Tietoturva osana kansainvälisen yrityksen toimintaa

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tieto- ja viestintätekniikka, insinööri (AMK), Riihimäen kampus

Syksy 2021

Juuso Toivonen

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka, insinööri (AMK) Tiivistelmä

Riihimäen kampus

Tekijä Juuso Toivonen Vuosi 2021

Työn nimi Tietoturva osana kansainvälisen yrityksen toimintaa

Ohjaajat Marko Grönfors, Teemu Similä

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli kartoittaa kansainvälisen yrityksen henkilöstön näkemystä tietoturvallisesta toiminnasta ja sen toteuttamiseen käytettävistä tekniikoista. Työn toimeksiantajana toimi Koskisen Oy, jonka koko henkilöstölle oli opinnäytetyöprosessin aikana järjestetty verkkopohjainen kysely. Kyselyn avulla saatiin näkemyksiä siitä, miten tietoturvan tekninen ja hallinnollinen toteutus on yhtiössä järjestetty.

Tietoturva on niin laaja käsite, ettei opinnäytetyössä ole käsitelty kuin pieni osa teknistä ja hallinnollista tietoturvaa. Näin ollen tässä työssä tutustuttiin yleisempiin teknisiin ratkaisuihin ja toimintoihin, joiden avulla yritysten tietoturvallinen liiketoiminta voidaan taata ja turvata.

Työssä järjestetyn kyselyn lopputulokset noudattavat suurelta osin tietohallinnon näkemystä, mutta samalla antavat arvokkaita näkökulmia jokapäiväisen työnteon kautta. Työn tuloksena saatuja vastauksia voidaan käyttää yhä edelleen tietoturvan kehittämiseen, henkilöstön työnteon selkeyttämiseen ja järjestelmien käyttömukavuuden parantamiseen.

Avainsanat Tietoturva, tutkimus, kysely, tietohallinto

Sivut 24 sivua ja liitteitä 6 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and Communication Technology
Riihimäki campus

Abstract

Author Juuso Toivonen Year 2021

Subject Information security as part of an international company

Supervisors Marko Grönfors, Teemu Similä

ABSTRACT

The aim of the thesis was to study the vision of the personnel of an international company on information security operations and the technologies used for its implementation. The thesis was commissioned by Koskisen Oy whose entire staff had provided with a web-based survey during the thesis process. The survey provides insights into how the technical and administrative implementation of information security was organized in the company.

Technical information security is such a broad concept that it has not been possible to deal with it in the thesis process and, so only a fraction has been introduced in this work. Therefore, this thesis introduces more general technical solutions and functions that can be used to securely deal with business of big companies. The results of the survey conducted in the work largely follow the view of information management of Koskisen Oy, but at the same time provide valuable perspectives through everyday work. The answers obtained as the result of the work can still be used to improve information security, to streamline the work of staff, and improve the user-friendliness of technical systems.

Keywords Information security, research, survey, information management

Pages 24 pages and appendices 6 pages

Sisällys

Kuvat ja taulukot

Liitteet

1 Johdanto

Tietoturvalla on tärkeä ja kasvava rooli tämän päivän yritysmaailmassa ja yritysten toiminnoissa. Yritysten toiminta nojautuu yhä enenevässä määrin tietotekniikkaan ja sen hyödyntämiseen. Yrityksissä käsitellään paljon luottamuksellista ja yrityksen toiminnalle kriittistä aineistoa ja tietomateriaalia. Tämän materiaalin päätyminen kilpailijalle tai vääriin käsiin on usein yritykselle katastrofaalinen tilanne. Juuri näiden seikkojen takia tietoturvaan tulee suhtautua vakavasti. Vallitsevan koronapandemian myötä yritysten työntekijät ovat siirtyneet suurelta osin etätyöhön ja tämä luo haasteita, niin yritysten tietoturvalle kuin tietohallinnon avainhenkilöille, sekä työntekijöille itselleen. Tämän opinnäytetyön aikana tutustutaan tarkemmin niihin seikkoihin, joilla tietoturvaa saadaan ylläpidettyä ja kehitettyä.

Tämän opinnäytetyön tilaajana toimii Kärkölässä sijaitseva puunjalostuksen kansainvälinen erikoisosaaja, Koskisen. Koskisen on yli satavuotias suomalainen perheomisteinen yhtiö, joka valmistaa korkealuokkaista vaneria, lastulevyä sekä sahatavaraa. Koskisen Puunhankinta, entiseltä nimeltään Koskitukki, vastaa yhtiön puutavaran hankinnasta yksityisiltä metsänomistajilta. Koskisen omat tuotantolaitokset sijaitsevat Päijät-Hämeessä Järvelässä, sekä Etelä-Savossa Hirvensalmella. (Koskisen today, 2020)

Koskisen konserniin kuuluu myös pakettiautojen lattia- ja seinäratkaisuja valmistava Kore-yksikkö Puolan Toporowissa. Koskisella on suomen ainoa toiminnassa oleva lastulevytehdas. Koskisella työskentelee n. 900 henkilöä ja heistä suurin osa Järvelässä vaneritehtaalla. Yhtiön liikevaihto vuonna 2020 oli 263 miljoonaa euroa ja siitä yli puolet syntyi ulkomaan viennistä. (Koskisen today, 2020)

Konsernin tietohallinnon tehtävistä vastaa Järvelässä pääkonttorilla sijaitseva ICT- osasto. Tietohallinto vastaa konsernin ICT peruspalveluista sekä ylläpitää- ja kehittää tietojärjestelmiä konsernin yhteiset tavoitteet huomioiden.
ICT-osaston tehtäviin kuuluu päivittäisen tietoteknisen ja tietoturvallisen toiminnan turvaamisen lisäksi mm. tietotekniset laitehankinnat, investoinnit, järjestelmien ja verkkojen ylläpito sekä käyttäjäoikeuksien hallinta ja koordinointi.

Opinnäytetyön tavoitteena on kartoittaa Koskisella toteutettavan tietoturvan tasoa, sekä tietoturvallisen liiketoiminnan toteuttamista henkilöstön näkemyksen kautta. Nykymaailmassa toimivat tietoliikennepalvelut ja järjestelmät ovat erittäin suuressa roolissa onnistuneen liiketoiminnan takaamiseksi. Viime vuosina tietoturvallisuus on noussut entistä suurempaan rooliin lisääntyneen etätyön myötä, suurilta osin vallitsevan Koronaviruspandemian takia. Yrityksien työntekijät työskentelevät paljon kotoaan, jolloin yrityksen tietohallinnolla on haasteita varmistaessaan ja valvoessaan tietoturvallista työskentely-ympäristöä ja toimintatapoja. Suureen rooliin nousee myös yhteiset sovitut pelisäännöt ja henkilöstön perehdyttäminen. Tietoturva voi olla osalle henkilöstöstä melko vieras tai etäinen käsite ja onkin eriarvoisen tärkeää, ettei sitä koeta liian vaikeasti lähestyttävänä asiana.

Tietoturvallisuus ja tietoturva ovat niin laaja käsite, että aihetta on rajattava hieman pienempään osaan. Tämän opinnäytetyön aikana tullaankin keskittymään tietoturvan perusteisiin sekä yleisemmin käytössä oleviin työkaluihin ja toimintatapoihin suuren kansainvälisen yrityksen näkökulmasta. Opinnäytetyöprosessin aikana on toteutettu verkkopohjainen tietoturvallisuuskysely kaikille Koskisella työskenteleville henkilöille. Tämän kyselyn tulosten avulla Koskisen tietohallinto saa aitoa käyttäjäpalautetta ja parannusehdotuksia kaikkiin jokapäiväisessä työssä käytettäviin järjestelmiin ja toimintatapoihin. Kyselyn purkamisen ja raportoinnin jälkeen tietohallinto pääsee suunnittelemaan mahdollisia jatkotoimenpiteitä yhä paremman tietoturvallisen ja sujuvan, mielekkään työskentelyn takaamiseksi.

2 Tietoturva

Sanalla “Tietoturva” tarkoitetaan niitä hallinnollisia, sekä teknisiä toimia, joilla pystytään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus (Kyberturvallisuuskeskus, 2020).

Tietoturva koostuu useasta eri elementistä ja palasesta ja siihen vaikuttavia asioita on monia. Tiedon luottamuksellisuudella tarkoitetaan yrityksen tai organisaation kohdalla sitä,

ettei tieto kulkeudu vääriin käsiin oman organisaation ulkopuolelle. Tieto voi kulkeutua vääriin käsiin tietoverkossa tai ohjelmistossa olevan haavoittuvuuden tai aukon kautta. Tällaisen tilanteen voi aiheuttaa myös yrityksen omat työntekijät. Yrityksen tai organisaation on tärkeää kouluttaa ja valvoa tiedon käsittelyä tai sen jakamista ja siitä on hyvä olla olemassa myös selkeä ohjeistus (Mtech, 2019).

Tiedon eheyden ylläpidolla tarkoitetaan tyypillisesti sitä, että tieto tai viesti ei muutu matkan varrella. Kirjoitettua tietoa pidetään aina parempana kuin sanallisesti sovittua. Tiedon eheydestä vastaa yleensä organisaation tietohallinto ja heidän tehtävänään on varmistaa, ettei yrityksen varastoima tieto vahingoitu ja pysyy muuttumattomana. Eheyttä usein ylläpidetään virustorjunnalla, mutta myös yrityksen sisäinen ohjeistus ja toiminta saattaa vaarantaa tiedon eheyttä, työntekijä saattaa esimerkiksi vahingossa tallentaa asiakirjan vanhan päälle tai poistaa sen kokonaan. Eheän tiedon säilyttämisen kannalta on erittäin tärkeää pitää yllä ajantasaisia varmuuskopioita, sekä kahdentaa kriittiset järjestelmät (Mtech, 2019).

Tiedon saatavuudella tarkoitetaan lyhyesti sitä, että yrityksen sisällä varmistetaan ja tarjotaan jokaiselle työntekijälle pääsy tietoihin ja järjestelmiin, joita hän omaan työskentelyynsä tarvitsee. Apuna käytetään yleensä pilvipalveluita tai dokumentinhallintajärjestelmiä. Tietohallinnon tehtävänä on jakaa ja valvoa käyttäjäoikeuksia näihin järjestelmiin, sekä ylläpitää käytettyjen järjestelmien tietoturvaa hyökkäyksiä vastaan. Usein järjestelmien ja oikeuksien apuna käytetään kirjautumisen kaksivaiheista tunnistautumista tai jotakin muuta vahvaa tunnistautumiskeinoa (Mtech, 2019).

