminen ja ylläpito	-	Kyllä	-	-
Tietojen ja tietojärjestelmien luokittelu	-	Kyllä	-	-
Sosiaalisen median ja tietoverkkojen käytön ohjeet	-	Kyllä	-	-
Henkilökunnan tietoturvakäytännöt	-	Kyllä	-	-
Organisaation verkko tulee erottaa julkisesta verkosta palomuureilla ja välityspalvelimilla (proxy) kaikissa rajapinnoissa julkista verkkoa vastaan	-	Kyllä	-	-
Kotisivujen ja verkkopalvelimien turvallisuus	-	Kyllä	-	-
Sähköpostin turvallisuus	-	Kyllä	-	-
Mobiililaitteiden turvallisuus	-	Kyllä	-	-
Toimitila- ja operatiivinen turvallisuus	-	Kyllä	-	-
Maksutietojen turvallisuus	-	Kyllä	-	-
Tietoturvapoikkeamien hallintamalli	-	Kyllä	-	-

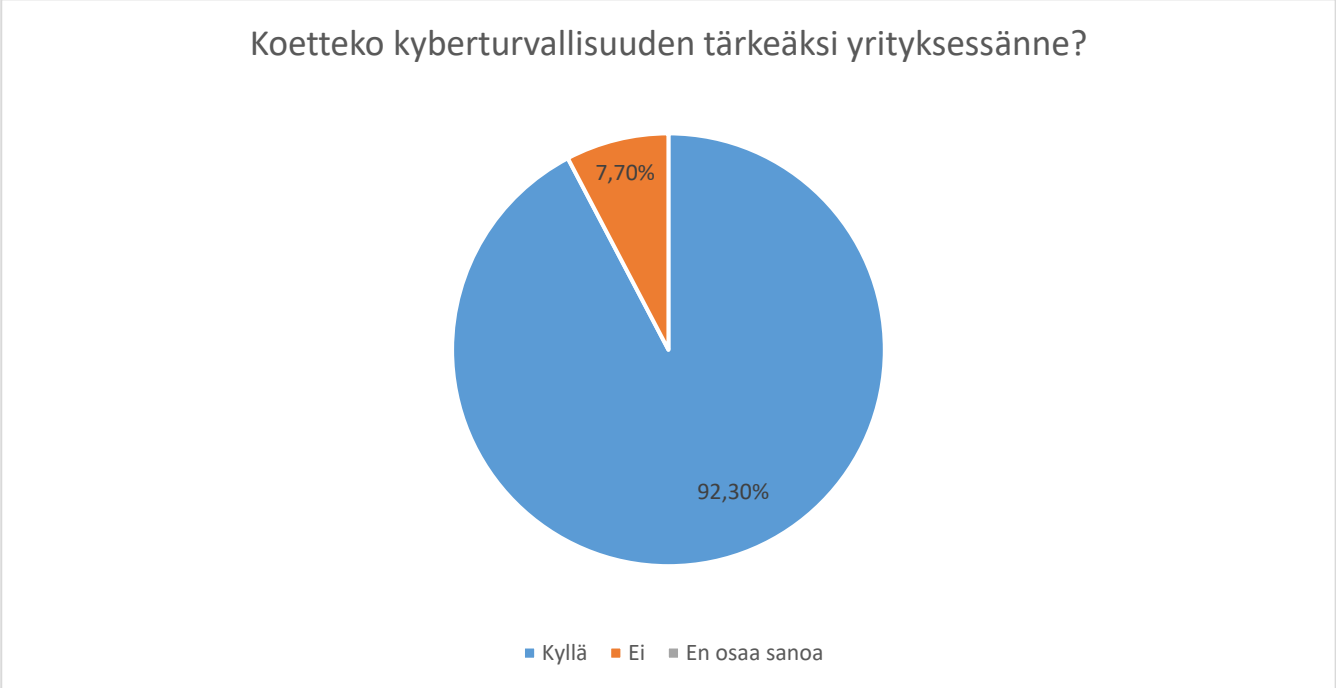
KUVA 2. Mitä tietoturvavakuutus korvaa (OPSEC, Mika Lindberg 2022).

