OHJEITA TURVALLISEEN ETÄTYÖHÖN

2021

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

www.huoltovarmuus.fi

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa. Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Julkaisija:
Huoltovarmuusorganisaatio.
Huoltovarmuusorganisaatio on verkosto, joka työskentelee yhdessä Suomen toimintakyvyn ja sen edellyttämän huoltovarmuuden hyväksi. Siihen kuuluvat Huoltovarmuuskeskus ja sen hallitus, huoltovarmuusneuvosto sekä eri toimialojen sektorit ja poolit.

Selvityksen tekijä:
Tämä ohje tehtiin yhteistyössä KPMG Oy Ab:n riippumattomien asiantuntijoiden kanssa.

Kuvat: Shutterstock

Taitto: Up-to-Point Oy

Julkaisuvuosi: 2021

ISBN: 978-952-7470-09-1

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

Sisältö

JOHDANTO

Pandemia-aika on lisännyt etätyötä tekevien määrää huomattavasti. Digipooli on jo aiemmin julkaissut pikaohjeen etätyövälineiden turvallisempaan käyttöön. Pikaoppaan löydät ***täältä***. Tämä ohje koskee laajemmin teknistoiminnallisia etätyöohjeita, joiden avulla yritykset voivat ottaa käyttöön entistä turvallisempia etätyöhön liittyviä sovelluksia ja järjestelmiä sekä kehittää henkilöstönsä etätyöohjeistusta ja osaamistasoa.

Työ etätyöohjeen laatimiseksi käynnistettiin kesäkuussa 2021. Vallitsevan tilanteen hahmottamiseksi laadittiin sähköinen kysely sekä toteutettiin haastatteluja elo-syyskuussa 2021. Kyselyn avulla kartoitettiin mm. mahdollisuutta etätyön tekemiseen, millä laitteilla (työnantajan / omilla) etätyötä voidaan tehdä sekä minkälaisin ratkaisuin (virtualisointi, web-sovellukset jne.), onko käytössä laitehallinta sekä mitä on määritelty työvälineiden säilytyksestä, matkustamisesta, tietoturvallisuusluokituksista jne. Kyselyyn vastaisi 125 yritystä ja sen tuloksia on kuvattu liitteessä 2. Kyselyn ajankohta vaikutti merkittävästi yrityksien näkökulmaan etätyöstä koronapandemian vaikutusten takia. Kyselyn tulosten sekä 21 haastattelun havainnot on analysoitu ja niitä on hyödynnetty osana tämän oppaan sisältöjä yhdessä muiden tietolähteiden kanssa. Tämä opas ei ole kaiken kattava eikä **pelkästään tässä kuvattuja oppeja noudattamalla voida taata riittävää tietoturvaa ja -suojaa** yrityksissä. Jokaisen yrityksen on luotava omaa toimintaympäristöä, yrityskulttuuria ja kyvykkyyksiä vastaavat tietoturvallisuuskäytännöt.

Kyselyn keskeiset havainnot:

- Hyvin ymmärrettyjen toimintamallien, prosessien ja käytäntöjen merkitys korostuu hajautuneessa etätyöympäristössä luonnollisen kanssakäymisen vähentyessä
- Yritykset ovat pääosin valmistautuneet etätyöskentelyyn
- Puolelle vastaajista ei ollut määritelty ohjeistuksia etätyön työympäristölle tai vaatimuksia työvälineiden säilyttämiseen
- Yleisin tekninen etätyön mahdollistava ratkaisu oli VPN-yhteys (88 %)
- Vahva tunnistautuminen oli käytössä 76 % vastaajista
- 33 %:lle vastaajista ei ollut määritelty turvaluokitukseen perustuvia etäkäyttövaatimuksia

Kyselyn perusteella haasteita oli ainakin:

- Yhteyksien muodostamisessa, vakaudessa ja nopeuksissa etätyön määrän nopeasti kasvaessa
- Verkkojen toimivuudessa, mikäli työntekijä käyttää mobiiliverkkoa syrjäisemmillä alueilla tai taajamissa
- Etätyöohjeiden tulkinnassa, esimerkiksi ohjeiden noudattamisessa kotiolosuhteissa
- Turvallisuusluokitellun tiedon käsittelyssä ja jakamisessa
- Käyttäjien eri osaamistasoissa, jonka vuoksi käyttäjille kaivattiin ”rautalankaohjeita”

Lähes kaikissa haastatelluissa yrityksissä oli olemassa etä-/joustotyön ohjeistus jo ennen koronaa. Osalla tämä on tarkoittanut etätyön määrittämistä työaikalainsäädännön mukaisesti, toisilla

käytännön toiminnan ohjeistusta (esimerkiksi toimiminen matkustettaessa tai julkisissa tiloissa). Pandemian vaikutus toimintatapojen muutokseen on ollut havaintojen perusteella vähäinen – huomio on ollut lähinnä VPN-yhteyksien kapasiteetissa ja toiminnan varmistamisessa. Kirjallisiin etätyöohjeisiin on tehty hyvin vähän (tai ei ollenkaan) muutoksia. Tarve etätyöohjeelle on kuitenkin ilmeinen, koska etätyöhön siirryttäessä ei ole enää mahdollista kysyä vieressä istuvalta kollegalta apua aiemmin itseään epäilyttävissä tietoturva tai -suoja-asioissa. Etätyötä tullaan myös jatkamaan erilaisissa hybridimalleissa, asiakas- ja luottamuksellisuusvaatimukset huomioiden. Haastattelujen perusteella moni yritys onkin panostanut tietoturvasta ja -suojasta muistuttamiseen sekä etätyössä jaksamiseen.

Yleinen havainto haastatteluista on, että tietojen suojaamiseen ja tietoturvaan pätevät samat ohjeet niin toimistolla kuin muuallakin. Sillä, missä tietoja käsitellään, ei ole niin paljon väliä, mikäli tiedon luokittelun, omistajuuden ja tallentamisen politiikat ovat yrityksessä dokumentoitu, ohjeistettu sekä viestitty. Tekniset ratkaisut esimerkiksi yhteyksien suojaamiseksi ovat yleisesti ottaen hyvällä tasolla, mutta sisällön suojaamisessa on parantamisen varaa. Tästä johtuen alla olevissa suosituksissa kehotetaan kiinnittämään huomiota esimerkiksi tietosisältöjen suojaamiseen sekä vahvan tunnistautumisen käyttöönottoon.

Huomioi ainakin nämä asiat yrityksessäsi ja tietoturvallisuutta koskevassa ohjeistuksessa:

- Turvaa verkkoyhteydet:
  - Määrittele, mitkä yrityksen käyttämät ohjelmat ja palvelut ovat VPN-yhteydellä suojattuja ja automatisoi suojattu point-to-point yhteys päätelaitteelta yrityksen verkkoon
  - Kytke yrityksen verkkoon ainoastaan yrityksen hyväksymiä laitteita

- Määrittele roolit ja suojaa sisältöä:
  - Määrittele roolipohjaisesti järjestelmät ja tieto, johon henkilöllä on roolinsa puitteissa oikeus eri käyttöympäristöissä
  - Laadi luokittelukäytännöt yrityksessä jaettavalle ja käsiteltävälle tiedolle
  - Varmista, että vahva tunnistautuminen on käytössä kaikissa tavoissa muodostaa yhteyksiä yrityksen suojattavaan tietosisältöön

- Tunnista käyttäjät:
  - Määrittele salasanoja ja niiden vaihtamista koskeva politiikka yrityksessä ml. salasanan pituus, monimutkaisuus ja vaihtaminen
  - Ohjeista työntekijöitä, että salasanaa ei tule tallentaa mihinkään työkoneella olevaan tiedostoon, ellei kyseessä ole salasanojen hallintaohjelmisto

- Varmista ohjelmien ja laitteistojen ajantasaisuus:
  - Varmista, että ohjelmistot ja niiden päivitykset jaetaan automaattisesti työasemiin
  - Varmista myös laitteiston ajureiden ja laiteohjelmistojen päivitysten toteutuminen etäkäyttötilanteissa
  - Älä anna työntekijän asentaa yrityksen tietokoneisiin omia ohjelmistoja tai päivittää niitä elleivät hänen työtehtävänsä ja roolinsa sitä edellytä

- Kouluta ja opasta riskien tunnistamiseen ja niiltä suojautumiseen:
  - Järjestä pakollisia tietoturvallisuuskoulutuksia työntekijöille säännöllisesti
  - Huolehdi koulutuksen avulla, että työntekijät tunnistavat tietoturva- ja suojariskit ja osaavat suojautua niiltä

Lisäksi ohjeista työntekijöitä varmistamaan tietoturva myös etätyöolosuhteissa:

- Toiminta muualla kuin yrityksen toimipisteellä:
  - Suojaa tieto näkemiseltä ja kuulemiselta, myös perheenjäsenten osalta
  - Älä liitä työasemaan ulkopuolista USB-laitetta
  - Vaihda kodin IoT-laitteiden oletussalasanat laitteiden käyttöönoton yhteydessä
  - Tunnista ulkomaanmatkoihin liittyvät riskit ja arvioi niiden edellyttämä varautuminen
  - Älä lataa puhelintasi tai tietokonettasi ulkopuolisten tarjoamilla latureilla

TEKNISET RATKAISUT

Verkkoyhteyksien turvaaminen

Yleisin ja yksinkertaisin ohje verkkoyhteyksien turvaamiseen on julkisten WLAN-verkkojen välttäminen. Osa yrityksistä suhtautuu myös työntekijän kotona olevaan henkilökohtaiseen WLAN-verkkoon samaan tapaan kuin julkisiin verkkoihin. Tyypillisimpiä murretuksi joutuvia laitteita ovat suojelupoliisin viimeisimpien havaintojen perusteella kotireitittimet ja verkkotallennusjärjestelmät.

WLAN on langaton lähiverkko, jossa tieto kulkee ikään kuin selkokielellä. Avoimen verkon liikennettä voi verrata LA-radiopuhelimen kuunteluun: jos vain on oikealla taajuudella, kuulee kaiken.

Yle.fi: Avoin wifi houkuttelee – älä unohda vaaroja

Verkkoyhteyksien turvaaminen voidaan toteuttaa useammalla eri tavalla. Yksi keino on ohjeistaa työntekijää käyttämään kodin WLAN-verkon sijaan älypuhelimen mobiiliyhteyttä. Toinen vaihtoehto on mobiiliyhteys itse työasemassa.

Ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun.

