Opinnäytetyö (AMK)

Tietojenkäsittely

2024

Osasumwen Ehirhieme

Pienyrittäjän tarkistuslista tietoturvalliseen työskentelyyn

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tietojenkäsittely

2024 | 34 sivua

Osasumwen Ehirhieme

Pienyrittäjän tarkistuslista tietoturvalliseen työskentelyyn

Tämä opinnäytetyö liittyy pienen tilitoimiston tietoturvallisen työskentelyn tukemiseen. Työn tavoitteena oli luoda käytännöllinen tarkistuslista, joka auttaa mikroyrittäjää parantamaan tietoturvaa liiketoimintaympäristössään. Tämä on erityisen tärkeää nykyajan digitaalisessa maailmassa, jossa tietoturvariskit ovat kasvaneet.

Työssä tarkasteltiin ensin nykyisiä tietoturvariskejä, joita pienyrittäjät kohtaavat. Tämän pohjalta luotiin yksityiskohtaisia tarkistuslistoja. Listat kattavat olennaiset osa-alueet, kuten tietokoneiden ja verkon suojaamisen, vahvan salasanasuojauksen, päivitysten säännöllisen tarkistamisen ja varmuuskopiointivälit.

Tarkistuslistan avulla saatiin aikaiseksi konkreettinen työkalu, joka on käytännönläheinen ja helposti sovellettava. Se tarjoaa selkeät ohjeistukset, jotka auttavat yrittäjää parantamaan yrityksensä turvallisuutta.

Työn tuloksena voidaan päätellä, että tietoturvan parantaminen on mahdollista selkeiden ja käytännöllisiä ohjeiden avulla. Jatkossa työtä voidaan laajentaa kattamaan muitakin yritystoiminnan osa-alueita, ja tarkistuslistaa voidaan päivittää vastaamaan uusia tietoturvariskejä. Tämä työ edistää tietoisuutta tietoturvasta ja tarjoaa resursseja, jotka auttavat vahvistamaan digitaalista turvallisuutta.

Asiasanat:

tietoturva, kyberturvallisuus, atk, riskienhallinta

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Business Information Technology

2024 | 34 pages

Osasumwen Ehirhieme

Small Business Owner’s Checklist for Working Securely

The digitalization of businesses increases challenges in cybersecurity, and many entrepreneurs need clear guidelines to improve their company’s security.

This thesis focuses on supporting the secure operation of a small accounting firm by creating a practical checklist for this purpose. The aim was to provide a practical and easily applicable tool that helps entrepreneurs improve cybersecurity in their business environment.

To achieve the purpose of this thesis, current cybersecurity risks that small business owners face were first examined. Based on these, a detailed checklist was created, covering essential areas such as computer and network protection, strong password protection, regular checking of updates, and backup intervals.

In conclusion, it can be inferred that improving cybersecurity is possible with clear and practical guidelines. In the future, these guidelines can be expanded to cover other areas of business operations, and the checklist can be updated to meet new cybersecurity risks. This thesis promotes awareness of cybersecurity and provides resources that help strengthen digital security.

Keywords:

Cybersecurity, Digital security, IT, Risk management

Sisältö

Liitteet

Kuvat

Taulukot

Käytetty sanasto

DDoS-hyökkäys	Distributed Denial of Service -hyökkäys, on tietoturvahyökkäyksen muoto, jossa useat tietokonejärjestelmät hyökkäävät yhdessä koordinoidusti yhtä tai useampaa kohdetta vastaan Internetissä. Hyökkäyksen tavoitteena on ylikuormittaa kohdejärjestelmän verkkoliikenne tai resurssit, jolloin oikeat käyttäjät eivät pääse käyttämään sitä normaalisti. (Osanaiye ym., 2016, 148–150.)
Mikroyritys	Mikroyritys määritellään yritykseksi, jonka palveluksessa on vähemmän kuin 10 työntekijää. Lisäksi vuodesta 2003 alkaen: jonka vuosiliikevaihto on enintään 2 miljoonaa euroa tai taseen loppusumma enintään 2 miljoonaa euroa. (Tilastokeskus s.a.)
PK-yritys	Pienet ja keskisuuret yritykset ovat yrityksiä, joiden työntekijöiden lukumäärä on alle 250 henkeä ja joiden liikevaihto on alle 50 miljoonaa euroa. (Tilastokeskus s.a)
RaaS	(Ransomware as a Service) haittaohjelma, jossa ammattimaisesti toimiva kyberrikollinen tarjoaa valmista haittaohjelmaa ja -infrastruktuuria muiden käyttöön maksua vastaan. (Kyberturvallisuuskeskus 2024b)
SaaS	(Software as a Service) tarkoittaa ohjelmiston jakelumallia, jossa palvelun tarjoaja ylläpitää sovellusohjelmistoa palvelimillaan ja tarjoaa palvelua asiakkaille internetin välityksellä. (Wikipedia 2023)

1 Johdanto

Tietoturva on kriittinen osa yrityksen toiminnassa ja sen huomioiminen on olennainen osa yrityksen riskienhallintaa ja liiketoiminnan jatkuvuuden varmistamista.

Tämän opinnäytetyön toimeksiantaja on Case Mikroyritys, jonka tavoitteena on parantaa tietoturvaansa ja suojata arkaluontoisia tietoja nykypäivän digitaalisessa ympäristössä.

Tarkasteltavan mikroyrityksen alueen yrittäjille ei ole tarjolla tietoturvakoulutusta tai vastaavaa, jolla yrittäjät ymmärtäisi ajankohtaiset tietoturvahaasteet ja -riskit. Tämä on huolestuttavaa, koska yrittäjät, jotka eivät ole tietoisia ajankohtaisista tietoturvahaasteista ja -riskeistä, voivat joutua kohtaamaan tietoturvauhkia. Näiden tiedostamattomuus voi aiheuttaa merkittäviä häiriöitä yrityksen toiminnalle ja jopa uhata sen olemassaoloa. Tietoturvaloukkaukset voivat vahingoittaa yrityksen mainetta ja asiakkaiden luottamusta, mikä voi johtaa asiakaskatoon ja taloudellisiin menetyksiin.

Opinnäytetyön tarkoituksena on analysoida, mitkä tietoturvakäytännöt ja -toimenpiteet soveltuvat parhaiten Case Mikroyrityksen tietoturvan parantamiseen. Työn tavoitteena on luoda yksilöllinen tarkistuslista, joka auttaa Case Mikroyritystä ylläpitämään tietoturvallista työympäristöä. Opinnäytetyön tuloksia käytetään Case Mikroyrityksen tietoturvakäytäntöjen kehittämiseen ja parantamiseen.

Työn teoriaosuudessa tarkastellaan erilaisia tietoturvauhkia, kuten kiristyshaittaohjelmia, palvelunestohyökkäyksiä, hakkeriaktivismia, esineiden internetiä (IoT) ja sosiaalista manipulointia. Työssä käsitellään myös kansainvälisiä tietoturvastandardeja, kuten ISO 27001, ja niiden soveltamista pienyrityksiin.

Opinnäytetyön soveltavassa osuudessa tarkastellaan Case Mikroyrityksen nykyistä tietoturvaympäristöä mukaan lukien sen käyttämät järjestelmät, ohjelmistot ja tietoturvatoimenpiteet. Tämän perusteella tunnistetaan yrityksen tietoturvauhat ja haasteet sekä kehitetään yksilöllinen tarkistuslista, joka auttaa yritystä parantamaan tietoturvaa ja suojaamaan sen tärkeitä tietoja.

Opinnäytetyön tarkoituksena on luoda Case Mikroyritykselle konkreettisia työkaluja ja ohjeita, jotka auttavat sitä ymmärtämään ja hallitsemaan tietoturvahaasteitaan tehokkaasti. Työ perustuu laajaan kirjallisuuskatsaukseen sekä käytännön esimerkkeihin, jotka on räätälöity Case Mikroyrityksen tarpeisiin. Opinnäytetyössä on mahdollista soveltaa teoreettista tietoa käytännön haasteisiin ja kehittää ratkaisuja todellisiin tietoturvaongelmiin.

2 Kirjallisuuskatsaus

Tässä luvussa käydään läpi pienyritysten kohtaamia uhkia sekä yrityksille luotuja standardeja. Lisäksi tarkastellaan ISO 27001-standardin soveltamista pienyrityksiin ja kybervakuutusten merkitystä ja tarpeellisuutta.

2.1 Pienyritysten tietoturvahaasteet

Verkko on muodostunut liiketoiminnan ja yhteiskunnallisten toimintojen keskeiseksi tekijäksi. Tämä globaali ympäristö edellyttää uudistettuja tapoja rakentaa luottamusta eri toimijoiden kesken. (Kyberturvallisuuskeskus, 2019.)

Mikroyritykset muodostavat suuren osan Suomen taloudesta ja toimivat täten talouden selkärankana (Taulukko 1) ja edustavat merkittävää osuutta työllisyydestä ja innovaatioista. Kuitenkin kyberturvallisuuden kehityksessä mikroyritysten erityistarpeet jäävät usein vähemmälle huomiolle, vaikka ne muodostavat suurimman osan kaikista yrityksistä (Ncubukezi ym. 2020). Tämä luo tarpeen räätälöidylle lähestymistavalle, jossa tietoturvapolitiikka ja -toimenpiteet mukautetaan vastaamaan mikroyritysten tarpeita ja resursseja.

Taulukko 1. Yritykset toimialoittain ja henkilöstön suuruusluokittain (Tilastokeskus 2022)

	Yritysten lukumäärä, yritykset	Liikevaihto, yritykset (1000 euroa)
2022		
0 - 4 henkeä	533 811	68 271 262
5 - 9 henkeä	17 728	30 092 376
10 - 19 henkeä	10 021	35 903 681
20 - 49 henkeä	6 380	55 893 207
50 - 99 henkeä	2 106	53 747 790
100 - 249 henkeä	1 027	58 783 005
250 - 499 henkeä	369	46 678 924
500 - 999 henkeä	176	47 949 847
1 000 henkeä tai enemmän	124	158 633 148

2.2 Tietoturvahaasteiden yleiset piirteet

Kyberturvallisuus on muodostumassa yhä tärkeämmäksi aiheeksi yrityksille ympäri maailmaa, kun tietomurtojen taloudelliset ja maineeseen liittyvät kustannukset aiheuttavat merkittäviä haasteita valmistautumattomille yrityksille. Teknologia auttaa organisaatioita optimoimaan toimintojaan monin innovatiivisin keinoin, mutta samalla

yritysten on käsiteltävä kasvavaa määrää kyberturvallisuusuhkia. (Kyberturvallisuuskeskus, 2020.)

2.2.1 Kiristyshaittaohjelmat

Kiristyshaittaohjelmat ovat kasvattaneet suosiotaan huomattavasti: pelkästään Yhdysvalloissa tämän tyyppiset kyberhyökkäykset lisääntyivät 200 % vuosien 2019 ja 2021 välillä. Tämä hyökkäystapa on peräisin 1980-luvulta, mutta siitä tuli merkittävä uhka yrityksille 2010-luvulla kryptovaluutan nousun myötä, joka on rikollisten suosima maksutapa. (Leo ym., 2022.)

Kiristyshaittaohjelmat estävät tyypillisesti käyttäjiä pääsemästä käsiksi tärkeään tietoon ja dataan tietokoneillaan tai verkoissaan, kunnes maksu suoritetaan. Kyberrikolliset eivät aina kuitenkaan vapauta laitteita lunnaiden maksamisen jälkeen ja yrittävät usein kiristää uhreiltaan vielä enemmän rahaa. (Leo ym., 2022.)