2.1 Tietoturvan termistöä

Tässä luvussa tutustutaan lyhyesti tietoturvaan liittyvään yleissanastoon, sekä termeihin ja käsitteisiin, joihin voi törmätä keskustelussa osana tietoturvaa.

2.1.1 Tietoturvauhka

Tietoturvauhalla tarkoitetaan sisäistä tai ulkoista, tietoturvaa kohtaan koettua uhkaa.
Sen voi aiheuttaa organisaation sisäinen toiminta tai ulkoinen tekijä, esimerkiksi virus tai sähköpostin mukana tullut tietojenkalasteluhyökkäys (Sanastokeskus, 2004).

2.1.2 Roskaposti

Roskapostia on vastaanottajan kannalta ei-toivotut viestit. Useimmiten roskapostia lähetetään suurelle vastaanottajajoukolle markkinointitarkoituksissa. Useimmissa sähköpostiohjelmissa on automaattinen roskapostisuodatin, joka tunnistaa ei-toivotut viestit ja siirtää ne automaattisesti roskapostikansioon (Sanastokeskus, 2004).

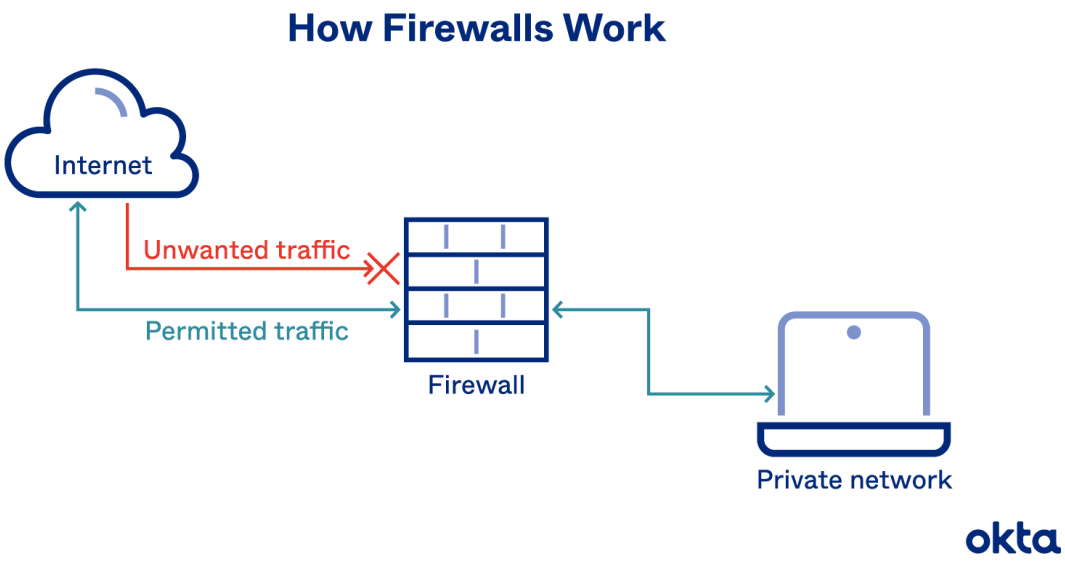
2.1.3 Hakkeri ja Hakkerointi

Hakkerilla tarkoitetaan yleisemmin puhekielessä henkilöä, joka tunkeutuu tietoverkkoon tai tietojärjestelmään ilman sen omistajan lupaa. Hakkereita voidaan kuitenkin katsoa olevan karkeasti kahta eri tyyppiä: mustahattuhakkerit toimivat luvatta ja pyrkivät saamaan aikaan vahinkoa, kun taas valkohattuhakkerit toimivat usein yrityksen tai organisaation palkkaamina ja yrittävät löytää tietoturva-aukkoja yrityksen omista järjestelmistä.
Suomen kielessä hakkerilla saatetaan myös usein tarkoittaa henkilöä, joka on tavallista aktiivisempi ja innokas tietokoneharrastaja (Sanastokeskus, 2004).

2.1.4 Palomuuri

Palomuuri on tekninen verkkoratkaisu, jolla hallitaan tai rajoitetaan liikennettä verkon sisällä tai verkosta toiseen. Palomuurille luodaan usein ennalta määrättyjä sääntöjä, joiden mukaan se rajoittaa liikennettä. Palomuuria käytetään usein yrityksissä julkisen internetin ja yrityksen oman sisäisen verkon välillä (Sanastokeskus, 2004).
Kuvassa 1 kaavio perinteisestä palomuurirakenteesta pienissä verkoissa.

Kuva 1. How firewalls work (Okta, n.d.).



2.2 Tietoturvan merkitys liiketoiminnassa

Tietoturva on hyvin suuressa roolissa yritys- ja liiketoiminnassa. Tärkeän palvelun vaarantuessa sillä voi olla katastrofaaliset seuraukset yrityksen liiketoiminnalle tai imagolle. Yrityksen sisällä on tärkeää tunnistaa, mitkä toiminnot ovat kaikkein tärkeimpiä suojata tietoturvauhilta. Ei ole taloudellisesti kannattavaa suojata kaikkia järjestelmiä vahvimmalla mahdollisella tavalla, vaan priorisoida kriittisimmät ja liiketoiminnan jatkumisen kannalta tärkeimmät osa-alueet. Riskienhallintaa ja jatkuvaa arviointia on hyvä suorittaa määräajoin. Tällöin minimoidaan häiriöitä ja toimintakatkoksia tai niihin voidaan varautua etukäteen. Liiketoiminnan jatkuvuuden varmistamisen kannalta on tärkeää luoda myös toimintamalli tai suunnitelma siitä, miten toivutaan mahdollisesta tietovuodosta, varkaudesta, vikaantuneesta järjestelmästä tai muusta poikkeustilanteesta. Hyvä ennakkovarautuminen voi pelastaa yrityksen suurilta taloudellisilta menetyksiltä tai jopa liiketoiminnan loppumiselta.

Tietoturvasta puhuttaessa on tärkeä muistaa, että se on yrityksen jokaisen työntekijän yhteinen asia, eikä pelkästään tietohallinnon tai IT- henkilöiden. Tietoturvan ylläpito ja kehittäminen on paljon helpompaa, kun jokainen omalta osaltaan ymmärtää ja toimii tietoturvallisten käytäntöjen mukaan. Yrityksessä on hyvä pyrkiä myönteiseen asenteeseen

tietoturvaa kohtaan, tämä omalta osaltaan helpottaa tietoturvakäytäntöjen jalkauttamisessa koko organisaatioon. Hienoista järjestelmistä ja tekniikoista ei ole apua, jos yrityksen sisäinen toiminta on riskialtista, eikä käytäntöjä noudateta.

Tietoturvan perusteellinen dokumentointi on erittäin tärkeässä roolissa. Myös mahdollisesta häiriötilanteesta toivuttaessa. Kirjallinen dokumentti auttaa henkilöstön perehdyttämisessä ja luo tukea turvalliseen toimintaan. Dokumenttiin on hyvä kirjata yrityksen yhteiset käytännöt ja ohjeistukset, jotta näitä voidaan noudattaa myös yhteistyökumppanien kanssa toimiessa. (Hyvönen, 2017)

3 Tietoturvan tekninen toteutus

Tässä luvussa perehdytään siihen, millaisia teknisiä keinoja suurilla yrityksillä on tietoturvallisen toiminnan takaamiseksi. Kappaleen aikana kerrotaan myös suurpiirteisesti, millaisia eri järjestelmiä Koskisella käytetään ja miten niitä hyödynnetään. Asioita ei voida kuitenkaan kuvata liian tarkasti tilaajayrityksen tietoturvan vaarantumisriskin takia. Teknistä tietoturvaa voidaan ylläpitää moninaisin eri keinoin. Tämän työn aikana tullaan tutustumaan yleisempiin teknisiin järjestelmiin ja palveluihin.

3.1.1 Etäyhteys ja VPN

VPN eli “Virtual Private Network” mahdollistaa laitteiden yhdistämisen verkkoon VPN-palveluntarjoajan ylläpitämän serverin kautta. VPN-yhteys parantaa käyttäjän yksityisyyttä luomalla yksityisen “tunnelin” käyttäjän ja esimerkiksi työpaikan verkkorakenteen välille. Yhteys antaa käyttäjälle mahdollisuuden piilottaa hänen oikean sijaintinsa ja “huijata” sen olevan jossakin muualla. Näin mahdollistetaan pääsy myös maantieteellisesti rajoitettuihin ja tavallisesti ulottumattomissa oleviin palveluihin.

VPN- teknologia onkin alun perin luotu juuri etätyöntekijöiden tietoturvallisen työskentelyn takaamiseksi. Luomalla yksityisen yhteyden työntekijän oman kotiverkon, sekä työpaikan verkon välille mahdollistetaan liiketoiminnan kannalta kriittisen datan turvallinen käsittely (vpnyhteys.fi, n.d.).

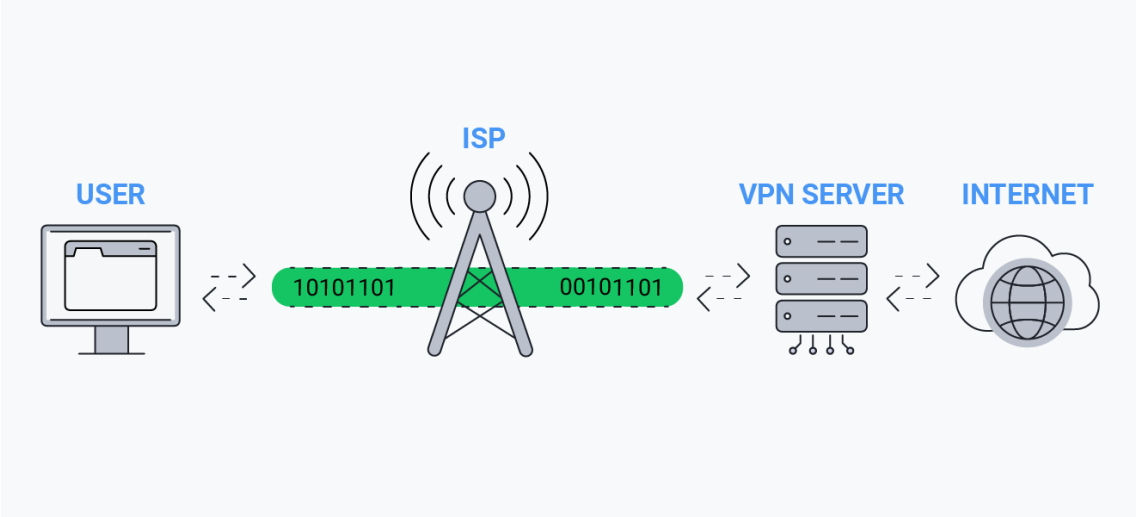
Tavallisesti tietokonetta tai muuta verkkoselaamiseen tarkoitettua laitetta käyttäessä ja verkkoon yhdistäessä, laite yhdistyy ensin internet palveluntarjoajaan eli lyhemmin ISP “Internet Service Provider” ISP:n kautta laite yhdistyy käyttäjän haluamalle verkkosivustolle. Normaalitilanteessa ilman VPN- yhteyttä kaikki verkkoliikenne kulkee ISP:n kautta, jolloin ISP:llä on mahdollisuus tarkkailla ja seurata käyttäjän verkkoliikennettä (vpnyhteys.fi, n.d.).

