
Kyberturvan
pelisäännöt
pienyrityksille
2023

Kyberturvan pelisäännöt pienyrityksille 2023
Julkaisija: Turun yliopisto
Kirjottajat: Juhani Naskali, Mikko Vermanen ja Jani Koskinen (Turun yliopisto)
Ulkoasu ja taitto: KMG Turku
Paino: Printworks
Painovuosi: 2023, 1. painos

ISBN 978-951-29-9397-0 (Verkko)
ISBN 978-951-29-9398-7 (Print)

TURUN YLIOPISTO

TURKU AMK

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto
Euroopan sosiaalirahasto

Kyberturvan pelisäännöt pienyrityksille 2023 on toteutettu Turun yliopiston toimesta 4K-kyberturvallisuus-hankkeessa, joka rahoitetaan osana Euroopan unionin covid-19-pandemian johdosta toteuttamia toimia.

Sisältö

1. Mikä kyberturva?

Kyberturva on laaja aihe, mutta pitää sisällään yksinkertaisia toimenpiteitä. Tämä opas kokoaa yhteen kyberturvan pelisäännöt pienyrittäjille ja tavallisille ihmisille. Oppaan alkupuoli käsittelee pienyrityksille tärkeitä prosesseja ja kyberturvan hallintaa.
Oppaan viimeinen luku kokoaa yhteen kyberturvan tärkeimmät pelisäännöt, jotka soveltuvat kaikille.

1.1. Tietoturva on nyky-yrittäjän pakollinen taito

Kyberturva pitää sisällään sähköisiin järjestelmiin liitetyn tiedon suojaamisen eri tavoin. Perinteisestä tietoturvasta kyberturvan erottaa keskittyminen eritoten sähköisiin uhkiin siinä missä tietoturva pitää sisällään myös esimerkiksi paperilla olevan tiedon turvaamisen.
Tässä oppaassa käsitellään molempia, joskin painopiste on kyberturvassa. Tietokoneiden suojaus ja varmuuskopiointi, tietoliikenneyhteydet ja -laitteet sekä huoli sähköpostilinkkien avaamisessa kuuluvat kaikki kyberturvallisuuteen. Hyvä kyberturva otetaan huomioon myös yrityksen toimintamalleissa ja henkilöstön koulutuksessa.

Menneisyydessä yrityksen pääoman suojaamiseksi riitti lukko ovessa ja kirjanpidon perustaidot. Paperiarkistot ja yritysten tiloissa sijaitsevat itsenäiset koneet olivat luonteeltaan erittäin tietoturvallisia. Teknologian kehitys on kuitenkin tuonut mukanaan uusia riskejä, joihin pitää osata varautua. Työkoneet ovat jatkuvasti kiinni verkossa, ja yrityksen tiedot liikkuvat usein internetin yli. Kiristyshaittaohjelmat voivat pahimmillaan kaapata ja poistaa kaiken yrityksen tiedon ja vaatia rahaa sen palauttamiseksi tai julkaisun estämiseksi. Palveluja ja jopa rahaa voidaan varastaa sähköisesti. Haittaa voidaan tehdä jopa vain kiusaksi tai huomion saamiseksi.

Liiketoiminnalle kriittisen tiedon ja toiminnan suojaaminen vaatii kyberturvan huomioimisen niin tiedon tallennuksessa, siirrossa kuin käsittelyssäkin. Perusasioiden turvaaminen ei kuitenkaan vaadi ohjelmointigurua. Riskien tunnistaminen ja maalaisjärki riittävät pitkälle.

1.2. Hyvät lähtökohdat pienyrittäjän kyberturvaan

Sopivat kyberturvaratkaisut vaihtelevat tilanteen mukaan, eikä raskain ja kaikkein turvallisin ratkaisu ole aina kannattavin liiketoiminnan kannattavuuden tai työn sujuvuuden kannalta. Tämä opas on pienyrittäjille suunnattu selkokielinen kyberturvan ohjekirja, joka kokoaa yksiin kansiin tärkeimmät pelisäännöt yritystoiminnan turvaamiseksi. Vaikka osa ohjeistuksesta on suunnattu yrityksille, opas ja etenkin sen lopussa olevat kyberturvan pelisäännöt pätevät myös yksityishenkilöille.

Oppaan alussa kerrotaan yleisesti kyberturvasta ja keinoista arvioida oman yrityksen kyberturvan tasoa. Tämän jälkeen kuvataan kyberturvan toteutusta ennakoidusti ja kriisitilanteissa, sekä miten kyberturvan huomioon ottaminen muuttuu liiketoiminnan kasvaessa.

Kirjan loppuosa sisältää hyvän kyberturvallisuuden pelisäännöt – kootut ohjeet, joilla perusasiat saadaan kuntoon ja pienyrityksen kyberturva nostettua hyvälle tasolle. Voit avata sivun suoraan ajankohtaisen aiheen kohdalta, ja napata tärkeimmät vinkit hyötykäyttöön, tai lukea koko oppaan saadaksesi kokonaiskuvan firman kyberturvan kartoittamiseksi.

Kyberturva-ratkaisut vaihtelevat tilanteen mukaan. Raskain ja turvallisin ei ole välttämättä kannattavin.

1.3. Kyberturvallisuus kehittyy jatkuvasti

Tämän kirjan ei ole tarkoitus sisältää kaikkea tietoa kyberturvallisuuteen liittyen. Etenkin sähköisiin palveluihin keskittyvien, arkaluonteista tietoa käsittelevien ja suurikokoisten firmojen tulee ottaa kyberturvallisuus huomioon laajemmin oman liiketoimintansa näkökulmasta. Kyberturvallisuus myös kehittyy jatkuvasti, ja omaa tietämystä joutuu päivittämään tasaisesti.

Hyvää ja ajantasaista lisämateriaalia kyberturvasta löytyy mm. Kyberturvallisuus-keskuksen nettisivuilta kyberturvallisuuskeskus.fi.

2. Kyberturvan hallinta

Hyvä kyberturva alkaa turvattavien tietojen ja niihin liittyvien riskien tunnistamisella. Riskien minimointi ja niihin liittyvät tekniset ja henkilöstön osaamiseen liittyvät toimenpiteet otetaan käyttöön siinä laajuudessa kuin riskien hallinta vaatii.

2.1. Mistä kyberturva koostuu?

Kyberturvalla suojataan yrityksen pääomaa (kuten tietoa). Yrityksen kyberturva rakentuu laajasta joukosta erilaisia osa-alueita. Aihetta käsitellään usein vain teknisestä näkökulmasta, mutta kokonaisuuteen nivoutuu paitsi teknologia, myös henkilöstön osaaminen ja toimintatavat, organisaatiokulttuuri sekä kumppanuusverkoston toiminta. Toki tekniset ratkaisut ovat tärkeitä ja niiden ylläpito (mm. päivitykset) muodostaa hyvän kyberturvan perustaa. Moderniin kyberturvastrategiaan tulee kuitenkin sisällyttää myös henkisen pääoman hyödyntäminen ja sen kehittäminen – ei ainoastaan vuotojen estäminen teknisillä toimilla.

Yleisellä tasolla tarkasteltuna kyberturvan hallinta viittaa tapaan tehdä kyberturvaa koskevia päätöksiä – kuka päätöksiä tekee, millä perusteilla ja menetelmillä niitä tehdään, ja kuinka usein niitä tehdään. Nämä asiat tulee selkeyttää, jotta kyberturvaan liittyvä toiminta on sujuvaa. Päätettäviin asioihin kuuluvat kyberturvariskien tunnistaminen ja niihin varautuminen, mutta myös kyberturvatyön organisointi; kenen vastuulle (sisäisesti tai ulkoisesti) mikäkin kyberturvan osa-alue luotetaan.

Tässä luvussa esitellään kyberturvan hallintaan liittyviä aiheita. Itse turvaamiseen liittyvät toimet käydään läpi seuraavassa luvussa osa-alueittain.

2.2. Tietoturvariskien tunnistaminen

Merkittävien uhkatekijöiden ja niiden toteutumiseen liittyvien liiketoiminta-riskien tunnistaminen auttaa tekemään fiksuja päätöksiä siitä mihin suoja-toimiin kannattaa panostaa eniten. Yrityksen eri toimijoiden välinen keskustelu on tässä tärkein työkalu. Johto voi usein ymmärtää parhaiten mikä yrityksen tieto on houkuttele-vinta hyökkäyksille ja toisaalta kriitti-sintä omalle liiketoiminnalle. Itse työn tekijät ja tekniset asiantuntijat tunte-vat usein parhaiten työnteon kriittiset vaiheet ja osaavat ottaa kantaa suoja-toimenpiteisiin. Pallotteluun voi myös hyödyntää ulkoisia lisäkäsiä teknisen toteutusprojektin ohessa tai lisäksi.

Riskien tunnistuksessa kannattaa ensin pohtia mikä tieto on arkaluonteista joko levitessään (esim. yrityssalaisuuksien vuotaminen) tai tuhoutuessaan (esim. kirjanpito tai asiakastiedot).

Tieto, jota yritys erityisesti tarvitsee liiketoiminnassaan kannattaa turvata vahvasti. Toisena näkö-kulmana kannattaa miettiä mihin tietoon kuvitteellinen hyökkääjä pääsee helposti käsiksi. Internetissä olevan palvelimen suojaukseen joutuu käyttämään enemmän ajatusta kuin valmiiksi melkoisen turvallisen toimiston lukitun kaapin turvaamiseen (paitsi varmuus-kopioinnin kannalta). Kolmantena huomioitavana asiana kannattaa miettiä yrityksen tietoihin kohdis-tuvia lakeja ja säännöksiä – tuleeko jotain toimenpiteitä tehdä, jotta yritys täyttää velvollisuutensa eikä joudu yllättäviin vaikeuksiin tule-vaisuudessa? Yksi tärkeä esimerkki tällaisesta on EU:n tietosuoja-asetus, GDPR, joka säätelee yritysten henkilötietojen käsittelyyn ja tur-vaamiseen liittyviä velvollisuuksia.

Kun riskit on listattu, ne kannattaa pisteyttää niiden kriittisyyden (kuinka paha tilanne on jos riski toteutuu) ja todennäköisyyden (kuinka helposti riski toteutuu) mukaan. Erittäin kriittiset ja todennäköiset riskit ovat kaikkein tärkeintä hallita. Tämän jälkeen riskien hallintaan voi alkaa järjestelmällisesti tekemään suunnitelmia. Kun tehtäviä asioita listaa ylös, muodostuu riskienhallintasuunnitelma, joka määrittelee yrityksen strategiaan toimenpiteitä riskien välttämiseksi. Strategiaa voi ja kannattaa päivittää ja kehittää. Yksinkertaisimmillaan tämä voi olla lista tyyliin: ”Riski: asiakastiedot vuotavat palvelimelta, erittäin kriittinen, melko todennäköinen. Tehtävä: kysy IT-palveluntarjoajalta voiko asiakastietoja siirtää verkosta vaikka toimiston koneelle tai voiko tietoja suojata muulla tavalla. Tee suunnitelma yhdessä asiantuntijan kanssa.” Suunnitelmissa kannattaa myös miettiä miten riskin toteutuminen tunnistetaan ja miten pahimmassa tilanteessa reagoidaan.

Kun jonkinasteinen suunnitelma on valmis, se täytyy laittaa käytäntöön. Paraskaan suunnitelma ei tee mitään laatikon pohjalla. Tarvittavat toimenpiteet täytyy tuoda kaikkien tekijöiden tietoisuuteen – joko kouluttamalla tai muuten yhdistämällä jokapäiväiseen toimintaan. Esimerkiksi riski ”Hyökkääjä soittaa puhelimella, esiintyy asiakkaana ja pyytää luottamuksellisia tietoja” voidaan ottaa haltuun ohjeistamalla puhelimeen vastaavat ihmiset siitä, että tietoja kysyvät asiakkaat täytyy aina varmistaa kysymällä asiakasnumeroa ja varmistamalla että pyyntö tulee tunnetusta puhelinnumerosta tai sähköpostiosoitteesta. Aika ajoin on hyvä varmistaa, että sovitut toimet tulevat tehdyksi ja pysyvät työkalupakissa, eivätkä pääse unohtumaan.

Kun suunnitelma on toiminnassa, voi keskittyä normaaleihin töihin, mutta riskejä täytyy silti tarkkailla. Tarkkailun ei tarvitse olla jatkuvaa, mutta jollain tavalla riskien toteutuminen olisi hyvä huomata, jotta tilanteeseen voidaan reagoida. Kriisitilanteisiin reagoinnista lisää luvussa 4.

Tärkeimmät vinkit riskienhallintaan

1. Tunnista riskit.
2. Tee riskienhallintasuunnitelma.
3. Kouluta henkilöstö ja pidä suunnitelma elossa.
4. Tarkkaile ja reagoi.

Ajantasaista tietoa eri riskeistä tarjoaa Kyberturvakeskuksen Kybermittari osoitteessa **kyberturvallisuuskeskus.fi/kybermittari**

Tietoturvariskiesimerkkejä

Yrityksen kyberturvariskit ovat moninaiset ja muuttuvat ajan saatossa, joten mikään valmis lista ei kata yksittäisen yrityksen kaikkia suojattavia osa-alueita. Tässä kuitenkin muutamia esimerkkejä huomioitavista riskeistä.

