TIETOKESKUS

TIETOTURVAN PIKAMANUAALI

Suojaa yrityksesi käyttäjät, laitteet ja data



Sisältö

Tietoturvasta huolehtiminen on jokaisen asia. Yrityksen tietoturvasta vastaavan tulee olla askeleen edellä, jotta yrityksen käyttäjät, laitteet ja data pysyvät turvassa. Tästä pikamanuaalista löydät käytännönläheiset vinkit yrityksen tietoturvan parantamiseksi.

01 SUOJAA KÄYTTÄJIEN IDENTITEETIT 3

02 SUOJAA LAITTEET 7

03 SUOJAA DATA 12



01

SUOJAA KÄYTTÄJIEN IDENTITEETIT

Kyberhyökkäykset johtuvat useimmiten inhimillisistä virheistä. Suojaa käyttäjien identiteetit ja herättele työntekijät huolehtimaan tietoturvasta myös itse!

Kaikenlaiset identiteetit ovat kovaa valuuttaa. Käyttäjätunnuksia ja salasanoja voidaan varastaa mistä vain – esimerkiksi verkkokaupasta tai harrastuksista. Varastetulla identiteetillä pääsee kirjautumaan monenlaisiin järjestelmiin ja sensitiiviset henkilötiedot yhteystiedoista henkilötunnukseen ovat vaarassa. Yritysten järjestelmät ja niihin varastetuille tiedoilla kirjautuminen eivät ole tästä poikkeus.

Osaako jokainen yrityksesi työntekijä vastata näihin kysymyksiin?

- Käytätkö samaa salasanaa monessa paikassa?
- Mitä teet, jos salasanasi varastetaan?
- Mistä tiedät, että salasanasi on varastettu?
- Onko sinulla salasanaton kirjautuminen käytössä (esim. PIN-koodi)?
- Käytätkö monivaiheista autentikointia aina kun voit?

Lisäksi, jos vastaat yrityksesi tietoturvasta, niin osaatko vastata näihin kahteen kysymykseen?

- Mitä yrityksessäsi tehdään työntekijöiden suojaamiseksi tietoturvauhilta?
- Mitä voisi tehdä paremmin?

Yritykset voivat ohjata henkilöstöään säännöillä ja rajoituksilla, mutta viime kädessä yksilö on vastuussa salasanoista ja suojaamisesta. Esimerkiksi samaa salasanaa ei tule koskaan käyttää monessa paikassa. Syy tähän on, että jos kuntosalin asiakastilille murtaudutaan ja samaa sähköpostiosoitetta ja salasanaa on käytetty muuallakin, niin silloin myös kaikki muut palvelut ovat vaarassa – pahimmassa tapauksessa myös yrityksen tiedot.

Näillä teknologioilla suojaat yrityksesi työntekijöitä

- Hyödynnä teknologioita, joilla voit laittaa jokaiseen palveluun suositusten mukaisen, uniikin salasanan. Markkinoilla on useita hyviä tuotteita, jotka auttavat tässä.
- Yrityksen hallinnoima identiteetti voidaan viedä salasanattomaan maailmaan. Tämä tarkoittaa käytännössä sitä, että salasanaa käytetään harvoin, jos koskaan. Salasana korvataan kuittaamalla esim. puhelimella olevasta sovelluksesta, kuten Microsoft Authenticator, tai käyttämällä yksinkertaista PIN-koodia tai biometriikkaa laitteelle kirjautumiseen.
- On myös erilaisia laiteratkaisuja, kuten FIDO2-turva-avaimet, jossa jokainen kirjautuminen voidaan varmistaa esimerkiksi koskettamalla fyysistä avainta, joka on liitetty laitteeseen.

Niin salasanattomassa kuin FIDO2-kirjautumisessa tarkoituksena on varmistua, että kirjautumisen takana on se henkilö, joka tämä väittää olevansa. Monivaiheinen autentikointi suojaa tiliä silloinkin, kun salasana on päätynyt vääriin käsiin: käyttäjätunnuksen ja salasanan lisäksi kirjautuminen pitää varmentaa käyttäjän omalla puhelimella.