VPN- yhteydellä on karkeasti rajattuna kaksi eri tyyppiä, etäkäytettävä VPN, sekä sivustojen välinen, virallisemmin ”site to site” VPN. Etäkäytettävän VPN- yhteyden avulla käyttäjät muodostavat yhteyden etäverkkoon, käyttämällä avuksi VPN- ohjelmistoa. Etäkäytettävää VPN- yhteyttä käytetään useimmiten työpaikkojen ja siellä työskentelevien työntekijöiden kotikonttorien väliseen yhteyteen. Yhteys mahdollistaa turvallisen ja helpon pääsyn yhtiön tietoihin ja resursseihin mistä tahansa.

Site to site VPN- on tarkoitettu pääsääntöisesti todella suurille yrityksille, joilla useita toimipisteitä ja toimistoja. Tällä tekniikalla yhtiön on mahdollista jakaa resursseja ja tietoja toimipisteidensä välillä tietoturvallisesti. (NordVPN, n.d.)

Kuvassa 2 kaavio yksinkertaisesta VPN- rakenteesta.

Kuva 2. How does a VPN work? (AVG, 2020)



Koskisella on käytössä VPN- etäyhteys, jotta etätyötä tekevien verkkoliikenne saadaan toteutettua tietoturvallisesti ja salattuna kotikonttorilta Koskisen verkkorakenteeseen. VPN-

etäyhteys mahdollistaa ICT- osaston hallinnoimien tiedostopalvelimien ja verkkoratkaisujen käytön, riippumatta siitä missä sijainnissa ja millaisella verkkoyhteydellä työntekijät kulloinkin työskentelevät.

3.1.2 Sähköposti ja palomuuri

Sähköposti on ehkä yleisemmin yrityksissä käytetty viestintäväline ja usein sitä käytetään yrityksen, asiakkaiden ja yhteistyökumppaneiden väliseen kommunikaation. Sähköpostin tietoturva ei kuitenkaan ole itsestäänselvyys, itseasiassa salaamatonta sähköpostia pääsee lukemaan lähes yhtä helposti kuin tavallista postikorttia. Sähköpostia käytetään usein myös luottamuksellisen tiedon välittämiseen. Sähköpostilla saatetaan lähettää henkilötietoja tai sopimuspapereita, liikesalaisuuksia ja salasanoja sisältäviä viestejä. Tällaisissa tilanteissa tulisi käyttää salattua sähköpostia.

Sähköpostiviesti kulkee useiden eri postilaatikkopalvelimien kautta ennen kuin se saapuu määränpäähänsä. Salaamaton sähköposti kulkee palvelimelta toiselle periaatteessa täysin luettavassa muodossa, jolloin asiansa osaava pääsisi lukemaan sen sisällön. Sähköpostia lähettäessä käyttäjä ei voi olla täysin varma saapuuko viesti koskaan perille tai muuttuuko se matkan varrella. Sähköposti on hyvin yleinen rikollisten käyttämä kanava haittaohjelmien levitykseen ja tietojen kalasteluun. Sähköpostia käyttäessä myös tavallisella käyttäjällä on vastuu toimia tietoturvallisesti. Viestiä lähettäessä täytyy olla tarkkana, ettei se mene vahingossa väärälle henkilölle. (Deltagon, n.d.)

Palomuurilla tarkoitetaan työkalua, jota käytetään suojaamaan ja suodattamaan käyttäjän tai suuremman verkon sisällä tapahtuvaa liikennettä. Yksi palomuurin keskeisimmistä tavoitteista on suojata käyttäjää haitalliselta verkkoliikenteeltä. Palomuurille luodaan tiettyjä ennalta määrättyjä sääntöjä tai portteja, joiden avulla se osaa suodattaa liikennettä. Säännöt perustuvat esimerkiksi domain- nimeen, porttiin, protokollaan tai IP- osoitteeseen. Palomuuri saattaa myös vaatia käyttäjän toimia esimerkiksi vahvistuspyyntöinä.

Palomuurit voidaan jakaa karkeasti kolmeen eri päätyyppiin; Ohjelmistopalomuurit, Laitteistopalomuurit ja Pilvipohjaiset palomuurit.

Ohjelmistopalomuuri toimii nimensä mukaisesti laitteen sisällä ohjelmallisesti. Tällainen palomuuri on tuttu mm. Windows- tietokoneista. Ohjelmistopalomuuri sopii tavalliselle käyttäjälle suojatessaan vain tämän yksittäisen laitteen, se ei kuitenkaan kykene suojaamaan koko verkkoa tai useampaa laitetta samanaikaisesti. Yrityskäytössä ohjelmistopalomuurin hallinta on hankalaa ja aikaa vievää.

Laitteistopalomuurit eroavat ohjelmistopalomuureista siinä määrin, että ne toimivat itsenäisinä fyysisinä laitteina ja kykenevät suojaamaan isompia verkkokokonaisuuksia. Laitteistopalomuurit sopivat hyvin yritysten käyttöön ja ne toimivat usein yrityksen sisäverkon ja julkisen internetin välillä. Laitteistopalomuureissa on kuitenkin omia heikkouksiaan eivätkä ne välttämättä ole parhain ja käytännöllisin vaihtoehto suurille yrityksille.

Välityspalvelimen sisällä toimivat Pilvipohjaiset palomuurit sopivat hyvin suurille ja laajeneville yrityksille. Pilvipohjaista palomuuria hallitaan pilvipalvelun kautta ja tällöin vältytään laitekohtaiselta huolenpidolta.

Palomuurit hyödyntävät toiminnassaan eri tekniikoita ja suodattimia. Paketteja suodattavat palomuurit tutkivat tietopaketteja, joita verkossa ja palomuurin ohitse kulkee. Paketit tarkastetaan päällisin puolin, mutta niiden sisältöön paketteja suodattava tekniikka ei pureudu. Circuit-level gateway – tekniikka tarkastaa liikenteen lähteen alkuperän ja vertaa sitä palomuurisääntöihin. Jos paketin lähde vastaa TCP- protokollan hyväksymää lähdettä, se päästetään läpi. Näitä kahta edellä mainittua tekniikkaa sovelletaan Tilattomassa pakettisuodatuksessa (Stateful firewall). Tämä tekniikka on ikään kuin hybridimalli edellä mainituista. Tämä tekniikka kuitenkin kuormittaa laitteistoa sen laajempien toiminnallisuuksien myötä.

Sovellustason palomuurit tai toiselta nimeltään välityspalvelinpalomuurit toimivat lähiverkon ja julkisen internetin välillä. Tällä tekniikalla tiedot käyvät erillisen pilvipohjaisen suodatuksen läpi ennen kuin ne päästetään esimerkiksi yrityksen omaa lähiverkkoon. Välityspalomuurit yhdistävät monia muiden tekniikoiden suodatustapoja ja suodattavat verkkoliikennettä paljon syvemmin. Tämä tekniikka saattaa kuitenkin hidastaa verkkoyhteyttä. (Klusaite, 2020)

Koskisella on käytössä useita palomuureja eri verkkojen välillä ja verkot ovat jaettu useisiin pienempiin palasiin. Yritysverkot ovatkin usein kotiverkkoja monimutkaisempia ja jaettuna useampaan palaseen. Esimerkiksi tehtaiden tuotantoverkot ovat tarkasti eristettyinä julkisesta internetistä palomuuriratkaisujen avulla, kun taas toimistoverkot ovat hieman vapaampia ja näistä on pääsy julkiseen internettiin.

3.1.3 Haittaohjelmien torjunta, virustorjunta ja EDR

Haittaohjelmat ovat tietokoneille ja mobiililaitteille haitalliseksi suunniteltuja ohjelmistoja. Haittaohjelmilla pyritään usein aiheuttamaan tuhoa tai taloudellista haittaa sen kohteelle, sekä kalastamaan tietoa yritysten tietoverkosta. Haittaohjelmien laatijat pyrkivät saamaan haltuunsa kriittistä tietoa ja näin kiristämään haittaohjelman saanutta uhria. Haittaohjelmatartunnan voi yleisemmin saada linkeistä, mainoksista ja sähköpostin kalasteluviesteistä. Usein ne piiloutuvat juuri sähköpostin liitetiedostoihin ja levittäytyvät sieltä uhrin laitteelle. Haittaohjelmat jaetaan useaan eri tyyppiin ja niitä ovat mm. Tietokonemadot, mainosohjelmat eli Adwaret, vakoiluohjelmat, virukset ja botit sekä kiristysohjelmat. Haittaohjelmien laatijat pyrkivät usein saavuttamaan taloudellista hyötyä (Kaspersky, n.d.).

Haittaohjelmien torjunnassa tärkeässä roolissa ovat erilaiset virustorjuntasovellukset. Nämä sovellukset skannaavat käyttäjän laitetta mahdollisien tartuntojen varalta. Sovelluksen löytäessä tartunnan tai haitallisen ohjelmiston, se ilmoittaa käyttäjälleen ja usein myös poistaa haitallisen ohjelmapätkän ilman erillisiä käyttäjän toimia.