8 KYSELYTUTKIMUS

Laadimme pienimuotoisen kyselytutkimuksen selvittämään eri yritysten suhtautumista kyberturvallisuuteen. Tutkimuksen kohteena olivat pienet ja keskisuuret yritykset. Kyselyn kohdistimme tilitoimistoihin, asianajotoimistoihin ja mainostoimistoihin. Kyselytutkimuksen tavoitteena oli selvittää millä tavalla nykyajan yritykset valmistautuvat erilaisiin kyberuhkiin. Kysely suoritettiin Google Forms kyselylomakkeen muodossa. Lähetimme kyselyn noin kahdellesadalle edellä mainittujen alojen yrityksille sähköpostilla. Kysely sai ainoastaan 14 vastausta, eli vastaus prosentti oli noin 6 %. Tästä voikin päätellä, ettei kyberturvallisuus ole monenkaan mielestä kovin mielenkiintoinen asia.

8.1 Kyberturvallisuuden tärkeys

Ensimmäinen kysymys käsittelee sitä, kuinka tärkeäksi yrittäjät kokevat kyberturvallisuuden. Vaikkakin kyselyn vastausprosentti jäikin aika alhaiseksi, huomaamme, että vastaajista suurin osa oli kyberturvallisuudesta kiinnostunut.



KUVIO 1. Kyberturvallisuuden tärkeys. Vastaajia oli 13

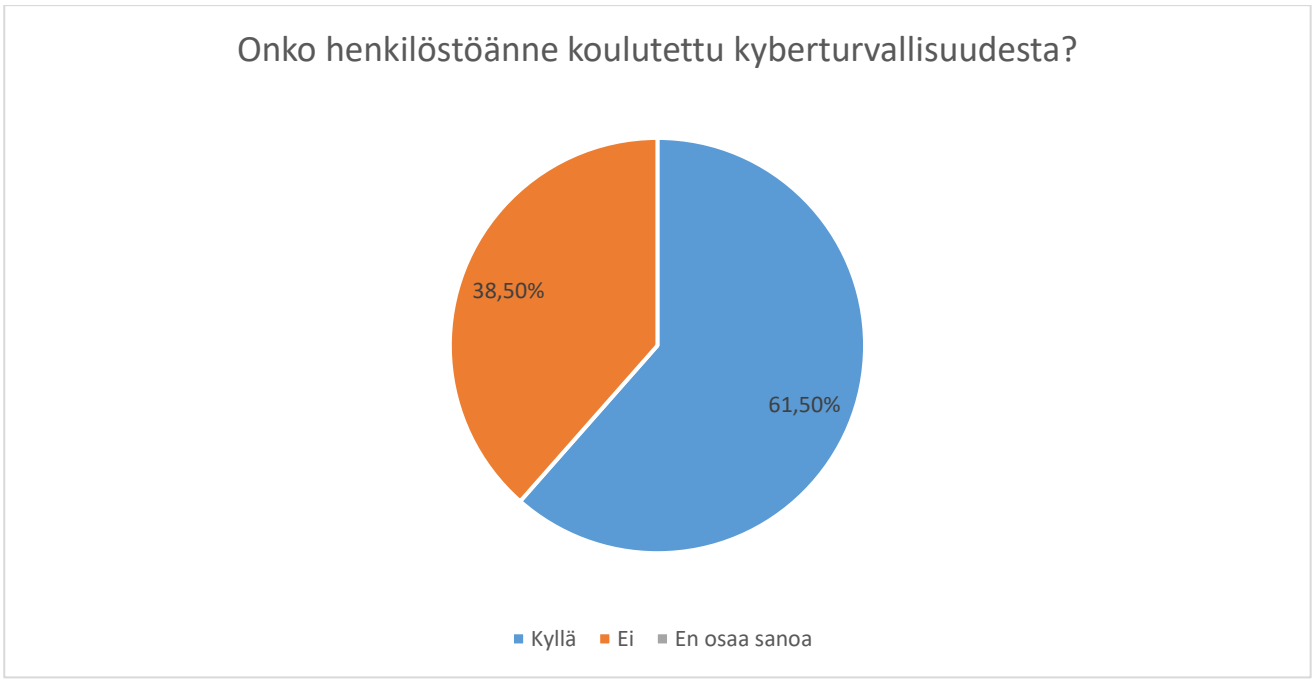
8.2 Kyberturvallisuuden huomiointi

Toisessa kysymyksessä selvitimme, onko yrityksissä otettu kyberturvallisuus jollakin tavalla huomioon. On hienoa nähdä, että yli 90 % ottavat kyberturvallisuuden tosissaam ja aktiivisesti taistelevat uhkia vastaan.