HEIKOT SALASANAT

Käyttäjien heikot salasanat tai jaetut ylläpitotunnukset lisäävät tietoturvaloukkausten riskiä. Monivaiheisen tunnistautumisen käyttöönotto suojelee suurelta osalta identiteettivarkauden riskejä.

PUUTTEELLISET PÄIVITYKSET

Päivityksillä korjataan tunnettuja tietoturva-aukkoja, ja ilman päivityksiä ulkoiset toimijat voivat helpommin murtautua palveluihin.

TIETOJEN KALASTELU

Tunnuksia tai muuta sensitiivistä tietoa voidaan kalastella sähköpostin tai puhelimen välityksellä – esimerkiksi viralliselta näyttävä sähköposti voi ohjata aidolta näyttävälle mutta hakkerin omistamalle sisäänkirjautumissivustolle, joka vuotaa salasanan hakkerin tietoon.

TIETOMURROT

Ulkopuoliset hyökkääjät voivat tunkeutua yrityksen järjestelmiin ja aiheuttaa haittaa tietoja varastamalla tai aiheuttamalla haittaa tietojärjestelmän toiminnalle. Myös tietojen vuotamisella voidaan uhkailla.

SOSIAALINEN MANIPULOINTI

Yksi hyökkääjälle helpoimpia tapoja murtautua tieto-järjestelmään on soittaa puhelimella ja kysyä sen käyttäjä-tunnusta tai pyytää tietojen muuttamista esimerkiksi työntekijänä tai yhteistyökumppanina esiintyen.

FYYSINEN TURVALLISUUS

Tietoja voi vuotaa tai hävitä varkauden tai luvattoman pääsyn takia.

SISÄISET UHAT

Henkilöstö, kumppanit tai alihankkijat voivat tahallisesti tai tahattomasti aiheuttaa tietoturvaloukkauksia esimerkiksi tietoja tuhoamalla tai vuotamalla.

HAITTAOHJELMAT

Erilaiset haittaohjelmat ovat yksi yleisimpiä kyberturva-riskejä ja altistavat tietojen menetykselle ja kiristykselle. Esimerkiksi lunnasohjelma voi estää pääsyn kaikkiin tietokoneella tai palvelimella oleviin tietoihin, ellei uhri maksa lunnasmaksua haittaohjelman tekijälle.

2.3. Kriittisen tiedon tunnistaminen

Yritykselle kriittisen tiedon tunnistaminen on hyvä aloittaa arvioimalla liiketoiminnan tavoitteet, ja määrittelemällä tälle kriittiset tiedot. Usein nämä tiedot sisältävät esimerkiksi asiakasrekisterit, liiketoimintasuunnitelmat ja taloudelliset tiedot. Mitä tietoja käytetään yrityksen jokapäiväisessä toiminnassa? Ilman mitä tietoja liiketoiminta olisi ongelmissa?

Toinen tapa tunnistaa kriittistä tietoa on miettiä tiedon arvoa liiketoiminnalle. Arvokasta tietoa voi olla esimerkiksi tuotekehitystieto tai -tietämys. Tieto ei välttämättä ole aina digitaalisessa muodossa, ja myös osaamisen säilyttäminen yrityksen jatkuvuuden varmistamiseksi voi olla osa kriittisen tiedon listausta.

Tietoja voi tunnistaa myös miettimällä tietovirtoja, eli miten tieto yrityksessä syntyy, miten se liikkuu ja miten sitä käsitellään: asiakas soittaa tilauksen puhelimella, se kirjoitetaan ylös työlistaan, toteutuksesta tehdään asiakkaalle kuitti ja itselle raportti. Usein tietovirrat kulkevat jonkin tietojärjestelmän kautta, ja tiedon liikkumista miettiessä on helppo tunnistaa erilaiset järjestelmät, jotka vaativat suojausta.

Ei myöskään tule unohtaa yksilöitä koskevan tiedon kriittisyyttä. Tallennetut henkilötiedot – riippumatta siitä ovatko ne liiketoiminnan kannalta merkityksellisiä – tulee tunnistaa ja suojata asianmukaisesti. Vastaavaa ajattelutapaa on syytä soveltaa paitsi omiin työntekijöihin, myös asiakkaita ja yhteistyökumppaneita koskevan tiedon kohdalla.

Listaa kaikki yritykselle tärkeät tiedot ja tee suunnitelma niiden turvaamiseksi. Suunnitelman tulisi sisältää ainakin tiedon käsittelyn pelisäännöt (miten sitä luodaan, kuinka kauan säilytetään, kuka siihen saa päästä käsiksi, miten sitä saa muuttaa), tekniset turvatoimenpiteet ja palautumissuunnitelman kriisin varalle, mikäli tiedolle käy jotakin.

2.3.1. Tietosuojalaki ja EU:n tietosuoja-asetus GDPR

Suomessa henkilötietojen käsittelyssä on aina noudatettava tietosuojalainsäädäntöä. Henkilötietoja täytyy käsitellä läpinäkyvästi, luottamuksellisesti ja turvallisesti. Tietoja saa kerätä vain tiettyjä ja laillisia tarkoituksia varten, vain siinä määrin ja niin kauan kuin toiminta sitä vaatii.

GDPR (General Data Protection Regulation) on Euroopan unionin yleinen tietosuoja-asetus, joka säätelee yritysten henkilötietojen käsittelyä ja suojelee kansalaisten yksityisyyttä. Henkilötiedoiksi katsotaan kaikki tiedot, jotka liittyvät tunnistettavissa olevaan henkilöön. Tämä sisältää esimerkiksi nimet, posti- ja sähköpostiosoitteet, puhelinnumerot ja paikannustiedot.

Kansalaisilla on oikeus tietää mitä tietoja organisaatiolla on hänestä, mihin tietoja käytetään, pyytää tietojen korjaamista tai poistamista ja käsittelyn rajoittamista, siirtää tiedot toisaalle ja vaatia että häntä koskevat päätökset tekee ihminen. Yritykset ovat velvollisia toteuttamaan nämä oikeudet ja osoittamaan että noudattavat tietosuoja-asetuksen säännöksiä. Lainsäädäntö vaatii myös aikaisemmin kuvatun riskianalyysin henkilötietojen käsittelystä.

Käytännössä henkilötietoja käsiteltäessä täytyy kirjoittaa seloste siitä, miten tietoja käsitellään. Pienen yrityksen satunnaiseen ja riskittömään käsittelyyn ei ole välttämättä pakko tehdä selostetta, mutta mahdolliset velvoitteet on hyvä tarkistaa esimerkiksi tietosuojavaltuutetun nettisivuilta, joka sisältää selkeät ohjeet asetuksen täyttämiseksi.

Lähtökohtaisesti tietojen käsittely pitää toteuttaa aikaisemmin mainitut oikeudet säilyttäen ja kansalaisia informoiden. Kun tietojen käsittelyn kuvaa kohderyhmille tarkoitettuun selosteeseen ja selittää miten ja miksi tietoa käytetään, ja minne sitä siirretään, ollaan jo aika pitkällä. Lisäksi järjestelmällinen tai laajamittainen arkaluontoisten tietojen keräys vaatii erillisen tietosuojavastaavan nimityksen.

Mikäli tuntuu että tietosuoja-asiat voisivat olla paremmin, eikä asia tunnu selkeytyvän omin voimin, on aiheen ympäriltä tarjolla paljon apua erilaisten kurssien ja konsultointipalvelujen muodossa.

Lisätietoja tietosuojavaltuutetun toimistosta, osoitteesta tietosuoja.fi/gdpr

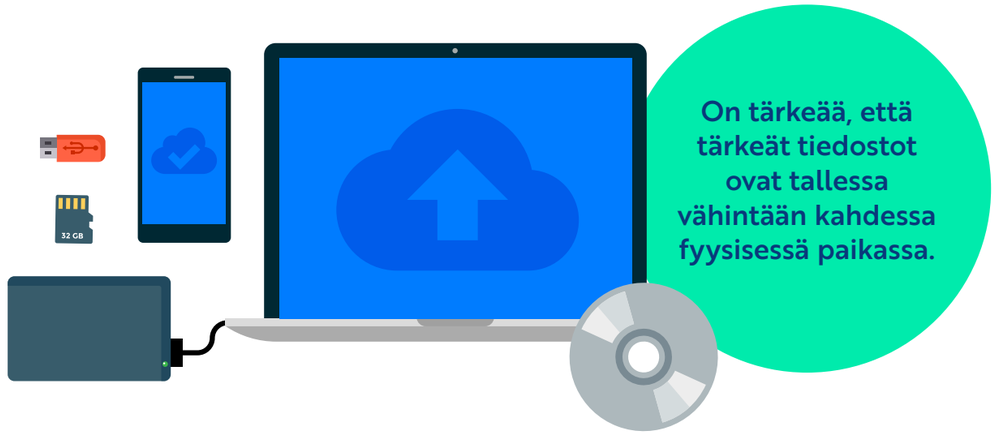
2.4. Pilvipalvelut ja kyberturvan ulkoistaminen

Jo vitsiksi muodostunut lausahdus ”Pilvi on vain jonkun toisen tietokone” on yhä tavallaan totta, joskin pilviratkaisujen tekniikka pitää nykyisin sisällään paljon automatisointia, joka parantaa palvelujen luotettavuutta ja on olemukseltaan erilainen kuin ”tavallinen” tietokone. Se, että palvelu on pilvessä, ei kuitenkaan suoraan tarkoita, että se olisi varmasti tietoturvallinen ja luotettava; joskin suurien toimijoiden kanssa toimittaessa voi usein luottaa perusasioiden olevan kunnossa. On kuitenkin hyvä tiedostaa, että palvelua käyttämällä antaa luottamuksensa palveluntarjoajaan – ja vain niiltä osin kuin palveluntarjoaja lupaa tarjota palveluaan.

Pilvipalvelua ostettaessa palvelun tietoturva on toimittajan vastuulla, ja tämä palvelun toimittamisen ja sen turvallisuudesta vastaamisen yhteen niputtaminen on usein helpompi ja halvempi ratkaisu kuin oman palvelun pystyttäminen. Esimerkiksi sähköpostipalvelimen asennus ja sen toimivuuden ja turvallisuuden takaaminen on massiivinen ponnistus, mutta sähköpostipalvelun ostaminen kuukausihintaan on helppoa. Kumppanin valinnan merkitys korostuu, kun hinnan lisäksi arvioidaan myös toimittajan tietoturvallisuutta ja luotettavuutta.

Monet suuretkin pilvipalveluntarjoajat sanovat käyttöehdoissaan, etteivät vastaa hävinneestä datasta. Tämä tarkoittaa, että tiedon varmennus jää asiakkaan vastuulle. Tietojen tallentaminen pilvipalveluun ei riitä varmuuskopioinniksi. Vaikka useat pilvipalveluntarjoajat ovat rakentaneet palvelunsa luotettavasti, on aina mahdollista, että tietoja häviää järjestelmän tai inhimillisen virheen vuoksi. Pilvipalveluun tallennettujen tiedostojen varmuuskopiot on siis hyvä säilyttää myös omalla koneella tai ulkoisella kovalevyllä.

Yleisten palvelun turvallisuuteen ja tiedon säilyvyyteen liittyvien kysymysten lisäksi kannattaa miettiä mitä riippuvuuksia palvelun käyttöönotto aiheuttaa. Onko palveluntarjoajaa mahdollista muuttaa myöhemmin? Yksinkertaisten verkkosivujen siirtäminen toiselle toimittajalle on mahdollista, mutta vain jos käyttöehdoissa mainitaan, että asiakas omistaa sivuston koodin. Usein siirtyminen eri toimittajien välillä voi olla työlästä ja hankalaa. Toimittajaa valitessa voi kysyä suoraan onko muutos myöhemmin mahdollista.



On tärkeää, että tärkeät tiedostot ovat tallessa vähintään kahdessa fyysisessä paikassa.

2.5. Kyberturva-ymmärryksen kehitys

Klikkaile harkiten, valitse salasanat huolella ja pidä mielessä mahdolliset huijaukset. Suurin osa tietomurroista tapahtuu huijaamalla ihminen klikkaamaan huijauslinkkiä tai liitetiedostoa tai kysymällä tunnuksia näyttelemällä luotettavaa tahoa. Itsensä ja työntekijöiden koulutus on iso osa kyberturvallisuuden ylläpitoa.

Teknisistä ratkaisuista tärkeimpiä ovat varmuuskopiot, päivitykset ja suojausohjelmistot. Monivaiheinen tunnistautuminen estää suurimman osan identiteettivarkauksista, joten se kannattaa ottaa käyttöön etenkin maineen ja liiketoiminnan kannalta kriittisten tunnusten kanssa.

Ymmärryksen lisäys teknisissä asioissa kannattaa aina. Turvallisuus on kaikkien vastuulla, puhutaanpa sitten paloturvallisuudesta tai kyberturvallisuudesta. Henkilöstön koulutus tietoturva-asioihin parantaa koko yrityksen turvallisuutta, ja esimerkiksi pelisäännöt asiakkaiden tunnistamisesta kannattaa sopia siten, ettei kuka tahansa voi soittaa ja kysyä asiakkaan tietoja ilman henkilöllisyyden varmentamista jollain tavalla.

2.5.1. Koulutus, etenkin onboarding ja offboarding

Henkilöstön koulutuksessa on hyvä olla muistilista läpikäytävistä asioista. Onboarding, eli käyttöönottokoulutus pitää sisällään kaiken tarvittavan uuden työntekijän vauhtiin pääsemiseksi, kuten tarvittavien tunnusten avaamisen, puhelinliittymien avaukset ja koulutuksen yrityksen kyberturvasäännöistä.