2.2.2 Hajautetut palvelunestohyökkäykset (DDoS)

DDoS-hyökkäys (Distributed Denial of Service) on tietoturvahyökkäyksen muoto, jossa useat tietokonejärjestelmät hyökkäävät yhdessä koordinoidusti yhtä tai useampaa kohdetta vastaan Internetissä. Hyökkäyksen tavoitteena on ylikuormittaa kohdejärjestelmän verkkoliikenne tai resurssit, jolloin oikeat käyttäjät eivät pääse käyttämään sitä normaalisti. (Osanaiye ym., 2016.)

DDoS-hyökkäyksen vaikutus voi olla laaja, aiheuttaen esimerkiksi verkkosivustojen kaatumisen tai verkkopalveluiden hidastumisen. Tämä voi johtaa merkittäviin taloudellisiin menetyksiin ja mainehaittoihin kohdeorganisaatiolle. (Osanaiye ym., 2016.)

2.2.3 Hakkeriaktivismi

Kaikki kyberrikolliset eivät ole voittoihin suuntautuneita, ja hakkeriaktivismin nousu tarkoittaa, että yhä useampi ihminen murtautuu tietojärjestelmiin poliittisista tai sosiaalisista syistä. Nämä hyökkäykset voivat olla jopa vahingollisempia kuin perinteiset uhat, koska hakkeriaktivistit yrittävät usein tuoda kantansa esille, joten heidän ponnistelunsa ovat yleensä hyvin julkisesti vahingollisia organisaation maineelle.
Hakkeriaktivismi on tärkeä tutkimusalue, koska hakkeriryhmien hyökkäyssuunnitelmat ja -toteutukset ovat yhä useammin perusteltuja sosiaalisten, poliittisten, taloudellisten ja kulttuuristen (SPEC) konfliktien kautta. (PytlikZillig ym., 2014.)

2.2.4 Esineiden internet (IoT)

Internetin käyttö on nykyään kasvamassa työkaluna sen rajattomien hyötyjen ja sovellusten vuoksi. Nykypäivänä tiedot kulkevat näiden viestintäverkkojen kautta internetissä. Internet of Things (IoT) eli esineiden internet on nykyään kaikista verkostoista laajimmin käytetty. IoT on internetiä käyttävien laitteiden välinen yhteys, joka mahdollistaa tietojen jakamisen. Nämä laitteet voivat olla pieniä kotitaloustavaroita tai suuria teollisuuskoneita, jotka kommunikoivat keskenään toimintojensa suorittamiseksi. IoT-laitteita voidaan käyttää esimerkiksi esineiden seurantaan, koneiden suorituskyvyn monitorointiin, pankkisiirtoihin sekä teollisiin tehtäviin. Vuoden 2020 loppuun mennessä maailmassa oli käytössä 90 miljoonaa laitetta. Teollisuus- ja terveyssektori ovat IoT-laitteiden suurimmat käyttäjät. Laitteet ovat laajimmin käytössä älykaupungeissa, ympäristön seurannassa, terveydenhuollossa, kaupankäynnissä, varastonhallinnassa ja liikkeenjohdossa. (Majeed ym., 2021.)

IoT-laitteiden suurin ongelma on niiden turvallisuus ja yksityisyys. Turvallisuus tarkoittaa valtuutettua pääsyä tietoihin ja suojaa luvattomilta käyttäjiltä. Teknologian kehittyessä turvallisuushaasteet kasvavat päivä päivältä. Pilviteknologia on lisännyt luvattoman pääsyn riskejä tietoihin. IoT-verkkoihin liittyvät hyökkäykset sisältävät siirto-protokollakatastrofit, palvelunestohyökkäykset, häirinnän, väärän identiteetin käytön eli spoofingin sekä viestintähyökkäykset. (Majeed ym., 2021.)

Esineiden internetissä piilee myös merkittävä yksityisyyden uhka, koska älylaitteet sisältävät tyypillisesti huomattavan määrän arkaluonteista tietoa, johon kyberrikolliset voivat päästä käsiksi. Julkisten USB-laitteiden käyttöön liittyy myös riskejä. Julkisista USB-latauspisteistä ja -laitteista voi olla mahdollista saada haittaohjelmia, jotka voivat vaarantaa käyttäjän laitteen ja tietojen turvallisuuden. (Brandao & Scanavez, 2021.)

2.2.5 Sosiaalinen manipulointi

Kun kyberturvallisuusteknologia ja ennaltaehkäisevät toimenpiteet muuttuvat monimutkaisemmiksi, rikolliset kääntyvät sosiaalisen manipuloinnin puoleen pyrkiessään ohittamaan tällaiset järjestelmät. (Erbschloe, 2019, 1)

Sosiaalinen manipulointi on erittäin tehokas hyökkäysmenetelmä, jolla toteutetaan yli 80 % kyberhyökkäyksistä. Näissä hyökkäyksissä keskitytään ihmisiin, eikä tietokoneiden tai verkkojen turvallisuuspuutteisiin. Turvallisten kyberjärjestelmien rakentamiseksi on tärkeää suojata paitsi tietokoneet ja verkot, myös kouluttaa käyttäjiä turvallisuuskäytännöistä. Ihmisiin kohdistuvia hyökkäyksiä kutsutaan sosiaaliseksi manipuloinniksi, koska niissä manipuloidaan tai johdatellaan käyttäjiä suorittamaan toivottuja toimintoja tai paljastamaan arkaluontoista tietoa. Yleisimmät sosiaalisen manipuloinnin hyökkäykset yrittävät saada tietämättömiä Internet-käyttäjiä klikkaamaan haitallisia linkkejä. Kohdennetummat hyökkäykset pyrkivät saamaan tietoon salasanoja tai yksityisiä tietoja organisaatioilta, tai varastamaan arvokkaita esineitä yksittäisiltä henkilöiltä. (Erbschloe, 2019, 1–2.)

Hyökkääjät pyrkivät yleensä saamaan ihmiset tekemään haluamiaan toimintoja. Tämän saavuttamiseksi heidän on voitettava uhrin luottamus, joka usein ansaitaan vuorovaikutuksen kautta tai kopioimalla tai varastamalla identiteetti. Riippuen hyökkäyksen monimutkaisuudesta nämä iskut voivat kohdistua yksilöihin, organisaatioihin tai laajoihin väestön osiin. Huijarit käyttävät usein tuttuja yritysnimiä tai teeskentelevät olevansa joku uhrin tuntema. Esimerkiksi vuonna 2018 tapahtuneessa tosielämän tapauksessa hyödynnettiin Netflixin nimeä. Netflixin nimellä lähetetyssä sähköpostiviestissä väitettiin, että käyttäjän tilaus oli keskeytetty, koska Netflixillä oli ongelmia nykyisten maksutietojen kanssa, ja käyttäjää kehotettiin päivittämään maksutapansa klikkaamalla linkkiä. (Erbschloe, 2019, 1–2.)

Sosiaalisen manipuloinnin hyökkäykset toimivat, koska käyttäjien on vaikea varmentaa kaikkia vastaanottamiaan viestejä. Lisäksi varmentaminen vaatii teknistä asiantuntemusta, jota useimmilla käyttäjillä ei ole. Ongelmaa pahentaa se, että suuri määrä käyttäjiä pääsee käsiksi arkaluontoisiin tietoihin, mikä luo laajan hyökkäyspinnan. Yksilöiden suostuttelu arkaluontoisten tietojen paljastamiseen ja niiden käyttäminen ilkeämielisiin tarkoituksiin on vanha toimintatapa. Sosiaalisen manipuloinnin hyökkäyksiä on esiintynyt Internetin alkuajoista lähtien, mutta ennen Internetin kasvua rikolliset käyttivät puhelinta, postipalvelua tai mainontaa esiintyäkseen luotettavana agenttina tietojen hankkimiseksi. (Erbschloe, 2019, 1–2.)

2.3 Pienyritysten erityishaasteet

Tietoturva on olennainen osa kaikissa yrityksissä ja sen laiminlyönti voi johtaa vakaviin seurauksiin. Kaikilla yrityksillä on riski joutua kyberrikollisuuden kohteeksi, suurempien yritysten alati tiukentuva tietoturva kasvattaa pienempien yritysten riskiä joutua rikollisten tähtäimeen. Isona tekijänä yritysten tietoturvalle on sen henkilöstön asenne tietoturvaa kohtaan. (Vainikka & Paavola, 2013.)
Resurssien rajallisuus, kuten budjetti ja tietoturvaosaaminen, rajoittavat usein tehokkaiden tietoturvaratkaisujen käyttöönottoa. Tämän seurauksena pienyritykset ovat haavoittuvaisia tietoturvauhkille. Nämä haasteet eivät ainoastaan uhkaa yritysten arkaluonteista tietoa vaan myös niiden taloudellista suorituskykyä ja mainetta. (Chidukwani, Zander & Koutsakis, 2022.)

2.4 Kansainväliset standardit

Tietoturvatoimenpiteiden ja -standardien noudattaminen varmistaa, että organisaation turvatoimenpiteet täyttävät sääntelystandardit ja –ohjeistukset (Taulukko 2). Nämä standardit on suunniteltu suojelemaan arkaluontoisten tietojen eheyttä, luottamuksellisuutta ja saatavuutta erilaisilta kyberuhilta. (Kyberturvallisuuskeskus, 2019.)

Taulukko 2. Viralliset standardointiorganisaatiot (Kyberturvallisuuskeskus, 2019)

	Sähköala	Yleinen standardointi	Teleala
Maailmanlaajuinen taso	IEC International Electrotechnical Commission	ISO International Organization for Standardization	ITU International Telecommunication Union
Eurooppalainen taso	CENELEC European Committee for Electrotechnical Standardization	CEN European Committee for Standardization	ETSI European Telecommunications Standards Institute
Kansallinen taso	SESKO	SFS Suomen Standardisoimis-liitto SFS toimiala-yhteisöineen	Liikenne- ja viestintä-virasto

Arkaluontoisten tietojen suojaamiseksi potentiaalisilta tietomurroilta on toteutettava tiettyjä turvatoimia ja -kontrolleja. Näihin toimenpiteisiin kuuluvat palomuurit, salausprotokollat, säännölliset ohjelmistopäivitykset sekä toistuvat auditoinnit ja arvioinnit. Yhdessä nämä prosessit varmistavat, että turvatoimet toimivat asianmukaisesti ja että organisaatio täyttää sääntelyvaatimuksensa. (Kyberturvallisuuskeskus, 2019.)

Maailmassa on monia erilaisia standardeja ja ohjeistuksia, mutta tässä kappaleessa käymme läpi eurooppalaisia tietosuojasäädöksiä ja kyberturvallisuuden noudattamisen viitekehyksiä, joista organisaatioiden tulisi olla tietoisia tehokkaan tietosuojan ja kyberturvallisuuskäytäntöjen varmistamiseksi. (Kyberturvallisuuskeskus, 2019)

2.4.1 GDPR (General Data Protection Regulation) ja Tietosuojalaki 2018

GDPR on EU:n asetus, joka on keskeinen henkilötietojen suojan ja yksityisyyden kannalta. Se vaatii organisaatioita toteuttamaan tiukkoja kyberturvatoimenpiteitä, kuten tietojen salauksen, käyttöoikeuksien hallinnan ja tietomurtoilmoitusmenettelyt EU:ssa asuvien henkilöiden henkilötietojen suojelemiseksi. (Tankard, 2016.)