Suojelupoliisin tiedote, 10.3.2021

Osa yrityksistä on luopunut henkilökohtaisen verkon suojaamisesta ja luottaa sen sijaan suojattuun P2P (point-to-point) -yhteyteen päätelaitteelta yrityksen verkkoon. Toiminnosta käytetään myös termiä VPN-tunnelointi (virtual private network). Yhteys muodostetaan joko automaattisesti tai käyttäjän toimesta. Näin toimimalla kaikki tai osa tietoliikenteestä menee salatun VPN:n kautta muodostaen ”tunnelin”, johon sivullisilla ei ole pääsyä. VPN:n koetaan vähentävän riskiä hakkerointiin ja tietovuotoihin.

On yrityksen omasta politiikasta kiinni, kulkeeko kaikki tietoliikenne VPN-yhteyden kautta. Osassa yrityksiä on jouduttu lisäämään kapasiteettia, jotta tietoliikenne kokonaisuudessaan voidaan ohjata VPN-tunnelin läpi. Tunnelin sisällä voi olla myös palvelukohtaisia rajoituksia. **Yrityksissä kannattaa määritellä minkä kaiken on oltava VPN:n kautta suojattua**. Esimerkiksi Google Meet, Teams ja Zoom voidaan jättää VPN-tunnelin ulkopuolelle, vapauttaen verkon kapasiteettiä muille tietoliikenneyhteyksille.

Työaseman suojaaminen pitää sisällään myös muita elementtejä kuten henkilökohtainen palomuuri sekä virusten, haittaohjelmien ja kehittyneiden uhkien suojaus. Tämän lisäksi voidaan hyödyntää lokitietojen tallennusta. Internetiin yhdistetyt laitteet ja operaattorit keräävät lokitietoja, joiden avulla on mahdollista selvittää mitä, miksi ja milloin jotakin on tapahtunut. Katso lisätietoa lokituksesta ***täältä***.

Verkkoyhteyksien turvaamisen osalta tietoturvan tasoa voidaan parantaa:

- Ohjeistamalla työntekijää välttämään julkisten WLAN-verkkojen käyttämistä
- Ohjeistamalla joko korvaamaan henkilökohtainen WLAN-yhteys kotona yrityksen (mobiili)yhteydellä tai koventamaan reititin ja käyttämään aina VPN-yhteyttä
- Määrittelemällä mitkä yrityksen käyttämät ohjelmat ja palvelut ovat VPN-yhteydellä suojattuja ja automatisoimalla suojattu point-to-point yhteys päätelaitteelta yrityksen verkkoon
- Hyödyntämällä tarvittaessa myös muita elementtejä, kuten henkilökohtaista palomuuria
- Määrittelemällä internet-selaimen tietoturva-asetukset
- Ohjeistamalla parhaat käytännöt reitittimien ja muiden verkkoon kytkettyjen laitteiden asetusten osalta, esimerkiksi
  - Pääsyn estäminen reitittimen hallintaan internetistä
  - Oletussalasanojen vaihtaminen vaikeasti arvattavaksi ja mahdollisimman pitkäksi, suosituspituutena on vähintään 20 merkkiä
  - Reitittimen koventaminen sulkemalla tarpeettomat avoimet portit
  - Reitittimen laiteohjelmiston päivittäminen

Tunnistautuminen ja käyttäjäryhmät

Vahva tunnistautuminen

Vahva tunnistaminen vähentää riskiä perinteiseen käyttäjätunnus ja salasana -yhdistelmään verrattuna lisäämällä uuden elementin tunnistautumiseen. Yleensä vahva tunnistaminen ei korvaa käyttäjätunnusta ja salasanaa, mutta saattaa piilottaa ne käyttäjältä tunnistamisen tehostamiseksi. Vahvaa tunnistamista voidaan toteuttaa käyttäen useita eri mekanismeja[1], joiden käytettävyys ja turvallisuus vaihtelevat käyttöympäristöstä ja vaatimuksista riippuen.

Yrityksissä on huomattavia eroja vahvaan tunnistautumiseen hyväksyttyjen mekanismien osalta. Erityisesti suhtautuminen biometriseen tunnistamiseen vaihtelee merkittävästi tietoturva- ja tietosuojasyiden takia.

Pelkän käyttäjätunnuksen ja salasanan käyttämiseen liittyvien riskien merkittävyyden takia **investointi vahvan tunnistautumisen käyttöönottoon on yksi parhaimmista keinoista parantaa etäkäytön tietoturvaa**. Vahva tunnistaminen tulisi olla käytössä kaikissa tavoissa muodostaa yhteyksiä yrityksen suojattavaan tietosisältöön eikä rajoittua pelkästään tiettyyn käytössä olevaan sovellukseen tai mekanismiin.

Käyttäjäryhmät

Yrityksissä on toimialaan ja yrityskulttuuriin liittyvää merkittävää vaihtelua siinä, miten ja kuka voi etätyötä tehdä ja mitkä ovat etätyön edellytykset ja ehdot. Työntekopaikkana yrityksen oma toimisto on joillekin yrityksille ainoastaan paikka muiden joukossa, mutta toisille se on kiinteä osa työntekoa. Toimiala ja kulttuuri ovat tässä merkittävässä asemassa. Tuotannollisissa yrityksissä on selvää, että työnteon vaatimien laitteiden käytettävyys yleensä ohjaa tekemiseen yrityksen tiloissa, ja yleensä näissä tehtävissä edellytykset etätöille on vähäiset.

Asiakassopimukset voivat myös asettaa rajoituksia työntekopaikkaan. Samoin turvallisuusluokitellun tiedon / järjestelmien käsittelyn osalta voidaan vaatia työnteon tapahtuvan yrityksen tiloissa. Yleensä asiakassopimuksiin liittyy myös muita fyysisiä ja teknisiä turvaratkaisuja.

Etätyön yleistymisen myötä työntekijöitä on jaettu erilaisiin käyttäjäryhmiin perustuen siihen, missä ja minkälaisin tietoteknisin ratkaisuin työtä tehdään. Jako voi olla esimerkiksi vain toimisto / tuotantolaitosympäristössä työtä tekevät, ajoittain etätyötä tekevät ja pääsääntöisesti etätyötä tekevät. **Kun tiedetään, ketkä etätyötä voivat tehdä ja millä edellytyksillä, on mahdollista määritellä roolipohjaisesti (RBAC[2]) mihin järjestelmiin ja tietoon henkilöllä on roolinsa puitteissa** oikeus eri käyttöympäristöissä (jos käyttöympäristöt poikkeavat toisistaan).

1) Esimerkiksi biometrinen tunnistus (kasvot, sormenjäljet, iiris), todentajasovellukset, kertakäyttötunnukset, tunnistus tai turva-avaimet, varmenteet, SMS tai sähköposti

2) Role-based access control

Tunnistautumisen ja käyttäjäryhmien osalta tietoturvan tasoa voidaan parantaa:

- Ottamalla yrityksessä käyttöön vahva tunnistautuminen ja varmistamalla, että vahva tunnistautuminen koskee kaikkia tapoja muodostaa yhteyksiä yrityksen suojattavaan tietosisältöön
- Määrittelemällä etätyön reunaehdot ja kommunikoimalla ne työntekijöille
- Määrittelemällä roolipohjaisesti järjestelmät ja tieto, johon henkilöllä on roolinsa puitteissa oikeus eri käyttöympäristöissä

Salasanojen hallinta

Salasanan tarkoituksena on estää käyttäjätunnuksen luvaton käyttö. Hyvällä ja **riittävän monimutkaisella salasanalla on merkitystä**, koska **itse käyttäjätunnus on usein helposti arvattavissa** (esimerkiksi henkilön nimestä muodostettu sähköpostiosoite).

Työntekijöitä tulee ohjeistaa siitä, että salasanaa ei saa tallentaa mihinkään työkoneella olevaan tiedostoon ellei kyse ole salasanojen hallintaohjelmasta. Jotta työntekijä ei valitsisi itselleen liian helppoa salasanaa, on salasanan pituudelle ja merkkivalikoimalle suositeltavaa asettaa palvelun turvallisuuttaa lisääviä vaatimuksia. Nyrkkisääntö on, mitä pidempi salasana, sen parempi.

Hyvin pitkä salasana on kuitenkin vaikeasti muistettava, jolloin vaarana on sen unohtaminen. Lisäksi pitkiin salasanoihin liittyy riski, että ne kirjoitetaan paperille, joka puolestaan päätyy vääriin käsiin. Salasanojen sijaan voidaan käyttää salalauseita kuten esimerkiksi ”EnsimmäinenautonioliVolkswagen”, joka on mahdollista päivittää muotoon ”1autonioliVolkswagen”.

Jokaisessa yrityksessä on **määriteltävä salasanoja ja niiden vaihtamista koskeva politiikka**. Toistuvien epäonnistuneiden kirjautumisyrityksien tulee johtaa tunnuksen lukkiutumiseen. Kyberturvallisuuskeskus muistuttaa, että harvoin käytettyjen (kerran vuodessa tai harvemmin) palvelujen yhteydessä salasanan voi pyytää jokaisella kerralla uudestaan omaan sähköpostiin.

Hyvä salasana

- *Vähintään 15 merkkiä*
- *Sisältää isoja ja pieniä kirjaimia*
- *Sisältää erikoismerkkejä (%&//()=)*

Kyberturvallisuuskeskus

Salasanojen hallintasovellukset

Kyberturvallisuuskeskus suosittelee käyttämään salasanojen hallintasovellusta[3]. Sovelluksen avulla käytössä on hallintasovelluksen pääsalasana, jonka takana muut salasanat ovat tallessa. **Pääsalasana ei saa koskaan olla sama kuin muissa palveluissa käytetty salasana**. Turvallisuutta lisää edelleen kaksivaiheisen tunnistautumisen käyttöönotto, joka suojaa hallintasovellusta silloinkin, jos pääsalasana paljastuu. Samalla on syytä muistaa, että pilvipalveluina tarjottavissa hallintasovelluksissakin on ollut tietoturvahaasteita.