Samanlainen lista tulee muodostaa myös työntekijän lähtöä varten: offboarding pitää sisällään kaikkien käytössä avattujen tunnusten, palvelujen ja avainten sulkemisen.

Tämä varmistaa että työntekijän lähtö ei jätä hallitsemattomia tunnuksia käyttöön. Käynnissä olevat projektit ja hiljainen tieto pyritään mahdollisuuksien mukaan siirtämään eteenpäin.

Työntekijän perehdytyksessä kannattaa pitää mielessä ainakin seuraavat kyberturvaan liittyvät asiat

- Hyvän salasanan periaatteet.
- Miten tulkita osoiteriviä ja tunnistaa luotettavat linkit.
- Koulutus kalasteluviesteihin ja siihen missä tilanteissa ja miten yhteyshenkilöt täytyy tunnistaa.
- Miten kyberturvallisuuteen liittyvissä kriisitilanteissa toimitaan.
- Sensitiivisen ja yritystoiminnalle kriittisen tiedon käsittelyn periaatteet.
- Ulkoisten muistitikkujen ja kovalevyjen käyttösäännöt.

2.6. Kyberturva etätöissä

Etätyöskentely on tullut entistä yleisemmäksi työelämässä, mikä asettaa uusia haasteita kyberturvallisuudelle. Käytettyjen työskentelylaitteiden tulee olla turvattu, vaikka ne eivät olisikaan pääasiallisia työkoneita. Yrityksen kannalta on usein kannattavaa tarjota antivirus- ja muu suojaus myös kotikoneisiin, jos niiltä on tarkoitus käyttää yrityksen järjestelmiä. Kaikkien yrityksen järjestelmiä käytettävien laitteiden tulisi sisältää ajanmukaiset tietoturvapäivitykset käyttöjärjestelmiin sekä samat suojausohjelmat kuin pääasiallisilla työkoneilla.

Videoneuvotteluratkaisu kannattaa valita käyttötarve ja turvallisuus huomioiden. Turvallisimmillaan yrityksen käyttöön asennetaan oma tekninen ratkaisu, jolloin tiedot eivät kulje minkään palveluntarjoajan järjestelmien läpi. Tämä on kuitenkin kallista ja usein yleisimpiä ratkaisuja hankalampaa, joten jonkin luotettavan toimittajan järjestelmän käyttö on usein perusteltua, kunhan tiedostetaan että keskustelut eivät voi sisältää valtionsalaisuuksia. Moni videoneuvottelujärjestelmä sisältää salauksen tiedonsiirron päästä päähän (end-to-end encryption), jolloin keskustelut ovat paremmin turvassa. Joihinkin videopuheluihin voi myös päästä osallistumaan ilman salasanaa, mikä tulee huomioida. Etenkin suurelle yleisölle jaetut videoneuvottelulinkit voivat kutsua paikalle häiriköitä, joiden varalta on hyvä osata potkia häirikkö ulos ja lukita neuvotteluhuone. Myös yksityisyyteen liittyvät asetukset kuten tallennusmahdollisuudet on hyvä huomioida.

Toinen keskeinen näkökohta etätyön kyberturvassa on turvalliset tietoliikenneyhteydet, mikä useimmiten tarkoittaa turvattua pääsyä yrityksen VPN:ään. VPN luo suojatun yhteyden kotikoneen ja yrityksen verkon välille, mahdollistaen turvallisen tiedonsiirron ja pääsyn yritysverkon palvelimiin. VPN on tarpeellinen etenkin, jos päätoimiston järjestelmiä on tarkoitus käyttää etäältä tai yhteyksiä muodostetaan ulkomailta tai turvattomista langattomista verkoista, esimerkiksi kahviloista tai hotelleista.

Tietojen tallennus kotikoneisiin kannattaa miettiä etukäteen. Sopiiko kotikoneisiin tallentaa yrityksen tiedostoja? Asiakkaiden henkilötietoja? Miten tiedot varmistetaan ja varmuuskopioidaan? Tiedon leviämistä kannattaa rajoittaa, mutta usein myönnytyksiä joudutaan tekemään työnteon sujuvuuden nimissä. Tällöinkin tietoturvariskit tulee tiedostaa ja hallita mahdollisimman hyvin. Tiedon käsittelyyn kannattaa luoda selkeät pelisäännöt, jotka käydään yhdessä läpi.

3. Kyberturva-tason arviointi

Tyypillisiä menetelmiä kyberturvan arviointiin ja varmistukseen ovat erilaiset sisäiset ja ulkoiset selvitykset, auditoinnit ja sertifioinnit. Alkuun pääsee kuitenkin helposti. Pk-sektorin yrityksissä kyberturvaan kohdennettavissa olevat resurssit ovat tyypillisesti rajalliset. Tärkeintä varmistaa, että tärkeät osa-alueet on tunnistettu, niiden toimenpiteet vastuutettu, ja kriisien varalle on suunnitelmat.

3.1. Kuinka kyberturvan toteutusta ohjataan

Yrityksen johto voi ohjata kyberturvatoteutusta määrittämällä tietoturvastrategian ja kirjoittamalla sen pohjalta eri osa-alueille toimintaa määrittävät tietoturvapolitiikat. Tietoturvastrategian tulisi olla linjassa yrityksen liiketoimintatavoitteiden kanssa, ja määritellä selkeät tavoitteet tietoturvalle sekä niiden vastuutuksen.

Kirjallisen ohjeistuksen lisäksi johdon tulee varmistaa, että toteutukselle on varattu riittävästi resursseja – tarvetta on usein sekä osaamiselle, työkaluille että työajalle, ja investointeja on tarpeen tehdä strategian mukaisesti.

Suunnitelmat riskien toteutumisen varalle tulevat erityisesti tarpeeseen silloin kun ongelmiin törmätään. Valmis suunnitelma varmistaa, että tilanteeseen osataan reagoida oikein ja ennen kaikkea nopeasti, mikä on kriisitilanteessa ensiarvoisen tärkeää.

Tilanteen seuranta on tärkeää myös normaalitilanteessa. Tulevatko päivitykset asennetuiksi aikataulussa? Onko henkilöstö tietoinen liikkeellä olevista kalasteluyrityksistä? Osataanko käyttäjien henkilöllisyys tarkistaa asianmukaisesti, kun puhelimessa pyydetään vaihtamaan salasanaa? Ilman jonkinlaista seurantaa ja mittaristoa tilannekuvan muodostus on mahdotonta.

3.2. Kyberturvan osa-alueet ja vastuutus

Vaikka kyberturva ulottuu monille työn osa-alueille, kyse on pohjimmiltaan yksinkertaisesta asiasta. Kyberturvan hallinnassa tärkein tehtävä on tunnistaa keskeiset riskit, ja ohjata niiltä suojautumista. Suojautumisen on syytä olla jatkuvaa, sillä teknologia kehittyy ja muuttuu jatkuvasti. Tästä syystä on erityisen tärkeää vastuuttaa suojautumistoimet ja päivittää niitä aika-ajoin.

Kattavan kyberturvallisuuden varmistamiseksi organisaation eri osa-alueet kannattaa käydä läpi osa-alueittain. Organisaation yleinen kyberturvakulttuuri rakennetaan korkealla abstraktiotasolla, mutta konkreettiset toimet kohdistuvat kulloinkin pääasiallisesti yksittäiseen riskikategoriaan. Parhaassa tapauksessa yritys nimeää yhden tai useamman kyberturvasta vastaavan henkilön osa-alueittain ja kohdistaa vähintään osan työajasta yksinomaan turvallisuuden ylläpitoa koskeviin tehtäviin. Ongelmien ennakoinnilla voi jopa säästää työaikaa ja rahaa verrattuna ongelmien ja mainehaittojen selvittämiseen niiden toteuduttua.

Pk-yrityksissä todellisuus on kuitenkin usein se, ettei henkilöresursseja ole mahdollista kohdistaa yksinomaan kyberturvaan. Näin ollen tyypillinen tilanne on, että teknisesti osaava henkilö hoitaa kyberturvaa oman työnsä ohessa. Rajallinen turvallisuuden ylläpitoon kohdistettu työaika kuitenkin riittää useissa tapauksissa.

Vastuutusta tukee vastuualueiden selkeä määrittely ja dokumentointi. Jo yksinkertaisen kyberturvatoimien lokitiedoston kirjoittaminen kutakin vastuualuetta koskien mahdollistaa kyberturvan ajantasaisuuden seurannan. Siten vältetään myös henkilöstön vaihtuvuuden ja hiljaisen tiedon yhdistelmän tuottamat haasteet, joissa henkilöiden vaihtuessa olennaista tietoa katoaa dokumentoinnin puutteesta johtuen.

Tärkeimmät vinkit kyber-turvan hallintaan

1. Käy yrityksen kyberturva läpi osa-alueittain riskien tunnistamiseksi.
2. Vastuuta turvallisuuden ylläpito.
3. Pidä kirjaa toimenpiteistä ja päivitä suunnitelmia tarpeen mukaan.

3.2.1. Henkilöstö

Henkilöstön osaamisen ylläpito on keskeisimpiä kyberturvan osa-alueita, sillä teknisten ratkaisujen hyödyt voivat mitätöityä inhimillisten virheiden seurauksena.

Suositeltavaa on järjestää paitsi uusia työntekijöitä koskeva perehdytys kyberturvaan, myös ylläpitää henkilökohtaista osaamista säännöllisellä koulutuksella. Jo ymmärrys perustason riskeistä, kuten kalasteluviesteistä ja hyvistä salasanojen periaatteista vähentävät potentiaalisia ongelmia merkittävästi. Henkilöstön osaamista voidaan seurata myös sisäisellä (tarvittaessa ulkoisen toimittajan tuottamalla) osaamisen testauksella. Käytännössä työntekijöille voidaan järjestää sähköisiä kokeita, joiden avulla kyetään selvittämään tarkemmin, mihin osa-alueisiin nämä tarvitsevat täydentävää koulutusta. Koulutuksen ei tarvitse olla muodollista tai raskasta – pienessä yrityksessä voi riittää, että ajankohtaisia asioita nostetaan tapetille aika-ajoin (esim. näittekö että taas tuli kalasteluviestejä – en klikannut linkkejä), ja yhteisiä suunnitelmia päivitetään esimerkiksi joka kevät.

Hallinnollisesta näkökulmasta on suositeltavaa, että yrityksessä käytetään mahdollisuuksien mukaan ainoastaan henkilökohtaisia käyttäjätunnuksia ja pidetään huolta niiden elinkaaren hallinnasta myös työntekijöiden vaihtuessa. Niin ikään salassapitosopimusten (NDA) soveltaminen on järkevää ulkopuolisten tahojen aiheuttamien tietovuotojen ehkäisemisessä.

3.2.2. Laitteisto ja verkot

Laitteiston osalta on suositeltavaa pitää yllä laiterekisteriä, johon yritys kirjaa kaikki käytössä olevat tekniset työvälineet ja verkkolaitteet. Siten kyberturvasta vastaavat tahot pysyvät ajan tasalla paitsi itse laitteista, myös mm. käyttäjätilien ja laitepäivitysten ajantasaisuudesta. Rekisterin luominen on käytännön tasolla yksinkertainen prosessi; yksinkertainen taulukko laitteistosta, niiden ominaisuuksista, omistajuuksista ja päivitystilanteesta kohentaa huomattavasti kykyä laitteiston seurantaan.

Laitteistoon kohdistuu paljon erilaisia kyberturvariskejä. Laitevarkaus voi sekä haitata työn edistymistä että vuotaa arkaluontoista tietoa. Varmuuskopiointi ja suunnitelma laiterikosta palautumiseksi auttaa palautumaan yllätyksistä ilman että tietoa häviää. Kovalevyjen salaus (kryptaus) voi suojata tietojen vuotamiselta varkaustilanteessa. Kryptauksen toteuttaminen on useimpien käyttöjärjestelmien kohdalla helppoa toteuttaa, ja hyödyt mm. varkaustilanteissa ovat merkittävät. Kryptaamattomalla kovalevyllä säilytetyt dokumentit on verrattain helppoa kerätä erilaisten sovellusten avulla, mutta kryptauksen myötä se on käytännössä mahdotonta.

Verkkoasetusten kunnostaminen kannattaa tehdä ammattilaisen toimesta niiden pystyttämisen yhteydessä. Riskianalyysissä kannattaa arvioida voiko kaikkiin verkkoa käyttäviin laitteisiin luottaa, ja miettiä pitäisikö osa laitteista olla erillisessä verkossa. Nykylaitteistoilla verkon segmentointi, eli useamman rinnakkaisen verkon pystytys, on erittäin helppoa ja estää esimerkiksi hyökkäykset yrityksen tiedostopalvelimelle samassa verkossa olevan heikon tietoturvan älyjääkaapin kautta. Verkkoasetuksia ei tarvitse ensimmäisen asennuksen jälkeen säätää kovin usein, mutta laitteiden tietoturvapäivityksistä kannattaa pitää huolta, esimerkiksi vaikka vuosikellossa. Jos päivitykset tilaa IT-ammattilaiselta, voi hän samalla katsoa onko asetuksiakin syytä päivittää.