Loppuvuodesta 2018 Tämä erityislaki sisältää GDPR:n ja lisää säännöksiä henkilötietojen käsittelystä ja suojasta. Se korostaa GDPR:n mukaisia tiukkoja kyberturvatoimenpiteitä. (Heikkinen, 2019.)

2.4.2 Verkko- ja tietoturvadirektiivi (NIS2)

Verkko- ja tietoturvadirektiivi (NIS2) laajentaa ja syventää aiempaa EU:n kyberturvallisuusdirektiiviä, NIS:iä (Network and Information Security). Se velvoittaa kriittisen infrastruktuurin ja olennaisten palvelujen tarjoajat toteuttamaan

turvatoimenpiteitä ja raportoimaan tapahtumista viranomaisille. NIS2 laajentaa turvavaatimusten ja sen kattamien sektoreiden soveltamisalaa, keskittyen toimitusketjun turvallisuuteen ja tiukempien toimenpiteiden ja sanktioiden käyttöönottoon Euroopassa. (Pier, 2022.)

2.4.3 Kyberturvallisuuden viitekehykset

Kyberturvallisuuden noudattamisen toteuttamiseksi erilaiset viitekehykset luovat rakenteellisia lähestymistapoja:

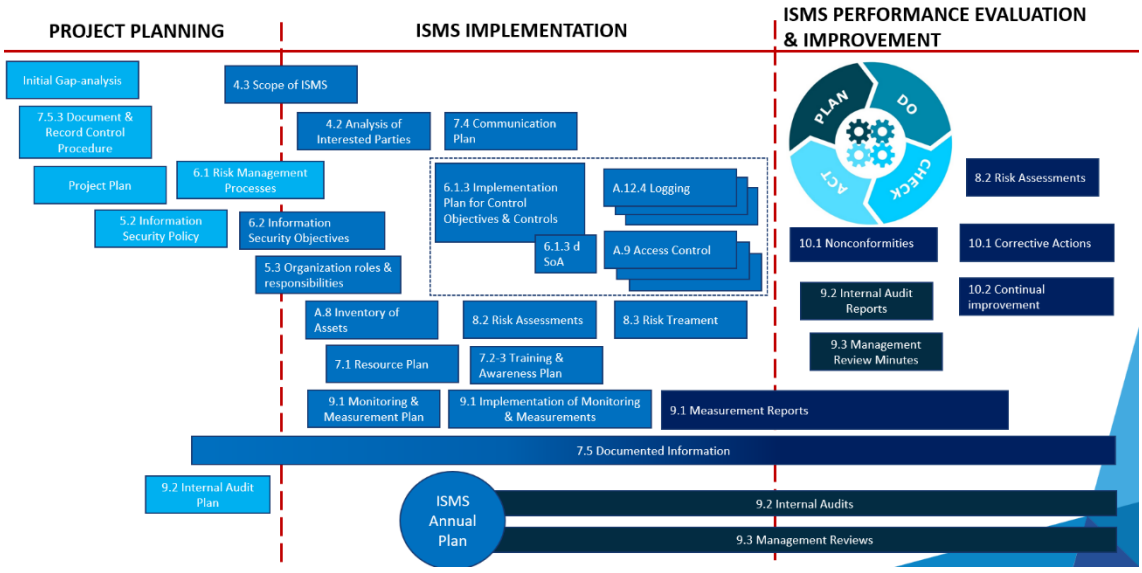
- CIP-007-6: NERC:n (North American Electric Reliability Corporation) standardi kriittisen infrastruktuurin suojaukseen suurjärjestelmien turvallisuuden hallinnassa.
- NIST (National Institute of Standards and Technology) kyberturvallisuuskehys: Tarjoaa ohjeita riskiperusteiseen lähestymistapaan kyberuhkien tunnistamisessa, suojauksessa, havaitsemisessa, vastaamisessa ja toipumisessa.
- ISO 27001: Tarjoaa systemaattisen lähestymistavan tietoturvariskien hallintaan ja organisaation tietoturvan hallintajärjestelmän jatkuvaan parantamiseen.
- CIS (Center for Internet Security) Controls: priorisoitu parhaiden käytäntöjen joukko, joka parantaa organisaation kyberturvallisuusasemaa.
- COBIT (Control Objectives for Information Technologies): Tietotekniikan prosessien hallinnan ja johtamisen viitekehys, joka tarjoaa kattavan joukon ohjausmekanismeja ja mittareita kyberturvallisuuden noudattamiseen.
- SOC 2 (Service Organization Control Type 2): Tietoturvan, saatavuuden, käsittelyn eheyden, luottamuksellisuuden ja tietojen yksityisyyden painottava palveluorganisaatioiden auditointistandardi.
- Näiden säädösten ja viitekehysten ymmärtäminen ja noudattaminen on tärkeää organisaatioille tietomurtojen ja kyberhyökkäysten torjumiseksi sekä lainsäädännöllisten vaatimusten täyttämiseksi. (Pier, 2022.)

2.5 ISO 27001 -standardin soveltaminen pienyrityksiin

Kansainvälisesti käytetty ISO 27001 -standardi, joka on kansainvälisesti tunnustettu tietoturvan hallintajärjestelmän ISMS (Information Security Management System) standardi, voi olla haastava ja mahdollisesti vähemmän hyödyllinen mikroyrityksille useista syistä:

- Kustannukset ja resurssit: ISO 27001 -sertifiointiprosessi voi olla kallis, ja sen ylläpitäminen vaatii jatkuvia investointeja. Mikroyrityksillä ei välttämättä ole taloudellisia tai henkilöstöresursseja sertifiointiprosessin ja sen jälkeisen ylläpidon hallintaan.

- Monimutkaisuus: ISO 27001 on laaja ja monimutkainen standardi, joka vaatii kattavaa dokumentointia ja tiukkojen prosessien noudattamista. (Kuva 1) Mikroyritykset, joilla on rajoitetut IT- ja tietoturva-asiantuntijat, voivat kokea tämän ylivoimaiseksi.
- Ylimitoitetut vaatimukset: Standardin vaatimukset on suunniteltu laaja-alaisesti ja ne voivat olla ylimitoitettuja pienille yrityksille, joiden tietoturvatarpeet ovat usein yksinkertaisempia kuin suurilla organisaatioilla.
- Joustamattomuus: Mikroyritykset saattavat tarvita enemmän joustavuutta toimintatavoissaan ja päätöksenteossaan. ISO 27001:n tiukat säännöt ja rakenteet voivat rajoittaa tätä joustavuutta.
- Liiketoiminnan painopisteet: Mikroyritykset keskittyvät usein ensisijaisesti kasvuun ja elinkelpoisuuteen, ja ne voivat nähdä tietoturvan vähemmän kriittisenä aspektina, varsinkin jos ne eivät käsittele suuria määriä arkaluontoista tietoa.
- Vaihtoehtoiset ratkaisut: Pienemmät yritykset voivat hyötyä enemmän yksinkertaisemmista ja kustannustehokkaammista tietoturvatoimenpiteistä tai kevyemmistä standardeista, jotka ovat paremmin sovitettavissa heidän tarpeisiinsa ja resursseihinsa. (Kyberturvallisuuskeskus, 2019.)

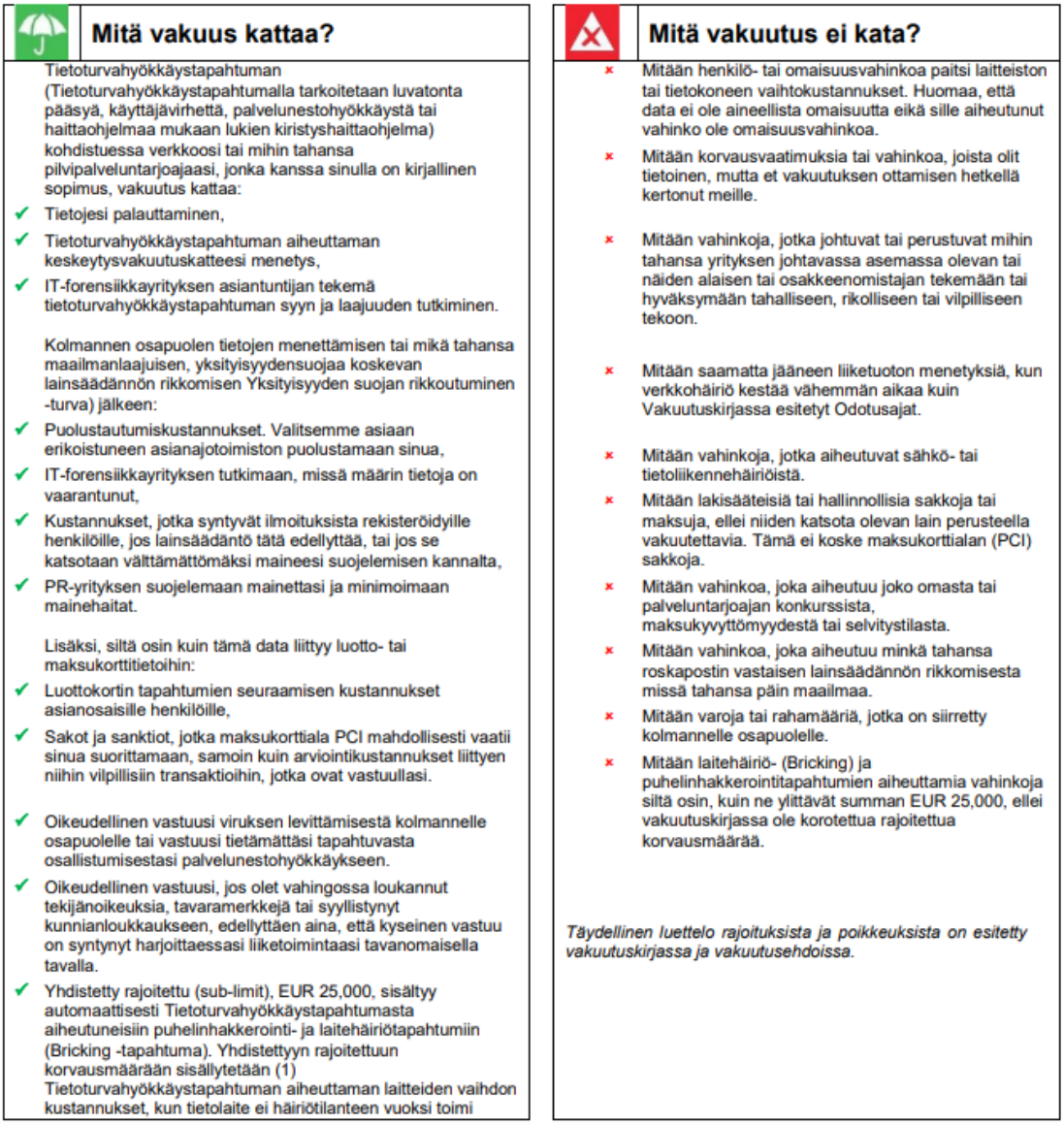


Kuva 1. Esimerkki ISO 27001 -projektin tehtävistä (Tolonen & Vepsäläinen, 2021)

2.6 Pienyritysten kybervakuutukset

Kybervakuutukset, jotka on suunniteltu suojaamaan yrityksiä kyberuhkilta ja tietoturvahäiriöiltä, eivät välttämättä ole parhaita ratkaisuja mikroyrityksille useista syistä:

- Kustannukset suhteessa hyötyihin: Kybervakuutusten hankkiminen voi olla kallista, erityisesti pienille yrityksille, jotka toimivat rajoitetulla budjetilla. Mikroyritysten on punnittava vakuutuksen kustannuksia suhteessa potentiaalisiin hyötyihin, jotka saattavat olla rajalliset niiden pienemmän toiminnan ja riskialttiuden vuoksi.
- Vakuutuksen kattavuus: Kybervakuutukset on suunniteltu usein laajempia organisaatioita silmällä pitäen, ja niiden kattavuus ei välttämättä vastaa mikroyritysten erityistarpeita. Vakuutus saattaa kattaa vain tiettyjä uhkia tai jättää huomioimatta pienille yrityksille kriittisiä riskejä.
- Vakuutusehtojen ymmärtäminen: Kybervakuutusehtojen ymmärtäminen ja arvioiminen voi olla haasteellista, erityisesti jos yrityksellä ei ole asiantuntemusta kyberuhista ja tietoturvasta. Tämä voi johtaa siihen, että mikroyritykset eivät täysin ymmärrä, mitä he ovat ostamassa tai miten vakuutus toimii vahingon sattuessa (Kuva 3).
- Ennaltaehkäisevien toimien puute: Vaikka kybervakuutukset voivat tarjota taloudellista turvaa tietoturvahäiriöiden jälkeen, ne eivät korvaa ennaltaehkäiseviä tietoturvatoimenpiteitä. Mikroyritysten tulisi keskittyä ensisijaisesti riskienhallintaan ja tietoturvan parantamiseen, mikä voi olla kustannustehokkaampi tapa suojautua kyberuhilta.
- Riippuvuus kolmansista osapuolista: Vakuutukset saattavat johtaa siihen, että yritykset luottavat liikaa kolmansien osapuolien tarjoamaan suojaukseen, sen sijaan, että kehittäisivät omaa tietoturvakulttuuriaan ja -käytäntöjään.
- Vakuutuskorvausten saaminen: Korvausten saaminen vakuutusyhtiöltä voi olla monimutkainen ja aikaa vievä prosessi. Joissakin tapauksissa vakuutusyhtiöt saattavat kieltäytyä maksamasta korvauksia tietyissä olosuhteissa tai jos yritys ei ole noudattanut kaikkia turvallisuusvaatimuksia.
- Vaikka kybervakuutukset voivat olla hyödyllisiä tietyissä tilanteissa, mikroyritysten on tärkeää arvioida huolellisesti niiden tarpeita ja riskejä sekä keskittyä ensisijaisesti vahvaan tietoturvapolitiikkaan ja -käytäntöihin. (Muhammad & Straub, s.a.)



Mitä vakuus kattaa?

Tietoturvahyökkäystapahtuman (Tietoturvahyökkäystapahtumalla tarkoitetaan luvatonta pääsyä, käyttäjävirhettä, palvelunestohyökkäystä tai haittaohjelmaa mukaan lukien kiristyshaittaohjelma) kohdistuessa verkkoosi tai mihin tahansa pilvipalveluntarjoajaasi, jonka kanssa sinulla on kirjallinen sopimus, vakuutus kattaa:

- ✓ Tietojesi palauttaminen,
- ✓ Tietoturvahyökkäystapahtuman aiheuttaman keskeytysvakuutuskatteesi menetys,
- ✓ IT-forensiikkayrityksen asiantuntijan tekemä tietoturvahyökkäystapahtuman syyn ja laajuuden tutkiminen.

Kolmannen osapuolen tietojen menettämisen tai mikä tahansa maailmanlaajuisen, yksityisyydensuojaa koskevan lainsäädännön rikkomisen Yksityisyyden suojan rikkoutuminen -turva) jälkeen:

- ✓ Puolustautumiskustannukset. Valitsemme asiaan erikoistuneen asianajotoimiston puolustamaan sinua,
- ✓ IT-forensiikkayrityksen tutkimaan, missä määrin tietoja on vaarantunut,
- ✓ Kustannukset, jotka syntyvät ilmoituksista rekisteröidyille henkilöille, jos lainsäädäntö tätä edellyttää, tai jos se katsotaan välttämättömäksi maineesi suojelemisen kannalta,
- ✓ PR-yrityksen suojelemaan mainettasi ja minimoimaan mainehaitat.

Lisäksi, siltä osin kuin tämä data liittyy luotto- tai maksukorttitietoihin:

- ✓ Luottokortin tapahtumien seuraamisen kustannukset asianosaisille henkilöille,
- ✓ Sakot ja sanktiot, jotka maksukorttiala PCI mahdollisesti vaatii sinua suorittamaan, samoin kuin arviointikustannukset liittyen niihin vilpillisiin transaktioihin, jotka ovat vastuullasi.

- ✓ Oikeudellinen vastuusi viruksen levittämisestä kolmannelle osapuolelle tai vastuusi tietämättäsi tapahtuvasta osallistumisestasi palvelunestohyökkäykseen.
- ✓ Oikeudellinen vastuusi, jos olet vahingossa loukannut tekijänoikeuksia, tavaramerkkejä tai syyllistynyt kunnianloukkaukseen, edellyttäen aina, että kyseinen vastuu on syntynyt harjoittaessasi liiketoimintaasi tavanomaisella tavalla.
- ✓ Yhdistetty rajoitettu (sub-limit), EUR 25,000, sisältyy automaattisesti Tietoturvahyökkäystapahtumasta aiheutuneisiin puhelinhakkerointi- ja laitehäiriötapahtumiin (Bricking -tapahtuma). Yhdistettyyn rajoitettuun korvausmäärään sisällytetään (1) Tietoturvahyökkäystapahtuman aiheuttaman laitteiden vaihdon kustannukset, kun tietolaite ei häiriötilanteen vuoksi toimi

Mitä vakuutus ei kata?

- × Mitään henkilö- tai omaisuusvahinkoa paitsi laitteiston tai tietokoneen vaihtokustannukset. Huomaa, että data ei ole aineellista omaisuutta eikä sille aiheutunut vahinko ole omaisuusvahinkoa.
- × Mitään korvausvaatimuksia tai vahinkoa, joista olit tietoinen, mutta et vakuutuksen ottamisen hetkellä kertonut meille.

- × Mitään vahinkoja, jotka johtuvat tai perustuvat mihin tahansa yrityksen johtavassa asemassa olevan tai näiden alaisen tai osakkeenomistajan tekemään tai hyväksymään tahalliseen, rikolliseen tai vilpilliseen tekoon.

- × Mitään saamatta jääneen liiketuoton menetyksiä, kun verkkohäiriö kestää vähemmän aikaa kuin Vakuutuskirjassa esitetyt Odotusajat.

- × Mitään vahinkoja, jotka aiheutuvat sähkö- tai tietoliikennehäiriöistä.
- × Mitään lakisääteisiä tai hallinnollisia sakkoja tai maksuja, ellei niiden katsota olevan lain perusteella vakuutettavia. Tämä ei koske maksukorttialan (PCI) sakkoja.
- × Mitään vahinkoa, joka aiheutuu joko omasta tai palveluntarjoajan konkurssista, maksukyvyttömyydestä tai selvitystilasta.
- × Mitään vahinkoa, joka aiheutuu minkä tahansa roskapostin vastaisen lainsäädännön rikkomisesta missä tahansa päin maailmaa.
- × Mitään varoja tai rahamääriä, jotka on siirretty kolmannelle osapuolelle.
- × Mitään laitehäiriö- (Bricking) ja puhelinhakkerointitapahtumien aiheuttamia vahinkoja siltä osin, kuin ne ylittävät summan EUR 25,000, ellei vakuutuskirjassa ole korotettua rajoitettua korvausmäärää.

Täydellinen luettelo rajoituksista ja poikkeuksista on esitetty vakuutuskirjassa ja vakuutusehdoissa.

Kuva 1. Dual -kybervakuutus (DUAL 2022)

3 Nykyisten tietoturvariskien tarkastelu

Kyberrikolliset kehittävät jatkuvasti uusia hyökkäystekniikoita ja pienyritykset ovat usein näiden hyökkäysten kohteina. Tässä kappaleessa tarkastellaan ajankohtaisia riskejä ja käydään läpi niiden vaikutuksia pienyrityksiin. Lopuksi käydään läpi mahdollisuuksia löytää ajankohtaista tietoa riskeistä.

3.1 Akira -kiristyshaittaohjelma

Kesäkuussa 2023 Suomessa ensimmäisen kerran havaittu Akira-kiristyshaittaohjelma on ollut erityisen aktiivinen vuoden lopussa, Kyberturvallisuuskeskuksen mukaan. Suurin osa joulukuussa raportoiduista kiristyshaittaohjelmatapauksista liittyi Akiraan, joka aktivoitui usein joulunajan pidempien lomien aikana. (Kyberturvallisuuskeskus, 2024b.)

Akira toimii Ransomware as a Service (RaaS) -mallilla, jossa kyberrikolliset tarjoavat haittaohjelman ja infrastruktuurin muiden käyttöön. Uhkatoimijat ovat taloudellisesti motivoituneita ja valitsevat kohteensa helppouden perusteella. He pyrkivät tutustumaan uhrin organisaatioon lunnasvaatimusten mitoittamiseksi ja neuvottelemaan uhrin kanssa. Monissa tapauksissa uhrin verkkoon on päästy huonosti suojattujen VPN-yhdyskäytävien, erityisesti Ciscon ASA- tai FTD-laitteiden kautta. Kyseisistä laitteista löytyi haavoittuvuus, joka mahdollistaa väsytyshyökkäyksen käytön VPN-tunnusten etsintään. Monivaiheisen tunnistautumisen puuttuminen on ollut riskitekijä. (Kyberturvallisuuskeskus, 2024b.)

Kiristyshaittaohjelmien hyökkäykset ovat korostaneet valmistautumisen ja ennalta mietittyjen toimintatapojen merkitystä. Varmuuskopiot ovat olleet erityisen tärkeitä, sillä hyökkääjät ovat pyrkineet hävittämään ne huolellisesti. Offline-varmuuskopiointi, eli varmuuskopiot, joihin ei ole verkkoyhteyttä, ovat osoittautuneet luotettavaksi suojakeinoksi. Lisäksi Akiraan liittyvät tietovuodot ovat uhka luottamuksellisuudelle, ja kiristäjät käyttävät varastettuja tietoja painostukseen, uhkaamalla niiden julkaisulla. Tietojen varastaminen on erityisen haasteellinen ongelma, koska vuodettua tietoa on vaikea saada täysin takaisin, eikä mikään takaa, että kiristäjät poistaisivat tiedot lunnaiden maksun jälkeen. (Kyberturvallisuuskeskus, 2024b.)

3.2 Tunnusten kalastelu

Kyberturvallisuuskeskus on saanut lukuisia ilmoituksia OmaKanta- ja Suomi.fi -palveluiden nimissä lähetetyistä tietojenkalasteluviesteistä. Nämä viestit ovat esimerkki sosiaalisen manipuloinnin muodosta, jossa rikolliset pyrkivät onkimaan tietoonsa pankkitunnuksia. (Kyberturvallisuuskeskus, 2024c.)

Huijausviesteissä vastaanottajaa kehotetaan päivittämään omat tiedot, ja väitetään, että tämä toimenpide on välttämätön jatkuvan ja parhaan palvelun takaamiseksi. Viesteissä annetaan päivämäärä, jota ennen päivitys on tehtävä, ja viestissä oleva linkki johtaa aidon näköiselle tietojenkalastelusivustolle. Tällaiset hyökkäykset korostavat tarvetta kouluttaa yksilöitä ja yrityksiä tunnistamaan ja torjumaan tietojenkalasteluyritykset. (Kyberturvallisuuskeskus, 2024c.)