KUVIO 2. Kyberturvallisuuden huomiointi. Vastaajia oli 13

8.3 Kyberkoulutus

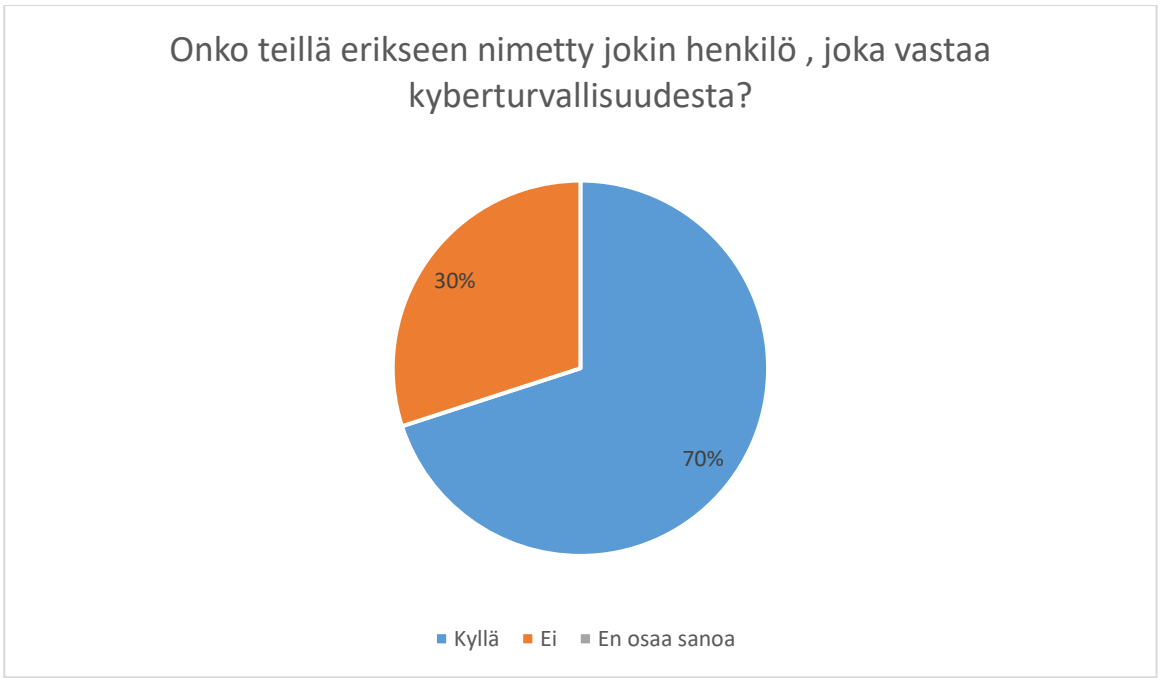
Kolmas kysymys käsittelee kyberturvallisuus koulutusta. On positiivista huomata, että yli puolet (61,5 %) ovat antaneet henkilöstölleen koulutusta kyberturvallisuudesta, mutta luvun toivoisi olevan vieläkin suurempi.



KUVIO 3. Kyberkoulutus. Vastaajia oli 13

8.4 Kybervastaava

Neljännessä kysymyksessä otimme selvää, löytyykö vastanneista yrityksistä kyberturvallisuuden vastuuhenkilöitä. Oli positiivista huomata, että valtaosa yrityksistä kokee asian tärkeäksi, sillä jopa 70 % oli nimennyt vastuuhenkilön.