EDR eli Endpoint Detection and Response on uudentyyppinen ratkaisu haittaohjelmien ja haitallisen verkkoliikenteen torjuntaan. EDR- järjestelmä toimii tietohallinnon apuna ja sillä varmistetaan loppukäyttäjän laitteen turvallisuus. EDR tunnistaa ja havaitsee haitallista verkkoliikennettä. Se pystyy myös keskustelemaan muiden laitteiden kanssa ja vertaamaan dataa, arvioidakseen sen haitallisuutta. EDR järjestelmät tallentavat dataa haitallisesta toiminnasta, jolloin tietohallinto pääsee näkemään minkälaisia tapahtumia käyttäjän laitteella on ollut. Järjestelmä mahdollistaa myös loppukäyttäjän laitteen etähallinnan, tyhjentämisen tai verkosta eristämisen. (Cynet, 2021)

3.1.4 Varmuuskopiot ja kahdentaminen

Varmuuskopioinnilla tarkoitetaan tärkeän tiedon varastointia kopioimalla se useammalle eri tallennusmedialle. Alkuperäisen tiedon tuhoutuessa tai hävitessä voidaan tieto palauttaa varmuuskopiosta. Varmuuskopiointi on yleinen toimenpide tietotekniikassa ja hyvin tärkeä toiminto esimerkiksi yrityksen toiminnan kannalta kriittisten tietojen säilyttämiseksi. Yleisesti käytössä olevat kiintolevyt ovat herkkiä vikaantumaan, joten on ensiarvoisen tärkeää, ettei tietoa säilytetä vain yhdellä levyllä, vaan se on kopioituna tai hajautettuna useammalle eri levylle tai tallennusvälineelle (Wikipedia, 2020).

Yrityksillä tiedostot ja palvelut säilytetään yleensä omilla palvelimillaan tai verkkolevyillä, jotka ovat keskitettyjä tiedostojen tallennuspaikkoja, eivätkä ne vaadi tavalliselta käyttäjältä erityisiä toimenpiteitä. IT- osaston tehtävänä on huolehtia, että nämä palvelut ovat aina saatavilla, eivätkä ne ole haavoittuvaisia sähkökatkoille, tietoturvahyökkäyksille tai laiterikoille. Yrityksen omat palvelimet tulisivat olla varmuuskopioituja, sekä kahdennettuina myös toiseen sijaintiin, mahdollisen suuremman vahingon varalta. Palvelimilla sijaitsee usein myös tiedostojen lisäksi tietokantoja, sekä toiminnanohjausjärjestelmiä. Poikkeustilanteessa tietokantojen ja järjestelmien palauttamisen täytyy olla varmistettu varmuuskopioilla ja kahdentamisen avulla, muutoin edessä saattaa olla useiden päivien uudelleenasennustyö (Palmu, 2019).

3.1.5 M-files

M-files on tehokas dokumentinhallintajärjestelmä. Toisin kuin perinteisen kansiorakenteen hallinnassa M-filesissa ei tarvitse tietää minne dokumentteja ja tietoa tallentaa, tarvitsee vain tietää mitä tallentaa. M-filesissa dokumentteja hallitaan metatiedoilla ja ominaisuuksilla, jotka täytetään metatietokorttiin dokumentin tallennusvaiheessa. Organisaation oman M-files tietovaraston sisältöä pääsee näkemään vain organisaation tunnukset omaava henkilö, näillä tunnuksilla pystytään hallitsemaan mitä yksittäisiä dokumentteja kukin yksittäinen käyttäjä pääsee näkemään tai muokkaamaan.
M-files on tietoturvallinen ratkaisu suuren tietomäärän hallintaan, dokumentit sijaitsevat varmistetuilla palvelimilla eivätkä ne vaarannu esimerkiksi yksittäisen käyttäjän koneen hajotessa. Dokumentteja on myös helppo hallita etänä ja jakaa eri käyttäjien tai

käyttäjäryhmien kesken. M-files dokumentit varataan aina muokattavaksi, tällöin usean eri käyttäjän päällekirjoitusvaara pystytään minimoimaan. M-files sisältää myös historiatiedon, tämä tarkoittaa sitä, että dokumentin kaikki versiot ensimmäisestä viimeisimpään on aina saatavilla ja palautettavissa käyttöön.

Koskisella käytetään M-filesia erittäin aktiivisesti eri osastojen ja toimintojen yhteistyössä. Se on myös ensisijainen dokumenttien tallennuspaikka. M-filesiin on rakennettu lisäosia ja integraatioita mm. verkkosivujen hallinnan helpottamiseksi. M-files toimii myös dokumenttien jakamisessa ulkopuolisten yhteistyökumppanien kanssa.

3.2 Tietoturvapolitiikka

Tietoturvapolitiikka tarkoittaa yhtiössä yhteisesti sovittua toimintamallia tietoturvallisen toiminnan takaamiseksi. Politiikassa määritellään ne toimet ja keinot, joilla varmistetaan yhtiön tietoturvan luottamuksellisuus, eheys – ja käytettävyys.
Koskisen toimintajärjestelmäohjeessa kuvataan tietoturvapolitiikkaa, sekä tietoturvaa seuraavasti; “tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai tahallisten, tuottamuksellisten ja tapaturmaisten inhimillisten tekojen aiheuttamilta uhilta ja vahingoilta. Tällaisia voivat olla esim. yhtiötä vastaan kohdistettu vakoilu, yritysvakoilu tai muu rikollinen toiminta, hallitsematon julkisuus ja tiedottaminen tai osaamattomuus tietoja käsiteltäessä”
Ohjeessa kerrataan vielä yhteenvetona politiikan antavan yhteisen pohjan yhtiön tietoturvamenettelyille, sekä muistutetaan kääntymään tietohallinnon puoleen kaikissa tietoturvaan liittyvissä asioissa (Koskisen sisäinen toimintajärjestelmäohje).

3.2.1 Henkilöstön ohjeistus ja pelisäännöt

Tärkeässä roolissa tietoturvallisessa toiminnassa on henkilöstön ohjeistuksen ja perehdytyksen asianmukainen ja looginen hoitaminen. Viimekädessä tietoturvallisen toiminnan ja yhteisen tietoturvapolitiikan toteuttamisesta vastaa yhtiön johto, mutta henkilöstöllä on myös vastuu toteuttaa tietoturvapolitiikassa kuvattuja seikkoja työnteossaan. Henkilöstö on myös velvoitettu ilmoittamaan tietoturvauhista ja poikkeamista esimiehilleen.

3.2.2 Käyttöoikeudet

Käyttöoikeudet ovat tärkeä osa tietoturvaa, niillä määritellään kuka ja mitä informaatiota kyseinen henkilö tai käyttäjäryhmä pääsee järjestelmissä näkemään tai hallitsemaan. Käyttöoikeudet määrittelee pääsääntöisesti henkilön esimies tai organisaation johtohenkilö yhteistyössä tietohallinnon kanssa. Oikeuksien määrittelijä vastaa samalla käyttäjätunnuksien elinkaaresta, jossa voidaan nähdä kolme selkeää vaihetta; käyttäjätilin perustaminen, mahdolliset muutokset sekä työsuhteen päättyessä käyttäjätilin sulkeminen. Tietoturvan näkökulmasta tavoitteena on antaa käyttäjälle tai käyttäjäryhmälle vain sellaiset oikeudet, joita he tarvitsevat jokapäiväisen työnsä hoitamiseen. Koskisella käyttäjäoikeudet hallitaan ServiceDeskin kautta, jonne muutospyyntö tiketöidään. Tällöin kaikki muutospyynnöt jäävät talteen ja ovat tarkasteltavissa jälkikäteen.

Koskisella prosessi etenee käyttäjän tai käyttäjän esimiehen toimesta tiketöinnin kautta esimiehen hyväksyntään. Tämän jälkeen prosessi etenee toteutusvaiheeseen, jolloin tietohallinto tai järjestelmän pääkäyttäjä validoi ja toteuttaa oikeusmuutoksen. (Koskisen sisäinen toimintajärjestelmäohje)

3.2.3 Tietoturvallinen käyttäytyminen

Etenkin yrityksissä ja suurissa organisaatioissa tietoturvallisen käyttäytymisen korostaminen on tärkeää. Usein parhaatkaan järjestelmät ja suojaukset eivät pysty auttamaan, jos ihmisen oma toiminta on hakoteillä tai hän omalla toiminnallaan edesauttaa rikollista toimintaa tietoverkkoja tai järjestelmiä kohtaan. Yhteiset turvalliset toimintatavat olisi hyvä kerrata organisaation asiantuntijoiden ja työntekijöiden kesken jo mahdollisessa perehdytysvaiheessa. Henkilöstön on hyvä tunnistaa potentiaaliset kalastelutilanteet, roskapostiviestit ja virushyökkäykset. Toisaalta myös tilanteet, jossa on hyvä kääntyä tieturvaa hallinnoivan tahon puoleen.

Usein tietoturvallinen ja tekninen osaaminen vaihtelee myös työtehtävien perusteella. Organisaatioissa olisi ensiarvoisen tärkeää varmistaa, että avainhenkilöiden ja järjestelmien pääkäyttäjien tietoturvallinen osaaminen olisi sillä tasolla, ettei se vaaranna yrityksen toimintaa. Joskus tällainen henkilö saattaa olla myös organisaation ulkopuolinen, esimerkiksi

palvelimen pääkäyttäjä. Yrityksen onkin siis tärkeää varmistaa myös ulkoisten yhteistyökumppanien tietoturvaosaamisen taso. Tässä apuna voivat toimia myös eri tietoturvasertifioinnit ja sertifikaatit. (Laakso, n.d.)

4 Kyselytutkimus Koskisen henkilöstölle

Koskisen koti- ja ulkomaan henkilöstölle lähetettävällä Webropol- kyselytutkimuksella (Liite 1) haluttiin kartoittaa henkilöstön osaaminen, toimintatavat ja näkemys tietoturvallisen liiketoiminnan saralla. Henkilöstöä työskentelee hyvin erilaisissa tehtävissä, onkin erityisen tärkeää saada selkeytettyä ja yhdenmukaistettua tietoturvallisia toimintatapoja eri tehtävien ja osastojen välillä. Tutkimuksen tavoitteena oli tarjota henkilöstölle mahdollisuus anonyymiin palautteeseen ja kehitysideoihin, sekä toisaalta avartaa ja vahvistaa myös tietohallinnon näkökulmaa toteutettavasta tietoturvan tasosta.
Kyselytutkimuksen lopputulosten ja raportoinnin avulla yhtiö pääsee kehittämään toimintasuunnitelmaansa ja strategiaa tietoturvan saralla tuleville vuosille.