Suomi.fi-palvelun nimissä levitetään myös huijausviestejä, joiden mukaan Suomi.fi-mobiilisovelluksessa olisi tekninen virhe, jonka vuoksi palveluun tulevia viestejä voi lukea toistaiseksi huijausviestissä olevan linkin kautta. Tämä on toinen esimerkki siitä, kuinka rikolliset käyttävät sosiaalista manipulointia hyväkseen pyrkiessään kalastelemaan pankkitunnuksia. (Kyberturvallisuuskeskus, 2024c.)

3.3 Hakkeriaktivismi palvelunestohyökkäykset

Palvelunestohyökkäykset ovat yksi merkittävä tietoturvariski, joka on otettava huomioon tietoturvakäytäntöjä suunniteltaessa. Viime aikoina useat kotimaiset organisaatiot ovat joutuneet venäläismielisten haktivistiryhmien palvelunestohyökkäysten kohteiksi. Nämä hyökkäykset ovat kohdistuneet erityisesti kunta- ja koulutussektorin toimijoihin, jotka eivät välttämättä ole aiemmin kohdanneet samankaltaisia tietoturvauhkia. (Kyberturvallisuuskeskus, 2024b.)

Vaikka monet organisaatiot ovat oppineet suojautumaan näiltä hyökkäyksiltä, uudet kohteet voivat olla haavoittuvia, koska ne eivät välttämättä ole varautuneet tällaisiin tietoturvauhkiin. Tämä korostaa tarvetta laaja-alaiselle tietoturvakoulutukselle ja tehokkaille tietoturvakäytännöille, jotka suojaavat organisaatioita erilaisilta tietoturvauhkilta. (Kyberturvallisuuskeskus, 2024b.)

3.4 Esineiden Internet (IoT) -laitteiden tietoturvauudistus

Kyberturvallisuuskeskuksen havaintojen mukaan nykylaitteiden tietoturvaa usein heikentävät oletuksena olevat heikot salasanat, tietoja suojaavan salauksen puuttuminen ja ohjelmistopäivitysten puute. Nämä tekijät korostavat tarvetta tehokkaille tietoturvakäytännöille ja -toimenpiteille. (Kyberturvallisuuskeskus, 2024d.)

EU on tarttunut tähän haasteeseen ja on asettanut pakolliset tietoturvavaatimukset älylaitteille. Nämä vaatimukset koskevat monenlaisia laitteita, kuten internetiin liitettäviä laitteita, leluja, lastenhoitoon liittyviä laitteita ja päälle puettavia laitteita. Tietoturvavaatimukset suojaavat viestintäverkkoja, parantavat käyttäjien yksityisyydensuojaa ja estävät taloudelliseen hyötyyn tähtääviä petoksia. 1.8.2024 alkaen tietoturvavaatimusten vastaiset laitteet voidaan poistaa myynnistä. Tämä tarkoittaa sitä, että valmistajien, maahantuojien ja myyjien on itse varmistettava tuotteidensa tietoturvataso. (Kyberturvallisuuskeskus, 2024d.)

3.5 Ajankohtaiset uhat

Kyberturvallisuuskeskuksen Kybersää (Taulukko 2) on kuukausittainen raportti, jossa käydään läpi viimeisimmän kuukauden aikana tapahtuneet kyberturvallisuuden merkittävimmät ilmiöt. Raportissa tarkastellaan kyberuhkia ja -tapahtumia, ja se sisältää tietoa, jota on jo käsitelty Viikkokatsauksessa. Raportissa kerrotaan kuukauden aikana annetuista varoituksista ja Kyberturvallisuuskeskuksen toimista. (Kyberturvallisuuskeskus, 2024a.)

Kybersään eri osiot käsittelevät:

- Tietomurtoja ja -vuotoja: Käsitellään suojauskeinoja ja tietomurroista sekä -vuodoista havaittuja trendejä. Tietomurrot voivat aiheuttaa merkittävää taloudellista ja mainehaittaa organisaatioille.

- Huijauksia ja tietojenkalastelua: Sisältää erilaisia huijausmenetelmiä, kuten tunnusten kalastelua, laskutuspetoksia ja kiristyksiä.

- Haittaohjelmia ja haavoittuvuuksia: Tarjoaa tietoa alan uusimmista julkaisuista ja havainnoista sekä toimenpidesuosituksia.

- Automaatiota ja IoT:tä: Seuraa alan uutisia ja ilmiöitä sekä niiden vaikutusta esimerkiksi teollisuudessa käytettäviin automaatiojärjestelmiin.

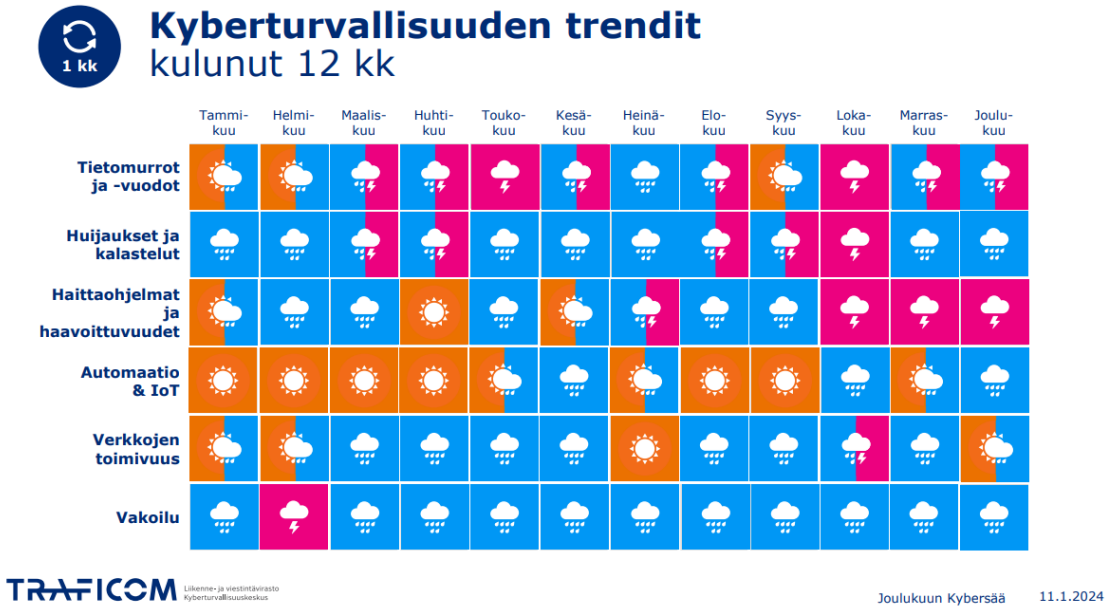
- Verkkojen toimivuutta: Käsitellään viestintäpalveluiden toimivuushäiriöitä ja merkittäviä ICT-palveluiden häiriöitä sekä palvelunestohyökkäyksiä.

- Vakoilua: Keskittyy valtiollisten toimijoiden tai niiden yhteydessä olevien ryhmien kybervakoiluun ja -vaikuttamiseen. (Kyberturvallisuuskeskus 2024a.)

Kybersäässä esiteltävät kuvaajat sekä tilastot julkaistaan 3–6 kuukauden välein. Lisäksi raportissa tarkastellaan ilmiöiden ja toimialojen trendejä, jotka antavat käsityksen ilmiöiden kehityksestä ja kontekstista. Kybersää esittelee myös pidemmän aikavälin kyberilmiöitä ja TOP 5 -uhkia, jotka perustuvat asiantuntijatiimien analyyseihin. Nämä osiot päivitetään säännöllisesti. (Kyberturvallisuuskeskus, 2024a.)

Lopuksi raportissa kerrotaan tietoturva-alan kehityksestä, sääntelystä ja standardeista, jotka ovat olennaisia niin organisaatioiden kuin kuluttajienkin kannalta. (Kyberturvallisuuskeskus, 2024a)

Taulukko 3. Joulukuun Kybersää (Kyberturvallisuuskeskus, 2024a)



4 CASE Mikroyritys

4.1 Tietoja yrityksestä

Opinnäytetyön tarkasteltavana oleva tilitoimisto on pieni, paikallisesti toimiva yritys, joka keskittyy kirjanpito- ja tilinpäätöspalveluihin. Tämä yhden omistajan hallinnoima yritys edustaa tyypillistä mikroyritystä ja sen asiakaskunta koostuu enimmäkseen lähialueen mikro- ja pk-yrityksistä. Yrityksen koko asettaa sille erityisiä tietoturvahaasteita, jotka liittyvät sekä sen toiminnan laajuuteen että rajallisiin resursseihin. Nämä tekijät ovat keskeisiä, kun arvioidaan yleisiä tietoturvallisuuskäytäntöjä ja niiden soveltuvuutta vastaavan kokoisten yritysten kontekstissa.

Tilitoimiston arjessa käytetään Visman toiminnanohjausjärjestelmää, Microsoft Officen tuotteita sekä palkka.fi- ja omavero.fi-palveluita, mikä kuvastaa digitalisaation merkitystä nykyaikaisessa tilitoimistossa. Yrityksellä on yhteistyösopimus ICT-palveluja tarjoavan kumppanin kanssa, joka vastaa muun muassa laitteistosta, teknisestä tuesta, työasematurvasta, Visman palveluista, työasemien varmistuksesta, O365-lisensseistä sekä verkkosivuston ylläpidosta. Yrittäjällä on lisäksi pääsy yhden asiakkaansa NetVisor-järjestelmään. Tärkeää on huomioida, että yrityksen toiminnan luonteen vuoksi yrittäjä ei tarvitse suoraa pääsyä asiakasyritystensä pankkipalveluihin tai tilien tietoihin. Yrittäjän itsensä mielestä tämän tietoturvatietämyksessä olisi parantamisen varaa.

4.2 Tietoturvan nykytila

Tarkasteltavan tilitoimiston tietoturva perustuu vahvasti ulkoistettuihin palveluihin ja nykyaikaisiin ohjelmistoihin. Yrityksen käyttämä Visma Nova-järjestelmä on suunniteltu tarjoamaan keskeytyksetöntä palvelua, johon kuuluu jatkuva valvonta operaatiokeskuksen toimesta, tietojen varmuuskopiointi useampaan sijaintiin sekä ISO 9001 -sertifiointia noudattava kehitys ja ylläpito. Lisäksi asiakasdataan pääsy on rajoitettu vain valtuutetuille henkilöille. (Visma s.a.)

Tämän lisäksi käytössä ovat valtion tarjoamat palkka.fi- ja omavero.fi-verkkopalvelut. Näihin palveluihin kirjautuminen vaatii vahvaa tunnistautumista, jonka avulla kuluttajat voivat turvallisesti vahvistaa henkilöllisyytensä eri palveluissa ja palveluiden tarjoajat voivat tunnistaa asiakkaansa. (Kyberturvallisuuskeskus, 2023c)
Viestinnässä ja toimistotyössä yritys hyödyntää Microsoftin Outlookia ja Exceliä, jotka ovat osa kolmannen osapuolen kautta saatua palvelusopimusta. Sopimus kattaa myös työaseman, joka on hankittu leasing-sopimuksella ja jonka tietoturva on taattu Withsecure-virusturvan sekä rajattoman työasemavarmistuksen kautta. Sähköpostipalvelut ja verkkotunnusten ylläpito hoidetaan kolmannen osapuolen tarjoaman M365 Business Standard -lisenssipaketin avulla.