KUVIO 4. Kybervastaava. Vastaajia oli 13

8.5 Kybervakuutus

Viidennessä kysymyksessä kysyttiin, onko yritys ottanut itselleen kybervakuutuksen. Neljästätoista vastaajasta yksitoista vastasi tähän kysymykseen. Vastauksista selvisi, että vain yksi vastaajista oli ottanut kybervakuutuksen. Kysymys näyttää meille siinä mielessä ristiriitaista tietoa, sillä suurin osa kertoo kokevansa kyberturvallisuuden tärkeäksi asiaksi, muttei kuitenkaan näe hyötyä hankkia kybervakuutusta.

Onko teillä kybervakuutus? Jos on, mitä se kattaa?
Ei
ei
Ei ole
Ei tietääkseni ole
En osaa sanoa
Kybervakuutuksemme kattaa potentiaalisia rahallisia menetyksiä

TAULUKKO 1. Kybervakuutus. Vastaajia oli 11

8.6 Arkaluonteiset tiedot

Kuudes kysymys käsitteli yrityksien tapoja suojata erilaisia arkaluontoisia tietoja. Neljästätoista vastaajasta kaksitoista vastasi tähän kysymykseen. Vastauksista näemme, että yrityksillä on paljon erilaisia tapoja suojata tietojansa. Suurin osa yrityksistä käytti normaaleja sähköisiä keinoja.

Millä tavalla suojelette/säilytätte yrityksen arkaluontoisia tietoja?
Salasanoilla, pääsy rekisteriin rajoitettu, toimintaohjeet olemassa
Paperimuodossa kassakaapissa/arkistossa, sähköisessä muodossa M-Files dokumenttihallintajärjestelmässä. Pääsy rajattu käyttöoikeuksiin.
Salasanat, varmuuskopiot pilvessä
Yhtiöryhmälaajuinen tietoturvastrategia
Tietoturvallinen palvelinratkaisu
BAT sovellettuna
N/A
Ulkoinen media
Sähköiset arkistot
Turhat poistetaan muut salasanojen takana
Salasanoilla ja varovaisuudella
Encryption tiedostot