Nämä asiat yrityksessä kannattaa tehdä

- Monivaiheinen autentikointi (MFA) käyttöön (kaikilla mahdollisella lisäkilkkeillä) kaikille työntekijöille, vierailijoille ja yhteistyökumppaneille.
- Valitse yrityksen käyttöön vain sovelluksia, jotka tukevat tietoturvallisia kirjautumismenetelmiä.
- Siirrä työskentelyä, viestintää ja dataa esimerkiksi monivaiheista tai salasanatonta kirjautumista edellyttävien, turvallisten palveluiden taakse.
- Lisää itsepalvelua loppukäyttäjille – salasanan vaihto tai resetointi pitää olla mahdollista ilman IT:n apua.
- Panosta salasanattomuuteen tulevaisuudessa.

Tekninen toteutus on näissä noin päivän homma, loppu on viestintää.

Kumoa väärät väitteet

Ei meillä mitään mielenkiintoista ole, miksi meistä kiinnostuttaisiin?

Verkkorikollista voi kiinnostaa esimerkiksi pyytää toimitusjohtajan nimissä rahasiirtoa talousjohtajalta silloin kun toimitusjohtaja itse lomailee, käyttäen murrettua sähköpostia. Yleensä tällaisissa viesteissä sähköposteihin luodaan vahva kiireellisyyden tuntu, jotta erikoiselta tuntuvaan pyyntöön olisi helpompaa suostua.

Emme halua tehdä työntekijöiden elämästä yhtään monimutkaisempaa kuin mitä se nyt on.

Lyhyet PIN-koodit tai sormenjäljet ovat huomattavasti turvallisempia ja helpompia käyttää kuin salasanat.

02
SUOJAA LAITTEET

Minkä tahansa laitteen, jolla käytetään yrityksen resursseja, täytyy olla turvattu, suojattu ja salattu. Tehokas laitehallinta mahdollistaa laitteiden nopean käyttöönoton sekä datan suojaamisen. On tärkeää, että laite on tunnistettavissa ja hallinnassa, jolloin se voidaan esimerkiksi varkaustapauksessa tyhjentää.

Yrityksen laite sisältöineen voi myös olla myynnissä nettikaupassa työntekijän poislähdön jälkeen. Vähintään silloin pitää perusasioiden perusasiat kunnossa: vaikka kierrätysprosessi ei olisi toimiva, on laite joka tapauksessa salattu ja suojattu PIN-koodilla.

Laitehallintaan on markkinoilla useita vaihtoehtoja ja useimmat Microsoft-lisenssit sisältävät tarvittavat tuotteet – ne pitää vain ottaa käyttöön.

Vaikka laitehallinnalla voidaan tehdä erilaisia asetuksia, yksi oleellisimmista asioista tietoturvan kannalta on tunnistaa, onko laite yrityksen oma vai hallitsematon vieras.

Laitteita on neljänlaisia – laitehallinnan tulee ottaa huomioon kaikki nämä skenaariot:

1. Mehukoneet ja aulatilan pädit

Tietoturvan kannalta helpoimmat laitteet ovat yrityksen mehukoneita tai aulatilan pädejä, joissa pädi on kaikkien kosketeltavissa ja käytettävissä. Nämä laitteet tarvitsevat hallintaa, mutta eivät niinkään suojausta. Näissä todennäköisesti ei ole yrityksen dataa. Oletteko nähneet hotelliaamupalalla mehukoneita, joissa valitaan mehu? Tarkoitamme juuri niitä laitteita.

2. Laitteet, joita käytetään vain puheluihin ja tiettyihin toimintoihin

Otetaan aamulla laturista, käytetään päivän ajan ja laitetaan takaisin lataukseen yöksi. Tehtaan tuotannossa käytetty pädi, tai jopa normaali matkapuhelin, joka on tarkoitettu vain työasioiden hoitamiseen. Tällainen laite tarvitsee suojausta, mutta se tuskin sisältää ihmisten henkilökohtaista dataa.