Asiakasyrityksen NetVisor-ympäristöön kirjautumisessa käytössä on mobiilivarmenne, joka lisää tietoturvan tasoa. Microsoftin palveluihin on asennettuna monivaiheinen

tunnistautuminen (MFA) käyttäen Microsoft Authenticatoria, jolla varmistetaan käyttäjän henkilöllisyys kahdella tai useammalla tunnistautumistavalla. Tämä on tärkeää tilanteessa, jossa rikollinen mahdollisesti saisi tietoonsa käyttäjätunnuksen sekä salasanan. (Kyberturvallisuuskeskus, 2023c.)

Huomionarvoista on, että yrittäjällä ei ole pääsyä asiakkaiden pankkitileille tai -oikeuksiin, mikä vähentää merkittävästi taloudelliseen väärinkäyttöön liittyviä riskejä. Koneen automaattiset päivitykset takaavat järjestelmien ajantasaisuuden ja auttavat suojautumaan uusilta uhilta. Vaikka yrityksellä ei ole kybervakuutusta, sen käyttämät tietoturvatoimenpiteet ja -ohjelmistot tarjoavat perustason suojan ja osoittavat yrittäjän tietoisuuden tietoturvan merkityksestä.

5 Tarkistuslista tietoturvalliseen työskentelyyn

Koska yrityksen tietoturvan tilanne on vahvasti ulkoistettu, keskitytään tämän opinnäytetyön tarkistuslistassa yrittäjän käytäntöihin ja toimenpiteisiin, joilla yrityksen tietoturva säilyy turvattuna.

5.1 Tietokoneiden suojaus

Vaikka yrityksen tietoturva on ulkoistettu kolmannelle osapuolelle, yrittäjän vastuulla on varmistaa, että yhteistyö on saumatonta. Yrittäjän tulee säännöllisesti tarkistaa, että kaikki tietoturvaprotokollat ovat jatkuvasti ajantasaiset. Lisäksi on tärkeää, että yrittäjä ymmärtää vastuunsa tietoturvahäiriöiden raportoinnissa ja ylläpitää avointa kommunikointia palveluntarjoajan kanssa mahdollisten tietoturvaongelmien ehkäisemiseksi. Yksi merkittävä etu tietokoneiden leasingista on se, että palvelulaitteet vaihtuvat säännöllisesti. Tämä takaa, että yritys käyttää aina ajantasaisia laitteita, mikä parantaa tietoturvaa ja tehostaa toimintaa.

5.2 Verkon suojaaminen

Verkon suojaus ja ylläpito on ulkoistettu kolmannelle osapuolelle, on yrittäjällä silti tärkeä rooli tietoturvan ylläpidossa. Yksi tehokas tapa parantaa verkon toimivuutta, nopeutta ja tietoturvaa on reitittimen säännöllinen uudelleenkäynnistys, joka myös tyhjentää reitittimen välimuistin. Tämä on erityisen tärkeää tietoturvan kannalta. Haittaohjelmat voivat tunkeutua reitittimeen ja jäädä huomaamatta, toimien taustalla. Reitittimen uudelleenkäynnistys voi kuitenkin pysäyttää haittaohjelmien toiminnan. On myös suositeltavaa tarkistaa myös muut verkkolaitteet mahdollisten tartuntojen varalta. Reitittimen uudelleenkäynnistys saa aikaan sen, että kaikki reitittimen asetusten muutokset tulevat voimaan kaikissa laitteissa, jotka käyttävät sitä. (Kyberturvallisuuskeskus, 2023a.)

5.3 Päivitysten säännöllinen tarkistaminen

Päivitykset ovat tärkeä osa tietoturvaa, koska ne korjaavat tietoturva-aukkoja ja parantavat ohjelmistojen suorituskykyä. (Kyberturvallisuuskeskus, 2023a)
Tässä tapauksessa päivitykset tulevat automaattisesti kolmannelta osapuolelta, mikä vähentää yrittäjän vastuuta ja työmäärää. Tämä ei kuitenkaan tarkoita, että yrittäjän ei tarvitse olla tietoinen päivitysprosessista. On tärkeää, että yrittäjä ymmärtää päivitysten merkityksen ja pitää yhteyttä palveluntarjoajaan varmistaakseen, että kaikki ohjelmistot ja järjestelmät päivitetään säännöllisesti. Yrittäjän tulisi myös varmistaa, että hän ymmärtää, mitä kukin päivitys tekee, ja että hän seuraa mahdollisia muutoksia, jotka saattavat vaikuttaa yrityksen tietoturvaan tai toimintaan.

5.4 Varmuuskopiointirutiinit

Mikroyrityksen tapauksessa varmuuskopiointi on ulkoistettu kolmannelle osapuolelle, mikä vähentää yrittäjän vastuuta ja työmäärää. On kuitenkin hyvä varmistaa, että varmuuskopiot otetaan sovituin aikavälein ja että yrittäjällä on tarpeen tullessa pääsy varmuuskopioihin.

6 Käytännön soveltaminen

Kuten kirjallisuuskatsauksesta (ks. Luku 2) huomataan, mikroyritykset kohtaavat jatkuvasti muuttuvia uhkia tietoturvassaan.

Tästä syystä opinnäytetyön kohteena oleva yritys hyötyy parhaiten yksilöllisistä tarkastuslistoista, jotka sopivat yrityksen arkeen. Paras tapa on luoda tarkistuslistat/ohjeistukset päivittäisiin sekä kuukausittaisiin toimenpiteisiin. Lisäksi erikoistilanteisiin on hyvä varautua sellaista varten luodulla erikoislistalla.

Yrityksen nykyinen tietoturvatilanne on vahva, mutta jatkuvasti muuttuvassa digitaalisessa ympäristössä on tärkeää olla valppaana ja päivittää tietoturvatoimenpiteitä säännöllisesti.

6.1 Tarkistuslistan luonti

Tarkistuslistan luontiprosessi alkaa yrityksen tietoturvatilanteen kattavalla arvioinnilla (ks. Luvut 4 & 5). Tämä sisältää kaikkien käytössä olevien järjestelmien ja ohjelmistojen tarkastelun, mukaan lukien niiden päivitystilanteen. Tämän jälkeen arvioidaan yrityksen tietoturvariskit ja määritellään toimenpiteet niiden hallitsemiseksi. Tarkistuslistat tullaan luomaan Diagrams.net-sovelluksella jotta tarkistuslistan päivittäminen tulevaisuudessa tulee olemaan helppoa.

Seuraavaksi laaditaan tarkistuslista, joka sisältää kaikki tarvittavat toimenpiteet tietoturvan ylläpitämiseksi. Toiminnot jaetaan sellaisiin, jotka on suoritettava päivittäin, ja sellaisiin, jotka voidaan suorittaa harvemmin. Tämä auttaa yrittäjää keskittymään tärkeimpiin tehtäviin ja varmistamaan, että kaikki tietoturvaan liittyvät tehtävät tulevat hoidetuiksi.

Tarkistuslistan käyttöönotto pitää olla yrittäjälle helposti toteutettava. On tärkeää, että yrittäjä ymmärtää tarkistuslistan merkityksen ja seuraa sitä säännöllisesti. Tarkistuslistan avulla yrittäjä voi helposti seurata yrityksen tietoturvatilannetta ja ryhtyä tarvittaviin toimenpiteisiin mahdollisten tietoturvaongelmien ehkäisemiseksi.

Lopuksi tarkistuslistan luontiprosessi ei ole kertaluonteinen toimenpide. Tietoturva on jatkuvasti muuttuva ala, ja uusia uhkia ilmenee jatkuvasti. Siksi on tärkeää, että tarkistuslista päivitetään säännöllisesti vastaamaan uusia tietoturvariskejä ja -standardeja. Tämä varmistaa, että yrityksen tietoturva pysyy ajan tasalla ja suojaa yrityksen tärkeitä tietoja tulevaisuudessakin.

6.2 Päivittäiset tietoturvatoimenpiteet

Päivittäisiin toimenpiteisiin lisätään asiat, jotka yrittäjän täytyy pitää mielessä päivittäin. Tähän listaan lisätään kohteet, jotka ylläpitävät tietoturvaa sekä vaikuttavat asiakastietojen säilytykseen. Tarkistuslista tulee sisältämään peruskäytäntöjä ovien sekä tietokoneiden lukitsemista, kun toimistolta tai tietokoneen äärestä poistutaan.

Lisäksi listaan lisätään maininnat suojattujen verkkojen tärkeydestä sekä järjestelmien sekä laitteiden päivittämisestä. Listassa on myös hyvä mainita käytäntöjä julkisten latausjohtojen käytöstä. (Liite 2)

6.3 Kuukausittaiset tietoturvatoimenpiteet

Tarkistuslistan luominen alkaa ymmärryksellä yrityksen kuukausittaisista toiminnoista ja niiden tietoturvavaikutuksista. Tämä sisältää kaiken aina reitittimen uudelleenkäynnistämisestä ja tietoturvaskannauksesta sovellusten käyttöoikeuksien tarkistamiseen ja kybersään tarkkailemiseen. Jokainen näistä toiminnoista voi olla mahdollinen tietoturvariski, ja niiden huomioiminen on ensiarvoisen tärkeää.

Tämä lista auttaa yrittäjää pitämään tietoturvan mielessä kuukausittaisissa rutiineissa ja toimii muistutuksena tärkeistä tietoturvakäytännöistä. (Liite 3)

7 Yhteenveto ja johtopäätökset

Tämä opinnäytetyö keskittyi mikro- ja pienyritysten tietoturvahaasteiden tarkasteluun ja käytännön ratkaisujen tarjoamiseen niiden hallintaan. Työn tavoitteena oli ymmärtää pienyritysten ainutlaatuisia tietoturvahaasteita, jotka johtuvat niiden koosta, resurssien rajoituksista sekä erityistarpeista.

Työssä käytiin läpi useita tärkeitä tietoturvariskejä, kuten kiristyshaittaohjelmat, palvelunestohyökkäykset, hakkeriaktivismi, esineiden internet (IoT) ja sosiaalinen manipulointi. On erittäin tärkeää, että mikroyritykset ymmärtävät nämä uhat ja torjuvat niitä tehokkaasti.

Työssä tarkasteltiin myös kansainvälisiä tietoturvastandardeja kuten ISO 27001 ja niiden soveltamista mikroyrityksiin. Vaikka standardeissa on ohjeita tietoturvan hallintaan, työssä korostettiin, että mikroyritysten on mukautettava näitä ohjeita omiin tarpeisiinsa ja resursseihinsa.

Lopuksi työssä luotiin käytännönläheiset ja helposti sovellettavat tarkistuslistat, jotka auttavat yrittäjää parantamaan tietoturvaa liiketoimintaympäristössään.

Johtopäätöksenä voidaan todeta, että pienyritysten tietoturva on monimutkainen ja jatkuvasti muuttuva haaste. Tämä opinnäytetyön tuloksena saatiin käytännön työkaluja, jotka auttavat pienyrityksiä ymmärtämään ja hallitsemaan tietoturvahaasteitaan tehokkaasti. Tulevaisuudessa on tärkeää jatkaa tutkimusta ja kehittämistä tällä alalla, jotta voidaan varmistaa pienyritysten tietoturvan jatkuva parantaminen ja niiden kyky vastata uusiin ja kehittyviin uhkiin.