Hallinta-sovelluksen hyödyt

- *Salasanat ovat tallessa pääsalasanan takana*
- *Vahvojen salasanojen luominen ja säilyttäminen helppoa*
- *Salasanoihin kohdistuvilta hyökkäyksiltä suojautuminen*

Salasanojen hallinnan osalta tietoturvan tasoa voidaan parantaa:

- Määrittelemällä salasanoja ja niiden vaihtamista koskeva politiikka yrityksessä, ml. salasanan pituus, monimutkaisuus ja vaihtaminen
- Ohjeistamalla työntekijöitä siitä, että salasanaa ei tule tallentaa mihinkään työkoneella olevaan tiedostoon
- Ohjeistamalla työntekijöitä turvaamaan eri salasanat salasanojen hallintasovelluksella – pääsalasana ei saa koskaan olla sama kuin muissa palveluissa käytetty salasana

3) Markkinoilta löytyviä hallintasovelluksia ovat esimerkiksi 1Password, Bitwarden, Dashlane, Enpass, F-Secure ID PROTECTION, KeePass, Keeper, LastPass ja RoboForm

Ohjelmistojen asentaminen ja ohjelmistopäivitykset

Usein yrityksissä on tehty **periaatepäätös** siitä, **että työntekijä ei saa asentaa yrityksen tietokoneisiin omia ohjelmistoja tai päivittää niitä**. Hyvänä käytäntönä voidaan pitää ohjelmistojen automatisoitua jakelua työasemiin, jolloin yrityksen tietohallinnossa nähdään mitä ohjelmia (ja mikä versio) työasemiin on asennettu. Kaikki asennukset ja päivitykset toteutetaan ohjelmistoportaalin (esimerkiksi Software center MS Windows -käyttöjärjestelmässä) kautta. Tämä käytäntö vähentää yrityksen työaseman käytön houkuttelevuutta muuhun kuin työkäyttöön, alentaen samalla mahdollisten uhkien riskiä.

Säännöllisesti toistuvilla ja automaattisesti tapahtuvilla ohjelmistopäivityksillä varmistetaan ohjelmien (ja sitä kautta tietoturvan) ajantasaisuus. Yleisesti yrityksissä hyödynnetty käytäntö on, että päivitykset tapahtuvat pakotetusti käyttäjän toiminnasta huolimatta. Lähestyvästä ohjelmistopäivityksestä ilmoitetaan etukäteen, jotta käyttäjä voi huomioida lähestyvän päivityksen ja järjestää työtehtävänsä sen mukaisesti. Päivitykset voidaan ohjelmoida tapahtumaan työajan ulkopuolella (esimerkiksi iltaisin tai viikonloppuisin), jolloin ne eivät kuormita työaikana käytössä olevia yhteyksiä.

Päivityksiä on yleensä mahdollista siirtää muutamalla tunnilla eteenpäin. Näin toimimalla pyritään välttämään tilanteet, joissa ohjelmistopäivitys tapahtuu pakotetusti esimerkiksi kesken asiakastapaamisen. Yrityksissä on kuitenkin varmistettava, että **mikäli päivityksiä ei ole tiettyyn aikarajaan mennessä ajettu, pääsy yritysverkkoon ja -palvelimille estetään**, kunnes päivitykset on asennettu. Keskitetyllä ohjelmistojen ja päivitysten jakelulla turvataan ajantasaisuuden valvontaa. Tietohallinnossa seurataan päivitysten toteutumista ja voidaan puuttua häiriötilanteisiin. Päivitysten ajantasaisuuden ei tule olla kiinni siitä, että työntekijän on mentävä toimipisteelle ja koneen oltava sisäverkossa. Useimmissa yrityksissä ohjelmistojen asennus ja päivitykset hoidetaan nykyään myös etäyhteyden kautta.

Laitteiston ajureiden ja laiteohjelmistojen päivitykset

Laitteiston ajureiden ja laiteohjelmistojen (firmware, BIOS) päivitykset ovat muodostuneet kriittisemmiksi havaittujen haavoittuvuuksien lisääntyessä. Myös niiden päivitysten toteutuminen etäkäyttötilanteissa tulisi varmistaa. Teknisiä ratkaisuja päivitysten hoitamiseksi on olemassa, mutta niiden hallinta ja luotettavuus saattaa aiheuttaa riskejä erityisesti etäkäyttöympäristössä.

Mobiililaitteiden osalta yrityksissä hyödynnetään laitehallintasovelluksia, joita käyttäen voidaan varmistaa laitteiden vaatimustenmukaisuus sekä sovellusten ja päivitysten jakaminen. Laitehallintasovelluksilla voidaan myös riskitilanteissa (laitteen varastaminen tai väärinkäyttö) estää luottamuksellisen materiaalin hyödyntäminen.

Laitehallintaratkaisujen tulee kattaa yrityksen suojeluvelvoite hallussaan olevaan kolmannen osapuolen tietoon ja suojeluintressi yhtiön tietoon. Tämän takia tuntemus tekniseen toteutukseen ja lainsäädännöllisiin vaatimuksiin täytyy olla riittävä erityisesti silloin, kun laitetta käytetään henkilökohtaisessa käytössä tai laite ei ole yrityksen omistama.

Ohjelmistojen asentamisen ja päivitysten osalta tietoturvan tasoa voidaan parantaa:

- Kieltämällä työntekijöitä asentamasta yrityksen tietokoneisiin omia ohjelmistoja tai päivittämästä niitä, elleivät hänen työtehtävänsä ja roolinsa sitä edellytä
- Varmistamalla, että ohjelmistot ja niiden päivitykset jaetaan automaattisesti työasemiin
- Mikäli päivityksiä ei ole tiettyyn aikarajaan mennessä ajettu, varmistamalla, että pääsy yritysverkkoon ja -palvelimille estetään, kunnes päivitykset on asennettu
- Varmistamalla myös laitteiston ajureiden ja laiteohjelmistojen päivitysten toteutuminen etäkäyttötilanteissa

Sisällön jakaminen ja suojaaminen

Yritysten toiminnassa syntyy paljon sellaista tietoa, jota on tarpeen jakaa ja käsitellä yhteisesti. Oikeanlaista jakamista ja käsittelyä voidaankin pitää perusedellytyksinä toimivalle yhteistyölle ja verkostotoiminnalle. Tietojen jakamista ja käsittelyä varten on olemassa säännöstöjä, joiden avulla tiedon luovuttava taho pystyy osoittamaan toivomuksensa tiedon käsittelylle ja edelleen jakamiselle. Tällaisia ovat esimerkiksi Traffic Light Protocol (TLP) -käsittelyluokitus ja Chatham House -sääntö. Ensin mainittu koskee laajemmin dokumentteja ja tiedonvaihtoa, jälkimmäinen puolestaan tiedonvaihtoa tapaamisissa, kokouksissa ja tiedotustilaisuuksissa. Koronapandemian aikana monet kokoukset toteutettiin Chatham House -sääntöön nojaten, jolloin kokouksen osallistujat voivat hyödyntää saamiaan tietojaan, mutta eivät voi paljastaa tiedon antajaa, hänen organisaatiotaan tai muiden kokouksen osallistujien identiteettiä. Voit tutustua Traffic Light Protocoliin ja Chatham House -sääntöön ***tästä***.

Tieto on myös hyvin monen yrityksen tärkein pääoma. Tästä syystä **tiedon eli sisällön suojaamisesta on tulossa yhä tärkeämpi tekijä kaikissa organisaatioissa**. Koska tietoa on niin paljon, ei sen suojaaminen kaikilta osin ole järkevää. Onhan yritystoiminnassa myös paljon sellaista tietoa (yrityksen tuotteet, ratkaisut ja palvelut), jonka asiakkaiden ja yhteistyökumppaneiden halutaan löytävän. Sen sijaan hinnat ja muut yrityssalaisuudet jokainen yritys haluaa pitää vain itsellään. Henkilötietojen suojaamisesta säädetään puolestaan EU:n yleisellä tietosuoja-asetuksella (GDPR). Lisätietoja henkilötietojen suojaamisesta löydät täältä.

Suomalaiset yritykset ovat saaneet yhteensä satojentuhansien eurojen arvosta sakkoja Euroopan unionin yleisen tietosuoja-asetuksen eli GDPR:n rikkomisesta.

Helsingin Sanomat 10.9.2021

"Ei suojata vain järjestelmää vaan myös sisältöä. Sisällön suojaaminen yhä tärkeämpää."

Microsoft Oy

Yrityksen oman tiedon luokittelu

Sisällön suojaamisessa jokaisen yrityksen tulisi huomioida tiedon luokittelu, omistajuus ja elinkaaren hallinta. Tieto voidaan luokitella kolmesta neljään luokkaan – esimerkiksi julkinen, sisäinen, luottamuksellinen ja salainen – joiden mukaan sitä hallinnoidaan. Hallinnoinnin mahdollistavat politiikat, joiden mukaan pääsyä luokiteltuun aineistoon ohjataan. Politiikoissa on myös määritelty omistajuus ja vastuut (mukaan lukien mahdolliset järjestelmänhallinnan tason oikeudet). Jokaisen yrityksen tulisi sisällyttää tiedon luokittelu ja suojaaminen osaksi tietoturvallisuuskoulutusta (ks. myös Tietoturva- ja tietosuojakoulutus).

Sisällön tekninen suojaaminen luokittelun kautta ei ole monimutkaista, mutta sen hyödyntäminen yritysten keskuudessa on suhteellisen vähäistä. Yllä kuvattuun tiedon luokitteluun on mahdollista hyödyntää kaupallisia palveluita. Sisällön suojaamista voidaan edistää myös rajoittamalla pääsyä tietoon ajallisesti, esimerkiksi myöntämällä 30–40 päivän aikaikkuna tietyn tason tietojen käsittelyyn. Turvallisuusluokitellun tiedon käsittelyä on avattu tarkemmin tämän oppaan liitteessä 1.

Teknologia harvemmin on rajoittava tekijä sisällön suojaamiseksi, vaikka se saattaakin olla nykyaikaisessa monitoimittajaympäristön muodostamassa ekosysteemissä hankalampaa kuin aiemmin. Sen sijaan **kypsyys tiedon luokittelussa, omistajuudessa ja erityisesti elinkaarenhallinnassa on haastavaa**. Yrityksen sisäisten prosessien tulee tukea tiedon omistajuutta organisaatiomuutoksissa kestävän ratkaisun luomiseksi.

Sisältöjen suojaamisessa on merkitystä sillä, missä ja mitä tietoa käsitellään. Mitä korkeammalle tasolle luokittelussa mennään, sitä vähemmän tietoa tulisi käsitellä etäyhteyksin. Eri tasoisia tietoja voi säilyttää vain tietyillä laitteilla. Hyvä sääntö on minimoida tiedon mukana kuljettaminen ja keskitettyjen ratkaisujen käyttö. Etätyön yleistyessä ja sen myötä Teamsin ja vastaavien palveluiden käytön lisääntyessä monessa yrityksessä Teamsiin alkoi kertyä paljon erilaisia aineistoja, joka tulee huomioida tiedonhallintarakenteessa ja elinkaarimallissa. Oman liiketoiminnan kannalta kriittistä tietoa käsiteltäessä ja tallennettaessa on edellytettävä luokittelua. Tällaisen tiedon tulee aina olla salaista ja sen välittämiseen omassa organisaatiossa voidaan käyttää turvallisia ja hyväksyttyjä mekanismeja kuten salattua sähköpostia tai vahvasti tunnistettuja tiedostopalveluita. Näin toimimalla varmistetaan, että tieto ei leviä yrityksen ulkopuolelle.