4.1 Tutkimuksen kohdeyleisö

Tutkimuksen kohdeyleisönä toimi Koskisen konsernin koti- ja ulkomaan henkilöstö. Henkilöstö työskentelee Koskisen tuotantoyksiköissä Järvelässä pääkonttorilla, vaneri sekä lastulevytehtaalla, sahalla ja puunhankinnan hallintotehtävissä sekä Hirvensalmella ohutviiluvaneritehtaalla. Ulkomaan henkilöstö koostuu pääosin myyntikonttorien henkilöstöstä, joita työskentelee ympäri maailman mm. Euroopassa, Aasiassa ja Amerikassa.

4.2 Tutkimuksen tekninen toteutus

Kyselytutkimuksen tekniseksi toteutustavaksi valikoitui verkkopohjainen Webropol-kyselytyökalu. Webropol on pohjoismaiden laajimmin käytetty kyselytyökalu. Se tarjoaa nopean ja monipuolisen ratkaisun verkkokyselyiden toteuttamiseen. Webropol on helppokäyttöinen, vastaa monipuolisesti teknisiin haasteisiin ja on erinomainen hinta-laatusuhteeltaan (Webropol, n.d.).

Työkalu valikoitui, koska olen käyttänyt sitä aiemmin työssäni. Webropol on melko helppokäyttöinen ja siinä on hyvät raportointiominaisuudet. Webropolin avulla on helppo toteuttaa käyttäjäystävällinen, yksinkertainen kyselytutkimus.

4.2.1 Kyselyn laatiminen

Kyselyä laatiessa pidin ensisijaisen tärkeänä, että kysely olisi mahdollisimman käyttäjäystävällinen. Kyselyn piti olla sellainen, että siihen on mielekästä vastata, eikä se näin ollen saanut olla liian tekninen. Koskisella työskentelee laaja-alaisesti henkilöitä erilaisella tietoteknisellä osaamisella ja taustalla, joten kyselyn tuli olla mahdollisimman yleispätevä, kuitenkaan teknistä aspektia unohtamatta. Tietoturvakysely suunniteltiin myös niin, että se voidaan toteuttaa anonyymisti, tällöin vastaajalle syntyy luottavainen mieli siitä, että hän voi vastata kyselyyn totuudenmukaisesti ja avoimesti. Tietoturvakysely koostuu kolmesta osasta. Kyselyn jokaisen osan jälkeen oli myös mahdollisuus antaa vapaata sanallista palautetta, sekä kehitysajatuksia koskien tiettyä osaa tai koko kyselyä.

Kyselyn ensimmäisessä osassa selvitettiin vastaajien taustoja, näin vastaajat voidaan jakaa myöhemmin työskentelyosastoittain ja kartoittaa eroavaisuuksia tietoturvallisessa osaamisessa ja käyttäytymisessä eri osastojen välillä. Taustakysymyksissä kartoitetaan myös vastaajan ikää, tällöin pystytään analysoimaan vaikuttaako vastaajan ikähaarukka tietämykseen tietoturvasta. Ensimmäinen osa sisältää myös muutaman peruskysymyksen, joilla tutkitaan henkilöstön asennoitumista tietoturvaa kohtaan, sekä yleistä tietämystä tietoturvasta.

Kyselyn toisessa osassa keskitytään Koskisella käytössä oleviin tietoturvallisuuden työkaluihin. Tässä osassa käsiteltiin yleisempiä, jokapäiväiseen työhön liittyviä työkaluja ja toteutuksia. Kyselyn toisen osan kysymykset ja tekniikat ovat erittäin ajankohtaisia vallitsevan pandemiatilanteen ja etätyösuositusten vuoksi. Tämän osan kysymysten avulla Koskisen ICT- osasto pääsee näkemään tärkeää palautetta jokapäiväiseen työhön liittyen.

Kolmannessa ja viimeisessä osassa kyselyä paneudutaan dokumentinhallintaan ja siihen liittyviin työkaluihin. Koskisella on käytössä M-Files dokumenttienhallintajärjestelmä, jonka

käyttöä suositellaan kaikille toimistotyötä tekeville. Kolmannen osan tulosten avulla tietohallinto näkee tärkeää tietoa siitä, miten Koskisen dokumentteja ja niiden oikeuksia hallitaan.

4.2.2 Kyselyn lähetys

Kysely lähetettiin ja julkaistiin tiistaina 15.6.2021 Kyselyn linkki julkaistiin Koskisen sisäisessä uutis- ja tiedotuskanavassa Intrassa. Intraan on pääsy kaikilla Koskisen koti- ja ulkomaan toimihenkilöillä ja työntekijöillä. Alun perin kysely oli tarkoitus lähettää vain sähköpostilla toimihenkilöille, mutta yhdessä ICT-osaston kanssa päätimme julkaista kyselyn kaikille.

Kyselystä lähetettiin muistutusviesti 13.7.2021 sähköpostitse koko Koskisen koti- ja ulkomaan henkilöstölle ennen kyselyn sulkeutumista. Kysely otettiin vastaan odotettua aktiivisemmin ja muutaman päivän lähetyksen jälkeen 17.6.2021 vastauksia oli jo yli 40 kappaletta.

4.2.3 Kyselyn raportoiminen

Kysely sulkeutui perjantaina 23.7.2021 jolloin vastauksia oli kertynyt 108 kappaletta, tasaisesti lähes jokaiselta osastolta, sekä ulkomailla työskenteleviltä henkilöiltä. Kyselyn vastausprosentti oli mielestäni positiivinen yllätys, ottaen huomioon henkilöstön kesäloma-ajat, sekä kyselyn tekninen luonne.

Kyselyn raportoiminen tapahtui ajamalla Webropol kyselyohjelmasta Excel raportti, joka siivottiin ja suodatettiin hieman luettavampaan muotoon yksiköittäin. Siivottua raporttia käytiin läpi Koskisen tietohallinnon avainhenkilöiden kanssa ja lopuksi Excel raportista koostettiin selkeä graafinen esitys, joka julkaistiin myös henkilöstön nähtäville Koskisen sisäiseen Intranettiin.

Selkeän raportoinnin avulla pääsee näkemään tietoturvallisen toiminnan kehitettävät selkeät kipukohdat ja kohdistamaan tulevaisuuden toimintasuunnitelmaa tiettyjen tekniikoiden ja asiakokonaisuuksien ympärille. Raportoinnin avulla nähdään myös ikäjakauman vaikutus tietoturvalliseen käyttäytymiseen ja tunnistetaan sen mahdolliset kehityskohteet.

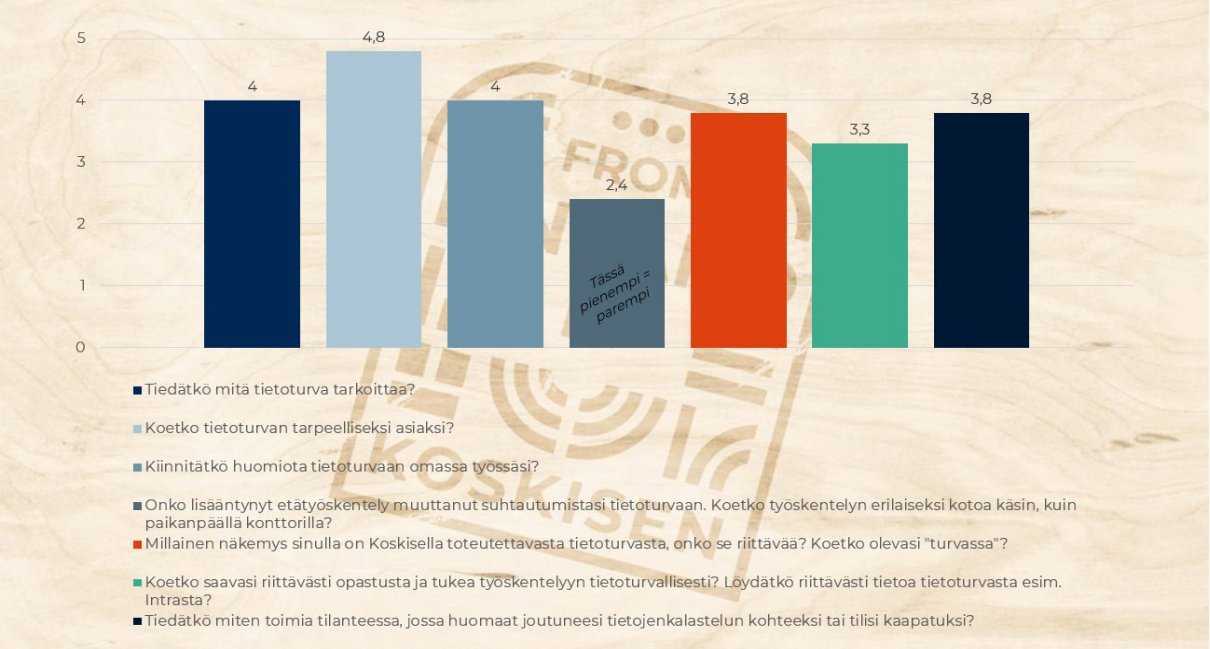
5 Tutkimustulokset ja johtopäätökset

Tämän kappaleen aikana pureudutaan tarkemmin kyselyn tuloksiin. Tuloksia käsitellään siinä järjestyksessä, kun ne alkuperäisessä kyselyssä olivat. Kyselyssä voidaan katsoa olevan kolme selkeää osuutta ja jatkossa tekstissä viitataankin kyselyn osiin 1–3.
Tässä kappaleessa esitettävät tulokset ovat keskiarvoja kaikkien osastojen välillä.
Numeroarvon 0 ollessa huonoin tulos ja 5 ollessa paras mahdollinen keskiarvo.

5.1 Henkilöstön näkemys tietoturvallisuuden toteutuksesta Koskisella

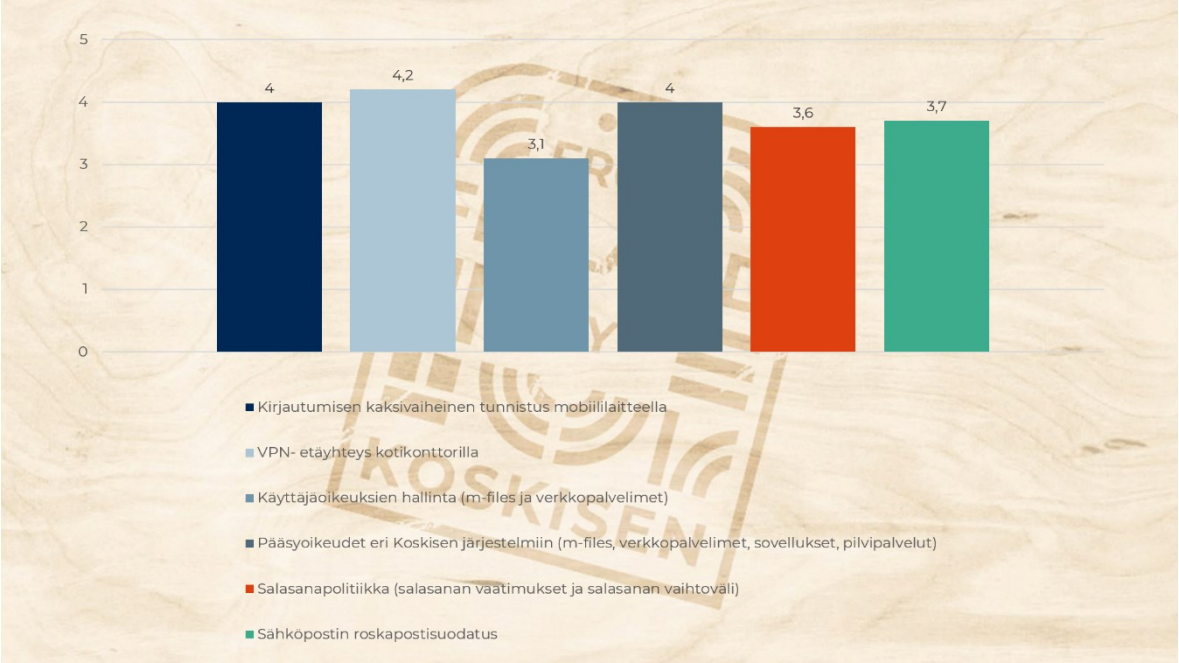
Kuten kuvassa 3 on esitelty, kyselyn lopputulosten avulla havaittiin tietoturvatietämyksen olevan yleisesti melko hyvällä tasolla, keskiarvon ollessa tasan 4. Henkilöstö tietää mitä tietoturva tarkoittaa ja se koetaan Koskisella tarpeelliseksi asiaksi, keskiarvo 4,8.
Tietoturvaan myös kiinnitetään huomiota oman työskentelyn ohella. Keskiarvo 4.
Vallitsevan Koronaviruspandemian takia, henkilöstöä on siirtynyt suurelta osin etätyöskentelyyn. Sen ei kuitenkaan koeta juurikaan vaikuttaneen työskentelyyn tietoturvallisesti. Koskisella on ollut mahdollisuus etätyöskentelyyn jo ennen Koronapandemiaa, jolloin järjestelmät sekä ohjeistus ja etätyöpolitiikka ovat olleet valmiita suuremmankin etätyöprosentin toteuttamista varten. Toisaalta vastauksen keskiarvoprosentti ei välttämättä kerro koko totuutta, sillä suurin osa tehtaalla työskentelevästä tuotannon väestä ei voi suorittaa työtehtäviään etätöinä, vaan ovat työskennelleet entiseen malliin paikan päällä, läpi koronapandemian ajan. Keskiarvo tälle kysymykselle oli neutraali 2,4 Tässä kysymyksessä akselit olivat kuitenkin väärinpäin, eli periaatteessa voidaan katsoa pienemmän vastauksen olevan parempi.
Hieman alhaisempaa keskiarvoa nähdään ensimmäisen osan kysymyksissä 5, 6 ja 7.
Tästä voi päätellä henkilöstön toivovan hieman parempaa opastusta tietoturvallisuudesta ja työskentelystä tietoturvallisin menetelmin. Olisi myös hyvä kerrata toimintamalli tilanteessa, jossa huomataan tietojenkalastelua tai pahimmassa tapauksessa käyttäjätilin kaappaustilanne. Kyselyn ensimmäisen osan vapaa palaute yhtyy hyvin keskiarvoistakin nähtävään trendiin. Henkilöstö toivoisi lisää opastusta ja koulutusta tietoturvasta, sekä entistä enemmän yleistä keskustelua aiheesta.

Kuva 3. Tietoturvakyselyn ensimmäisen osan vastaukset



Kyselyn toisen osan kysymykset koskivat tietoturvan teknistä toteuttamista Koskisella. Kuvassa 4 olevista vastauksista voidaan päätellä eri palveluiden kirjautumisien ja kaksivaiheisen tunnistautumisen toimivan pääsääntöisesti melko mutkattomasti. Myöskään VPN- yhteyden muodostamisessa ei nähdä suuria haasteita, toki tekniset ratkaisut ovat herkkiä vikatilanteille ja inhimillisille virheille. Vikatilanteissa palvelut on kuitenkin saatu lähes poikkeuksetta kuntoon eikä niistä ole raportoitu aiheutuneen merkittäviä esteitä sujuvan työn tekemiselle.

Kuva 4. Kyselyn toisen osan vastaukset

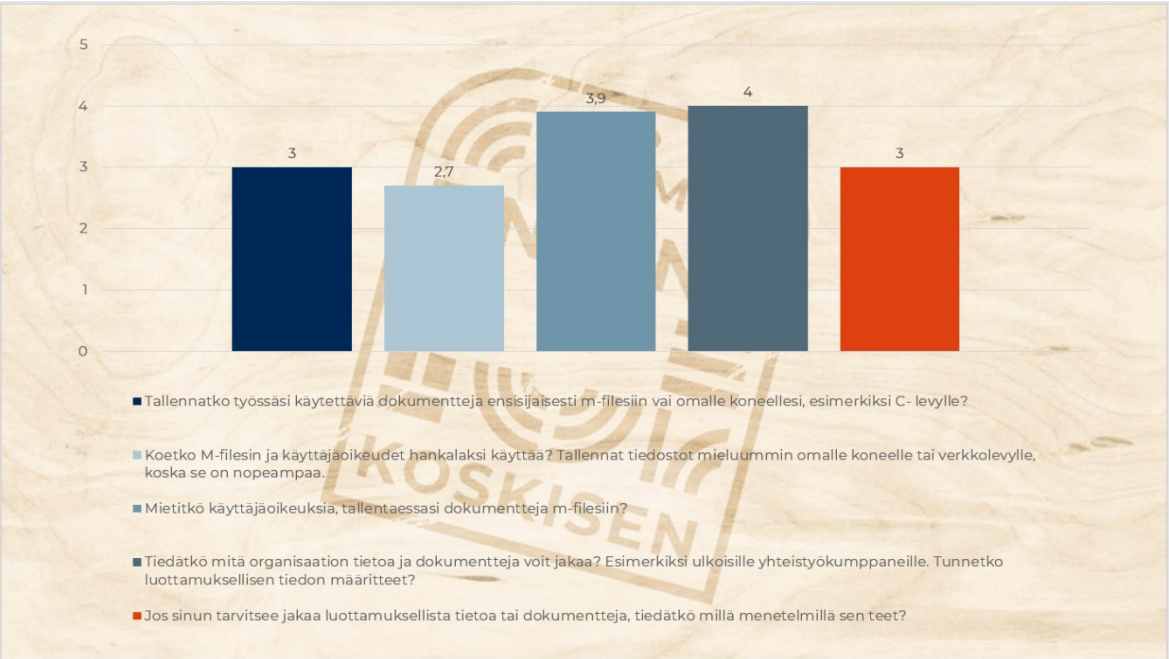


M-files ja sen dokumenttikohtaisessa oikeuksien hallinnassa nähdään olevan vielä parantamisen varaa. Eri järjestelmien pääsyoikeuksissa ei kuitenkaan nähdä suurta parannettavaa. Henkilöstö kokee heillä olevan riittävästi oikeuksia tehokkaaseen työskentelyyn ja mahdollisia lisäoikeuksia tai hallintatunnuksia saa tarvittaessa, kun niiden antamiseen nähdään olevan riittävät perustelut.

Salasanapolitiikka koetaan pääsääntöisesti selkeäksi, kyselyn perusteella on kuitenkin noussut esille muutamia poikkeamia, jotka on syytä ottaa lähempään tarkasteluun. Nämä poikkeamat ovat liittyneet lähinnä salasanakäytäntöihin. Myöskään muutaman sanallisen palautteen perusteella politiikkaa ei koeta tarpeeksi selkeäksi, eikä salasanan tarkkoja kriteerejä aina tiedetä. Muutaman palautteen mukaan salasanoja kysellään liian usein tai eri järjestelmiin kirjautumisissa koetaan olevan epäloogisuutta. Sähköpostin kautta tulevaa roskapostia tulee osalle henkilöstöstä melko paljo, osalle taas ei juuri ollenkaan. Tällaisen tilanteen arvioidaan johtuvan verkkosivuilla olevista yhteystiedoista. Verkkosivuilla halutaan avainhenkilöiden, myyjien ja yksiköiden johdon yhteystietojen olevan helposti saatavilla asiakkaille. Tämä toimintamalli aiheuttaa kuitenkin tilanteen, jossa sähköpostisoitteet ovat helposti eri automatisoitujen roskapostibottien, kaupustelijoiden ja muiden ei-toivottujen tahojen saatavilla. Roskapostisuodatinta kiristämällä saattaa aiheutua tilanne, jossa myös toivotut yhteydenotot ja asiakaskontaktit saattavat jäädä roskapostisuodattimen kynsiin, eivätkä ne tavoittaisi vastaanottajaansa.

Kyselyn kolmannen osan kysymykset keskittyivät tiedon tallentamiseen ja jakamiseen. Kuvassa 5 esiteltävien vastausten perusteella näemme tämän aiheen olevan henkilöstölle vieraampaa. Tietoa tallennetaan herkästi oman koneen sisäiseen muistiin tai pilvitallennuspalveluihin, kuten Microsoftin Onedrive. Toisaalta ensimmäisten kysymysten johdatteleva sävy saa herkästi vastaamaan tähän kysymykseen myönteisesti, mutta myös vapaat vastaukset ja aikaisemmat kokemukset aiheesta tukevat keskiarvosta nähtävää suuntaa.

Kuva 5. Kyselyn kolmannen osan vastaukset

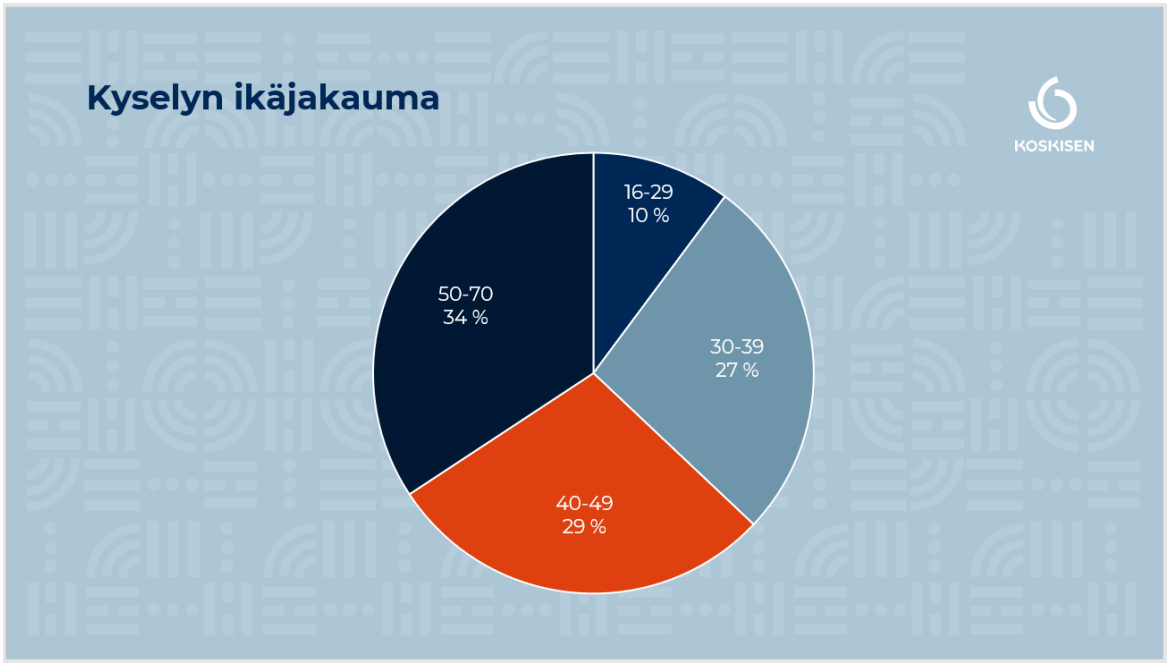


Kyselyn ja sanallisen kirjoitetun palautteen perusteella saa tilanteesta helposti sellaisen kuvan, ettei M-Filesia käytetä kovinkaan mielellään, koska se koetaan hankalaksi tai hitaaksi käyttää. Kyselyn sanallisen palautteen perusteella dokumentteja ei myöskään löydetä kovin helpolla M-Filesin rakenteesta. Tämä johtaa helposti sellaiseen skenaarioon, jossa käyttäjä tallentaa mieluummin tietoa muiden ulottumattomille esimerkiksi oman koneensa kiintolevylle, koska se on nopeampaa. Tällöin esimerkiksi yhteisen tiedon saatavuutta muille käyttäjille ei voida varmistaa. Tiedon eheys ja luottamuksellisuus saattaa myös vaarantua, jos ei sitä tallenneta sellaiseen paikkaan, missä sen olemassaolo voidaan tietoteknisin ratkaisuin turvata. Toisin sanoen M-Filesin käytettävyyteen ja sen toimintojen tehokkaaseen hyödyntämiseen toivotaan parempaa opastusta, sekä koulutusta.

Kyselyn viimeiset kolme kysymystä keskittyivät käyttäjäoikeuksiin M-filesin sisällä, sekä luottamuksellisen tiedon tallentamiseen- ja jakamiseen. Se osa henkilöstöstä, joka käyttää M-Filesia aktiivisesti miettii pääsyoikeuksia ja heille tuntuu olevan melko selkeää miten eri käyttöoikeusryhmät ja osastot M-Filesin sisällä toimivat. Vastauksien perusteella luottamuksellisen tiedon määritteet tunnetaan hyvin ja tiedetään mitä tietoa tai dokumentteja talon ulkopuolelle voi jakaa. Sanallisten vastausten perusteella se osa henkilöstöstä, joka työnsä puolesta on tekemisissä luottamuksellisen tiedon kanssa, osaa hallita ja jakaa sitä asiaankuuluvilla menetelmillä tai ottaa selvää, miten se kuuluisi oikeaoppisesti tehdä. Kuitenkin jakamiseen käytettävät tekniset ratkaisut eivät selvästi ole täysin tuttuja ja siihen olisi syytä kiinnittää huomiota ja antaa ohjeistusta.

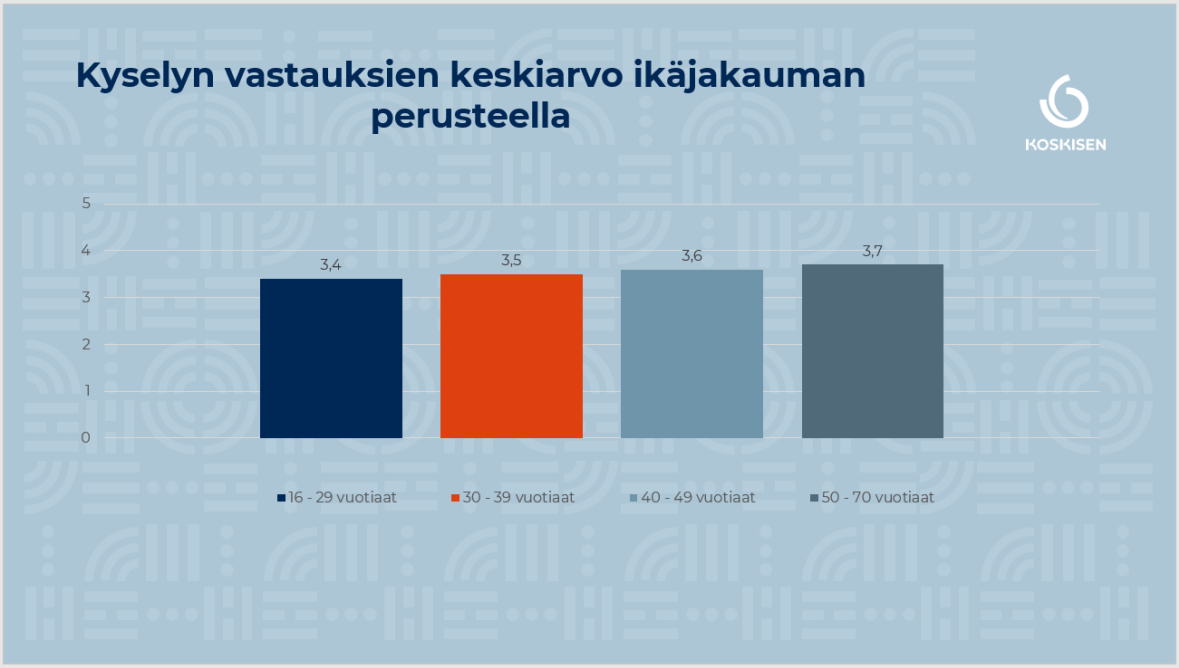
Kyselyyn vastasi kaiken kaikkiaan 108 henkilöä ja Kuvan 6 perusteella nähdään, että myös henkilöstön vanhempi ikäpolvi on ottanut kyselyn hyvin vastaan ja käynyt antamassa vastauksia hyvällä osallistumisprosentilla, kyselyn aiheen ja sisällön teknisestä luonteesta huolimatta. Jakauman perusteella voisi vetää johtopäätöksiä, että myös vanhempi ikäpolvi on kiinnostunut ja kokee tietotekniikan, sekä tietoturvan tärkeäksi asiaksi.
Ikäjakauma on hyvin linjassaan myös Koskisen henkilöstön ikäjakauman kanssa, joten voidaan päätellä kaikilla ikäluokilla olleen tasainen vastausprosentti.

Kuva 6. Kyselyyn vastanneiden ikäjakauma



Kyselyn ikäluokkien vastauksista kuvassa 7 nähdään, ettei vastaajan ikä vaikuta juurikaan tietämykseen tietoturvasta. Koskisen henkilöstö vaikuttaisi olevan tasavertaista tietoturvatietämyksessä iästään riippumatta. Tämän voidaan katsoa olevan erittäin hyvä asia. Tarkempien tulosten saamiseksi täytyisi tutkia osaamista isommalla joukolla, koska nyt kyselyyn vastasi vain hieman yli 10 % koko Koskisen konsernin henkilöstömäärästä.

Kuva 7. Vastauksien keskiarvot ikäluokittain



5.2 Tietohallinnon näkemys henkilöstön tietoturvallisesta käyttäytymisestä

Koskisen tietohallinto muodostuu noin 10 hengen tiimistä. Osa tiimiläisistä työskentelee tiiviisti osana eri tuotantoyksiköitä ja toimipisteitä, osa taas Järvelässä pääkonttorilla koko konsernin ja keskushallinnon palveluiden kehittämisessä. Tietohallinnolla on siis hyvä kokonaiskuva kaikista konsernin toiminnoista, heidän tehdessä tiivistä yhteistyötä tietoteknisten ratkaisujen parissa.

Kyselyn tuloksia on purettu yhteisesti tiimin kanssa ja saadut tulokset ovat olleet melko hyvin linjassaan tietohallinnon aikaisemmasta näkemyksestä henkilöstön tietoturvallista käyttäytymistä kohtaan. Yleinen näkemys on, että palveluita tulee kehittää entistä

käyttäjäystävällisempään suuntaan ja näin saada mielekkyyttä työtä ja siinä tarvittavia välttämättömiä teknisiä ratkaisuja kohtaan.