Lähteet

Brandao, P., & Scanavez, R. 2021. Bad USB: why must we discuss this threat in companies? *RRJ*, *2*(3). Viitattu:10.2.2024 https://doi.org/10.52865/RR/2021-2-3-1

Chidukwani, A.; Zander, S., & Koutsakis, P. 2022. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access. Viitattu: 10.1.2024 https://ieeexplore.ieee.org/abstract/document/9853515

DUAL 2022. Dual kybervakuutus. Viitattu 13.1.2024 https://www.dualfinland.com/sites/g/files/mwfley696/files/inline-files/DUAL%20kybervakuutus%201.4.2022%20IPID_0.pdf

Erbschloe, M. 2019. *Social Engineering : Hacking Systems, Nations, and Societies*. Taylor & Francis Group. Viitattu: 25.1.2024 http://ebookcentral.proquest.com/lib/turkuamk-ebooks/detail.action?docID=5890629

Heikkinen, P. 2019. Tietosuojalaki tuli voimaan vuoden alussa. *Signum*, *52*(1). Viitattu: 25.1.2024 https://journal.fi/signum/article/view/80279

Kyberturvallisuuskeskus 2023a. *Kotiverkon ja reitittimen tietoturva* | *Kyberturvallisuuskeskus*. Viitattu 10.2.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kotiverkon-ja-reitittimen-tietoturva?toggle=K%C3%A4ynnist%C3%A4%20reititin%20uudestaan%20tietyin%20v%C3%A4liajoin

Kyberturvallisuuskeskus 2024a. Kybersää. Viitattu 26.1.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

Kyberturvallisuuskeskus 2023b. Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. Viitattu 5.2.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Kyberturvallisuuskeskus 2019. *Näkökulmia tietoturvan standardointiin ja sertifiointiin*. Traficomin julkaisuja. Viitattu 24.1.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

Kyberturvallisuuskeskus 2024b. *Suomalaiset organisaatiot Akira-kiristyshaittaohjelmien kohteena | Kyberturvallisuuskeskus*. Tietoturva Nyt! Viitattu 26.01.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suomalaiset-organisaatiot-akira-kiristyshaittaohjelmien-kohteena

Kyberturvallisuuskeskus 2020. *Kyberturvallisuus ja yrityksen hallituksen vastuu*. Traficomin julkaisuja. Viitattu 10.2.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Kyberturvallisuuskeskus 2024c. Kyberturvallisuuskeskuksen viikkokatsaus - 06/2024 | *Kyberturvallisuuskeskus*. Tietoturva Nyt! Viitattu 15.2.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-062024

Kyberturvallisuuskeskus 2024d. Älylaitteiden heikko tietoturva sääntelyllä kuriin| *Kyberturvallisuuskeskus*. Tietoturva Nyt! Viitattu 15.2.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/alylaitteiden-heikko-tietoturva-saantelylla-kuriin

Leo, P., Isik, Ö., & Muhly, F. 2022. The Ransomware Dilemma. *MIT Sloan Management Review*, *63*(4). Viitattu 25.1.2024 https://www.proquest.com/scholarly-journals/ransomware-dilemma/docview/2678515108/se-2?accountid=14446

Kyberturvallisuuskeskus 2023c. Sähköinen tunnistaminen. Viitattu 5.2.2024 https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

Majeed, R., Abdullah, N. A., & Mushtaq, M. F. 2021. IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm. *International Journal of Advanced Computer Science and Applications*, *12*(7). Viitattu 25.1.2024 https://www.proquest.com/scholarly-journals/iot-based-cyber-security-drones-using-naïve-bayes/docview/2655113197/se-2?accountid=14446

Muhammad, Z., & Straub, J. s.a. *Telling Small Businesses to Buy Cyber Insurance Isn't Enough*. Viitattu 28.1.2024 https://www.darkreading.com/cyber-risk/telling-small-businesses-to-buy-cyber-insurance-isnt-enough

Ncubukezi, T., Mwansa, L. and Rocaries, F. 2020. A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. IEEE Xplore. Viitattu: 10.1.2024 https://ieeexplore.ieee.org/abstract/document/9351339

Osanaiye, O., Choo, K.-K. R., & Dlodlo, M. 2016. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal*

of Network and Computer Applications, *67*. Viitattu 25.1.2024 https://www.sciencedirect.com/science/article/pii/S1084804516000023

Pier, G. C. 2022. The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law, Computers & Technology*, *36*(2). Viitattu 25.1.2024 https://www.proquest.com/scholarly-journals/iot-new-eu-cybersecurity-regulatory-landscape/docview/2691276073/se-2?accountid=14446

PytlikZillig, L. M., Wang, S., Soh, L.-K., Tomkins, A. J., Samal, A., Bernadt, T. K., & Hayes, M. J. 2014. Exploring Reactions to Hacktivism Among STEM College Students: A Preliminary Model of Hacktivism Support and Resistance. *Social Science Computer Review*, *33*(4), 479–497. Viitattu: 25.1.2024 https://www.proquest.com/docview/2691276073?accountid=14446&sourcetype=Scholarly%20Journals

Tankard, C. 2016. What the GDPR means for businesses. *Network Security*, *2016*(6), 5–8. Viitattu: 25.1.2024 https://www.sciencedirect.com/science/article/pii/S1353485816300563

Tilastokeskus 2022. Yritysten lukumäärä ja liikevaihto henkilöstön suuruusluokan mukaan (kuvio). Viitattu 10.1.2024, StatFin-tietokannasta: https://pxdata.stat.fi/PxWeb/pxweb/fi/StatFin/StatFin__yrti/statfin_yrti_pxt_13w1.px/table/tableViewLayout1/

Tilastokeskus s.a. Käsitteet, PK-yritys. Viitattu 13.1.2024 https://www.stat.fi/meta/kas/pk_yritys.html

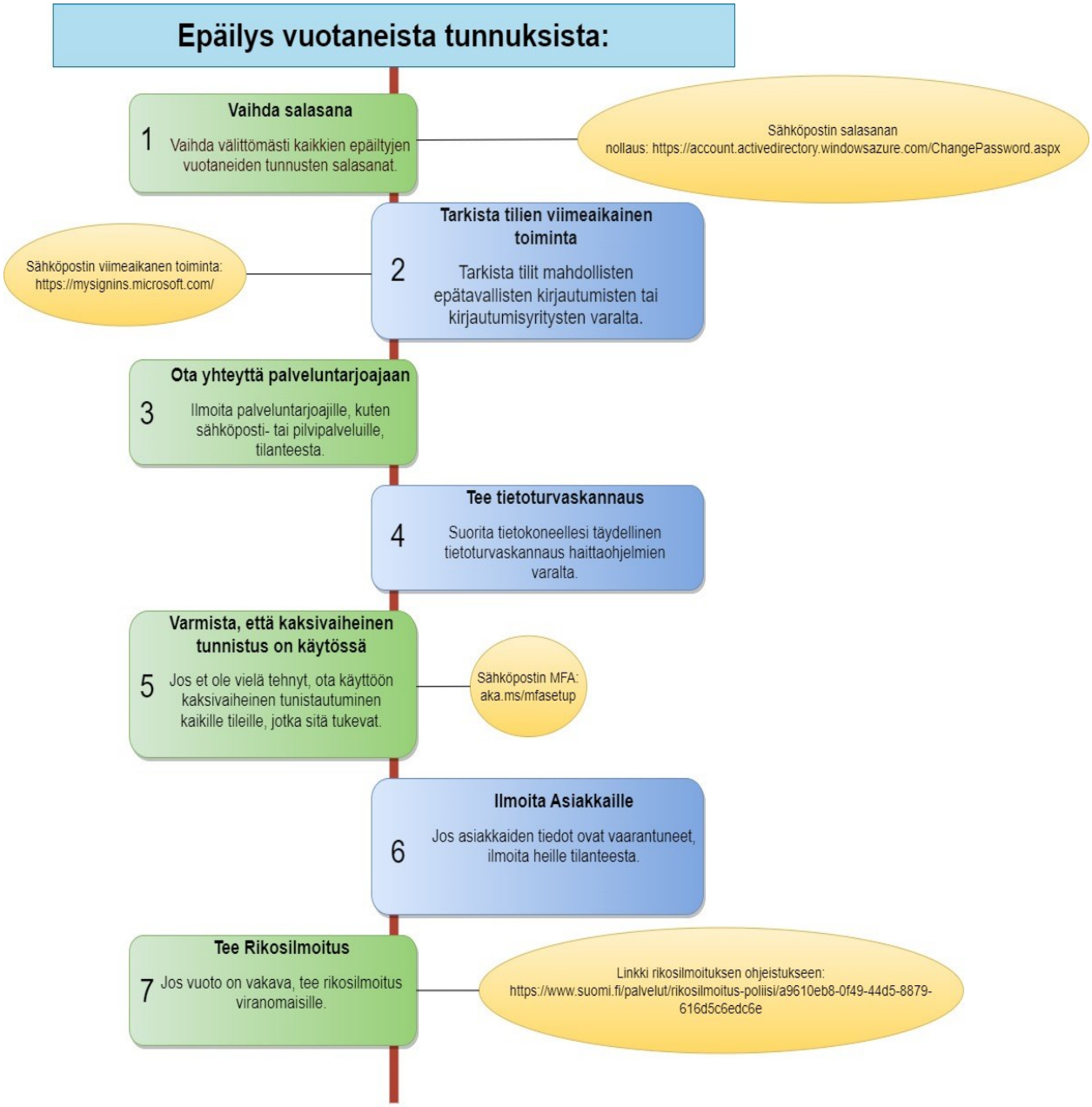
Tilastokeskus s.a. Käsitteet, Mikroyritys. Viitattu 19.1.2024 https://www.stat.fi/meta/kas/mikroyritys.html