Sähköpostin salaukseen ja toisen osapuolen luotettavaan tunnistamiseen on runsaasti kaupallisia ratkaisuita, jotka mahdollistavat niiden joustavan käyttämisen.

On huomattavaa, että tietosuojasäädökset asettavat velvoitteita rekisterinpitäjälle, joista ei voida poiketa edes rekisteröidyn suostumuksesta. Suojaamis- ja salassapitovelvoite vaatii riittävän vahvaa salausta[4] ja osapuolten tunnistamista.

”Erityistä huomiota etätyössä tulee kiinnittää luottamuksellisen tiedon suojaamiseen sekä rajata kokonaan pois korkeaa tai kohtuutonta riskiä aiheuttavat tehtävät etätyön piiristä.”

CSC – Tieteen tietotekniikan keskus

Sisällön jakamisen ja suojaamisen osalta tietoturvan tasoa voidaan parantaa:

- Huolehtimalla myös sisällön suojaamisesta – pelkkä järjestelmän suojaaminen ei riitä
- Huolehtimalla yrityksessä henkilötietojen käsittelystä ja suojaamisesta GDPR-asetuksen mukaisesti
- Laatimalla luokittelukäytännöt yrityksessä jaettavalle ja käsiteltävälle tiedolle
- Varmistamalla, että sisältöä suojataan em. käytäntöjen mukaisesti
- Kouluttamalla työntekijöitä yrityksen käytännöistä ja varmistamalla, että työntekijät toimivat niiden mukaisesti
- Varmistamalla, että korkeamman luokitustason aineistoja ei käsitellä etäyhteyksin tai estämällä se teknisesti

4) *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf*

TOIMINNALLISET RATKAISUT

Tietoturva- ja tietosuojakoulutus

Tietoturvan ja -suojan osalta on olennaista ymmärtää, mikä tieto on sensitiivistä ja miten sitä tulisi suojata. Perinteinen ”maalaisjärki” ei riitä. **Tietoturva- ja suojakäytäntöjen tulee olla ohjeistettu, dokumentoitu ja koulutettu**. Henkilöstön kouluttaminen lukeutuu jokaisen yrityksen tietoturvallisuuden ja tietosuojan peruspilareihin. Yrityksellä tai organisaatiolla tulee olla turvallisuusohjeistus, josta työntekijä voi palauttaa koulutusten aiheita muistiin.

Nokian tytäryhtiö joutui tietomurron kohteeksi – järkyttävä totuus paljastui kaksi kuukautta myöhemmin

Tivi 24.8.2021

Koulutuksia tietoturvallisuudesta tulee järjestää säännöllisesti, mieluiten vuosittain, ja niihin osallistuneista työntekijöistä kannattaa pitää kirjaa, jotta varmistutaan osaamisen jalkauttamisesta työntekijöiden päivittäiseen työhön. On erityisen tärkeää sitouttaa yrityksen johtoporras tietoturvalliseen toimintaan, jolloin he voivat osoittaa resursseja työntekijöiden koulutukseen. Tietoturvallisuuskoulutusten tulee olla pakollisia. Vaikka itse koulutus järjestettäisiin kerran vuodessa, on työntekijöitä hyvä muistuttaa tietoturvallisuudesta ja siihen liittyvistä riskeistä (esim. tietojenkalastelu) ajoittain.

Koulutuksen tulisi valmentaa työntekijöitä tiedon luokitteluun, jotta työntekijä ymmärtää, mikä tieto on sensitiivistä ja mihin luokkaan mikäkin tieto kuuluu (ks. Sisällön jakaminen ja suojaaminen). Tietojen jakaminen työntekijöiden kesken tulee tehdä yrityksen hyväksymällä tavalla ja tiedon luokittelun mukaisesti. Yrityksen tulisi selväkielisesti kertoa, minkä laatuista tietoa voidaan jakaa missäkin kanavassa, esimerkiksi Teams, Onedrive for Business ja Workplace by Facebook. Esimerkiksi Teams-kanavaa ei tulisi käyttää korkeampaan luokitukseen kuin luottamuksellinen.

Yrityksen politiikka sosiaalisen median ja yrityksen ulkopuolisten viestisovellusten käytön suhteen

Varsinkin etätyössä henkilökohtaisen elämän ja työasioiden raja voi hämärtyä, jolloin yrityksen turvallisuusohjeiden tulisi ottaa kantaa myös henkilökohtaisten viestivälineiden käyttöön työasioiden hoitamisessa. Sosiaalisen median kanavat[5] ja yrityksen ulkopuoliset viestisovellukset[6] eivät sovellu työasioiden käsittelyyn, vaikka viestisovelluksia voidaankin pitää matkapuhelinta turvallisempana vaihtoehtona. Sosiaaliseen mediaan ei tule myöskään jakaa työhön liittyviä valokuvia, sillä ne saattavat vahingossa sisältää yrityksen sisäistä tietoa tai viittauksia asiakkuuksiin. Lisäksi kuvien metadata voi sisältää sijaintitietoa ja paljastaa muun suojattavan kohteen.

Tietoturva- ja tietosuojakoulutuksen osalta tietoturvan tasoa voidaan parantaa:

- Järjestämällä pakollisia tietoturvallisuuskoulutuksia työntekijöille säännöllisesti
- Kouluttamalla työntekijät ymmärtämään millainen tieto on sensitiivistä ja miten sitä suojataan
- Seuraamalla koulutusten suorittaneiden prosenttiosuutta ja sitä, miten tieto on sisäistetty
- Varmistamalla, että yrityksessä on turvallisuusohjeistus ja että työntekijät tietävät mistä sen löytää

Verkkokokoustyökalut

Etäkokouksissa tietoturvaa voi parantaa pienillä teoilla, kuten valmistautumisella. Jo ennen kokouksen alkua on hyvä varmistaa, että työasemalla on auki vain sellaista aineistoa, jonka joutuminen ulkopuolisten nähtäväksi ei aiheuta yritykselle merkittävää haittaa. Näin toimimalla kukaan ei vahingossa jaa etäkokousten aikana näytöllä näkyvää, vain yrityksen sisäiseen käyttöön tarkoitettua aineistoa.

Mikäli verkkokokouksen aikana on tarve esittää aineistoa muille osallistujille, kannattaa työntekijöitä ohjeistaa jakamaan vain kyseinen ohjelma (Word, PPT, Excel jne.) koko ruudun jakamisen sijaan. Hyvänä, turvallisena ja kohteliaana käytäntönä voidaan pitää videon päällä pitämistä aina silloin, kun verkkokokouksessa on uusia tai toisilleen vieraita osallistujia. Alun jälkeen video voidaan ottaa pois päältä, jolloin se kuluttaa vähemmän kapasiteettia verkkoyhteydeltä. Videoissa moni yritys suosii taustakuvaa, joka toimii brändäyksen tukena ja – mikä tärkeämpää – vaikeuttaa henkilön fyysisen sijainnin paljastumista.

Uhkia ajatelleen yrityksissä on lisäksi ohjeistettava, millaisista asioista verkkokokouksissa saa puhua. Osallistujan on arvioitava riskejä ja huomioitava keskustelun aihepiiri. Moni yritys on lisäksi linjannut, että tiedostoja ei jaeta esimerkiksi Teamsin kautta. Teknisesti on mahdollista huolehtia siitä, että chat-toiminnon kautta lähetetyt viestit tallentuvat eri paikkaan kuin liitetiedostot. Tiedostojen jakamiseen käytetään omaa palvelinympäristöä yrityksen luokittelupolitiikan mukaisesti.

Verkkokokousten tietoturvaa on edelleen mahdollista parantaa edellyttämällä kirjautumista avoimien linkkien sijaan. Ominaisuus löytyy ainakin Zoom-verkkosovelluksesta. Jos Zoomia halutaan käyttää organisaation sisäiseen viestintään tai luottamuksellisen tiedon välitykseen, on suositeltavaa käyttää Zoomin Business tai Enterprise-versioita (ks. Ohjeita turvallisten etätyövälineiden valintaan).

5) Esimerkiksi Facebook, Snapchat, Instagram, Twitter ja Linkedin
6) Esimerkiksi WhatsApp, Signal ja Telegram

Verkkokokoustyökalujen osalta tietoturvan tasoa voidaan parantaa ohjeistamalla käyttäjiä seuraavasti:

- Ennen verkkokokousta sulje kaikki tarpeettomat ohjelmat ja tiedostot työasemalta
- Kokouksen alussa pidä video päällä ja esittäydy vieraille osallistujille
- Jos kokouksessa on tarve jakaa jotain omalta työasemalta, jaa vain kyseinen ohjelma, älä koko ruutua
- Käytä taustan peittävää kuvaa (verkkotyökalun tarjoamaa tai yrityksen omaa)
- Tiedosta minkälaisista asioista kokouksessa voi puhua, minkälaisia tiedostoja jakaa ja mitä tallentaa

Laitteiden käyttö ja säilyttäminen (muualla kuin toimitiloissa)

Useissa yrityksissä etätyötä koskevat samat perusperiaatteet kuin toimitiloissa. Ohjeistuksissa on kiinnitetty huomiota tietoaineistojen käsittelyyn, tulostamiseen, näkemiseltä ja kuulemiselta suojaamiseen sekä laitteiden säilyttämiseen. Työntekijöitä on hyvä ohjeistaa jo työsuhteen alussa, että työasemat ovat tarkoitettu vain työkäyttöön. **Toisin sanoen työkone ei ole vapaa-ajan kone eikä se ole missään tilanteessa muiden perheenjäsenten käytettävissä**. Muistisääntönä voidaan käyttää seuraavaa: **älä tee työasemalla asioita, joita teit aikaisemmin omalla kannettavalla tietokoneellasi**. Tästä on myös syytä muistuttaa koulutuksissa. Vaikka ohjeistus on suhteellisen tiukka, yrityksissä harvoin yritetään estää pienimuotoinen henkilökohtainen käyttö. Yrityksissä ymmärretään, että työntekijällä voi olla tarve käydä esimerkiksi verkkopankissa tai lukea henkilökohtaista sähköpostia.

Työntekijän vastuulla on varmistaa, että hänen työssään käymänsä keskustelut eivät kantaudu sivullisten korviin eikä ulkopuolinen pääse lukemaan koneen näytöltä arkaluontoisia asioita. Sivullisilla tarkoitetaan perheenjäsenten ja vieraiden lisäksi myös sellaisia tahoja, joilla on pääsy asuinhuoneistoon (esimerkiksi huoltomiehet, isännöitsijä ja vuokranantaja).