5.3 Johtopäätökset

Tietotekniikka ja erilaiset palvelut kehittyvät koko ajan, siitä syystä on hyvä pysyä ajan tasalla ja mukana kehityksessä. Koskisella tietoturvan voidaan katsoa olevan jo nyt hyvällä mallilla ja siihen on syytä panostaa myös jatkossa. Kyselyn pohjalta esiin tulleita asioita käydään jatkossakin yhteisesti läpi ja negatiivisiin käyttäjäkokemuksiin pyritään saamaan ratkaisuja. Kyselystä ehkä vahvimpana esiin noussut M-Filesin käytön hankaluus tai epämielekkyys pyritään korjaamaan tulevaisuudessa järjestämällä erilaisia koulutus ja opastustilaisuuksia. Konsernin yhteisessä sisäisessä tiedotuskanavassa tullaan jakamaan vinkkejä ja opastusta tietoturvalliseen työskentelyyn ja sen tekniikoihin liittyen. Opinnäytetyön kirjoittamisen aikana tietohallinnon toimesta on aloitettu kyselyn aiheisiin liittyvä videosarja, jossa henkilöstöä muistutetaan tietoteknisistä vaaroista ja turvallisista yhteisistä toimintatavoista, sekä neuvotaan toimintaan poikkeustilanteissa.

Kyselyn perusteella henkilöstöä selvästi kiinnostaa tietoturva aiheena ja siitä toivotaankin yhä enemmän tietoa, sekä vapaampaa keskustelua. Tähän pyritään kehittämään ratkaisuja, joilla tekninen ja osittain etäiseltäkin tuntuva aihe saataisiin kaikkien tietoisuuteen ja näin osaamistasoa nostettua yhä paremmalle tasolle.

Lähteet

AVG. (2020). *How does a VPN work?* [kuva]
https://www.avg.com/en/signal/what-is-a-vpn-and-why-should-you-use-one

Cynet (07/2021). *Top 6 EDR Tools Compared – A Complete Guide* haettu 27.8.2021 osoitteesta https://www.cynet.com/endpoint-protection-and-edr/top-6-edr-tools-compared/

Deltagon (n.d.). *Miksi sähköposti tulisi salata?*
https://www.deltagon.com/fi/blogi/sahkopostin-salaus

Hyvönen, T. (14.8.2017). *Tietoturva yrityksen tehokkaan liiketoiminnan ja häiriöttömän toimintaympäristön takeena.* Tuokko.fi https://tuokko.fi/yrityksen-tietoturvallisuus-luo-takeet-tehokkaalle-liiketoiminnalle/

Kaspersky. (n.d.). *Miten haittaohjelmista pääsee eroon?*
https://www.kaspersky.fi/resource-center/threats/malware-protection

Klusaite, L. (20.12.2020). *Mikä on palomuuri?*
https://nordvpn.com/fi/blog/palomuuri/

Koskisen today. (2020). *Koskisen vuosittainen esitejulkaisu*

Kyberturvallisuuskeskus. (07/2020). *Tietoturva* haettu 30.7.2021 osoitteesta
https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Laakso, M. (n.d.). *Henkilöstöturvallisuus*
https://tietojesiturvaksi.fi/tietoturvasuunnitelma/henkilostoturvallisuus

Mtech. (12/2019). *Mistä yrityksen tietoturva*
https://www.mtech.fi/blogi/mista-yrityksen-tietoturva-koostuu/

NordVPN. (n.d.). *Mikä on VPN?*
https://nordvpn.com/fi/what-is-a-vpn/

Okta. (n.d.). *How firewalls work* [Kuva]
https://www.okta.com/au/identity-101/firewall/

Palmu, P. (10/2019). *Miksi varmuuskopiointi on tärkeää – näin turvaat tiedostosi*
https://www.etevat.fi/blogi/miksi-varmuuskopiointi-on-tarkeaa-nain-turvaat-tiedostosi

Sanastokeskus. (2004). *Tiivis tietoturvasanasto* haettu 13.8.2021 osoitteesta
https://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf

vpnyhteys.fi. (n.d.). *VPN-yhteys suojaa yksityisyyttä internetissä*.
https://www.vpnyhteys.fi/

Webropol. (n.d.). *Kysely- ja raportointityökalu*
https://webropol.fi/kysely-ja-raportointityokalu/

Wikipedia. (2020). *Varmuuskopiointi* haettu 23.7.2021 osoitteesta
https://fi.wikipedia.org/wiki/Varmuuskopiointi

Liite 1: Tietoturvakysely Koskisen koti- ja ulkomaan henkilöstölle

KOSKISEN

Tietoturvakysely henkilöstölle

Osio 1/3

Taustakysymyksiä.

Osion lopussa kenttä vapaalle palautteelle ja kehitysajatuksille.

1. Missä tehtävissä työskentelet?

- ◯ Myynti
- ◯ Markkinointi
- ◯ ICT
- ◯ Talous
- ◯ Tuotanto
- ◯ Osto/Logistiikka
- ◯ HR
- ◯ Hallinto
- ◯ Kunnossapito
- ◯ Muu

2. Vastaajan ikähaarukka

- ◯ 16 - 29 vuotta
- ◯ 30 - 39 vuotta
- ◯ 40 - 49 vuotta
- ◯ 50 - 70 vuotta

3. Tiedätkö mitä tietoturva tarkoittaa?

	1	2	3	4	5	
En tiedä	○	○	○	○	○	Koen tietäväni paljon tietoturvasta

4. Koetko tietoturvan tarpeelliseksi asiaksi?

	1	2	3	4	5	
En ollenkaan	○	○	○	○	○	Koen sen erittäin tärkeäksi

5. Kiinnitätkö huomiota tietoturvaan omassa työssäsi?

	1	2	3	4	5	
En ollenkaan	○	○	○	○	○	Mietin tietoturvaa jatkuvasti

6. Onko lisääntynyt etätyöskentely muuttanut suhtautumistasi tietoturvaan. Koetko työskentelyn erilaiseksi kotoa käsin, kuin paikanpäällä konttorilla?

	1	2	3	4	5	
En ole huomannut eroa	○	○	○	○	○	Etätyöskentely on muuttanut ajattelutapaani ja toimin nyt erilailla kuin ennen

7. Millainen näkemys sinulla on Koskisella toteutettavasta tietoturvasta, onko se riittävää? Koetko olevasi "turvassa"?

	1	2	3	4	5	
Toteutus ei ole riittävää	○	○	○	○	○	Koskisella toteutetaan tietoturvaa erittäin hyvin

8. Koetko saavasi riittävästi opastusta ja tukea työskentelyyn tietoturvallisesti? Löydätkö riittävästi tietoa tietoturvasta esim. Intrasta?

1	2	3	4	5

	1	2	3	4	5	
En ollenkaan	○	○	○	○	○	Saan tukea ja ohjeita riittävästi

9. Tiedätkö miten toimia tilanteessa, jossa huomaat joutuneesi tietojenkalastelun kohteeksi tai tilisi kaapatuksi?

	1	2	3	4	5	
En tiedä miten toimia	○	○	○	○	○	Tiedän miten toimia ja osaan ottaa yhteyttä oikeaan tahoon.

10. Vapaa palaute ja kehitysajatukset Taustakysymykset- osioon.

Osio 2/3

Koskisella käytössä olevat tietoturvallisuuden työkalut

Kullekkin eri työkalulle on varattu oma arvosteluasteikko. Voit myös halutessasi antaa palautetta ja kehitysajatuksia sille varattuun laatikkoon sivun lopussa.

11. Kirjautumisen kaksivaiheinen tunnistus mobiililaitteella

	1	2	3	4	5	
Toimii huonosti	○	○	○	○	○	Toimii hyvin

12. VPN- etäyhteys kotikonttorilla

	1	2	3	4	5	
Toimii huonosti	○	○	○	○	○	Toimii hyvin

13. Käyttäjäoikeuksien hallinta (m-files ja verkkopalvelimet)

	1	2	3	4	5	
Oikeuksien hallinta on hankalaa	○	○	○	○	○	Oikeuksien hallinta on helppoa

14. Pääsyoikeudet eri Koskisen järjestelmiin (m-files, verkkopalvelimet, sovellukset, pilvipalvelut)

	1	2	3	4	5	
Minulla ei ole riittävästi oikeuksia	○	○	○	○	○	Minulla on riittävät oikeudet ja saan lisää tarvittaessa

15. Salasanapolitiikka (salasanan vaatimukset ja salasanan vaihtoväli)

	1	2	3	4	5	
Salasana vaihtuu liian usein ja sillä on liian tiukat kriteerit	○	○	○	○	○	Salasanan vaihtoväli on sopiva ja sillä on sopivat kriteerit.

16. Sähköpostin roskapostisuodatus

	1	2	3	4	5	
Toimii huonosti / saan paljon roskapostia	○	○	○	○	○	Toimii hyvin / en saa juurikaan roskapostia

17. Vapaa palaute ja kehitysajatuksia Tietoturvallisuuden tekniikat- osioon

Osio 3/3

Dokumentinhallinta

Yleiskysymyksiä dokumentinhallinnasta. Voit antaa palautetta ja kehitysajatuksia osion lopussa olevaan laatikkoon.

18. Tallennatko työssäsi käytettäviä dokumentteja ensisijaisesti m-filesiin vai omalle koneellesi, esimerkiksi C- levylle?

	1	2	3	4	5	
Oma tietokone / yhteinen verkkolevy	○	○	○	○	○	M-files

19. Koetko M-filesin ja käyttäjäoikeudet hankalaksi käyttää? Tallennat tiedostot mieluummin omalle koneelle tai verkkolevylle, koska se on

nopeampaa.

	1	2	3	4	5	
Koen M-filesin hankalaksi käyttää	○	○	○	○	○	M-files on helppokäyttöinen ja tallennan dokumentit ensisijaisesti sinne

20. Mietitkö käyttäjäoikeuksia, tallentaessasi dokumentteja m-filesiin?

	1	2	3	4	5	
En mieti käyttäjäoikeuksia, annan dokumenteille isot oikeudet	○	○	○	○	○	Mietin käyttäjäoikeudet tarkkaan ja harkitusti

21. Tiedätkö mitä organisaation tietoa ja dokumentteja voit jakaa? Esimerkiksi ulkoisille yhteistyökumppaneille. Tunnetko luottamuksellisen tiedon määritteet?

	1	2	3	4	5	
En ajattele asiaa.	○	○	○	○	○	Mietin tarkkaan mitä tietoa voin jakaa ulkoisille yhteistyökumppaneille.

22. Jos sinun tarvitsee jakaa luottamuksellista tietoa tai dokumentteja, tiedätkö millä menetelmillä sen teet?

	1	2	3	4	5	
En ole täysin varma, tarvitsen lisäopastusta	○	○	○	○	○	Tiedän ja tunnen menetelmät sekä käytännöt

23. Vapaa palaute ja kehitysajatuksia Dokumentinhallinta- osioon tai mihin tahansa tietoturvaa koskevaan asiaan.