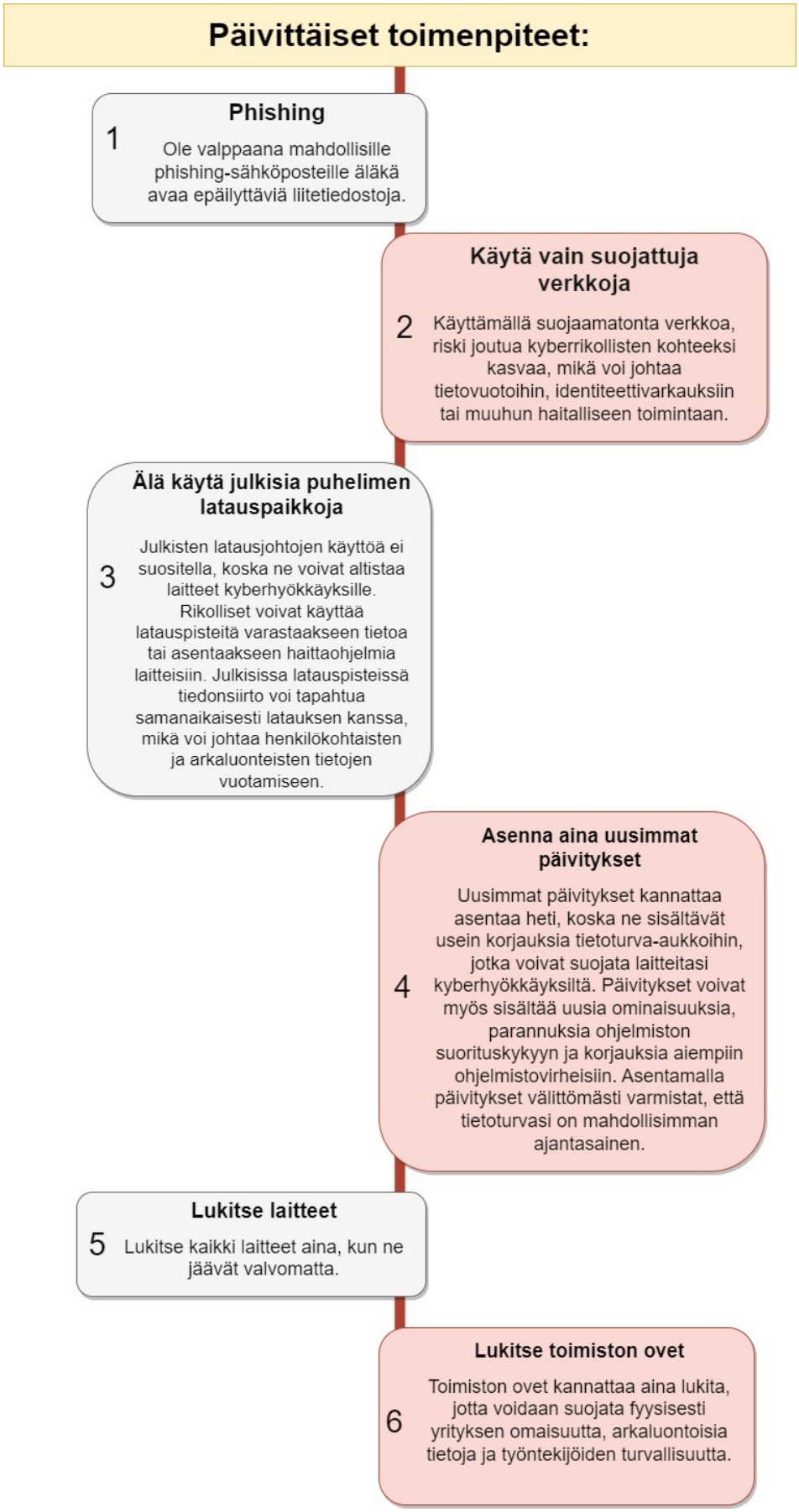
Tolonen, P., & Vepsäläinen, P., 2021. ISO 27001 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄN KYPSYYSARVIOINTI. Viitattu 13.1.2024 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Sote_ISO_27001_Tietoturvallisuuden_hallintaj%C3%A4rjestelm%C3%A4n_kypsyysarviointi_v1.0r1.pptx

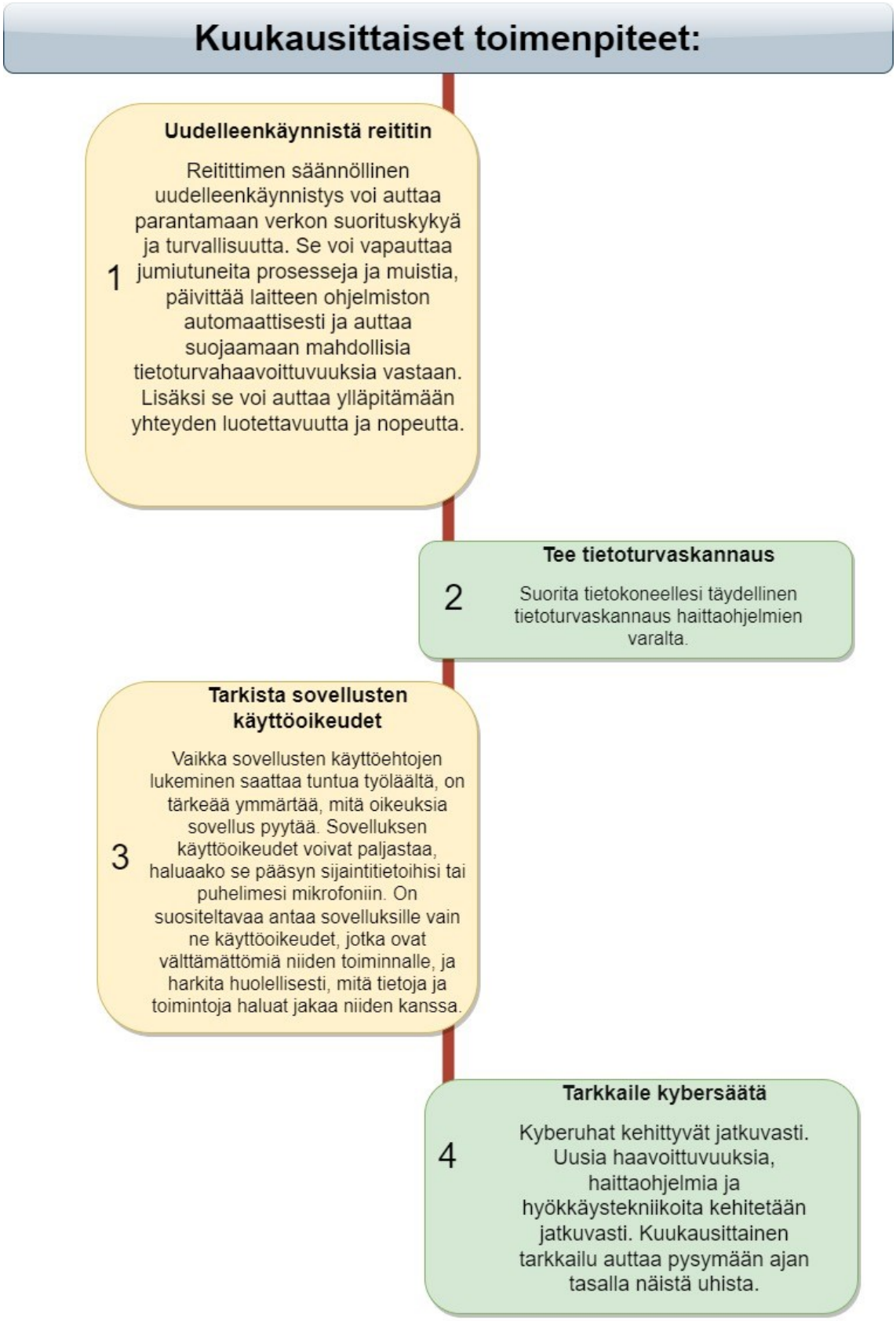
Vainikka, E., & Paavola, J. 2013. Näkökulmia tietoturvaan. *Turun ammattikorkeakoulun raportteja 167*. Viitattu: 15.1.2024 https://julkaisut.turkuamk.fi/isbn9789522163998.pdf

Visma. (s.a). *Turvallinen & luotettava toiminnanohjausjärjestelmä - Visma*. Viitattu: 5.2.2024 https://www.visma.fi/vismanet/tietoturva/

Wikipedia. 2023. SaaS. Viitattu 10.2.2024 https://fi.wikipedia.org/wiki/Software_as_a_Service


Epäilys vuotaneista tunnuksista:
Vaihda salasana
1 Vaihda välittömästi kaikkien epäiltyjen vuotaneiden tunnusten salasanat.
Sähköpostin salasanan nollaus: https://account.activedirectory.windowsazure.com/ChangePassword.aspx
Tarkista tilien viimeaikainen toiminta
2 Tarkista tilit mahdollisten epätavallisten kirjautumisten tai kirjautumisyritysten varalta.
Sähköpostin viimeaikanen toiminta: https://mysignins.microsoft.com/
Ota yhteyttä palveluntarjoajaan
3 Ilmoita palveluntarjoajille, kuten sähköposti- tai pilvipalveluille, tilanteesta.
Tee tietoturvaskannaus
4 Suorita tietokoneellesi täydellinen tietoturvaskannaus haittaohjelmien varalta.
Varmista, että kaksivaiheinen tunnistus on käytössä
5 Jos et ole vielä tehnyt, ota käyttöön kaksivaiheinen tunistautuminen kaikille tileille, jotka sitä tukevat.
Sähköpostin MFA: aka.ms/mfasetup
Ilmoita Asiakkaille
6 Jos asiakkaiden tiedot ovat vaarantuneet, ilmoita heille tilanteesta.
Tee Rikosilmoitus
7 Jos vuoto on vakava, tee rikosilmoitus viranomaisille.
Linkki rikosilmoituksen ohjeistukseen: https://www.suomi.fi/palvelut/rikosilmoitus-poliisi/a9610eb8-0f49-44d5-8879-616d5c6edc6e


Päivittäiset toimenpiteet:
1
Phishing
Ole valppaana mahdollisille phishing-sähköposteille äläkä avaa epäilyttäviä liitetiedostoja.
2
Käytä vain suojattuja verkkoja
Käyttämällä suojaamatonta verkkoa, riski joutua kyberrikollisten kohteeksi kasvaa, mikä voi johtaa tietovuotoihin, identiteettivarkauksiin tai muuhun haitalliseen toimintaan.
3
Älä käytä julkisia puhelimen latauspaikkoja
Julkisten latausjohtojen käyttöä ei suositella, koska ne voivat altistaa laitteet kyberhyökkäyksille. Rikolliset voivat käyttää latauspisteitä varastaakseen tietoa tai asentaakseen haittaohjelmia laitteisiin. Julkisissa latauspisteissä tiedonsiirto voi tapahtua samanaikaisesti latauksen kanssa, mikä voi johtaa henkilökohtaisten ja arkaluonteisten tietojen vuotamiseen.
4
Asenna aina uusimmat päivitykset
Uusimmat päivitykset kannattaa asentaa heti, koska ne sisältävät usein korjauksia tietoturva-aukkoihin, jotka voivat suojata laitteitasi kyberhyökkäyksiltä. Päivitykset voivat myös sisältää uusia ominaisuuksia, parannuksia ohjelmiston suorituskykyyn ja korjauksia aiempiin ohjelmistovirheisiin. Asentamalla päivitykset välittömästi varmistat, että tietoturvasi on mahdollisimman ajantasainen.
5
Lukitse laitteet
Lukitse kaikki laitteet aina, kun ne jäävät valvomatta.
6
Lukitse toimiston ovet
Toimiston ovet kannattaa aina lukita, jotta voidaan suojata fyysisesti yrityksen omaisuutta, arkaluontoisia tietoja ja työntekijöiden turvallisuutta.


Kuukausittaiset toimenpiteet:
Uudelleenkäynnistä reititin
1
Reitittimen säännöllinen uudelleenkäynnistys voi auttaa parantamaan verkon suorituskykyä ja turvallisuutta. Se voi vapauttaa jumiutuneita prosesseja ja muistia, päivittää laitteen ohjelmiston automaattisesti ja auttaa suojaamaan mahdollisia tietoturvahaavoittuvuuksia vastaan. Lisäksi se voi auttaa ylläpitämään yhteyden luotettavuutta ja nopeutta.
Tee tietoturvaskannaus
2
Suorita tietokoneellesi täydellinen tietoturvaskannaus haittaohjelmien varalta.
Tarkista sovellusten käyttöoikeudet
3
Vaikka sovellusten käyttöehtojen lukeminen saattaa tuntua työläältä, on tärkeää ymmärtää, mitä oikeuksia sovellus pyytää. Sovelluksen käyttöoikeudet voivat paljastaa, haluaako se pääsyn sijaintitietoihisi tai puhelimesi mikrofoniin. On suositeltavaa antaa sovelluksille vain ne käyttöoikeudet, jotka ovat välttämättömiä niiden toiminnalle, ja harkita huolellisesti, mitä tietoja ja toimintoja haluat jakaa niiden kanssa.
Tarkkaile kybersäätä
4
Kyberuhat kehittyvät jatkuvasti. Uusia haavoittuvuuksia, haittaohjelmia ja hyökkäystekniikoita kehitetään jatkuvasti. Kuukausittainen tarkkailu auttaa pysymään ajan tasalla näistä uhista.