3. Yrityksen omistama laite, jota työntekijä käyttää myös henkilökohtaisessa elämässään

Esimerkkinä tästä on puhelin. Kun puhelin tulee elinkaarensa päähän, käyttäjä ei saa pitää sitä itsellään. Tällaisessa laitteessa täytyy olla huomioituna tietoturvallinen kierrätys, suojaukset jne. Myös silloin kun puhelin on käytössä, täytyy yrityspuoli ja henkilökohtainen puoli eristää. Eristyksellä tarkoitetaan sitä, että työhön liittyvät applikaatiot ovat selkeästi työprofiilin puolella ja tiedonsiirtoa näiden kahden profiilin välillä voidaan rajoittaa. Esimerkiksi työprofiilin puolella olevasta Teams-keskustelusta ei voi ottaa ruutukaappausta ja jakaa sitä henkilökohtaisen profiilin Whatsapp-sovelluksessa.

4. Loppukäyttäjä omistaa laitteen, mutta käyttää sitä työssään

Täytyy varmistua siitä, että yritys pystyy esimerkiksi työpaikanvaihdoksen yhteydessä poistamaan kaiken työhön liittyvän datan ja sovellukset.

Kuvittele työntekijä, joka haluaa käyttää aina uusinta tekniikkaa, ja haluaa itselleen uuden 1500 euroa maksavan puhelimen. On ymmärrettävää, ettei yritys välttämättä tue työntekijää tässä harrastuksessa. On myös ymmärrettävää, ettei työntekijä halua käyttöönsä markkinoiden edullisimman pään mallia, jota hän käyttäisi pelkkien työasioiden hoitamiseen. Tällainen puhelin ei voi olla täysin yrityksen hallinnassa, sillä kyse on yksityishenkilön omistamasta laitteesta, jonka hän voi halutessaan esimerkiksi myydä tai vaihtaa uudempaan.

Yrityksen pitää pystyä hallitsemaan tietoturva-asetuksia yrityksen datan osalta, mutta hallinta ei saa estää esimerkiksi puhelimen jälleenmyyntiä tai käyttöä jossain muussa tarkoituksessa.

Kumoa väärät väitteet

Työnantaja maksaa puhelimen. Eihän näillä tehdä muuta kuin toitä!

Kyse ei ole pelkästään busineksesta vaan koko työntekijän elämästä. Puhelin voi sisältää kuvat elämän tärkeimmistä hetkistä ja viestiketjut. Hyvä hallintamalli mahdollistaa sen, että tämä voidaan tehdä yrityksen tietoturvaa vaarantamatta ja rajoittamatta työntekijän yksityiselämää.