3.2.3. Ohjelmistot

Yksinkertaisia ohjelmiston kyberturvaa tehostavia käytäntöjä ovat virustorjuntasovellusten ja palomuurien käyttö. Tilanteen hallittua ylläpitoa ajatellen on laitteiston tavoin järkevää hyödyntää rekisteriä käytetyistä ohjelmistoista. Ohjelmistorekisteri yksinkertaistaa sekä työasemille asennettujen ohjelmistojen että palvelinsovellusten päivitystilanteen seurantaa, joskin suurin osa työasemien perusohjelmistoista päivittyy automaattisesti.

Yritysten on hyvä määritellä myös ohjelmistojen asennusta koskevat säännöt ja käytännöt. Perussääntönä on suositeltavaa, että koneille asennettavien sovellusten määrä pidetään minimissä. Erityistä varovaisuutta tulee noudattaa muiden kuin yleisesti tunnettujen ohjelmistotuottajien tarjoamien sovellusten kohdalla. Jokainen lisäsovellus kasvattaa mahdollisten tietoturva-aukkojen määrää, ja riski korostuu entisestään, mikäli ohjelmistopäivitysten ajantasaisuudesta ei ole huolehdittu (ks. ohjelmistorekisteri).

3.2.4. Tiedonsiirto

Tietoliikenneyhteydet, mukaan lukien sähköpostiliikenne ja verkkosivut, on tärkeää suojata ulkoisilta tunkeutujilta. Turvallisuuden takaamiseksi on suositeltavaa hyödyntää lähtökohtaisesti tunnettuja tai muutoin luotettaviksi osoittautuneita palveluntarjoajia, joiden kyberturvakäytännöt ovat ajan tasalla.

Fyysisten tiedonsiirtovälineiden, kuten ulkoisten kovalevyjen, usb-muistien ja tulosteiden kohdalla suositellaan määrittämään selkeät yrityksen sisäiset käytännöt ja pelisäännöt, koskien käytön luvallisuutta, suojaus- ja salausmenetelmiä sekä hävityskäytäntöjä. Ulkoiset usb-muistitikut voivat levittää haittaohjelmia, ja pienikokoiset laitteet voivat myös helposti hukkua ja vuotaa tietoja.

3.2.5. Ulkoiset toimijat

Pelkkä sisäisten käytäntöjen turvallisuus ei takaa kattavaa kyberturvaa verkottuneessa liiketoimintaympäristössä, jossa tietoa välitetään asiakkaiden, kumppanien tai alihankkijoiden kanssa. Näin ollen yrityksen on syytä selvittää, ovatko ulkoisten toimijoiden kyberturvakäytännöt ajan tasalla ja riittävän kattavia.

Ulkoisten toimijoiden kyberturvatason rooli kasvaa silloin, kun käytössä on jaettuja järjestelmiä. Moni yritys tarjoaa kumppaneilleen ja asiakkailleen kirjautumista edellyttäviä portaaleja, joiden takana sijaitsee salattua tietoa. Mikäli ulkoisen toimijan turvallisuustilanne on heikko, ovat nämä tiedot haavoittuvassa asemassa. On suositeltavaa, että kumppanien kanssa jaetun informaation laajuus pidetään mahdollisimman suppeana; määrittele ennakkoon, mikä tieto on yhteistyön kannalta välttämätöntä. Kaikkien kumppanien ei tarvitse päästä käsiksi kaikkeen tietoon.

3.2.6. Fyysinen turvallisuus

Myös fyysinen turvallisuus on olennainen osa yrityksen kyberturvaa. Laitteisto- ja materiaalivarkauksien ehkäisemiseksi on kannattavaa hyödyntää paitsi riittäviä lukituskäytäntöjä, myös kulunvalvontaa. Vastaavasti tulee huomioida, että kukin verkkoon kytketty laite voi itsessään muodostaa turvallisuusuhan; mm. kameravalvontaa hyödynnettäessä tulee palveluntarjoajan kanssa selvittää, minkälainen suojaus laitteisiin on saatavilla ulkopuolisten tunkeutujien estämiseksi.

Tärkeää on varautua myös tilanteisiin, joissa laitteistoa on jo onnistuttu varastamaan. Tällöin kriittiseen rooliin nousevat mm. edellä mainitut salasanakäytännöt, huolehtiminen kovalevyjen kryptauksesta sekä tulosteiden minimoinnista tai niiden asianmukaisesta säilytyksestä. Markkinoilla on yleistyvästi tarjolla myös teknisiin välineisiin kiinnitettäviä seurantalaitteita, jotka varkauden sattuessa voivat auttaa varastetun omaisuuden paikantamisessa. Lähtökohtaisesti turvaratkaisut on kuitenkin suositeltavaa määrittää sillä oletuksella, ettei menetettyä laitteistoa saada takaisin.

3.3. Kyberturvan hallinnan tasot

Kyberturvatason arvioinnin tueksi on olemassa erilaisia mittaristoja. Tässä opaskirjassa esitellään viisiportainen arviointimalli, jonka avulla yritykset voivat arvioida turvatasonsa kyberturvan eri osa-alueilla. Malli pohjautuu NIST (National Institute of Standards and Technology) kyberturva-aihioon, joka on kokonaisuudessaan luettavissa osoitteessa www.nist.gov/cyberframework.

"Ei meillä tässä suuria riskejä ole. Jotain on tehty."

3.3.1. Taso 1: Vajavainen

Vajavainen hallintataso saattaa olla riittävä, jos liiketoiminnan riskit ovat erittäin pieniä, kyberturvalle ei ole ulkoisia vaatimuksia eikä yrityksellä oleva tieto vääriin käsiin ajautuessaan voi aiheuttaa yritykselle tai asiakkaille kriittisiä ongelmia. Turvatoimien tarpeettomuudesta on kuitenkin miltei mahdotonta olla varma, ellei tee riskianalyysiä.

Vajavaisesti hallitussa tilanteessa kyberturvaa voi hoitaa joku työnsä ohessa ja rajallisin aikaresurssein, tai kyberturvatehtäviä ei ole erityisesti osoitettu kenellekään.

Yhdistettynä puuttuvaan tai hyvin rajalliseen sisäiseen kyberturvaosaamiseen puhutaan vajavaisesta hallintatasosta.

Vaarana tässä tilanteessa on luonnollisesti se, että olennaisia riskejä on jäänyt huomaamatta, ja jotakin ikävää pääsee käymään. Vastuu kyberturvasta on viime kädessä toimitusjohtajalla.

Siirtyminen seuraavalle tasolle: systemaattinen riskianalyysi ja tietoturvakartoitus.

"Olemme selvittäneet riskit ja tehneet oleelliset."

3.3.2. Taso 2: Suoritettu

Nimi viittaa siihen, että ainakin kerran on suoritettu systemaattinen tietoturvakartoitus ja tehty sen osoittamat toimenpiteet. Tällöin on tunnistettu puutteet ja otettu käyttöön tavanomaiset suojauskäytännöt. Vastuu on selkeytetty mutta asiaan ei välttämättä vielä kohdistettu investointeja tai jatkuvia prosesseja, ja tietoturvan jatkuva ylläpito on haasteellista.

Suoritettu-tasoa voidaan pitää kyberturvan vähimmäisvaatimuksena silloin, kun yritys käsittelee missään määrin arkaluontoista dataa, jonka leviäminen tai kadottaminen voi johtaa liiketoiminnallisiin tai henkilökohtaisiin riskeihin.

Tällä tasolla yleisimmät riskit on yleensä tunnistettu ennalta, mutta järjestelmällisyyden puutteesta johtuen turva ei ole täysin vakaa. Toiminta on vielä tässä vaiheessa paikoin reaktiivista, eli kyberturvaongelmiin vastataan vasta niiden tapahduttua. Vaikka yritys pystyisi tietoturvakartoituksen avulla tunnistamaan sen hetkiset yleiset riskit, on kyberturva jatkuvasti kehittyvä aihealue, ja ilman jatkuvaa osaamisen ja tietoisuuden kehittämistä jäävät uusiutuvat riskit mahdollisesti huomioimatta.

Henkilöstön osaamista tuetaan tällä tasolla tiedotusluonteisesti, mutta osaamista ei välttämättä testata. Tyypillisesti kyberturvaosaamisen ylläpito tapahtuu sisäisin voimavaroin, eikä ulkoisia palveluntarjoajia hyödynnetä laajalti.

Siirtyminen seuraavalle tasolle:
käytäntöjen huolellinen dokumentointi ja toimintatapojen jalkauttaminen organisaation laajuisesti.

”Ollaan varauduttu ja prosessit kunnossa; erityisesti niihin, jotka on meille kriittisiä.”

3.3.3. Taso 3: Hallittu

Vastuu – selvitysten luonne – aikajänne – ohjaustapa – osto vs. itse tekeminen

Hallitulla tasolla kyberturvasta vastaa selkeästi määritetty tai määritetyt henkilöt joko oman työnsä ohessa tai nimenomaisesti kyberturvaan keskittyvässä roolissa. Kyberturvaan liittyvät tehtävät ja prosessit on dokumentoitu, ja niiden tekeminen uudestaan onnistuu helposti. Työntekijöiden osallisuus kyberturvaan on passiivinen, tarkoittaen sitä, että vastuu osaamisen ylläpidosta ja tiedonjaosta keskittyy vastuutetuille henkilöille. Työntekijöiden osaamista saatetaan kartoittaa ajoittaisesti, mutta osaamisen järjestelmällistä testausta ei toteuteta.

Siirtyminen seuraavalle tasolle:
toimintatapojen kehittäminen sekä riskien ja osaamisen jatkuva seuranta.

”Osa-alueiden turvallisuutta mitataan ja arvioidaan aina kun tehdään päätöksiä.”

3.3.4. Taso 4: Mitattu

Mitattu taso kuvaa tilannetta, jossa kyberturvaa ylläpidetään ja seurataan systemaattisesti ja ennakoivasti. Toimintatavat on dokumentoitu huolellisesti ja niiden noudattamista monitoroidaan. Työntekijöille tarjotaan kyberturvakoulutusta ja näiden osaamista ylläpidetään ja seurataan jatkuvasti sisäisten tai ulkoisten auditointien avulla.

Vastuu kyberturvasta on kohdistettu ja määritelty selkeästi ja dokumentoidusti. Kyberturvasta vastaava henkilö tai henkilöt kommunikoivat aktiivisesti koko henkilöstön kanssa, ja ennalta tunnistetuista riskeistä informoidaan viiveettä. Dokumentaatiota ylläpidetään jatkuvasti uusien riskien havaitsemisen myötä.

Sisäinen kyvykkyys ja siihen kohdistuvat rajoitteet on tunnistettu ennalta, ja ulkoisia palveluntarjoajia hyödynnetään paikkaamaan osaamista tarpeellisilta osin.

Siirtyminen seuraavalle tasolle:
prosessien optimointi ja ennakoivan kyberturvan jalkauttaminen osaksi koko organisaation kulttuuria.

"Tietoturva on olennainen ja jatkuvasti kehittyvä osa liiketoiminnan johtamista."

3.3.5. Taso 5: Optimoitu

Optimoidussa tilanteessa kyberturva on kauttaaltaan jalkautettu keskeiseksi osaksi organisaation kulttuuria, kattaen paitsi operatiivisen toiminnan, myös johtamisen toimintatavat. Vastuu koskee koko organisaatiota: kyberturvasta ja yksittäisistä turvatehtävistä vastaa yksi tai useampi henkilö, mutta laajemmassa kuvassa kukin työntekijä on velvollinen paitsi täyttämään organisaation asettamat vaatimukset, ylläpitämään osaamistaan.

Kyberturvatietoisuutta pidetään yllä jatkuvasti ja järjestelmällisesti, ja koko henkilöstön osaamista seurataan säännöllisin väliajoin. Auditoinnit on toteutettu luotettavien ulkoisten organisaatioiden toimesta, yrityksen kyberturvan tilannekuvaa päivitetään jatkuvasti ja toimintatapoja päivitetään mahdollisiin tuleviin uhkiin reagoiden. Riskien ennakointi on korkealla tasolla ja käytäntöjen dokumentointi on jatkuva prosessi.

Kyberturvahallinnan tasot

Turvatason mittari	Taso 1: Vajavainen	Taso 2: Suoritettu	Taso 3: Hallittu	Taso 4: Mitattu	Taso 5: Optimoitu
Suhtautuminen tietoturvaan/ motto	Ei meillä tässä suuria riskejä ole. Jotain on tehty.	Olemme selvittäneet riskit ja tehneet oleelliset.	Ollaan varauduttu ja prosessit kunnossa; erityisesti niihin, jotka on meille kriittisiä.	Osa-alueiden turvallisuutta mitataan ja arvioidaan aina kun tehdään päätöksiä.	Tietoturva on olennainen ja jatkuvasti kehittyvä osa liiketoiminnan johtamista.
Vastuu tietoturvasta	Vastuuta ei ole määritetty.	Tietoturvaa hoidetaan, mutta vastuu määritetty epämuodollisesti (tietoturvasta saattaa vastata esim. henkilö oman työn ohessa).	Vastuu määritetty tietylle/tietyille resursseille.	Vastuu määritetty, jonka lisäksi johto mukana vastuussa. Mahdollisesti myös ulkopuolisia palveluja käytössä.	Kaikki henkilöstön tasot ylimmästä johdosta toteuttajiin on sitoutettu kyberturvan ylläpitoon ja kehitykseen.
Tietoturvan painotus	Koetun tarpeen mukaan. Varautumisessa voi olla myös aukkoja.	Varautuminen ennakoivaa, muttei systemaattista.	Perustason varautuminen kaikilla tietoturvan osa-alueilla ja kriittisiin liiketoiminnan riskeihin erityisvarautuminen.	Jatkuva riskien seuranta ja arviointi sekä varautumiskyvyn ylläpito.	Best practicet käytössä laaja-alaisesti, sis. systemaattinen riskeihin varautuminen, jatkuva kehitys ja ennakoiva mukautuminen.
Toimenpide seuraavalle tasolle pääsemiseksi	Systemaattinen riskianalyysi ja tietoturvakartoitus.	Käytäntöjen huolellinen dokumentointi ja toimintatapojen jalkauttaminen organisaation laajuisesti.	Toimintatapojen kehittäminen sekä riskien ja osaamisen jatkuva seuranta.	Prosessien optimointi ja ennakoivan kyberturvan jalkauttaminen osaksi koko organisaation kulttuuria.	

