Matti Laakso
Tietoturva-asiantuntija, Turun ammattikorkeakoulu

Etätyön tietoturva – 10 käytännön vinkkiä

Avainsanat: **etätyö, tietoturvallisuus**

Etätyö laajentaa yrityksen IT-ympäristöä työntekijöiden koteihin. Tämä luo erilaisia haasteita tietoturvallisuudelle niin yrityksen kuin työntekijänkin näkökulmasta.

Etätyön tietoturva muodostuu monesta asiasta. Erityisesti korostuvat työntekijän osaaminen ja oma vastuu ympäristön fyysisestä ja teknisestä turvallisuudesta. Kotitoimistolla on huomioitava eri asioita kuin työpaikalla. Ohessa kymmenen käytännön vinkkiä tietoturvallisempaan etätyöhön.

Koti etätyöympäristönä

Käytä työtehtävien tekemiseen työantajan tarjoamia laitteita. Työpaikan laitteissa on käytössä erilaisia tietoturva-asetuksia ja -suojauksia, joita kotikoneessa ei ole. Omat laitteet on tarkoitettu omien asioiden hoitamiseen. Kotitaloudessa näillä laitteilla voi olla myös muita käyttäjiä. Käyttämällä työasioihin vain työantajan laitteita voidaan edistää sitä, että muiden taloudessa asuvien toimet eivät vaikuta työasioiden tietoturvallisuuteen.

Suojaa laitteiden fyysistä turvallisuutta etätyöpisteessä. Kerro samassa taloudessa asuville ja vierailijoille, mitkä ovat työnteossa käytettäviä laitteita. Sovi heidän kanssaan, että näihin laitteisiin ei kosketa. Fyysinen suojaaminen korostuu kotioloissa erityisesti silloin, kun etätyölle ei ole erillistä työhuonetta, jossa laitteita voidaan säilyttää. Työpisteeltä poistuessa kannattaa lukita tietokoneen ja puhelimen näyttö. Siirrä työlaitteet suojaan työpäivän päätteeksi.

Hyödynnä suojattuja verkkoyhteyksiä ja -laitteita. Etätyöpisteen WLAN-verkon osalta on tärkeää, että verkkoyhteys on salattu. Varmista verkkoyhteyden asetuksista, että käytössä on esimerkiksi WPA2-salaus. Muista suojata myös itse verkkolaite vaihtamalla sen oletussalasana. Voit luoda itsellesi suojatun WLAN-verkon myös älypuhelimesi kautta.

Tiedosta kodin muista älylaitteista aiheutuvat riskit. Vältä esimerkiksi älytelevision ja striimauspalveluiden käyttöä, niin etäyhteydet toimivat luotettavammin ja nopeammin. Eristä kodin muut älylaitteet omaan verkkoonsa, niin kodin laitteissa mahdollisesti olevat tietoturvaongelmat eivät leviä työlaitteisiin. Eristäminen voidaan toteuttaa esimerkiksi toisella WLAN-reitittimellä.

Lisävinkki: Kuuntele Talk-podcastin jakso kodin älylaitteiden kyberturvallisuudesta **https://talk.turkuamk.fi/talk-podcast/kyberturvaa-kotiin-pitaako-olla-huolissaan/**

Tietoturvallinen toiminta verkossa

Asenna tietoturvapäivitykset ajallaan. Käyttöjärjestelmän, sovellusten ja tietoturvaohjelmiston päivitysten merkitys korostuu entisestään, kun siirrytään pois työpaikan tietoverkosta. Yrityksen omassa IT-ympäristössä voi olla käytössä tietoturvateknologiaa, joka ei välttämättä suojaa työntekijän päätelaitetta yrityksen tietoverkon ulkopuolella. Tällöin on erityisen tärkeää, että päätelaite on muilta osin tarpeeksi hyvin suojattu.

Tiedosta IT-palveluiden normaali toiminta etätyöympäristössä. Opettele tunnistamaan, miten IT-palveluihin kirjaudutaan työpaikan ympäristössä ja miten kirjautuminen toimii etätyöpisteestä. Jos IT-palvelu kysyy käyttäjätunnusta ja salasanaa tilanteessa, jossa se ei sitä normaalisti tee, pysähdy ja ajattele. Johtuuko tilanne etätyöstä? Vai oletko syöttämässä tunnuksiasi huijaussivustolle?

Tallenna työtiedostot sovittuun paikkaan. Käytä työantajan tarjoamaa tiedostojen tallennuspalvelua. Jos yhteydet työpaikan verkkoon ei toimikaan, tallenna tiedostot koneellesi. Muodosta käytäntö, jossa viimeistään etätyöpäivän päätteeksi siirrät tiedostot työantajan tallennuspalveluun ja poistat turhat versiot koneeltasi.

Jaa tietoa järkevästi ja turvallisesti. Tiedostoja ei aina ole tarvetta lähettää sähköpostilla. Laita tiedosto digitaaliseen työtilaan ja jaa tiedosto linkillä. Näin kaikki näkevät uusimman version. Vältät myös tiedoston lähettämisen väärille vastaanottajille.

Käytä etätöissä työnantajan tarjoamia ja ohjeistamia IT-palveluita. Näin kannat omalta osaltasi vastuun digiturvallisuudesta ja autat organisaatiotasi noudattamaan tietosuojalainsäädännön vaatimuksia. Jos jokin työpaikan ohjelmisto ei sovellu etätyöhön, kerro asiasta esimiehellesi ja yrityksen IT-palveluista vastaavalle henkilölle. On kaikkien etu saada käyttöön järjestelmä, joka tukee paremmin työn tekemistä ja nostaa tuottavuutta.

Ota selvää, miten varmuuskopiointi toimii. Käytännöt ja tekniikat vaihtelevat yrityksittäin. On tärkeää tietää, mitä pitää varmuuskopioida itse ja mikä kopioidaan automaattisesti. Tallenna varmuuskopiot sovittuun paikkaan. Älä tee omia varmuuskopioita esimerkiksi USB-muistille, jos sitä ei ole yrityksen tietojenkäsittelyohjeissa sallittu.

Edellisten vinkkien lisäksi on hyvä muistaa myös muut tietoturvallisen työn perusasiat, kuten järkevät salasanakäytännöt sekä tarkkaavaisuus sähköpostin liitetiedostojen ja linkkien kanssa. Näin tietoturvallisuus tulee huomioitua kokonaisvaltaisesti, oli työpiste sitten kotona, kahvilassa tai työpaikalla.

Lisätietoja:

Kyberturvallisuuskeskus 2020. Tee etätyöstä turvallista vinkkiemme avulla. Viitattu 23.3.2020. **https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tee-etatyosta-turvallista-vinkkiemme-avulla**

SANS 2020. SANS Security Awareness Work-from-Home Deployment Kit. Viitattu 20.3.2020. **https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit**

23.03.2020