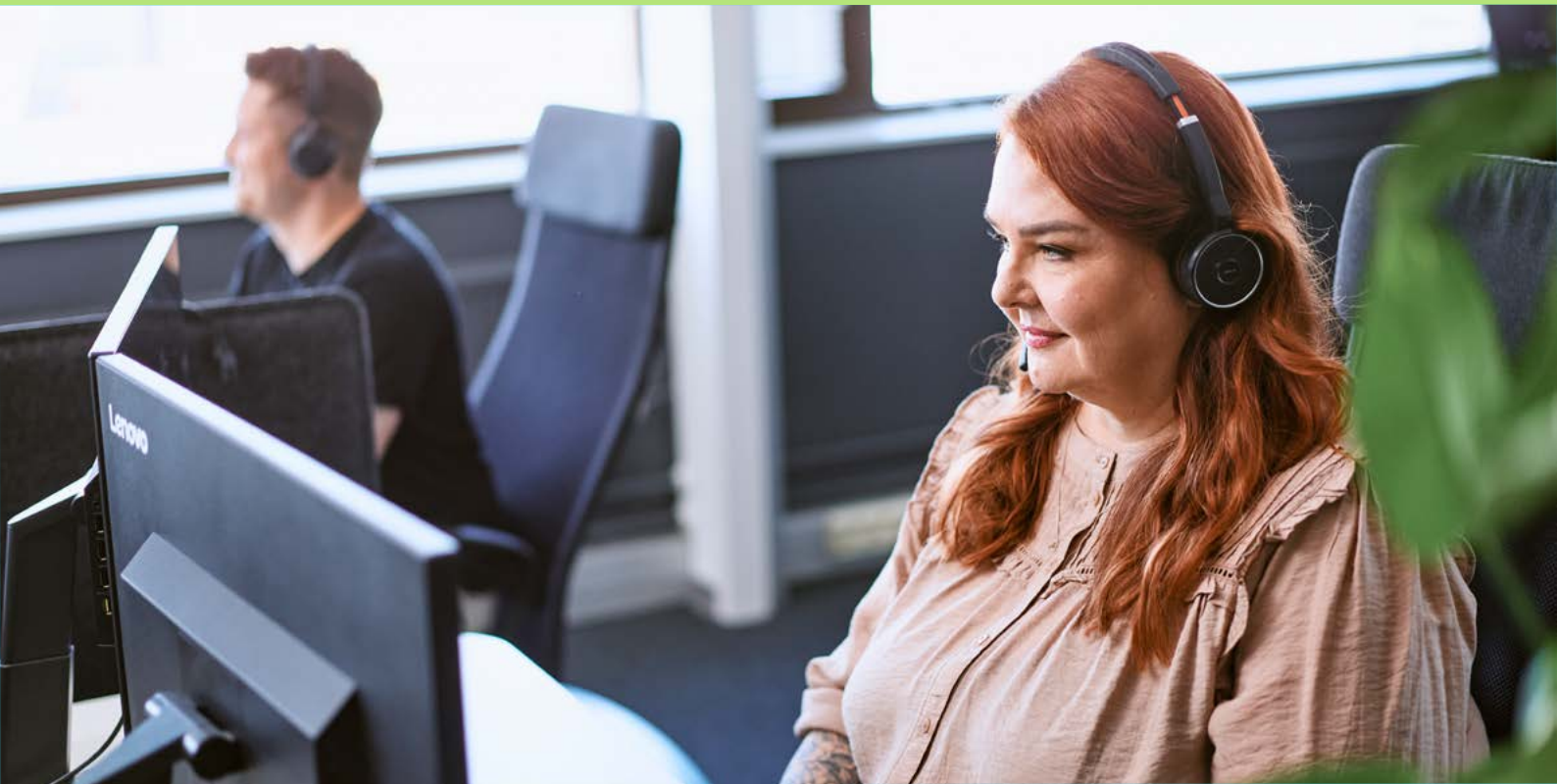
Pelkkä PIN-koodi riittää.

Ilman hallintaa et tiedä, onko laitteessa PIN-koodia. Laitehallinnalla voidaan pakottaa tietyt tietoturva-asetukset, ovat ne sitten kuinka yksinkertaisia tahansa. PIN-koodistakaan ei ole mitään hyötyä, jos se on 1234. Laitehallinnalla voidaan estää helposti arvattavien ja yleisimpien PIN-koodien käyttöä.

Nämä asiat yrityksessä kannattaa tehdä

Laita perusasiat kuntoon laitehallinnan avulla eli huolehdi, että:

- Laite on salattu
- Laite on suojattu salasanalla ja/tai PIN-koodilla
- Laitetta voidaan hallita etänä ja siihen voidaan lähettää tyhjennyskomento
- Laite on määritetty oikein, turvalliseksi ja vakioiduksi
- Laitteeseen on pääsy, jotta ei ole tarvetta huolestua yrityksen datasta, jos laite häviää, varastetaan, kierrätetään, tai myydään työntekijälle
- Itse laitteen lisäksi huomioidaan inventaariot, sovellusjakelut, päivitykset sekä sovelluskaupat.