3.4. Kyberturvatason arviointi

Kaikkien yritysten ei ole välttämätöntä edetä korkeimmille tasoille, joilla myös liiketoiminnan johdon ja asiantuntijoiden aikaa päätöksentekoon alkaa kulua enemmän. Varautumisen taso tulee sovittaa tunnistettuihin riskeihin.

Olennaisinta on, että yritys kykenee seuraamaan kyberturvansa tilaa omalle toiminnalleen riittävällä tasolla, kriittisimmät sudenkuopan välttäen. Sopivan hallintatason valinta viime kädessä yrityksen oman päätöksenteon varassa.

Avainasia on selvittää kriittisimmät riskit omalla kohdalla, ja varautua niihin. Mikäli datan menettäminen tai leviäminen ei vaarantaisi liiketoimintaa tai yksilöitä, ei kyberturvaan ole välttämätöntä kohdentaa laajamittaisia panostuksia. Vastaavasti kriittistä tai arkaluontoista tietoa käsitellessä panostus kyberturvallisuuteen on lähes välttämätöntä.

3.5. Sertifioinnit

Erilaiset sertifioinnit ovat hyödyllisiä, erityisesti mikäli yritys käsittelee sensitiivistä tietoa tai toimii turvallisuusalalla. Usein sertifioinnin tarve nousee kuitenkin ajankohtaiseksi vasta, kun asiakkaat kysyvät niiden perään. Perusasiat voi laittaa kuntoon myös ilman ulkopuolista sertifiointia. Tässä muutama tunnetuimmista:

ISO 27001 on kansainvälinen standardi, johon sisältyy laaja joukko vaatimuksia ja suosituksia, jotka koskevat organisaation tietoturvallisuuden hallintaa. NIST CSF, eli National Institute of Standards and Technologyn kehittämä tietoturvakehikon arviointimalli (Cybersecurity Framework Assessment), pitää sisällään joukon käytäntöjä ja menetelmiä tietoturvallisuuden kehittämiseen ja ylläpitoon.

CIS Controls (Center for Internet Security Controls) tarjoaa konkreettisia suosituksia ja ohjeita tietoturvatoimenpiteiden toteuttamiseen. Cloud Security Alliancen kehittämä Cloud Controls Matrix (CSA CCM) auttaa organisaatiota arvioimaan pilvipalvelujen tietoturvaominaisuuksia niitä hankittaessa ja käytettäessä.

Mainituista sertifioinneista löytyy helposti lisätietoa internetistä ja niiden hankkimiseen voi ostaa apua kotimaisilta konsulteilta.

4. Kyberturva-toiminta kriisi-tilanteissa

Kriisit pääsevät usein yllättämään, ja niihin tulee pystyä vastaamaan nopeasti. Parhaimmassa tapauksessa kriittiset pisteet on tunnistettu etukäteen, ja stressaavassa kriisitilanteessa voi tukeutua etukäteen tehtyyn suunnitelmaan.

4.1. Havainnointi

Kyberturvapoikkeaman ensimmäinen havainto voi olla IT-järjestelmän lamauttava massiivinen tietokato tai vähemmän dramaattinen outo rivi palvelun käyttötilastoja selatessa. Kriisin voi välttää tai ainakin hallita paremmin, mikäli kriittiset järjestelmät on suojattu ja riskeihin varauduttu etukäteen. Aina pahinta ei voi välttää, ja tietoturvapoikkeamaan täytyy joka tapauksessa reagoida aina.

Tietomurrot havaitaan parhaiten palvelinten lokitiedostoista. Mikäli lokitiedot on kerätty asianmukaisesti, niihin jää tietomurrosta jälkiä, jotka on mahdollista tunnistaa. Hyökkäys voidaan myös havaita myöhemmin, kun jokin järjestelmä lakkaa toimimasta, hyökkääjä lähettää yritykselle kiristyskirjeen tai järjestelmä tekee jotakin outoa, jota kukaan työntekijä ei usko tehneensä.

Vuotaneet tunnukset huomataan usein vasta kun tunnuksia käytetään epäilyttävään toimintaan. Yritys voi saada ilmoituksen tästä asiakkaalta, yhteistyökumppanilta, sosiaalisesta mediasta tai kenties omalta some-tililtä huomataan lähtevän erikoisia viestejä.

Palvelunestohyökkäys tapahtuu kuormittamalla palvelua sen kantokyvyn yli, mikä näkyy palvelun ajoittaisena tai täydellisenä toimimattomuutena. Yleisesti tietoliikennehäiriöiden vastuu on IT-palveluntarjoajalla, joten palvelun korjaamisessa tarvitaan tiivistä yhteistyötä teknisen osaajan kanssa.

4.2. Reagointi, arviointi ja ilmoitukset

Mikäli kyberturvapoikkema liittyy vain johonkin tiettyyn laitteeseen, saastunut laite kannattaa eristää välittömästi. Vaarantuneiden tunnusten salasanat tulee myös vaihtaa nopeasti. Laitteita ei kuitenkaan välttämättä kannata sammuttaa hätäpäissään, jos niiden toiminta voidaan estää muilla tavoin, sillä tämä voi hävittää tärkeää hyökkäyksen selvittämiseen liittyvää tietoa. Lentotila tai verkkokaapelin irrottaminen voi olla paras tapa eristää saastunut laite, ellei se ole keskeinen. Ota yhteys IT-asiantuntijaasi tai IT-palveluntarjoajaan asian hoitamiseksi, jos tarvitset ulkoista apua.

Arvioi seuraavaksi mitä on tapahtunut. Selvitä mitä yhteyksiä poikkeamalla on muihin järjestelmiin: pääseekö altistuneilla tunnuksilla muualle ja onko tietoja käytetty kalasteluyrityksiin. Listaa vaarantuneet tunnukset. Haastattele tunnusten käyttäjiä syyllistämättä, selvittääksesi miten poikkeama on tapahtunut. Käyttäjillä ei välttämättä ole osuutta poikkeaman aiheutumiseen, mutta heiltä voi saada tärkeää lisätietoa siitä miten poikkeama on päässyt tapahtumaan. Arvioinnin edetessä saattaa selvitä, että yhden järjestelmän poikkeama osoittaa muidenkin järjestelmien altistuneen. Nämäkin järjestelmät tulee eristää ja tutkia. Mikäli kyse on vakavasta poikkeamasta, tallenna kaikki selvinnyt tieto, kuten tekniset lokitiedostot, verkosta eristetylle kovalevylle myöhempää tarkempaa tutkimusta varten.

Ilmoita poikkeamasta tarpeellisille tahoille. Onko henkilötietoja vaarantunut? Jos on, tee ilmoitus tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle osoitteessa **tietosuoja.fi** 72 tunnin kuluessa. Vaikuttaako poikkeama asiakkaiden, palveluntarjoajien tai yhteistyökumppanien toimintaan? Ilmoita asiasta ja selvitystyön edistymisestä heille. Muut toimijat voivat suojata omia järjestelmiään mitätöimällä mahdollisesti väärinkäytettävät tunnukset, avaimet tai varmenteet. Mikäli epäilet että on tapahtunut rikos, tee poliisille sähköinen rikosilmoitus.

Epävarmassa tilanteessa poliisille voi silti vinkata asiasta nettivinkki-palvelussa osoitteessa **poliisi.fi/nettivinkki**

On suositeltavaa tehdä poikkeamasta ilmoitus kyberturvallisuuskeskukselle (**kyberturvallisuuskeskus.fi** tai **cert@traficom.fi**), joka kerää luottamuksellisesti tietoa erilaisista hyökkäyksistä ja voi konsultoida ilmaiseksi vahinkojen rajaamiseksi ja tilanteen korjaamiseksi. Tiedottaminen myös auttaa suojelemaan muita samanlaisilta hyökkäyksiltä ja auttaa kansallisen tilannekuvan luomisessa.

Ilmoituksen tietoturvaloukkauksesta voi tehdä useaan paikkaan: tietosuoja.fi/tietoturvaloukkaukset sekä kyberturvallisuuskeskus.fi

4.3. Palautuminen

Palautuminen kannattaa aina aloittaa kriittisimmistä järjestelmistä. Liiketoiminta voidaan parhaassa tapauksessa palauttaa osittain nopeasti laajempien palautumis- ja selvitystöiden jatkuessa.

Tietomurron tai kryptaushyökkäyksen kohdalla palauta saastuneet järjestelmät ja hävinneet tiedot varmuuskopioista. Mikäli järjestelmä puhdistetaan käsin ilman että kaikki saastuneet tiedostot korvataan puhtailla, on aina mahdollista, että järjestelmään pääsee tunkeutumaan uudestaan jonkin avatun aukon kautta. Varmuuskopioiden palautuksen jälkeen on tärkeä asentaa kaikki tietoturvapäivitykset, jotta järjestelmä ei saastu uudestaan samaa kautta. Jos varmuuskopioita ei ole, tulee järjestelmä ja tarvittavat ohjelmat asentaa kokonaan uudestaan. Huomioi myös että saastuneessa järjestelmässä olevia tietoja, kuten asiakastietoja ja tunnuksia, on voitu muuttaa.

Vuotaneiden tunnusten kohdalla kaikki vuotaneet salasanat otetaan takaisin hallintaan ja varmistetaan, että tunnukset ovat turvassa. Salasanat vaihdetaan, sähköpostien kohdalla varmistetaan että outoja uudelleenohjauksia ei ole voimassa, eikä muita vaarantavia asetuksia kuten salausavaimia ole muutettu. Palvelimella olevat tiedostot on parasta palauttaa varmuuskopioista, sillä niihin on voitu lisätä takaovia ja haittaohjelmia.

Palvelunestohyökkäyksistä palautuminen vaatii paljon teknistä ymmärrystä, joten toimi yhdessä verkko-operaattorin tai palveluntarjoajan kanssa. Liikennettä voidaan rajoittaa esimerkiksi kohdemaan perusteella, ja verkkokonfiguraation avulla voidaan tehdä järjestelmästä kyvykkäämpi sietämään rasitusta. Oikeiden toimenpiteiden tunnistaminen vaatii kuitenkin teknistä silmää ja järjestelmän tarkkaa läpikäyntiä, esimerkiksi lokitiedostojen lukemista hyökkäyksen identifioimiseksi, jotta toimenpiteet voidaan kohdistaa estämään hyökkääjät ja päästämään oikeat käyttäjät läpi. Mikäli hyökkäys käyttää jotain tunnettua haavoittuvuutta, voivat tietoturvapäivitykset auttaa tilannetta.

4.4. Jälkiselvitys

Liiketoimintojen normalisoiduttua on tärkeä tehdä asianmukainen jälkiselvitys tulevaisuutta ajatellen. Miten kriisi vältetään tulevaisuudessa? Päivitä kriisinhallintasuunnitelmat ja tee tarvittavat tekniset muutokset.

Omaa suojauksen tehokkuutta kannattaa arvioida niin ennalta varautumisen, hyökkäyksen havaitsemisen kuin hälytykseen reagoinnin onnistumisen valossa. Mitkä tekniset ja toimintaan liittyvät seikat johtivat tilanteeseen? Noudatettiinko tehtyjä suunnitelmia käytännössä? Saatiinko tilanteesta ajantasainen hälytys? Olivatko vastuut selvillä? Miten viestintä onnistui? Onko tapahtumien kulku selvä ja varautuminen jatkossa kunnossa?

Toimi näin, kun huomaat tietoturvapoikkeaman

SOS

1. Tunnista tietoturvapoikkeama (pidä silmät auki).
2. Arvioi ongelman vakavuus.
3. Ilmoita asianosaisille (tietosuojavaltuutettu, kyberturvallisuuskeskus, poliisi, asiakkaat).
4. Tutki mitä on tapahtunut.
5. Palaudu, korjaa tilanne.
6. Tee jälkiselvitys ja jatkosuunnitelmat.

Tarkempaa ohjeistusta ja lisätietoa mm. tietomurtoihin, käyttäjätunnusten vuotamiseen, kiristyshaittaohjelmiin sekä palvelunestohyökkäyksiin tai toimitusketjuhyökkäyksiin varautumiseen ja niistä palautumiseen löytyy kyberturvakeskuksen sivustolta: kyberturvallisuuskeskus.fi hakusanalla toimintaohje.