Hyviä yleisohjeita kuulemiselta ja näkemiseltä suojaamiseen ovat **kuulokkeiden käyttäminen** (sivulliset eivät kuule toisen osapuolen ääntä), puhumisen välttämistä avoimena olevien ikkunoiden läheisyydessä sekä **näytönsuojaimien käyttö**. Arkaluontoisista asioista keskusteltaessa on huomioitava, että edes perheenjäsenet eivät kuule käytävää keskustelua. Etätyön yleistymisen myötä on suositeltavaa hankkia yrityksen kaikkiin työasemiin näytönsuojat. Osa yrityksissä hyödyntää koneissaan lisäksi teknisiä suojausratkaisuja.

Laitteiden turvallinen säilyttäminen

Laitteiden säilyttämisen suhteen ohjeistukset vaihtelevat sen mukaan, minkälaista materiaalia niillä voidaan käsitellä. Yleisesti ottaen tärkeänä pidetään **koneen näytön lukitsemista aina, kun ollaan hetkellisesti pois koneelta**. Monissa yrityksissä on erikseen varmistettu teknisesti **näytön automaattinen lukitus**, mikäli konetta ei käytetä esimerkiksi viiteen tai kymmeneen minuuttiin. Kun työkonetta ei käytetä, se tulee sammuttaa ja siirtää pois näkyvältä paikalta. Koneen säilyttämistä lukitussa kaapissa ei yleensä edellytetä, koska sammutettu ja kryptatulla kovalevyllä varustettua konetta pidetään riittävän turvallisena perinteisiä riskejä vastaan. Yleisenä ohjeena voidaan pitää sitä, että kone tulee sijoittaa sellaiseen paikkaan, josta muut eivät saa sitä käsiinsä. **Lähtökohtaisesti työkonetta tai – puhelinta ei kuitenkaan tule säilyttää esimerkiksi autossa**.

Yksi tietoturvalliseen toimintaan liittyvä osa-alue on myös tulostaminen. Koronapandemian myötä tulostaminen on monissa organisaatioissa vähentynyt ja helpottanut ns. puhtaan pöydän periaatteen toteuttamista. Puhtaalla pöydällä tarkoitetaan, että työpisteeltä lähdettäessä sinne tai sen läheisyyteen ei jätetä asiakirjoja, lomakkeita tai mitään muutakaan paperia. Tämä sama periaate pätee yrityksissä sekä toimisto- että kotiympäristössä. Hyvä käytäntö tietoturvalliseen tulostamiseen on **käyttäjän tunnistaminen tulostamisen yhteydessä**, jolloin asiakirja tulostuu vasta sen jälkeen, kun käyttäjä on tunnistautunut laitteella esimerkiksi RFID-tunnisteen ja PIN-koodin yhdistelmällä. Tulostinta voidaan myös säilyttää lukitussa huoneessa, jonne pääsee vain henkilökunnan avaimilla. Näin voidaan vähentää riskiä, että epähuomiossa tulostettu materiaali päätyisi ulkopuolisten käsiin.

Laitteiden käytön ja säilyttämisen osalta tietoturvan tasoa voidaan parantaa ohjeistamalla:

- työntekijöitä työsuhteen alussa, että työasemat ovat tarkoitettu vain työkäyttöön
- työntekijä antamasta työasemaa kenenkään muun (edes perheenjäsenen) käyttöön
- kaikkia työntekijöitä suojaamaan työaseman ulkopuolisten silmiltä ja korvilta
- kaikkia työntekijöitä lukitsemaan työasema aina, kun on poissa koneelta
- kaikkia työntekijöitä sammuttamaan työasemaa ja siirtämään työasema pois näkyvältä paikalta, kun sitä ei käytetä
- että yhdenkään työntekijän ei tule koskaan säilyttää työasemaa tai -puhelinta autossa
- että työntekijät eivät tulosta työhön liittyviä dokumentteja kotonaan. Jos näin tehdään, tulee dokumentit suojata näkemiseltä

IoT-laitteet

Kotitalouksista löytyy enenemissä määrin IoT-laitteita (Internet of Things), jotka kuuntelevat puhetta tiettyjen toimintojen aloittamiseksi. Uudet teknologiat vaativat aina totuttelua ja säännöllistä riskien arviointia.

Kuuntelevat älykotilaitteet tulee ottaa huomioon työskentelyalueen läheisyydessä ja tarvittaessa laittaa ne pois päältä tai ottaa kuuntelutila pois päältä. **Turvallisuusluokat I-III kattavasta tiedosta keskusteltaessa kuuntelevia laitteita ei saa olla ollenkaan samassa tilassa**.

Kodissa voi olla myös kuvaa tallentavia älylaitteita tai kameratekniikkaa, jotka lähettävät näkemänsä verkkoyhteyden kautta pilvipalveluun prosessoitavaksi tai tallennettavaksi. Verkkoyhteyden kautta käytettävissä laitteissa voi olla ominaisuus, jolloin ne lopettavat ja aloittavat tallentamisen verkkoyhteydellä annettavalla komennolla. Varmuutta tallennuksesta ei kuitenkaan voi saada, ellei laitetta tehdä virrattomaksi tai sen eteen laiteta estettä. Kuvaa tallentavia laitteita tulisikin käsitellä koko ajan tallentavina eikä niiden näkyvissä saisi käsitellä luottamuksellista materiaalia salakatselun estämiseksi.

IoT-laitteita tulee käsitellä verkon liityntäpisteinä, joilla on mahdollisuudet skannata ja tarkastella verkon toimintaa. Laitteiden lisääntyessä verkossa käytettävän VPN-tunnelin ja yhteyksien salaamisen merkitys korostuu. Kodin IoT-laitteiden tulisikin olla eri verkossa kuin työasema ja työpuhelin.

Yrityksen tulee kouluttaa henkilöstöään IoT-laitteiden muodostamista riskeistä, mutta myös suojata oman verkkonsa liikenne luotettavasti. Työasemiin ei tule asentaa tai liittää mitään ulkoisia laitteita ilman lupaa, sillä ne voivat asettaa vaaraan tiedon luottamuksellisuuden.

IoT-laitteiden osalta tietoturvan tasoa voidaan parantaa ohjeistamalla työntekijöitä:

- Vaihtamaan laitteiden oletussalasanat niiden käyttöönoton yhteydessä
- Laittamaan kuuntelevat älykotilaitteet pois päältä tai poista kuuntelutila käytöstä töiden ajaksi
- Suhtautumaan kuunteleviin ja kuvaa tallentaviin älykotilaitteisiin kuin sivullisiin tai vieraisiin ihmisiin
- Olemaan asentamatta tai liittämättä työasemiin mitään ulkoisia laitteita ilman lupaa
- Kytkemään yrityksen verkkoon ainoastaan yrityksen hyväksymiä laitteita

Ulkomaanmatkat

Matkustamiseen – myös kotimaassa – pätevät samat ohjeistukset kuin toimintaan julkisissa tiloissa. Aiemmin tässä oppaassa on neuvottu suojaamaan tieto salakatselulta ja -kuuntelulta. Ulkomaille matkustettaessa riskit voivat olla suurempia ja osin erilaisia. Varautuminen ulkomaan matkaan tulee tehdä hyvissä ajoin. Esimerkiksi suojelupoliisi neuvoo päivittämään mukaan otettavat laitteet ja sovellukset uusimpiin versioihin jo ennen matkaa. Toinen hyvä neuvo on aktivoida laitteisiin pääsykoodi ja säätää sen viive mahdollisimman lyhyeksi. Lisää ohjeita löydät ***täältä***.

Yrityksen tarve suojata koneita ja laitteita ulkomaan matkojen aikana vaihtelee yrityksen toiminnan sisällöstä ja liikematkojen kohdemaista riippuen. Lähinnä kotimaassa tai muissa Pohjoismaissa matkustaville suunnattu ohjeistus on yleisemmällä tasolla kuin niin sanottujen korkean riskitason maiden

ohjeet. Perusohje kaikkeen matkustamiseen liittyen – oli kyseessä sitten kotimaan tai ulkomaan matka – on samankaltainen kuin julkisissa tiloissa: **julkisten WLAN-verkkojen** (esimerkiksi lentoasemat ja hotellit) **käyttöä tulisi välttää, ulkopuolisten kuullen ei tulisi puhua työasioista, työasemat tulisi suojata näytönsuojilla** ja **itse yhteys suojata VPN:llä**. WLAN-verkkojen sijaan on suositeltavaa käyttää yrityksen matkapuhelimen mobiiliverkkoa.

Ulkomaanmatkoilla käyttäjiä kehotetaan valppauteen sekä paikallisten olosuhteiden ja riskien tunnistamiseen. Osa yrityksistä ohjeistaa esimerkiksi olemaan luottamatta hotellien turvalokeroihin. Työntekijän tulee matkan aikana olla koko ajan tietoinen työhön käytettävien koneiden ja laitteiden (työasema ja matkapuhelin) sijainnista. Toisin sanoen henkilökohtaisen koneen hallussa pitämiseen tulee kiinnittää erityistä huomiota. Samoin matkapuhelimesta tulee huolehtia kuin omasta luottokortistaan - älä koskaan luovuta sitä toiselle henkilölle.

Jos työskentelet esimerkiksi politiikassa, virkamiehenä tai elinkeinoelämässä, saatat olla tehtäväsi vuoksi kiinnostava tiedustelun kohde.

Harkitse, mitä tuntemattomalle kannattaa kertoa. Muista myös, että runsas alkoholin käyttö voi tehdä sinusta alttiimman vaikutuspyrkimyksille.

Suojelupoliisi

Varautuminen korkean riskitason maihin matkustamiseen

Riskeihin varautumista on mahdollista lisätä maissa, joissa tietoturva- tai tietovuotoriskit ovat korkeammat. Ennen matkaan lähtöä suositellaan riskiarvion tekemistä ja voidaan jopa tehdä päätös olla matkustamatta. Varautumisen näkökulmasta **on myös syytä miettiä erilaisia skenaarioita – minkälaisissa tilanteissa riskit kasvavat**. Jos jokin asia vaikuttaa liian hyvältä ollakseen totta, se yleensä ei ole totta. Vaikka teollinen vakoilu ja henkilöiden huumaaminen kuulostaa pikemminkin toimintaelokuvan juonelta kuin todellisuudelta, ei riskejä tule aliarvioida. Jos yksin matkustavan henkilön seuraan yllättäen liittyy esimerkiksi tuntematon henkilö, joka haluaa nauttia yhdessä virvokkeita, on kyseisen henkilön motiiveihin syytä suhtautua varauksella.