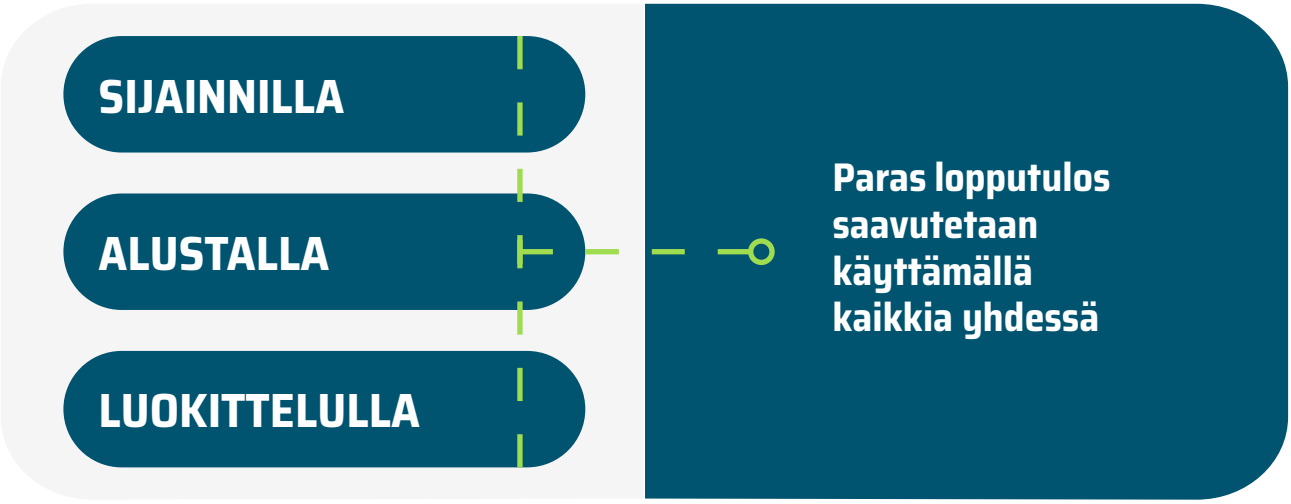
03
SUOJAA DATA

Datan osalta oleellista:

- Onko data palautettavissa? Päästäänkö dataan usealta eri laitteelta?
- Ei välttämättä maantieteellinen sijainti, vaan yhteisesti sovitut säännöt siitä mihin dataa laitetaan
- Alustat kuten Microsoft Teams on erinomainen tapa suojata myös tiedostoja – parempi tapa kuin perinteiset verkkoasemat
- Tiedostoihin ja keskusteluihin pääsevät käsiksi vain tiimiin kuuluvat henkilöt
- Palveluita voidaan käyttää mistä vain – laitevapaasti ja turvallisesti

Niin salasanattomassa kuin FIDO2-kirjautumisessa tarkoituksena on varmistua, että kirjautumisen takana on se henkilö, joka tämä väittää olevansa. Monivaiheinen autentikointi suojaa tiliä silloinkin, kun salasana on päätynyt vääriin käsiin: käyttäjätunnuksen ja salasanan lisäksi kirjautuminen pitää varmentaa käyttäjän omalla puhelimella.

Data voidaan suojata



Sijainnista

Olemme tottuneet siihen, että kun laitamme datan yrityksen palvelimelle, esimerkiksi Y-asemalle, se on ”suojassa”. Näin se ei mene. Jokainen, jolla on pääsy tiedostoon, voi halutessaan kopioida tiedoston haluamaansa paikkaan. Sillä hetkellä tiedosto perii käyttöoikeudet siitä paikasta, minne tiedosto siirretään. Tässä tapauksessa tiedoston sijainti ei enää suojaa dataa.

Alustasta

Entä jos datan sijainnin sijaan dataa suojataan alustalla? Ja Y-aseman sijaan käytetäänkin esimerkiksi Teams:iä?

Tämän jälkeen jokaiselle käyttäjälle on selvää, että kaikki, jotka kuuluvat tiimiin, näkevät tiedostot. Jos halutaan, että ulkopuoliset käyttäjät näkevät tiedoston, heidät täytyy kutsua tiimiin tai tiedosto täytyy siirtää sellaiseen paikkaan, jonne kaikilla on pääsy. Tämä automaattisesti lisää ymmärrystä siitä, kenellä kaikilla on pääsy tähän dataan ja keskusteluihin. Tämä ei ole tilanne, kun työskentelemme Y-asemalla.