5. Kyberturvan hallinta liiketoiminnan kasvaessa ja digitalisoituessa

Tämä luku on tarkoitettu erityisesti kasvaville yrityksille ja firmoille, joiden liiketoiminnassa digitalisaatio on keskeinen tekijä. Yhteistä tällaisille yrityksille on kasvava tarve erityisesti korkean osaamiseen ja tietoon, sekä niiden systemaattiseen hallintaan. Tietoturva on näissä tapauksissa tarpeen liittää osaksi yrityksen strategiaa.

5.1. Tietoturva strategiana – ei erillisenä teknisenä toimenpiteenä

Strategisen tietoturvan tulee tukea perustellusti yrityksen liiketoimintamallia. Perinteisen tietoturvan lisäksi tämä sisältää kysymykset esimerkiksi tiedon jakamisesta ja liiketoimintakriittisyydestä sekä ihmisten toimintaan liittyvät kysymykset, kuten tietosuojan, henkilökunnan sitouttamisen ja hyvinvoinnin koko liiketoimintaverkosto huomioiden.

Tietoturva nähdään usein teknisinä ja taktisina toimenpiteinä, joiden tarkoituksena on organisaatioon liittyvien tietojen, järjestelmien ja toimintojen suojaaminen.

Kyberturvallisuuden huomiointi tällä tavoin on edellytys ja jopa itsestäänselvyys, jotta yritys voi toimia nykyisen kaltaisessa digitalisoituneessa ympäristössä. Tämä näkökulma on kuitenkin rajoittunut ja sen rinnalle tarvitaan myös strategisen tason ymmärrys, jos halutaan luoda tietoturvasta kilpailuetu ja kehittää yritystä vastaamaan digitalisaation haasteet kestävästi. Strategisessa tietoturvallisuudessa keskiössä ei ole vain yrityksen suojaaminen. Strategisessa tietoturvallisuudessa keskitytään strategisiin mahdollisuuksiin, joita voidaan tuoda liiketoimintaan ja sen kehittämiseen turvallisesti.

Kun tietoturvassa kysymys on miten ja mitä suojataan, strategisessa tietoturvallisuudessa keskiössä on mitä haluamme tehdä ja miten se mahdollistetaan turvallisesti yrityksen toimintaympäristössä sekä huomioidaan yrityksen liiketoimintasuunnitelmassa.

Myös tarkastelun taso on korkeampi. Tietoturva perinteisesti keskittyy yrityksen järjestelmiin ja niiden suojaamiseen, kun taas strateginen tietoturvallisuus tulee nähdä laajempana toimintana, joka ylettyy ekosysteemeihin/verkostoihin joihin yritys kuuluu ja osallistuu.

5.2. Liiketoiminnan tavoitteet nyt ja tulevaisuudessa määrittelevät tietoturvan suuntaa

Tietoturva ei ole irrallinen osa, jota voi käsitellä liiketoimintamallia huomioimatta, vaikka useassa tapauksessa näin käytännössä toimitaan. Yrityksen liiketoimintaidea ja sen toteutus on lopulta se ydinasia, mikä määrittää mitä erilaisia toimia yrityksessä tulee tehdä, myös tietoturvaan liittyen. Liiketoiminnan asettamat reunaehdot ovat erilaisia eri organisaatioissa ja täten ne tulee huomioida tapauskohtaisesti.

On eri asia pohtia pienen luomutilan tietoturvaratkaisuja kuin esimerkiksi verkkokaupparatkaisuja tarjoavan yrityksen kohdalla. Kun ensimmäisellä voi riittää, että sen käytössä olevassa tietokoneessa on ajantasainen ja päivitetty ohjelmisto, toisella taas tulee olla vahva osaaminen ja kyky suojata tarjoamiensa palvelujen turvallisuus. Lisäksi liiketoiminnan tavoitteet eivät ole stabiileja, vaan yrityksillä

on myös tulevaisuuden suunnitelmia niin lyhyelle kuin pitkälle aikavälille. Näiden tavoitteiden huomioiminen tietoturvassa mahdollistaa myös pitkäjänteisempää ja systemaattisempaa tietoturvan toteuttamista ja riskien ennakointia myös liiketoiminnan muuttuessa.

5.3. Tieto, osaaminen ja niiden verkostoituva luonne strategian näkökulmasta

Ensimmäisiä asioita strategisessa tietoturvassa on tarkastella mikä on yrityksen strategia ja minkälaisia resursseja sen toteuttamiseen tarvitaan (katso seuraavan aukeaman kuva). Tieto ja osaaminen ovat nykyisessä yritysmaailmassa keskeinen osa yrityksen resursseja. Ongelmana on kuitenkin se, että yrityksen omaisuus nähdään usein vain fyysisinä omaisuuslajeina. Todellisuudessa patenttien ja muiden immateriaalisten omaisuuksien (ei-rahallinen pääoma) arvon merkitys on monesti suurempi kuin perinteisen pääoman. Ongelmana on että yrityksen kriittisimmän ”omaisuuden” eli tiedon ja osaamisen arvo on vaikeammin määriteltävissä ja siksi usein ohitettu tai huonosti kuvattu. Tämä pääoma kuitenkin on se kriittinen komponentti, joka mahdollistaa arvon luonnin yrityksessä ja sen tarkastelu tulisikin ottaa strategisen tietoturvallisuuden ytimeen. Tiedon merkityksen ja osaamisen kartoitukseen löytyy jo olemassa olevia työkaluja ja menetelmiä (kts. esim. **theodi.org/knowledge-opinion/guides**).

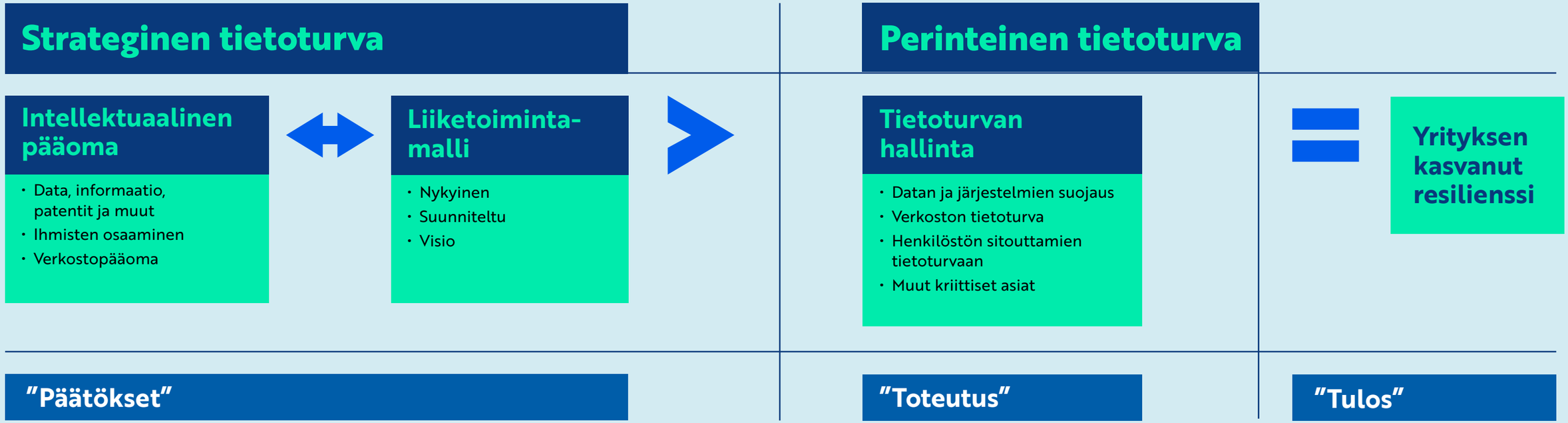
Osaaminen nousee myös keskeiseen osaan erityisesti pienissä ja keskisuurissa yrityksissä, joissa osaaminen voi olla usein yksittäisten ihmisten hallussa. Tästä nouseekin esiin tarve osaamisen jakamiselle ihmisten kesken. Samoin henkilöstön sitouttamiseen ja työntekijöiden hyvinvointiin tulee kiinnittää erityistä huomiota, jotta yrityksen kriittistä osaamista ei menetetä.

Strategisessa kyberturvassa tulisi olla keskiössä erityisesti se, miten tietoa käytettään turvallisesti, ei vain se miten tietoa voidaan suojata tai eristää. Erityisesti dataan perustuvan talouden kasvu ja leviäminen yhä laajemmin eri liiketoiminta-alueille korostaa tarvetta ymmärtää datan merkitystä organisaatiolle ja sen kilpailukyvylle, yrityksen jatkuvuudelle.

Datan arvo kasvaa sitä mukaa kun sitä pystytään lisäämään, rikastamaan ja sitomaan liiketoimintaan. Tämä korostuu verkostoituneessa liiketoiminnassa, jossa yritykset ovat enemmän ja enemmän riippuvaisia esimerkiksi tiedon jakamisesta toimitusketjuissaan. Eli tiedon hyödyntäminen tapahtuu dataekosysteemissä, joka menestyy vain kokonaisuutena, organisaatioiden yhteistyöhön perustuen.

Tietoturvastrategiakaavio

Perinteinen tietoturva ajatellaan yleensä erillisenä toiminnallisen tason asiana, mutta parhaimmillaan se on kiinteä osa yrityksen liiketoimintaa ja pääoman vaalimista.



6. Kyberturvan pelisäännöt

Tämä luku sisältää aakkosellinen listauksen kyberturvan pelisäännöistä, joilla saat perusasiat kuntoon. Tärkeimpinä nostoina kannattaa laittaa kuntoon ainakin päivitykset ja salasanat, ja harkita monivaiheista tunnistautumista tärkeisiin tileihin.

Antivirus

Antivirus on hyvä ja tarpeellinen työkalu työkoneen turvaamiseksi, mutta ei vielä varmista tietoturvaa kokonaisuutena. Nykyisin Windowsin mukana tuleva Defender antaa kotikoneille riittävän suojan haitta-ohjelmia vastaan. Antivirus estää tunnettujen haittaohjelmien ja viruksien ajon koneella, mikä antaa kattavan muttei täydellisen suojan.

Antiviruksen käytön lisäksi on tärkeää olla avaamatta tiedostoja, jotka eivät ole tulleet luotettavista lähteistä (mukaan lukien luotettavilta ihmisiltä tulleita outoja tiedostoja, jotka voivat olla haittaohjelmien lähettämiä).

Fyysinen turvallisuus

Vaikka fyysinen turvallisuus on tarkalleen ottaen osa yleistä tietoturvaa, muutama sana siitä on paikallaan myös kyberturvaoppassa. Fyysinen turvallisuus sisältää paljon muutakin kuin vain lukot ja avaimet. Erilaisiin fyysisen maailman uhkiin voi varautua monella tasolla – esimerkiksi varkauden estoon voivat liittyä (sähkö)lukot, kulunvalvonta, vartiointi ja ohjeistus siitä mitä tavaroita saa ja ei saa jättää toimistolle valvomatta. Lisäksi varkauteen ja siitä palautumiseen voidaan varautua mm. salauksella (varkaus ei anna pääsyä tietoihin) ja varmuuskopiolla (varkaus ei johda työn menetykseen).

Kuten kyberturvassa yleisesti, fyysisessä turvassakin tärkein näkökulma on riskien pienentäminen: älä jätä sensitiivisiä papereita tai IT-laitteita sinne tänne, mieti kuinka avoin pääsy on tarpeellinen eri tiloihin, miten varkauksiin tai pahantahtoisiin toimijoihin varaudutaan, ja kuinka tarkka turvallisuus tunnistettujen riskien valossa riittää. Mikäli varkauden todennäköisyys on pieni, tiedot kryptattu ja varkauden varalle on nopea palautumissuunnitelma, johon kuuluu uusien työkoneiden ostaminen lähimarketista ja ajantasaisten varmuuskopioiden palautus parissa tunnissa, tilanne on erittäin hyvä.

Kalasteluyritykset (phishing)

Sähköpostilinkit ovat vaarallisia. Nykyisin ei enää pysty erottamaan ulkonäön perusteella väärää sisäänkirjautumissivua oikeasta, joten ellei osoiteriviä lukiessa ole tarkkana ja huomaa että osoite poikkeaa perinteisestä, voi pankkitunnukset lähettää suoraan hakkerille, kun luulee kirjautuvansa pankkipalveluun. Etenkin verkkopankki kannattaa aina avata kirjoittamalla osoite itse selaimen osoiteriville. Yrityksen käyttämät palvelut voi kerätä selaimen kirjanmerkkeihin tai johonkin palveluhakemistoon (esim. intranet), jolloin niihin kirjautuminen on nopeaa ja turvallista. Jopa Googlen ensimmäiset hakutulokset saattavat sisältää maksettuja mainoksia, jotka eivät välttämättä ole luotettavia.

Tietoisuutta kalasteluyrityksistä kannattaa jakaa, kun tilanteita tulee eteen. Esimerkiksi kuvankaappauksen jakaminen yrityksen pikaviestimellä kertoo kaikille että ”taas on kalastusyrityksiä liikkeellä”, mikä toimii samalla muistutuksena olla tarkkana linkkien avaamisessa ja kouluttaa tunnistamaan outoja viestejä.

Pankkitunnusten lisäksi erilaiset sosiaalisen median tunnukset ja sähköpostitilit kannattaa suojata hyvin. Identiteettivarkaus voi johtaa maineen menetykseen, ja yrityksen virallista sähköpostia voidaan käyttää eteenpäin asiakkaiden tai yrityskumppanien huijaamiseen.