Matkan aikana keskitytään koneiden ja laitteiden turvallisuuteen sekä luvattoman käytön ennaltaehkäisyyn. Jos yrityksen tietojen pelätään joutuvan väärien tahojen haltuun, voidaan matkaan lähteä laitteilla (työasema ja matkapuhelin), joissa on vain minimaaliset tiedot. Tällöin työntekijä ei ota mukaan päivittäisessä käytössä olevia laitteita. **Suojelupoliisin ohjeen mukaisesti matkalle ei tulisi ottaa älylaitteita, kuten tietokonetta, tablettia, matkapuhelinta tai älykelloa**. Riskimaihin lähdettäessä on mahdollista käyttää myös tätä tarkoitusta varten suunniteltuja turvapusseja. Hyvä käytäntö on ottaa tällaisia matkoja varten käyttöön elinkaarensa loppupuolella oleva laite, joka voidaan matkan jälkeen poistaa käytöstä. Vaihtoehtoisesti voidaan riskiarvion perusteella päätyä asentamaan laite uudelleen. Lisäksi tiedonvaihtoa varten voidaan ottaa muuten tyhjiä USB-tikkuja, joita ei enää tuoda takaisin Suomeen.

Ulkomaanmatkojen osalta tietoturvan tasoa voidaan parantaa ohjeistamalla työntekijöitä:

- Tunnistamaan riskit ja arvioimaan niiden edellyttämä varautuminen
- Välttämään julkisten WLAN-verkkojen käyttöä matkustettaessa
- Harkitsemaan, mitä tuntemattomalle kannattaa kertoa ja olemaan ottamatta vastaan lahjoja
- Välttämään puhelimen tai tietokoneen lataamista ulkopuolisten tarjoamilla latureilla
- Välttämään ulkopuolisen USB-laitteet liittämistä työasemaan
- Tarvittaessa ottamaan matkalle käyttöön laite, joka voidaan poistaa käytöstä matkan jälkeen

Liite 1. Täydentävä aineisto

TURVALLISUUSLUOKITELTU AINEISTO

Käsiteltävä aineisto tulisi luokitella ja sen omistajuus määrittää. Tämä mahdollistaa luokitellun tiedon asianmukaisen käsittelyn ja elinkaarenhallinnan. Yrityksillä on käytössä sekä omia turvallisuusluokittelukäytäntöjä ja sen lisäksi ulkopuolisiin viitekehyksiin- tai kumppanuuksiin liittyviä vaatimuksia. Koska vaatimukset poikkeavat toisistaan, tulee käytäntöjen pystyä vastaamaan eri liiketoimintatarpeisiin tältäkin osin.

Monet yritykset tarjoavat palveluita viranomaisille ja toisinaan palvelun tuottamiseen sisältyy turvallisuusluokitellun aineiston käsittelyä. Valtionhallinnon asiakirjojen turvallisuusluokittelusta (TL) on säädetty **julkisuuslaissa** (16 §, 24 § ja 25 §), **tiedonhallintalaissa** (18 §) sekä **valtioneuvoston asetuksessa turvallisuusluokitelluista asiakirjoista** (3 §). Aineistot on jaettu sisällön mukaan neljään luokkaan (I-IV); mitä pienempi numero, sitä kriittisempää tietoa aineisto sisältää.

Kaikissa organisaatioissa tulisi pyrkiä siihen, että tietojen käsittely on aina turvallista riippumatta luokituksista. Turvallisuusluokiteltujen aineistojen käsittelystä viranomaisen ja muiden tahojen välillä sovitaan aina sopimusperusteisesti ja aineistojen tietoturvalliselle käsittelylle on asetettu tarkat kriteerit. TL I-III luokan aineistoja on sallittua vastaanottaa, katsella ja säilyttää ainoastaan yrityksen turva-auditoiduissa toimitiloissa. Pääsy TL-tietoon sallitaan tietyille henkilöille aina tarveperustaisesti (ks. Tunnistautuminen ja käyttäjäprofiilit, sivu 8). Teknisesti tietoturva on varmistettu siten, että etäyhteyksin ei ole mahdollista päästä käsiksi TL IV -luokkaa ylittäviin tietoihin.

Missään yrityksessä tai organisaatiossa ei tulisi sallia TL I-III -luokkien tietojen tulostamista ja mukaan ottamista. Tulostamisen myötä mahdollisuus inhimilliseen virheeseen sekä siihen, että turvallisuusluokiteltu aineisto päätyy ulkopuolisen tahon nähtäväksi, lisääntyy. Samasta syystä **pääsyä turvallisuusluokiteltuun tietoon ei tule sallia etäyhteyksin omalla päätelaitteella**: on suljettava pois mahdollisuus, että esimerkiksi liikennevälineessä vieressä tai takana istuva matkustaja pääsisi katselemaan turvallisuusluokiteltua aineistoa.

Etätyön lisääntyminen koronan myötä on johtanut siihen, että joissakin tapauksissa viranomais-asiakkaan asettamissa vaatimuksissa on esiintynyt tapauskohtaisesti joustoa. Tämä koskee vain TL IV-luokan tietoa, jonka käsittely on väliaikaisesti sallittu myös etäolosuhteissa sillä edellytyksellä, että olosuhteet ovat turvalliset ja että aiempaan toimintamalliin palataan heti koronatilanteen ja sen asettamien rajoitusten hellittäessä.

Sama ohjeistus koskee myös puhetta. **Turvallisuusluokitellusta aineistosta ei tule keskustella missään sellaisessa ympäristössä, jossa puhe voi kulkeutua sivullisten korviin**. Esimerkiksi puhelinkeskustelu yleisellä paikalla on katkaistava, mikäli siinä käsitellään TL-tietoa. Matkapuhelimiin kohdistuva tiedustelu-uhka on todellinen. Myös muiden viestintävälineiden ja -alustojen käytössä on oltava tarkkana. Yleisohje on, että turvallisuusluokiteltua aineistoa käsiteltäessä käytetään asiakkaan määrittämää työkalua, joka ei ole Teams tai vastaava. Katso tarkemmat ohjeet turvallisten viestivälineiden valinnasta **täältä**.

Turvallisuusluokitellun aineiston osalta tietoturvan tasoa voidaan parantaa:

- Varmistamalla, että turvallisuusluokiteltua aineistoa käsitellään aina lainsäädännön edellyttämällä ja sopimuksissa määritellyllä tavalla
- Varmistamalla, että TL I-III -luokkien aineistoon ei ole pääsyä etäyhteyksin
- Varmistamalla, että TL I-III -luokkien tietoja ei ole mahdollista tulostaa ja ottaa mukaan
- Varmistamalla, että turvallisuusluokitellusta aineistosta ei keskustella missään ympäristössä sivullisten kuullen

Oulun yliopisto joutui laajan tietojen-kalastelun kohteeksi – yli 750 ihmisen salasanat joutuneet vääriin käsiin

Helsingin Sanomat 3.9.2021

Tietojen kalastelu

Tietojen kalastelu on lisääntynyt viime aikoina voimakkaasti. Yleisiä tapoja ovat huijaussoitot sekä huijausviestit (sähköpostin tai tekstiviestin välityksellä), joilla henkilöä pyritään luovuttamaan tietoa kolmannen osapuolen käyttöön.

Yritykset informoivat tietojen kalastelusta monikanavaisesti ja seuraavat mm. Kyberturvallisuuskeskuksen tiedottamista huijauskampanjoista. Työntekijöiden valistamista uhkaa vastaan pidetään hyvin tärkeänä. Valistamisessa hyödynnetään mm. tietoturvakoulutusta, kohdennettuja sähköpostiviestejä tai kampanjoita (varoitetaan huijausten olemassaolosta tai nousevista trendeistä) koko organisaatiolle, blogikirjoituksia (esimerkiksi havainnollistava case-kuvaus kalastelusta) sekä tiedottamista ja vinkkejä intranetissä.

Valistamisen lisäksi henkilöstölle voidaan korostaa lähes kyllästymiseen saakka, että **oma IT-tuki ei koskaan kysy salasanoja tai pankkitunnuksia**. Samoin useissa organisaatioissa IT-tukihenkilöt eivät ole englanninkielisiä ja **ottavat yhteyttä työntekijään vain työntekijän tekemän palvelupyynnön seurauksena**.

Hyväksi havaittu keino työntekijöiden valistamiseen on pelillisten palvelujen käyttö. Monet yritykset kertovat käyttävänsä kalasteluyritysten simulaatiopalvelua[7], jossa tätä tarkoitusta varten laadittu sähköposti lähetetään yrityksen työntekijöille ja seurataan kuinka moni tunnistaa viestin huijaukseksi. Viesteissä on tärppejä, kuten virheellinen sähköpostiosoite, kirjoitusvirheitä jne. Kun työntekijä raportoi viestin eteenpäin kalasteluna, hän saa siitä pisteitä tai hänet voidaan ohjata koulutukseen, jossa kerrataan huijausviestin keskeiset kohdat. Myös koulutuksesta saa pisteitä ja henkilöstö voi kisata keskenään sijoituksesta. Yritys seuraa palveluntarjoajan kanssa sitä, minkälaisiin viesteihin yleisimmin langetaan ja tätä tietoa voidaan hyödyntää koulutuksen sisältöjen suuntaamisessa. Tällaisen kampanjan jälkeen tulokset tulee avoimesti kertoa henkilöstölle.

Avoin toimintakulttuuri ja nopea reagointi avainasemassa

Yrityksissä tulee kannustaa pikemminkin avoimeen ja palkitsevaan kuin virheistä tuomitsevaan toimintakulttuuriin. Tällöin ilmoittamiskynnys pysyy matalana. Työntekijöille on syytä antaa positiivista palautetta tarkkaavaisuudesta silloinkin, kun kyse ei ole ollut aidosta huijausviestistä. Kannustavan toimintakulttuurin mukaisesti työntekijöitä voidaan lisäksi palkita kalasteluviestin tai tietoturvariskin tunnistamisesta.

7) Esimerkiksi Hoxhunt

Mitä nopeammin puutteet tai vaaratilanteet tietoturvassa havaitaan, sitä helpommin niihin voidaan puuttua ja vaikutukset minimoida. Työntekijöiden tulee pystyä avoimesti raportoimaan kaikesta mitä on tapahtunut. Tietoturvariskeistä ilmoittaminen tulisi tehdä teknisesti mahdollisimman helpoksi. MS Outlookiin saa esimerkiksi phishing-painikkeen käyttämällä Report message- tai Report phishing -lisäosaa. Globaalit admin-oikeudet omaavat henkilöt voivat ottaa toiminnon käyttöön yrityksissä ja Microsoft hyödyntää sitä sähköpostien suodattamiseen. Googlen Gmail-palvelu tunnistaa automaattisesti roskapostikansioon siirrettyjen viestien tunnistetiedot ja asiasisällön suodattimen kehittämiseksi. Huijausviestien valvonnassa voidaan hyödyntää tekoälyä ja automatiikkaa, jolloin security operation center valvoo tietoliikennettä ympäri vuorokauden. Jos tietoliikenteessä tapahtuu jotain epäilyttävää, järjestelmä antaa hälytyksen ja altistuneet käyttäjätunnukset voidaan sulkea.