Vaihtamalla alustaa tietoturvaa datan suhteen voidaan parantaa. Alustan täytyy olla sellainen, että jokainen näkee mihin omat oikeudet riittävät. Oikeuksia täytyy pystyä hallinnoimaan ilman IT-osaston apua. Alustan vaihtaminen tarkoittaa myös sitä, että tiedostot ovat käytettävissä kaikilla laitteilla. Päästäkseen tiedostoihin käsiksi, vaaditaan monivaiheinen autentikointi (kuten luit kohdasta 1).

Luokittelusta

Jos tiedosto napataan muistitikulle tai mobiililaitteeseen tai lähetetään väärälle vastaanottajalle, mikään yrityksen järjestelmiin rakennettu tietoturvakuvio ei ole enää voimassa. Voimme kuitenkin ottaa käyttöön luokittelun. Luokittelun mukana tiedostolle voidaan antaa käyttöoikeudet, jotka seuraavat tiedostoa minne vain: käyttöoikeuksia voi rajata esimerkiksi vain yrityksen työntekijöille / tiimille / johtoryhmälle. Tämä tarkoittaa, että jatkossa tiedostoon pääsevät vain siihen määritellyt ihmiset – sijainnista tai alustasta riippumatta.

Kumoa väärät väitteet

Meillä on miljoonia tiedostoja. Miten ikinä voisimme luokitella ne kaikki?

Aloittakaa yhdestä yksiköstä, esim. HR tai tuotekehitys, jotka käsittelevät työntekijöihin tai liiketoimintaan liittyvää kriittistä dataa. Voitte edelleen turvautua sijaintin ja alustoihin perustuviin ratkaisuihin kaikkien ei-niin-kriittisten tietojen osalta. Työpaikkaruokalan lounaslista voi olla edelleen kaikkien saatavilla, myös kilpailijoiden.

Meidän ei tarvitse luokitella tietojamme. Luotamme työntekijöihimme.

Kyse on usein inhimillisestä virheestä. Oletko joskus lähettänyt sähköpostia väärälle vastaanottajalle? Oliko sähköpostissa liitetiedosto?

Jos tiedosto olisi ollut luokiteltu ja luokittelun mukana olisi määritelty käyttöoikeudet, väärä vastaanottaja ei saisi liitetiedostoa auki.

Nämä asiat yrityksessä kannattaa tehdä

- Ei tallenneta vain työasemille.
- Ihmisiä ei yksinkertaisesti pysty opettamaan eroon ”työpöydälle tallentamisen” tavasta, joten kopioidaan myös työpöytä pilveen. Silloin työpöydän tiedostot ilmestyvät myös uudelle koneelle.
- Suojaa tiimejä, jottei niihin pysty kutsumaan ulkopuolisia.
- Ota käyttöön Sensitivity Labels -tekniikka M365-lisenssien avulla.
- Kouluta yksi tiimi kerrallaan Sensitivy Labels -tekniikan käyttöön.



Laitetaanko yrityksesi tietoturva kuntoon?

Tietoturva koostuu identiteettien, laitteiden ja tiedon turvaamisesta. Nämä perusasiat kannattaa laittaa kuntoon ennen kuin on liian myöhäistä:

- Monivaiheinen autentikointi (Multifactor Authentication, MFA) työntekijöille, vierailijoille ja yhteistyökumppaneille
- Laitehallinta: luotetut ja vaatimusten mukaiset laitteet osaksi kirjautumista
- Salasanaton kirjautuminen
- Datan suojaaminen: verkkolevyasemasta luopuminen ja Teamsiin siirtyminen
- Datan luokittelu niin, että arkaluontoista dataa sisältävään tiedostoon pääsevät käsiksi vain määritellyt henkilöt.

Kaikki nämä ovat 1–2 konsultointipäivän projekteja, eli tietoturvan tasoon saa huomattavaa parannusta jo pienellä panostuksella. Meiltä järjestyy myös tietoturvauhkien valvonta kuukausihinnalla.



Jutellaanko lisää?

myynti@tietokeskus.fi

Valtakunnallinen vaihde:
03 233 5100