Kalastelua tapahtuu nykyisin myös muilla tavoin, kuten puhelimen välityksellä. Avulias asiakaspalvelija voi auttaa asiakasta unohtuneen salasanan kanssa muistamatta tarkistaa soittajan henkilöllisyyttä, ja antaa uudet tunnukset kenelle tahansa kysyjälle. Viralliselta näyttävällä laskulla voikin olla väärä tilinumero. Eri tilanteisiin on hyvä olla ohjeistus siitä, miten viestijän henkilöllisyys todennetaan ja mitä kautta palveluihin kirjaudutaan sisään.

Käyttäjätunnukset

Käyttäjätunnusten hallinnassa kannattaa käyttää segmentointia, eli välttää avaamasta kaikille täyttä pääsyä kaikkiin palveluihin, mikäli se ei ole tarpeen. Parhaassa tapauksessa jaettuja tunnuksia (kuten ”admin” tai ”ylläpito”) ei käytetä, vaan jokaisella työntekijällä on oma tunnus samaan palveluun. Monivaiheinen tunnistautuminen kannattaa ottaa käyttöön kaikissa kriittisissä palveluissa.

Perusmuotoisen käyttäjätunnuksen (admin, hallinta tai etunimisukunimi), muuttamisesta on pieni hyöty. Tilien turvaaminen kannattaa tehdä turvallisilla salasanoilla ja monivaiheisella tunnistautumisella. Perusmuotoiset salasanat taas ovat suuri tietoturvariski, ja vakio-salasanat täytyy vaihtaa. Lue myös erillinen osio salasanoista.

Laitteisto

Tärkein sääntö laitteistojen tietoturvassa on tehdassalasanojen muuttaminen, mikäli laite on yhteydessä verkkoon. Kaikki tehtaalla asetetut valmissalasanat löytyvät internetistä, ja valmiiksi tiedossa oleva salasana on kuin punainen matto hakkerille. Normaalisti tehdassalasanat ovat lisäksi erittäin yksinkertaisia, kuten 12345, joita kokeillaan ensimmäisenä. Uusissa laitteissa on alettu käyttää satunnaisia laitekohtaisia salasanoja, joissa ei ole yhtä suurta riskiä, mutta salasanan vaihdosta ei silloinkaan ole haittaa.

Lähes yhtä tärkeä sääntö on päivitysten hoitaminen. Nykylaitteistossa on ohjelmistoja, jotka tulee päivittää tietoturva-aukkojen varalta. Jopa älyjääkaapit voivat sisältää hakkeroinnin mahdollistavia aukkoja, ja hakkerin pääsy muihin verkon palveluihin helpottuu huomattavasti, kun yksi laite on murrettu. Kaikki älyä ja tietotekniikkaa sisältävät laitteet tulee päivittää säännöllisesti.

Valmistajan nettisivuilta löytyy usein laitteen tuotenumeroa vastaava firmware- eli laitteisto-ohjelmisto-tiedosto, sekä ohjeet sen lataamiseksi laitteeseen. Yleensä tiedosto ladataan paikoilleen joko usb-tikun tai selaimen kautta aukeavan hallintapaneelin avulla. Päivitystiedoston ohessa on tarkat ohjeet päivityksen tekemiselle. Kuten muissa päivityksissä, työn voi myös ostaa toimittajalta joko palveluna tai tuntihintaan.

Herkän tietoteknisen laitteiston turvaamisessa voi lisäksi olla tietoturvan lisäksi muita huomioitavia seikkoja. Mikäli laite tallentaa dataa, voi se olla herkkä sähkökatkoksille. Tällaiset herkät laitteet, kuten palvelimet, kannattaa suojata varavoimajärjestelmällä (UPS – uninterruptible power source), joka turvaa sähkönsyötön akkuvirralla lyhyissä sähkökatkoksissa ja varmistaa pidemmissä katkoksissa laitteen turvallisen alasajon. Nämä laitteet yleensä suojaavat myös salamaniskuilta, ja ukonilman varalta voi ostaa myös pelkän suojan ilman akkua.

Mikäli laitteiden mukauttamiseen ja asetusten säätöön on laitettu paljon aikaa, voi niiden varmuuskopiointi olla hyödyllistä. Lisäksi kannattaa tehdä riskianalyysi laiterikkojen varalle. Kriittinen infrastruktuuri voi olla järkevää turvata varalaitteistolla, ja suunnitelma laiterikkoon varautumiseksi voi lyhentää toimintavalmiuden palauttamista, kun aikaa ei mene ihmettelyyn.

Tärkeimmät tietoturvavinkit

- Vaihda uusi salasana tehdassalasanojen tilalle kaikkiin laitteisiin
- Aikatauluta ja suorita tietoturvapäivitykset myös laitteistolle
- Tee riskianalyysi ja suunnitelma laitteisto-rikkojen varalta

Massamuistit, kovalevyt ja usb-tikut

USB-muistien ja ulkoisten kovalevyjen käytössä kannattaa välttää tuntemattomia tai epäluotettavia laitteita. Käytä ainoastaan luotettavilta valmistajilta ja myyjiltä peräisin olevia massamuisteja. Älä käytä suojaamattomissa laitteissa olleita massamuisteja tai löydettyjä usb-tikkuja.

Arkaluontoinen materiaali kannattaa suojata salauksella (kryptauksella). Yksinkertaisimmillaan tämä tapahtuu klikkaamalla levyä tiedostonhallintaohjelmassa hiiren oikealla napilla ja salaamalla se avautuvasta valikosta Bitlocker- (Windows) tai Finder-ohjelmalla (Mac). Salaus estää tietoja vuotamasta, jos laite joutuu vääriin käsiin.

Monivaiheinen tunnistautuminen

Monivaiheinen tai kaksivaiheinen (MFA tai 2FA) kysyy salasanan lisäksi tunnistautumista jollain toisella tavalla – esimerkiksi tekstiviestikoodilla tai mobiilisovelluksella, jolloin varmistetaan, että sisään kirjautuva käyttäjä on oikean puhelimen tai muun MFA-työkalun omistaja. Tämä varmistaa, että vaikka salasana vuotaisi kolmannelle osapuolelle, he eivät voi kirjautua järjestelmään pelkällä salasanalla.

Monivaiheinen tunnistautuminen estää suurimman osan identiteettivarkauksista ja phishing-hyökkäyksistä. Se suojaa tilisi erittäin luotettavasti, sillä järjestelmään tunkeutuakseen hakkerin täytyy päihittää monta suojaustasoa. Etenkin liiketoiminta- ja mainekriittisten järjestelmien kirjautuminen on hyvä suojata monivaiheisella tunnistautumisella.

Hyökkäystyökalujen kehittyessä MFA-suojauksenkaan päihittäminen ei ole täysin mahdotonta, esimerkiksi kysymällä lisäkoodia huijauspankki-sivustolla, joten salasanaa käytettäessä kannattaa aina tarkistaa selaimen osoiteriviltä, että palvelu on luotettava (lisää kohdassa Osoiterivin ja nettilinkkien lukutaito).

Sähköposti ja tekstiviesti ovat fyysisiä salausavaimia ja MFA-tunnuslukuohjelmia hieman heikompia, mutta mikä tahansa monivaiheinen tunnistautuminen lisää turvallisuutta erittäin paljon.

Monivaiheinen tunnistautuminen estää suurimman osan identiteettivarkauksista.

Osoiterivin ja nettilinkkien lukutaito

Hyvänä esimerkkinä ymmärryksen kasvattamasta kyberturvasta toimii osoitekentän lukutaito. Osoitekentän vasemmalla puolella on yleensä lukon kuva, joka tarkoittaa että yhteys avatulle sivulle on salattu, eli tietoja ei pysty helposti lukemaan välistä esimerkiksi kahvilan huonosti suojatun verkon kautta.

Se ei kuitenkaan tarkoita, että sivun sisältö olisi luotettava. Myös väärennetty sivu voi olla salattu. Ensimmäisenä osoitteessa lukee protokolla, yleensä http (salaamaton) tai https (salattu), joskin monet selaimet piilottavat tämän näkyvistä.

Varsinaisen osoitteen ensimmäinen osa on domain tai verkkotunnus, jonka eri osat erotetaan pisteellä. Sitä luetaan käänteisesti oikealta vasemmalle. Päätason domain voi olla maakohtainen .fi tai viestiä sivuston tyypistä (esim. .org on usein voittoa tavoittelematon organisaatio). Seuraavana oikealta on toisen tason domain, joka on pitänyt ostaa ja jota hallinnoi jokin organisaatio tai yksityishenkilö. Tämän edessä voi olla yksi tai useampi pisteellä erotettu alidomain, jotka voidaan ohjata eri sivustoille tai palveluihin. Esimerkiksi google.com on Googlen omistama domain, jonka alidomainit mail.google.com ja drive.google.com ovat Googlen eri palveluja.

Domainin oikealla puolella on osoitteen polku – kansiorakenne, jota domainin takana olevalta tietokoneelta kysytään. Kansiot ja alikansiot erotellaan / -merkillä. Polun jälkeen voi vielä olla kysymysmerkki, jonka jälkeen sivulle annetaan parametrejä ja/tai ristikkomerkki (”risuaita”), jonka jälkeinen teksti osoittaa sivun osioon.

Tärkeintä tietoturvan kannalta on toisen tason domain. Esimerkiksi domain nordea.x64.secure.app.com ei liity mitenkään Nordea-pankkiin, vaan on app.com -domainin alla, eikä siten luotettava pankkiasioinnissa, vaikka lukon kuva osoiteriviltä löytyisikin. Secure on toisen alidomainin nimi, eikä sekään kerro turvallisuudesta.

Pilvipalvelut ja palvelimet

Pilvipalvelujen käyttö on tietoturvan kannalta helpompaa kuin omien palvelimien ylläpito, mutta kyberturva tulee silti ottaa huomioon palvelujen asetuksissa ja käyttäjätunnuksissa.

Jaettuja käyttäjätunnuksia ei kannata tehdä, vaan jokaiselle käyttäjälle tulee luoda omat tunnukset heidän tarvitsemiinsa palveluihin. Parhaassa tapauksessa käyttäjätunnukset hallinnoidaan keskitetysti, jolloin käyttäjän tarvitsee kirjautua sisään vain kerran käyttääkseen kaikkia palveluja, mutta usein pienessä yrityksessä tähän ei ole resursseja. Silloinkin kannattaa käyttäjille luoda omat tunnukset eri palveluihin, ja käyttää jonkinlaista salasanojen hallintaohjelmaa (katso oma luku salasanoista).

Mikäli pilvipalveluja käytetään omien virtuaalipalvelimien hallinnointiin, kannattaa niiden tietoturva-asetusten suunnitteluun käyttää ammattiapua.

Palveluna toimitettavan pilvisähköpostin tai muun paketin asetukset riippuvat palveluntarjoajasta, joten riskien määrä riippuu valitun kumppanin tietoturvatasosta.

Vaikka pilvipalvelujen toimintavarmuus on melko hyvä, kannattaa niiden tieto silti varmuuskopioida itse. Suurenkin yhteistyökumppanin palvelimet voivat vioittua, ja paikallinen varmuuskopio esimerkiksi ulkoiselle kovalevylle voi pelastaa paljon, jos kaikki pilven tiedot häviävät.

Päivitykset

Suurin osa tietokoneista ja älypuhelimista päivittää itsensä automaattisesti, kunhan varmistaa että päivitysten haku on päällä. Myös pilvipalvelut päivittyvät toimittajan toimesta, ellei toisin ole esimerkiksi käyttöehdoissa sovittu. Erityistä huomiota tulee kiinnittää palvelimien, laitteistojen ja erityisohjelmien kanssa, sillä niiden päivityksistä joutuu huolehtimaan erikseen.

Mikäli päivityslistan asioita ei pysty laskemaan sormilla, kannattaa miettiä ohjelmistorekisterin perustamista. Yksinkertaisimmillaan se voi olla lista käytössä olevista laitteista, niiden käyttäjistä ja viimeisimmästä päivityspäivämäärästä.

Aikatauluta päivitykset sopivalla syklillä, esimerkiksi pari kertaa vuodessa. Parhaassa tapauksessa päivitystilannetta valvotaan ja uusiin päivityksiin reagoidaan heti.

Laitteiden päivitystiedostot ladataan yleensä valmistajan nettisivuilta, joilta löytyy myös niiden päivitysohjeet. Voit myös pyytää osaavan IT-tekijän päivittämään laitteet joko jatkuvana palveluna tai tuntihintaan sovituin väliajoin. Mikäli laitteelle ei enää ole valmistajan tukea eikä sille tehdä tietoturvapäivityksiä, on vain ajan kysymys, milloin se lakkaa olemasta turvallinen. Tällainen laite kannattaa korvata uudemmalla tai vähintään eristää verkosta.

Työkoneilta kannattaa mahdollisuuksien mukaan poistaa tarpeettomat ohjelmistot, etenkin jos niitä käytetään kriittisen tiedon käsittelyyn. Mitä enemmän ohjelmia on, sitä enemmän on myös tietomurtomahdollisuuksia. Työtä ei kuitenkaan tule hankaloittaa liiallisella turvallisuudella.

Tärkeimmät vinkit ohjelmistopäivitysten hallintaan

- Varmista että automaatti-päivitykset ovat käytössä
- Aikatauluta palvelimien, laitteistojen ja ohjelmistojen päivitysten seuranta ja asennus
- Älä käytä ohjelmia tai laitteita, joita ei tueta ja joille ei enää tehdä päivityksiä

Salasanat

Älä käytä samaa salasanaa useaan paikkaan.