Haittaohjelmat päätyvät puhelimille tavallisesti suojaamattomien Wi-Fi-verkkojen, epävirallisten sovelluskauppojen, sähköpostiliitteiden ja haitallisten nettisivujen kautta.

F-Secure

Mikäli vahinko on päässyt tapahtumaan, tulee selvittää vahingon laajuus (onko tapahtunut tietovuoto). Mikäli tietoturvaloukkaus koskee henkilötietoja ja siitä voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille, tulee loukkauksesta ilmoittaa tietosuojavaltuutetun toimistolle - katso tarkemmat ohjeet **täältä**. Pelkän epäilyn perusteellakin on mahdollista vaihtaa käyttäjätunnukset. Muissa tapauksissa kone otetaan heti pois verkosta, tietoturvaosasto tutkii koneen ja tekee diagnoosin ja sen edellyttämät toimenpiteet. Lopuksi kone voidaan asentaa uudelleen ja ottaa jälleen käyttöön. Tärkeää on, että tähän on olemassa selkeä, kaikkien tiedossa oleva prosessi.

Tietojen kalastelun lisäksi käyttäjää uhkaavat erilaiset haittaohjelmat. Erityisen yleisiä haittaohjelmat ovat mobiililaitteissa, joissa ne tekevät ei-toivottuja asioita (esimerkiksi mainosten näyttäminen tai käyttäjän vakoileminen). Mikäli epäilet, että mobiililaitteeseesi on päässyt haittaohjelma, ole yhteydessä yrityksesi IT-asiantuntijoihin ja toimita laite huoltoon.

Tietojen kalastelun osalta tietoturvan tasoa voidaan parantaa:

- Sisällyttämään tietojen kalastelu teemana osaksi tietoturvallisuuskoulutusta
- Varmistamaan, että mahdollisten tietovuotojen osalta yrityksessä on prosessi, jolla näihin puututaan
- Varoittamalla henkilöstöä erikseen liikkeellä olevista tietojenkalastelukampanjoista
- Muistuttamalla, että yrityksen oma IT-tuki ei koskaan kysy salasanoja tai pankkitunnuksia
- Kannustamalla avoimuuteen – mitä matalampi kynnys yrityksessä on ilmoittaa mahdollisesta tietovuodosta, sitä nopeammin tilanne voidaan korjata ja vahingot rajata
- Reagoimalla nopeasti - jos henkilötiedot ovat vaarassa, loukkauksesta tulee ilmoittaa tietosuojavaltuutetun toimistoon

Jaksamisen ja esihenkilötyön tukeminen osana tietoturvaa

Tietoturvallinen etätyö ei koostu pelkästään teknisistä ratkaisuista ja tietynlaisesta, työntekijän omasta toiminnasta. Myös työntekijän jaksamisella on merkitystä tietoturvan kannalta. Väsyneempänä tekee helpommin virheitä eikä huomioi riskejä samalla tavalla kuin virkeänä.

Jaksamista voidaan tukea parantamalla työolosuhteita etätoimistolla. Työnantaja voi myöntää rahallista tukea ergonomisempien kalusteiden (esim. työtuoli) hankintaan tai aiemmin toimistolla olleita laitteita (esim. erillinen näyttö) on voitu tuoda kotiin. Erityisesti on syytä kiinnittää huomiota jaksamiseen, koska lisääntyneen etätyön riskeinä korostuvat fyysinen ja psykososiaalinen kuormittuminen sekä tapaturmavaarat. Työntekijöitä tulee kannustaa pitämään taukoja ja huolehtimaan vireystilasta. Yrityksissä voidaan esimerkiksi sopia, että Teams- tai vastaavat palaverit lopetetaan aina viittä minuuttia vaille, jotta työntekijöille jää pieni hetki hengähtää ennen seuraavaa palaveria. Edelleen on tärkeää sopia työpäivän pituudesta, koska korona-aikana työn ja vapaa-ajan suhde on muuttunut entistä häilyvämmäksi.

Yhtäältä etätyö on lisännyt työn tekemisen joustavuutta, mutta toisaalta haastaa aiempia rutiineja sekä aikatauluja. Kuormittumisen havaitseminen on käynyt haastavammaksi, kun ei olla enää aiempaan tapaan tekemisissä työyhteisön kanssa. Myös tarpeet paineiden ja stressin hallinnalle ovat lisääntyneet. Esihenkilöiden rooli ja osaaminen korostuvat tässä aiempaakin enemmän. Esihenkilöille voidaan tarjota koulutusta työhyvinvoinnin ja tiimihengen ylläpitämisessä sekä hyvän ergonomiaa edistämisessä. Terveyden ja hyvinvoinnin laitos on laatinut ohjeita etätyön tekemisen tueksi. Voit tutustua ohjeisiin **täältä**.

Yleisesti ottaen jaksamisessa tulisi huomioida ainakin:

- Pitkittyessään perinteiset etätyön edut eivät välttämättä enää toteudu
- Yrityksissä tulisi kehittää yksittäisen työntekijän ja yhteisön tarpeet huomioiva tapa tehdä etätöitä (mitä tehtäviä voidaan tehdä etänä ja mitkä vaativat läsnäoloa toimistolla/asiakkailla)
- On tärkeää viestiä työntekijöille millaisia työkykyä ylläpitäviä toimintatapoja kannattaa noudattaa, mitä apua ja tukea on saatavissa, mitä työterveyshuolto tarjoaa sekä miten työnantaja osallistuu mm. työtilojen ergonomian parantamiseen
- Etä- ja lähityötä voidaan vuorotella ryhmissä, jolloin työpaikalla on kerrallaan pienempi määrä henkilöitä ja turvaetäisyyksiä on helpompi ylläpitää
- Esihenkilön säännöllinen yhteydenpito työntekijöihin tulee varmistaa
- Uusien työntekijöiden perehdyttäminen virtuaaliseen viestintään ja kokouksiin on tärkeää

Terveyden- ja hyvinvoinninlaitos (THL)

Jaksamisen ja esihenkilötyön tukemisen osalta tietoturvan tasoa voidaan parantaa:

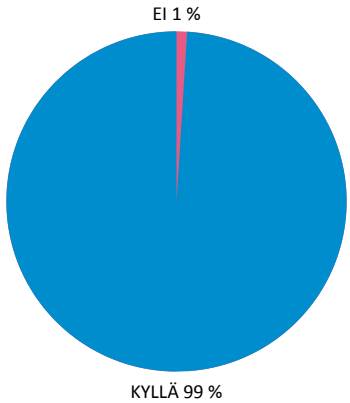
- Huolehtimalla työntekijöiden jaksamisesta myös etätyöympäristössä[8]
- Kannustamalla työntekijöitä pitämään taukoja ja huolehtimaan vireystilasta
- Olemaan ajoittamatta työpäivään useita perättäisiä etäkokouksia ilman taukoja
- Tukemalla esihenkilöitä kehittämällä työhyvinvointiin ja tiimihengen ylläpitämiseen liittyvää osaamista

8) Esimerkiksi kävelykokoukset

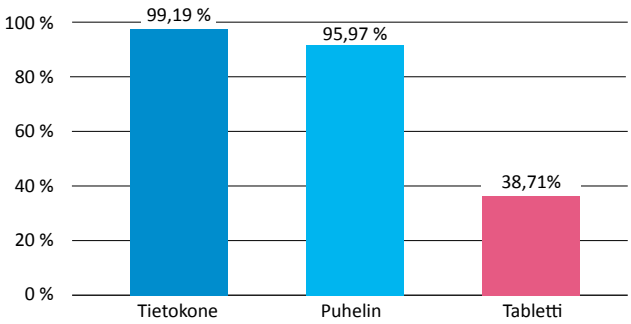
Liite 2.

KYSELYN TULOSTEN KOONTI

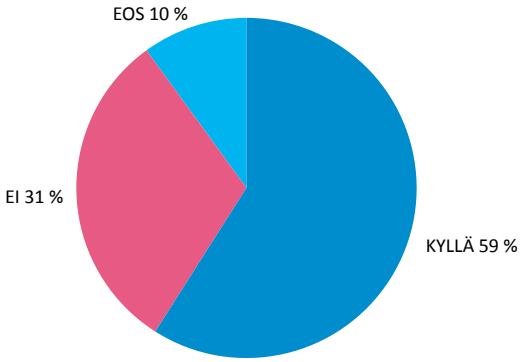
Onko yrityksessänne mahdollisuus tehdä etätöitä? (n = 125)



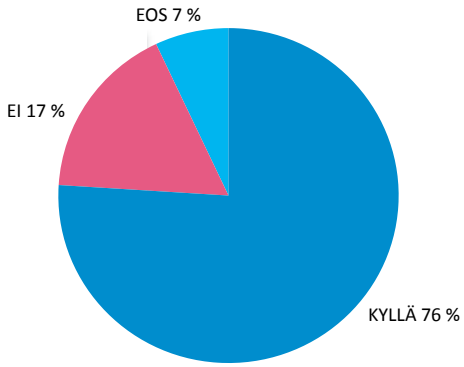
Onko yrityksessänne mahdollisuus tehdä etätöitä yrityksen tarjoamilla laitteilla? (n = 124)



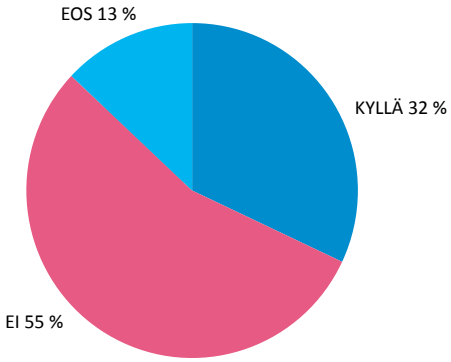
Yrityksen tietokone: Tarjoatteko mahdollisuutta käyttää yrityksen palveluita virtualisointiratkaisuiden kautta? (n = 123)