TAULUKKO 2. Arkaluonteiset tiedot. Vastaajia oli 12

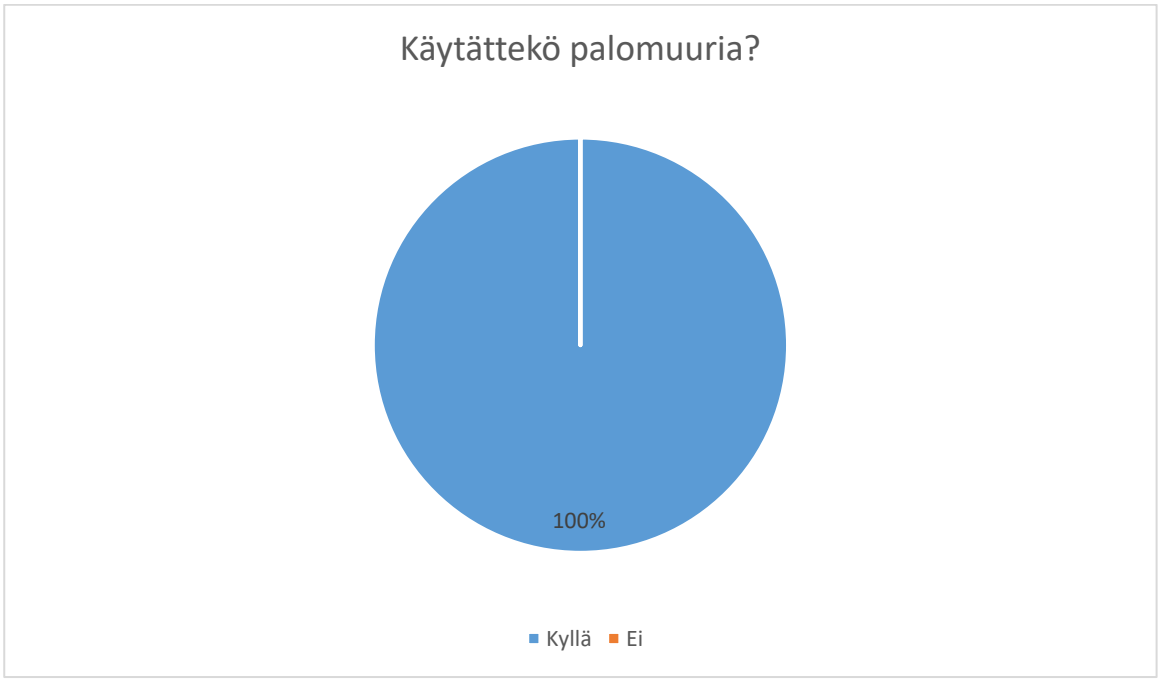
8.7 Sähköposti

Seitsemännessä kysymyksessä selvitimme, onko yrityksillä käytössä salattu sähköposti. Neljästätoista vastaajasta kymmenen eli 70 % käytti salattua sähköpostia.

KUVIO 5. Sähköposti. Vastaajia oli 14

8.8 Palomuuri

Kahdeksannessa kysymyksessä selvisi, että kaikilla neljällätoista vastaajalla on käytössä palomuuri.



KUVIO 6. Palomuuri. Vastaajia oli 14

8.9 Kyberhyökkäykset

Yhdeksännessä kysymyksessä käsitellään kyberhyökkäyksien ja uhkien kohtaamisia. Näemme, että suurin osa yrityksistä (70 %) ei ole kokenut minkäänlaista uhkaa.

KUVIO 7. Kyberhyökkäykset. Vastaajia oli 14

8.10 Hyökkäyksen muoto

Kymmenes kysymys selvitti kohdattujen hyökkäyksien muodot ja seuraukset.

Jos yrityksenne on kokenut kyberhyökkäyksen, minkälainen se oli ja mitä siitä seurasi?
En osaa sanoa
Sähköposteja kaapattu, käyttäjien nimissä lähetetty roskaposteja. Seuraukset jäivät lieviksi
Ei
N/A
Kerran työntekijän sähköpostiin murtauduttiin.

TAULUKKO 3. Hyökkäyksen muoto. Vastaajia oli 5

8.11 Seuraukset

Viimeisenä kysyimme hyökkäyksien lopullista seurausta. Oli ilo huomata, ettei kyberuhkista kuitenkaan hirveän suuria vahinkoja ollut kenellekään aiheutunut. Yhtä yritystä hyökkäys kuitenkin motivoi hankkimaan vakuutuksen.

Jos jouduitte kyberhyökkäyksen kohteeksi, miten selvisitte siitä?
Ei aiheuttanut isompaa vahinkoa. Muistutettiin käyttäjiä vaihtamaan salasanat saannollisesti
En ole joutunut
-
Aika hyvin
Otimme yhteyttä palvelun tarjoajaan, jonka jälkeen saimme tunnukset takaisin, tämän jälkeen hankimme kybervakuutuksen

TAULUKKO 4. Seuraukset. Vastaajia oli 5

9 JOHTOPÄÄTÖKSET JA KYBERUHKIEN TULEVAISUUS

Kuten jo aiemmin työssä mainitsimme, on kyberhyökkäyksine määrä ollut vain nousemaan päin monien siirryttyä etätöihin korona aikana. On vaikea nähdä syytä, miksi tämä trendi muuttuisi. Vaikka tulevaisuutta onkin mahdoton ennustaa, on tässä asiassa pakko ennustaa kyberuhkien määrän kasvavan ja muotojen lisääntyvän. Etenkin muutamana viimevuotena hurjaa vauhtia kehittyvä tekoäly tuonee oman panoksensa pöytään, kuka tietää missä muodossa. Vaikka tekoälyn avulla voidaankin kehittää erilaisia automatisoituja suojauskeinoja kyberhyökkäyksiä vastaan, on asialla kääntöpuolensa. Bob Violino kirjottaa aiheesta CNBC:n artikkelissaan: ”Artificial intelligence is playing a bigger role in cybersecurity, but the bad guys may benefit the most” (Violino 2022, CNBC). Artikkelissa kerrotaan, että organisaatiot voivat hyödyntää uusimpia tekoälyyn perustuvia työkaluja havaitakseen uhkia paremmin ja suojatakseen järjestelmiään ja tietovarantojaan. Verkkorikolliset voivat kuitenkin käyttää teknologiaa myös kehittyneempien hyökkäysten käynnistämiseen.
https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html

Yksi suuri ongelma nopeasti kehittyvän teknologian ja tekoälyn kanssa lienee se, että harva organisaatio haluaa tai pystyy käyttämään rajallisia resurssejaan jatkuvasti muuttuvien uhkien torjumiseen, sillä tämä vaatii paljon työtä ja tietämystä siitä, mihin kaikkeen on oltava valmiina ja samalla keskittyminen täytyisi kuitenkin olla oman liiketoiminnan pyörittämisessä. Etenkin kun ajatellaan että organisaatioilla on vastassa verkkorikollisia, joiden ei tarvitse välittää välimatkoista tai paikan päällä kiinni jäämisestä, on heillä kaikki aika ja intressit keskittyä ja opiskella nykyisiä ja erilaisia tulevaisuuden keinoja murtaa organisaatioiden käyttämiä tietosuojia joko tekoälyn kanssa tai ilman.

On mahdoton sanoa, kehittyykö tekoäly lopulta enemmän organisaatioille vai rikollisille suotuisaksi. Tekoälyn avulla pyöritettävässä kyberturvallisuudessa hyvä puoli organisaatioiden kannalta ajatellen on se, että sen avulla kyberturvallisuus voidaan saada tulevaisuudessa mahdollisesti lähes kokonaan automatisoiduksi. Tämä ei vaatisi yrityksiltä niin paljon henkilöstöä tai muita rahallisia resursseja kyberhyökkäysten torjumiseen.

LÄHTEET

Australian Goverment 2021. Protect your business from cyber threats. Saatavissa: https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats Viitattu: 13.11.2022

Baker K 2021.The 14 Most Common Cyber Attacks. Crowdstrike. Saatavissa: https: //www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-cyberattacks/ Viitattu: 13.11.2022

Craigen D, Diakun-Thibault N, ja Purse R 2014. Defining Cybersecurity. Technology Innovation Management Review. Saatavissa: https ://www.timreview.ca/article/835 Viitattu: 13.11.2022

Cybint Author 2021. Cybersecurity Training for Employees: What You Need to Know. Cybint. Saatavissa: https://www.cybintsolutions.com/cybersecurity-training-for-employees-what-you-need-to-know/ Viitattu: 13.11.2022

howden 2022. Kybervakuutus. Saatavissa: https://howdenfinland.fi/kybervakuutus/ Viitattu: 13.11.2022

iED Team 2020. Importance of Cybersecurity in Business: Top Reasons. iED. Saatavissa: https://ied.eu/blog/cybersecurity-business-reasons/ Viitattu: 13.11.2022

Jang-Jaccard J ja Nepal S 2014. A survey of emerging threats in cybersecurity. Science Direct. Saatavissa: https: https://www.sciencedirect.com/science/article/pii/S0022000014000178#br0010 Viitattu: 13.11.2022

Lindberg M 2022. Tarvitseeko yritys tietoturvavakuutuksen? opsec. Saatavissa: https://www.opsec.fi/fi/2019/03/14/kuukauden-kysymys-tarvitseeko-yritys-tietoturvavakuutuksen/ Viitattu: 13.11.2022

NIST 2022. CYBERSECURITY MEASUREMENT. Saatavissa: https://www.nist.gov/cybersecurity-measurement
Viitattu: 13.11.2022

Poston H 2022. 10 most popular password cracking tools. INFOSEC. Saatavissa: https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/ Viitattu: 13.11.2022

Verizon 2022. Antivirus. Saatavissa: https://www.verizon.com/info/definitions/antivirus/ Viitattu: 13.11.2022

Violino B 2022. Artificial intelligence is playing a bigger role in cybersecurity, but the bad guys may benefit the most. CNBC. Saatavissa: https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html Viitattu: 6.12.2022

LIITTEET