Salasana on vain niin turvassa kuin heikoin paikka, jossa sitä on käytetty. Niinpä eri sivustoille kannattaa tehdä eri salasanat, jotta harrastefoorumilta hakkeroidulla salasanalla ei voida kirjautua sähköpostiin tai maksupalveluihin.

Laitteiden tehdasasetusten vakio-salasanat ovat käytössä laaja-alaisesti ja yleisesti tiedossa, joten niiden vaihtaminen on erityisen tärkeää.

Monen eri salasanan muistaminen on hankalaa, joten käytännössä eri salasanan luominen jokaiseen palveluun vaatii salasanojen kirjoittamisen ylös. Paperimuistion sijaan kannattaa käyttää salasanojen hallintaan luotua salattua sovellusta. Hyviä ja helppoja työkaluja salasanojen hallintaan ovat mm. Bitwarden, NordPass ja KeePassXC. Salasanojen hallintatyökalu vaatii yhden salasanan muistamisen – ohjelma muistaa loput salasanat.

Hyväkin salasana on mahdollista vuotaa, joten paras turva saadaan kun pelkkä salasana ei riitä, vaan sisäänkirjautumiseen vaaditaan monivaiheinen tunnistautuminen.

Salasana voi nykyisin olla hyvinkin pitkä salalause, sillä salasana on sitä turvallisempi mitä pidempi se on. Hyvä salasana on helppo muistaa, joten erinomainen salasana voi olla jokin isoja kirjaimia ja erikoismerkkejä sisältävä lause. Salasanoja automaattisesti arvaavat ohjelmat käyttävät usein sanakirjaa, joten puhekielen ilmaukset, murresanat ja kirjoitusvirheet tekevät salasanasta vahvemman. Salasanojen hallintaan käytetyt ohjelmat voivat myös luoda täysin satunnaisen salasanan, joka kopioidaan palvelun salasanakenttään.

Tärkeää on myös, että kaikilla työntekijöillä on henkilökohtaiset salasanat eri palveluihin, eikä yhtä yhteistä salasanaa. Näin salasanan vuotaessa tai henkilön vaihtuessa on helppo sulkea vain yksi tili. Tärkeimmät tilit kannattaa suojata monivaiheisella tunnistautumisella.

Yrityksen salasanaohjeistuksen tulisi sisältää ohjeet salasanan tekemiseen ja käyttöön. Tunnusten luovutuksen ja sulkemisen tulisi myös olla hallittua – joko jonkin keskitetyn järjestelmän kautta tai muistilistana, jotta esimerkiksi työntekijän poistuttua muistetaan sulkea tai muuttaa kaikki hänellä käytössä olleet tunnukset.

Tärkeimmät vinkit turvallisen salasanan luomiseen

- Peruskäytössä ei tule käyttää järjestelmänvalvojan (admin/root) oikeuksia
- Käytä monivaiheista tunnistautumista tärkeissä palveluissa, kuten sähköpostissa
- Käytä salasanalistaa/ohjelmaa – älä käytä uudelleen samaa salasanaa moneen palveluun
- Hyvä salasana voi olla pitkä erikoismerkkejä sisältävä salalause

Salasanojen hallintatyökaluja ovat mm. Bitwarden, NordPass ja KeePassXC.

Luo tällaiseen palveluun yksi salalause, jonka muistat, ja tallenna loput salasanat työkaluun.

Huolehdi myös varmuuskopioista ja ota tärkeissä palveluissa käyttöön monivaiheinen tunnistautuminen.

Selaimen valinta

Minkä tahansa yleisen ja päivityksissä ajan tasalla olevan selaimen käyttö on itsessään turvallista. Yksityisyyden kannalta selaimissa on kuitenkin eroja. Chrome- ja Edge-selaimet tallentavat käytöstään tietoja Googlen tai Microsoftin palvelimille käyttökokemuksen parantamiseksi, ja käyttäjien tietoja on helppo käyttää myös mainostukseen. Mikäli omien tietojen yksityisyydestä haluaa pitää kiinni, kannattaa käyttää jotakin muuta selainta. Incognito-tilan käyttö ei estä tiedon keräämistä, vaan ainoastaan pitää käyttäjän itsensä näkemän selainhistorian puhtaana.

Firefox on ilmainen avoimen lähdekoodin selain, joka on vakaa ja luotettava. Siitä on myös Librewolf-nimellä toimiva versio, joissa asetukset on valmiiksi säädetty suojaamaan yksityisyyttä ja estämään mainokset. Brave on toinen, Chromeen pohjautuva selain, jossa asetuksia on säädetty yksityisempään suuntaan. Brave jakaa kuitenkin mielipiteitä, sillä yritys on käyttänyt selainta kryptovaluuttapalvelujen mainostamiseen. Yksityisyyden suojausasetukset saattavat kuitenkin aiheuttaa ongelmia joidenkin nettisivujen toiminnassa. Valitse selain oman riskiprofiilin mukaan.

Parasta voi olla asentaa tiukasti turvattu selain päivittäiseen käyttöön ja toinen selain, jota voi käyttää jos eteen tulee yhteensopivuusongelmia. Firefox on aina hyvä valinta, jos ei halua kokeilla eri vaihtoehtoja.

Yksityiseen ja salattuun selailuun paras työkalu on Tor Browser, joka salaa selailuun liittyvän tiedonsiirron kuten VPN ja pitää selainhistorian salassa. Ohjelma on suunniteltu vastustamaan seurantaa ja ohittamaan yhteydentarjoajien verkkosivuestot. Ohjelman voi ladata osoitteesta www.torproject.org.

Tiedonsiirto ja lähiverkot

Nykypäivänä isojen toimittajien verkkolaitteet, kuten internet-yhteyden mukana tuleva reititin, ovat perusasetuksiltaan melko hyvin suojattu. On kuitenkin hyvä varmistaa, että langaton verkko kysyy salasanaa, ja että laitteiden pohjaan merkitty salasana on jotain muuta kuin perusmuotoinen 1234, abcd tai muuta vastaavaa.

Tällainen yleisesti tiedossa oleva perussalasana on kuin punainen matto tunkeutujalle, joka voi automatisoidusti kokeilla kaikki tunnetut salasanat läpi sekunneissa.

Yrityksen tietoverkot on hyvä jakaa eritasoisiin verkkoalueisiin, jotta turvattomat laitteet eivät vaaranna turvallisuutta vaativia toimintoja. Yksinkertaisimmillaan tämä tarkoittaa sitä, että toimistolla tulisi olla erillinen vierasverkko, josta pääsee internettiin mutta ei yrityksen järjestelmiin. Vaikka tämä verkko ei ole teknisesti normaalia turvattomampi, siihen voi liittää erilaiset vierailijoiden koneet, kotitabletit, televisiot, älylaitteet ja muut järjestelmät, jotka eivät ole yhtä turvallisia kuin yrityksen muu laitteisto. Nykypäivänä on tavallista, että yrityksen palomuuri onnistutaan ohittamaan jonkin huonosti päivittyvän älylaitteen, kuten jääkaapin, avulla.

Helposti murretun laitteen jälkeen tunkeutuja pääsee yhdistämään suoraan lähiverkon muihin laitteisiin ilman palomuurin suojaa – siksi heikot laitteet on syytä rajata omaan verkkoonsa. Monissa reitittimissä on erillinen vierasverkko-asetus, jonka osaava henkilö laittaa päälle helposti.

Pääsyä eri verkkopalveluihin kannattaa rajoittaa mahdollisuuksien mukaan. Mikäli palvelua ei ole missään tilanteessa tarpeen käyttää ulkomailta, voidaan sen toiminta rajoittaa kotimaahan palomuuriasetuksilla. Yrityksen kriittiset järjestelmät voidaan rajata toimimaan vain toimiston verkosta.

VPN suojaa tiedonsiirron päätelaitteen ja palvelimen välillä, suojaten epäluotettavien yhteyksien salakuuntelulta ja mahdollistaen turvalliset yhteydet yritysverkon palveluihin. Lisätietoja erillisessä VPN-aliluvussa.

Varmuuskopiot

Varmuuskopiointi opitaan yleensä kantapään kautta sen jälkeen, kun tietoa on ensimmäisen kerran hävinnyt. Varmuuskopioiden palautus opitaan yleensä kantapään kautta sen jälkeen, kun tietoa on toisen kerran hävinnyt. Tästä on kehittynyt sanonta: varmuuskopiot ovat olemassa vasta kun niiden palautus on testattu käytännössä.

Tietojen palauttamisen voi testata vaikka uutta tietokonetta käyttöön otettaessa leikkimällä, että vanha kone on hävinnyt – tai kuivaharjoituksella, jossa jokin viime viikon tiedosto haetaan varmuuskopioista ja todetaan toimivaksi. Myös tietojen ylikirjoittamisesta palautuminen kannattaa varmistaa – saako varmuuskopiosta oikeat tiedot palautettua, jos tärkeän tiedoston päälle kopioi samalla nimellä väärän tiedoston? Tällöin voidaan palautua myös kiristyshaittaohjelmien vaikutuksista.

Varmuuskopiot ovat olemassa vasta kun niiden palautus on testattu käytännössä!

Kuinka nopeasti uudella koneella pääsee tekemään normaalisti töitä, jos tietoja ei saa kopioida vanhalta koneelta vaan ne pitää palauttaa varmuuskopioista? Parhaassa tapauksessa kaikki tarpeellinen tieto saadaan täysin käyttöön ilman että tähän kuluu paljoakaan työaikaa. Työhön liittyvän tiedon säilyttäminen esimerkiksi Dropbox, Onedrive tai Tresorit -tyyppisen pilvipalveluun peilattavan kansion alla tekee palautumisesta erittäin helppoa: asenna pilvipalvelun ohjelma ja kirjaudu sisään. Tiedot ovat tallessa sekä omalla tietokoneella että pilvessä.

Varmista kuitenkin ennen pilvipalvelun käyttöönottoa, että sinne tallennettava data saa siirtyä pilveen. Esimerkiksi GDPR-säädöksen puitteissa yritysten tallentaman henkilötiedon pitää ensisijaisesti pysyä EU-alueella, ja joillain palveluntarjoajilla tulee erikseen valita palvelimen sijainti USA:n ja EU:n välillä.

Pilvipalvelu ei kuitenkaan ole varmuuskopio, mikäli tietoa säilytetään vain pilvessä. Myös pilvipalveluntarjoajan laitteisto voi rikkoutua, ja tietoa hävitä. Tästä syystä on tärkeää että, tieto on tallessa vähintään kahdessa paikassa.

Liiketoimintakriittisen tiedon tallennukseen kannattaa käyttää 3-2-1-sääntöä: Tee tiedosta kolme kopiota, kahdelle erityyppiselle medialle (DVD, kovalevy, pilvi), joista yksi on fyysisesti eri paikassa kuin muut.

VPN

VPN (Virtual Private Network) salaa internet-yhteyden tietokoneelta VPN-tarjoajan palvelimelle, mistä yhteys jatkaa eteenpäin normaalisti. VPN-palvelimen voi myös asentaa oman toimiston verkkoon, jolloin esimerkiksi kotoa voi yhdistää VPN-yhteydellä toimiston verkkoon.

VPN-yhteyden käytöllä on kaksi vaikutusta tietoturvaan:

1) Tieto on salattu VPN-tarjoajalle asti, eli internet-yhteyden tai langattoman verkon tarjoaja ei pysty salakuuntelemaan mitä tietoa linjalla kulkee;

2) Ulospäin näkyvä yhteysosoite, eli koneen IP-osoite, näyttää käytetyille palveluille tulevan VPN-tarjoajan tietokoneelta. Vierailtu sivusto ei siis näe käyttäjän oikeaa IP-osoitetta tai geografista lokaatiota, vaan VPN-yhteyden osoitteen ja lokaation.

VPN-yhteys suojaa tiedonsiirtoa etenkin epäluotettavilta yhteydentarjoajilta, mikä saattaa olla isompi huolenaihe ulkomaisessa hotellissa kuin kotona suomalaisen yhteydentarjoajan liittymiä käytettäessä. Se myös mahdollistaa sellaisten palvelujen käytön, joiden toiminta on rajattu johonkin tiettyyn maahan, mikäli VPN-yhteys muodostetaan sopivan maan kautta.

VPN-palvelimen käyttö toimistolla mahdollistaa sisäisten palvelujen, kuten yrityksen tiedostopalvelimen, käytön estämisen julkisesta verkosta. Tällöin palvelu toimii vain fyysisesti toimistolla ja yrityksen VPN-yhteydellä. Tämä mahdollistaa rajattujen palvelujen paremman suojauksen, kun niiden käyttö vaatii VPN-tunnuksen tietämisen.

VPN-yhteys voi jonkin verran lisätä viivettä ja hidastaa latausnopeuksia, sillä yhteys kiertää VPN-tarjoajan laitteiston läpi ja voi ruuhkautua. Lisäksi kaikki se salaamaton tieto, joka olisi kulkenut internet-yhteydentarjoajan läpi, kulkee nyt VPN-tarjoajan palvelinten läpi, ja epäluotettava VPN-tarjoaja voi jopa itse kuunnella yhteyksiä ja myydä tietoja eteenpäin. VPN-tarjoajan valinta kannattaa tehdä luotettavuutta silmällä pitäen