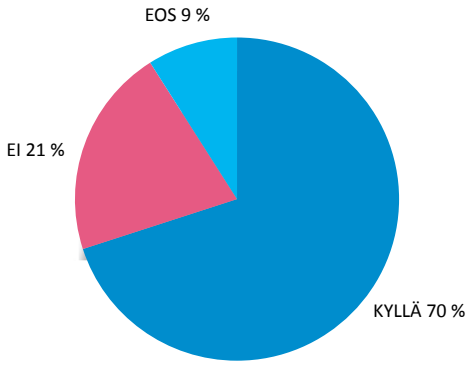
Yrityksen tietokone: Tarjoatteko mahdollisuutta käyttää yrityksen palveluita web-sovellusten kautta? (n = 123)



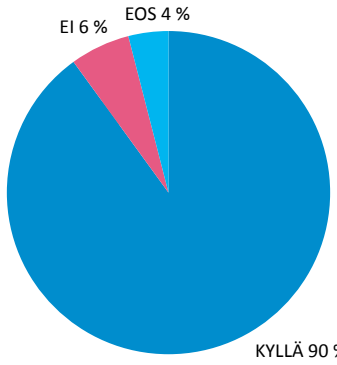
Yrityksen puhelin: Tarjoatteko mahdollisuutta käyttää yrityksen palveluita virtualisointiratkaisuiden kautta? (n = 119)



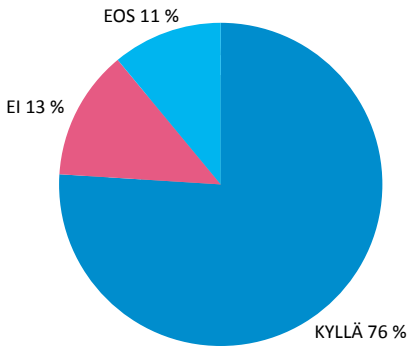
Yrityksen puhelin: Tarjoatteko mahdollisuutta käyttää yrityksen palveluita web-sovellusten kautta? (n = 119)



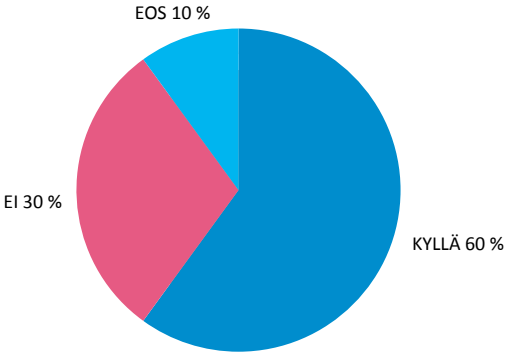
Laitehallinta käytössä (tietokoneet) (N = 114)



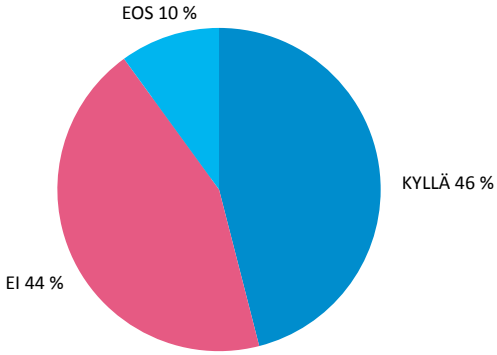
Onko käytössänne laitehallinta yrityksen puhelinten osalta? (n = 74)



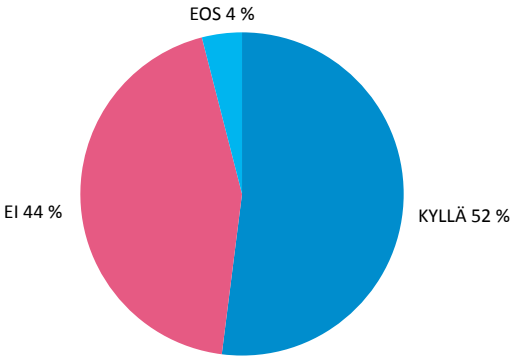
Onko etätyössä käytettävät ohjelmistot ja palvelut rajattu käyttöympäristön mukaan? (n = 124)



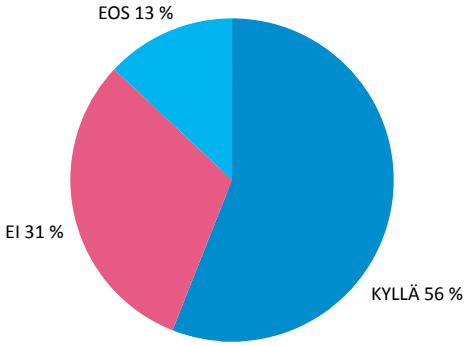
Onko etätyössä tehtäviä työtehtäviä rajoitettu teknisesti tai ohjeistuksella käyttöympäristön mukaan? (n = 124)



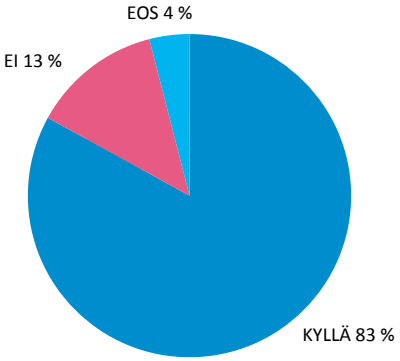
Onko yrityksessänne määritetty etätyön työympäristön vaatimukset (tila, välineet, ympäristö)? (N=124)



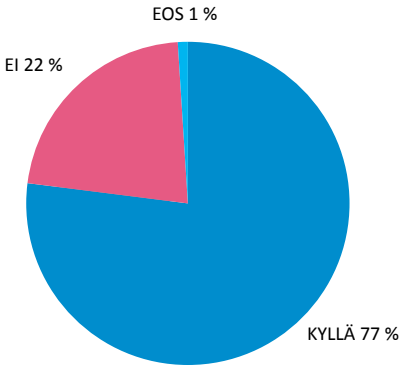
Onko etäkäyttövaatimukset määritetty tietoturvaluokituksen mukaisesti? (n = 79)



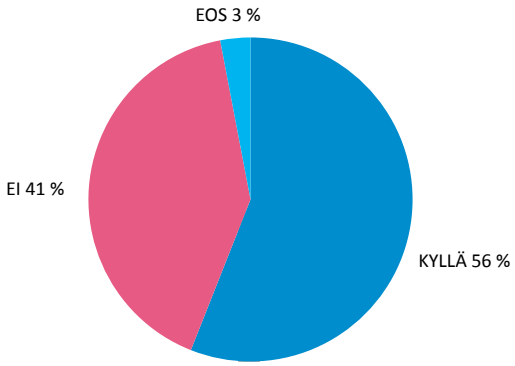
Onko käytössänne politiikka salasanojen turvallisen hallinnan osalta? (n = 124)



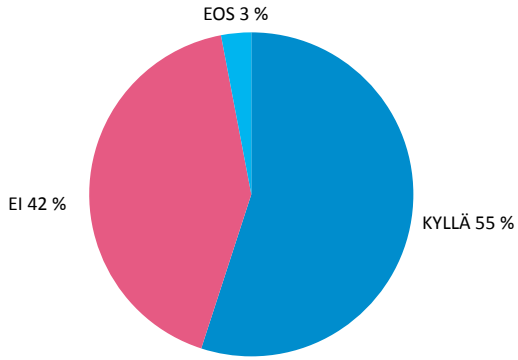
Onko käytössänne vahva tunnistautuminen palveluiden käytön yhteydessä? (n =124)



Etätyön työvälineiden säilytys määritelty (N=124)



Matkustamisen käytännöt määritelty (N=124)



Liite 2.

HAASTATTELUKYSYMYKSET

Alkutiedot

1. Milloin yrityksen etätyöohjeet on laadittu?
2. Onko ohjetta ollut tarpeen päivittää? Jos kyllä, mistä syistä?

Riskianalyysit

3. Onko etätyöohjeistuksiin tehty riskianalyysejä ennen niihin siirtymistä?
4. Onko ohjeet kirjoitettu sisäisesti vai onko se ulkoistettu kolmannelle osapuolelle? Onko ohjeita tehtäessä konsultoitu ulkoisia toimijoita tai muita asiantuntijoita?

Käytössä olevat etätyöohjeistukset

5. Mitkä käytössä olevat tekniset ratkaisut ovat osoittautuneet parhaimmiksi? (mahdollisia teemoja: kotikäyttäjä, matkustuskäyttäjä, admin-käyttäjä)
6. Entä helpoiten toteutettavaksi?
7. Oletteko ohjeistaneet miten henkilökohtainen WLAN suojataan (SSID, oletussalasanan vaihto, MAC-suodatus, portaalin oletustunnusten vaihto)?
8. Oletteko ohjeistaneet tai tarjoatteko salasanojen turvallisen hallinnan (KeePass, ym.)?
9. Miten olette huomioineet ohjeistuksessa paperimateriaalin käsittelyn etätyöskentelyssä yrityksessänne?
10. Miten olette huomioineet ohjeistuksessa työvälineiden säilyttämisen kotona?
11. Miten olette huomioineet ohjeistuksessa turvallisen etätyöskentelyn matkustamisen aikana? Eroaako ohjeistus koti- ja ulkomaanmatkojen osalta
12. Millä tavalla olette huomioineet ohjeistuksessa ulkoiset henkilöt kotiolosuhteissa (perheenjäsenet, naapurit, vieraat)?
13. Millä tavalla olette huomioineet ohjeistuksessa päivitykset ohjelmistoihin, onnistuuko päivitysten tekeminen kotoa käsin? Miten päivitysten ajoa seurataan?
14. Millä tavalla korona-aika on vaikuttanut etätyöohjeistuksiinne

Havaittuja ongelmia / parannettavaa

15. Minkälaisiin haasteisiin etätyöohjeistuksella on erityisesti pyritty puuttumaan?
16. 16. Onko yrityksissä määritetty erilliset prosessit etätyöhön liittyviin ongelmatilanteisiin vai noudatetaanko samoja prosesseja kuin toimistoympäristössäkin?
17. Kyselyn perusteella työntekijöillä on ollut ongelmia yhteyksien muodostamisessa ja VPN-tunneleiden luotettavuudessa. Miten teidän yrityksessänne on otettu huomioon yhteyksien luotettavuus?
18. Miten yrityksenne on varautunut kalasteluyrityksiin?

19. Miten yrityksenne toteuttaa yhteyksien seuraamista (esim. kalastelulla saadut tunnukset)?
20. Millaisia ohjeita toivoisitte yhteyksien suojausta varten?

Teams

21. Onko teillä ohjeita / toivoisitteko ohjeistusta Teamsin turvallisesta käytöstä (millaista tietoa voi jakaa, millaisesta tiedosta voi puhua)?
22. Onko teillä ohjeistusta kodin ulkopuolella tehtävästä Teams-kokouksista?

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI