Yrittäjän tietoturvaopas

2025

lennu it

Sisältö

1. Mitä tarkoittaa tieto- ja kyberturvallisuus?

Viime vuosina tietoturvasta on puhuttu mediassa, sosiaalisessa mediassa ja kahvipöydissä yhä enemmän. Mitä tietoturva oikein on ja miten yrittäjä voi parantaa yrityksensä tietoturvaa?

Tietoturva ja siitä huolehtiminen ei koske vain suuria organisaatioita, valtion virastoja tai isoja yrityksiä. Myös pienyrittäjän kannattaa varmistaa, että kaikki yrityksen tärkeät tiedot ovat turvassa. Tässä oppaassa käymme läpi yrittäjän kannalta oleellisimmat tietoturvaan liittyvät asiat, termit ja ilmiöt.

Tieto- ja kyberturvallisuus

Tietoturvalla tarkoitetaan kaikkia niitä järjestelyitä tai keinoja, joilla varmistetaan tiedon saatavuus, luottamuksellisuus ja eheys.

Tiedon merkitys

Usein nykyaikana termiä “data” käytetään kuvaamaan sitä tietoa, mitä käsittelemme digitaalisilla laitteilla kuten tietokoneilla. Data onkin tietojärjestelmiin tallennettua “raakatietoa” jolle usein asetetaan jokin merkitys tai väline, jota käytetään tiedon jalostamiseen. Esimerkiksi powerpoint-esitykseen voidaan jalostaa dataa (kuvia, tekstejä jne.) tiedoksi.

Tiedon osalta tulee muistaa, että osa tiedoista on edelleen paperilla tai muussa muodossa. Yritykselle tärkeää tietoa voivat esimerkiksi olla maksuliikenne, salasanat ja viestintään liittyvät tiedot ja tietolähteet, kuten asiakasrekisteri. Nämä osaltaan ovat tietojärjestelmissä olevaa dataa, mutta niiden käyttäminen välineiden ja laitteiden avulla muodostaa niistä tietoa.

Sanat ja selitykset

Saatavuus = Tieto on käytettävissä ja hyödynnettävissä, kun sitä tarvitaan.

Eheys = Tieto säilyy muuttumattomana ja eheänä.

Luottamuksellisuus = Tietoa käsittelevät vain siihen oikeutetut henkilöt ja tiedon luottamuksellisuus säilyy.

Tietoturva voidaan jakaa kolmeen osaan: fyysinen, hallinnollinen (johtaminen) ja tekninen. Fyysiseen tietoturvaan lukeutuu esimerkiksi liikehuoneiston tulipalo tai luvattoman henkilön pääsy yrityksen laitetilaan ja laitteisiin. Hallinnollisella taas tarkoitetaan sitä, miten tietoa käsitellään yrityksessä ja kenen saatavissa se on, kuten vaikka missä asiakastietoja säilötään liikkeen kiinnioloaikana, tai saako työntekijä käyttää kannettavaansa oman puhelimen lataamiseen. Tekniseen tietoturvaan kuuluvat ne, mitä useimmiten käsitämme tietoturvauhiksi, eli esimerkiksi virukset tai muut haittaohjelmat.

Tietoturvauhkien osalta ensimmäinen tärkeä askel on tunnistaa ne uhat, mitkä liittyvät yritykseen, sen sidosryhmiin ja liiketoimintaan. Tunnistamisen jälkeen arvioidaan riskejä suhteessa uhan toteutumiseen ja mitoitetaan näin oikeasuhtainen tietoturva ja -suoja. Tietoturvariskien toteutuessa yrittäjälle aiheutuu usein taloudellista haittaa tai lisätyötä kadonneen tai vääristyneen tiedon korvaamiseksi. Riskien toteutuminen voi tuottaa myös mainehaittaa, jos esimerkiksi tietomurron seurauksena sidosryhmien ja asiakkaiden luottamuksellinen tieto vaarantuu.

Pahimmillaan koko liiketoiminta voi keskeytyä, kun tietoturva pettää, virus pääsee tuhoamaan tietokoneelta tiedostoja tai huijari saa tyhjennettyä yrityksen tilin. Tietoturvallisuudesta huolehtiminen onkin osa liiketoiminnan jatkuvuuden varmistamista ja yrityksen riskienhallintaa siinä missä taloudellisesta jatkuvuudesta huolehtiminen.

Kyberturvallisuudella tarkoitetaan kokonaisuutta, joka käsittää tiedon, tietojärjestelmien, laitteiden ja verkostojen turvallisuuden. Se eroaa tietoturvallisuudesta siten, että tietoturvallisuudella pyritään suojaamaan tietoa eli varmistamaan tietosuoja sekä tiedon saatavuus, luottamuksellisuus ja eheys, kun kyberturvallisuus toimii ikään kuin kattokäsitteenä koko kybermaailman turvallisuudelle. Tässä oppaassa keskitymme tietoturvallisuuteen kyberturvallisuuden sijaan johtuen siitä, että yrittäjän kyberturvallisuus kannattaa aloittaa tiedon suojaamisesta sekä tietoturvallisuuden perusteista.

2. Pienen ja keskisuuren yrityksen tavallisimmat tietoturvauhat

Juuri sinun yrityksellesi keskeiset uhat riippuvat yrityksesi koosta, toimialasta ja käsiteltävän tiedon asettamista vaatimuksista. Toimiala, toiminnan laajuus sekä käsittelemäsi tiedon arkaluonteisuus vaikuttavat tietoturvauhkien laajuuteen ja luonteeseen. Samoin laitteet ja verkot mitä yrityksellä on käytössä muodostavat kokonaisuuden sille, minkälaisia uhkia yritykseen, sen tietoon ja liiketoimintaan voi kohdistua.

Esimerkiksi konsulttiyrittäjä käsittelee asiakkaidensa tietoja ja liikesalaisuuksia, joten hänen on erityisen tärkeää varmistua tietoturvallisuudesta ja suojata tietojen käsittely ulkopuolisten silmiltä ja korvilta. Toisaalta kukkakauppiaalle merkittävämpi tietoturvauhka voi olla laskujen ja tilausten katoaminen järjestelmästä. Entä muistatko muutamien vuosien takaa tapauksen, jossa hakkeri oli päässyt tekemään ison puhelinlaskun maatalousyrittäjälle hakkeroimalla lypsyrobotin?

Tietoturvauhkien tunnistamisessa on usein syytä käyttää ammattilaista apuna, sillä suojattavien tietojen ja laitteiden määrä voi yrityksen pienestäkin kokoluokasta huolimatta olla laaja ja toisaalta uhista muodostuvien riskien määrittämisessä sekä hallinnassa on syytä mitoittaa toimet oikein.

1. Tietoturvamurrot ja tiedon saatavuus

Tiedon turvallinen säilytys on ensisijaisen tärkeää. Tietoturvan ja -suojan keskiössä on tiedon turvaaminen siten, että tieto ei vaarannu missään tilanteessa. Tiedon vaarantuminen ei tarkoita välttämättä sitä, että hakkeri murtautuu järjestelmiin vaan myös arkisia tilanteita, joissa paperi on jäänyt väärään paikkaan tai näytönsuojakalvo puuttuu junassa etätöitä tehdessä.

Tietotekniikkan liittyvät tietoturvamurrot johtuvat usein heikkojen salasanojen käyttämisestä tai tiedon käsittelystä siten, että sitä ei suojata

tarpeellisin osin. Yhtenä esimerkkinä tästä voidaan pitää suojaamatonta verkkoa tai samojen tunnuksien käyttöä useassa eri palvelussa.

Tiedon ja sen turvaamisen osalta tulee tunnistaa ne käsittelytavat, jotka ovat alttiita tiedon häviämiselle, muuttumiselle tai vaarantumiselle. Esimerkiksi paperisen tiedon käyttäminen vaatii yhtälailla tietoturvallisuuden huomioimista, jotta tiedon luottamuksellisuus ja eheys voidaan varmistaa.

2. Huijaukset

Erilaiset huijaukset ovat hyvin yleinen tapa murtautua yrityksen tietojärjestelmiin tai tietoliikenteeseen. Tyypillisimmin huijauksen välineinä käytetään sähköposteja ja sosiaalisen median palveluita. Viestinnän osalta sosiaalisen median tilit ja profiilit ovat riski huijauksille, kun nämä ovat usein julkisia. Sosiaalista mediaa voidaankin hyödyntää huijauksiin ja esimerkiksi hakkeroitua yrityksen sosiaalisen median tilille ja esiintyä yrityksen edustajana.

Ei ole myöskään harvinaista, että huijauksen kohde ei havaitse mitään epänormaalia toimintaa, vaan tietoja käytetään hyödyksi esimerkiksi teollisuusvakoiluun tai muuhun tietojen keräämiseen, jolla voidaan myöhemmin kiristää yritystä tai saavuttaa kilpailuetua.


7:17
+1 (321) 213-123
SCAM
Message
Voicemail
slide to answer

Huijausten tarkoitus on saada huijauksen kohde luovuttamaan tärkeitä tietoja, kuten salasanoja, henkilötietoja, maksukorttien tietoja tai kerätä tietoa varsinaista tietoturvamurron yritystä varten. Huijarit saattavat nähdä paljonkin vaivaa saadakseen toimintansa vaikuttamaan uskottavalta. Usein huijausviestejä lähetetään tunnettujen, virallisten tahojen nimissä tai muuten aidoilta vaikuttavilla keinoilla. Toisinaan huijarit voivat esiintyä esimerkiksi yrityksen toimitusjohtajana ja näin ollen pyrkivät saamaan työntekijän luovuttamaan yrityksen toimintaan liittyvää tietoa.

Joskus viesteissä myös ohjataan kohde hyvin uskottavilta vaikuttaville sivustoille. Pienet yksityiskohdat paljastavat huijauksen, joten ole tarkkana, jos saat viestin, jossa pyydetään arkaluontoista informaatiota.

3. Haittaohjelmat

Haittaohjelmien tarkoituksena on käyttää kohteen laitteita tai ohjelmistoja siten, että niillä oleva tieto vaarantuu. Mahdollisia tavoitteita tälle voi olla tiedon anastaminen, kiristäminen, huijaaminen tai pelkkä haitanteko.

Haittaohjelmille altistumisen todennäköisyys kasvaa mitä useammassa eri viestintäkanavassa tai järjestelmässä toimitaan. Haittaohjelmia vastaan ensiarvoisen tärkeää on suojata yrityksen tietoliikenne ja ohjelmistot siten, että haittaohjelmat torjutaan jo verkkotasolla niin, että ne eivät koskaan edes saavuta yksittäisen käyttäjän laitetta tai ohjelmistoa.

Suurin riski haittaohjelmalle altistumiselle muodostuu, jos yrityksen verkkoliikennettä tai laitteita ei ole suojattu ajantasaisilla ohjelmistoilla tai laitteilla, kuten päätelaitesuojauksella ja palomuurilla. Samoin riski kasvaa, jos käytetään useita erilaisia ohjelmistoja tai alustoja (esimerkiksi internetin kautta toimivat laskutus-, asiakkuudenhallinta-, viestintäsovellukset).

Haittaohjelmat voidaan havaita tai estää jo tietoliikenteessä nykyaikaisen palomuurin avulla. Palomuuri toimii myös etätyössä, jos yrityksellä on käytössä VPN-yhteys, mikä luo suojatun yhteyden yrityksen lähiverkkoon. Tulee myös huomata, että edullisimmat palomuurit ja verkkolaitteet on yleensä suunniteltu kotikäyttöön ja erilaisia uhkia vastaan, joten näiden käyttöä yrityskäytössä yrityksen kokoon katsomatta ei suositella.

Esimerkki huijauksesta: Sähköpostit – tietojen kalastelu

Yrittäjä saa viralliselta vaikuttavan sähköpostin, joka pikaisesti arvioiden näyttää tulevan luotettavalta toimijalta (esimerkiksi pankki tai sidosryhmä) tai muutoin uskottavasta lähteestä. Viestissä kehotetaan yrittäjää varmistamaan kiireellisesti henkilöllisyytensä ja luovuttamaan tietoja (kuten maksutiedot) varmistaakseen, ettei jokin tärkeä tieto tai maksu katoa.

Huijauksen taktiikka on kiireen tunteen luominen, jotta kohde ei ajattelisi vaan toimisi nopeasti. Tarkempi tarkastelu paljastaa pienet epäilyttävät virheet esimerkiksi sähköpostiosoitteessa tai sivuston osoitteessa.

4. Fyysiset uhat

Vaikka tietoturva usein liitetään tietotekniikkaan, ei tule unohtaa fyysistä tietoturvallisuutta. On syytä huomioida, miten ja missä laitteita sekä tietoa käytetään ja säilytetään ja kenellä niihin on pääsy.

Tärkeää on tunnistaa, että kenellä on pääsy yrityksen laitteisiin ja onko tämä pääsyoikeus tarpeellinen kyseisen henkilön osalta. Osaltaan pilvipalveluiden käyttö mahdollistaa paremman tietoturvan, kun tieto säilytetään muualla kuin yrityksen omissa tiloissa.

Useimmat yritykset huolehtivat hyvin teknisestä tietoturvastaan, mutta fyysinen turvallisuus jää huomiotta. Asiantuntijoiden kanssa on hyvä tarkistaa, mitkä ovat riittävät suojaustoimet ja kenellä tulisi olla pääsy sellaisiin laitteisiin ja tiloihin, joiden toiminta on oleellista yritykselle.

Esimerkiksi video- ja kulunvalvonta sekä hälytyslaitteet tarjoavat jo hyvän suojan yrityksen toimitiloihin ja tuovat turvallisuutta fyysisen murron varalle. Kuitenkin on hyvä huomioida, että jos yrityksellä on omia palvelimia tai verkkolaitteita toimitiloissaan, tulisi näiden olla erillisessä tilassa, johon on rajattu pääsy.

5. Palvelunesto-hyökkäys

Palvelunestohyökkäys tarkoittaa verkkohyökkäystä, jossa pyritään estämään verkkosivuston käyttö. Yleisin palvelunestohyökkäyksen tyyppi on sellainen, jossa verkkosivustolle kohdistetaan niin paljon liikennettä, että sivusto ei ole enää toimintakykyinen. Useimmiten palvelunestohyökkäykset kohdistuvat yrityksen internetissä toimiviin palveluihin, kuten verkkosivuihin, varauskalentereihin ja asiakasportaaleihin.

Palvelunestohyökkäykset eivät ole kohdistettu yleensä suoraan pieniin ja keskisuuriin yrityksiin, koska näistä hyökkääjän saama hyöty suhteessa riskiin on pieni. Kuitenkin mikäli yritys käyttää esimerkiksi jotakin julkista palvelua osana liiketoimintaansa (esimerkiksi erilaiset rekisterit tai muut ulkoiset lähteet) voi osa yrityksen toiminnoista olla alttiita palvelunestohyökkäyksille.

3. Miten yrittäjä voi suojautua tietoturvauhilta?

Yrityksen tietoturvasta huolehtiminen on lopulta hyvin yksinkertaista. Tärkeintä on tunnistaa suojeltavan tiedon kokonaisuus ja laajuus sen sijaan, että takertuisi pieniin yksityiskohtiin. Kuten olemme aikaisemmin oppaassa tuoneet ilmi, kokonaisuuteen liittyy sekä fyysisiä, hallinnollisia että teknisiä ratkaisuja. Nämä ovat yhteydessä toisiinsa ja usein jo yhden osa-alueen parantamisella saavutetaan jo huomattavia hyötyjä.

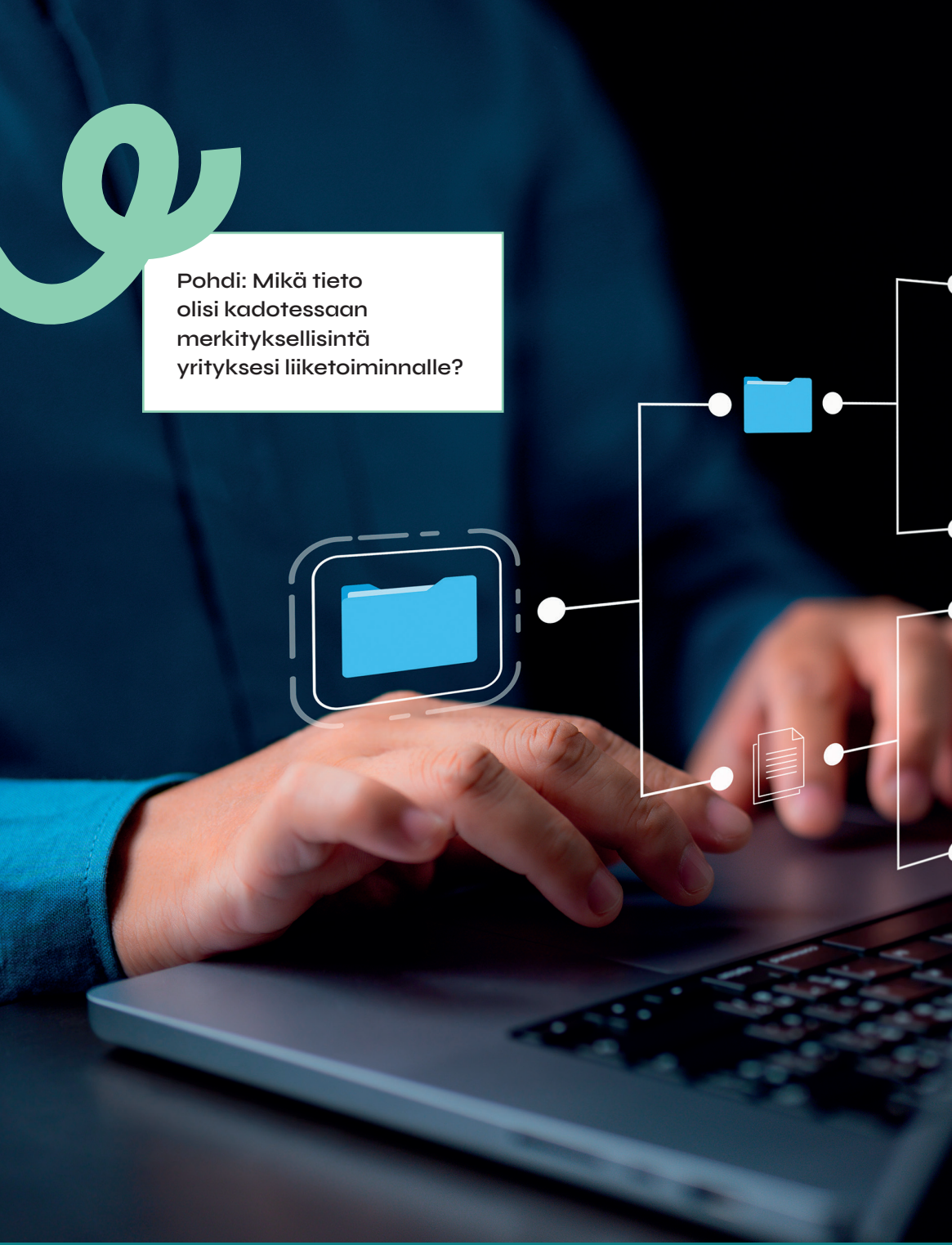
Miten syvällisesti tietoturvaan on perehdyttävä? Mitoita toimet oikein!

Pienyrittäjän tietoturva tarkoittaa luonnollisesti pienempää kokonaisuutta kuin suuryrityksellä. Oikein mitoitettu tietoturva ja -suoja ovat tasapainossa saatavuuden kanssa, jolloin ratkaisut ja toimintatavat ovat helppoja noudattaa arjessa. Oikeasuhtainen tietoturva mahdollistaa ennemmin kuin rajoittaa tiedon käyttämistä.

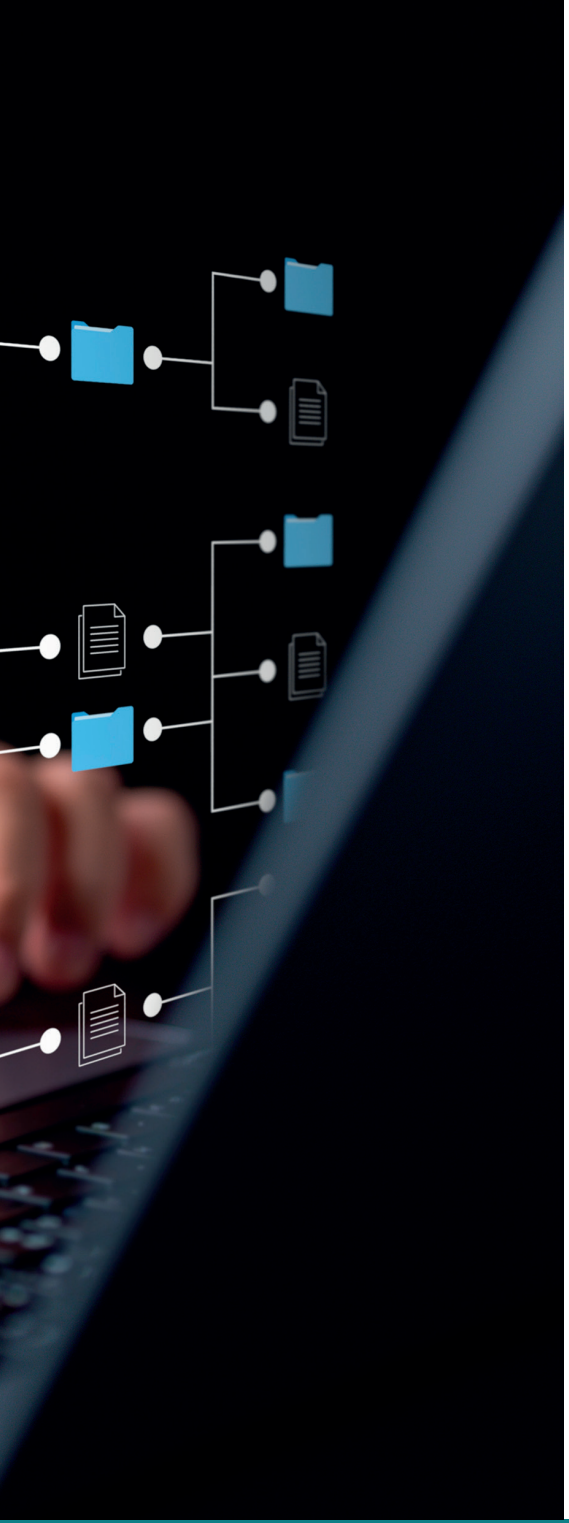
Pohdi siis sitä, miten paljon sinun yritykselläsi on suojattavaa tietoa, ja kuinka luottamuksellisia tiedot ovat. Huomioi, että tietoturvan ja -suojan vaatimukset eivät kosketa ainoastaan yritystäsi, vaan siihen kiinteästi liittyviä sidosryhmiä ja yrityksesi työntekijöitä.

Oman yrityksesi maksutiedot ja asiakasrekisteri on aina hyvä suojata. Jos lisäksi käsittelet asiakkaidesi liikesalaisuuksia, maksutietoja ja rahaliikennettä, tai vaikkapa terveystietoja, voi olla syytä kartoittaa tilanne tarkemmin asiantuntijan kanssa. Usein tällaisissa tapauksissa tulee myös huomioida lailliset velvoitteet, esimerkiksi jos käsittelet henkilötietoja.

Seuraavaksi kerromme, miten pääset tietoturvauhkien torjumisen alkuun kolmen kohdan kautta. Otettuasi nämä asiat haltuun, neuvomme mielellämme, millainen tietoturvan kokonaisuus on sopiva juuri sinun yrityksellesi.



Pohdi: Mikä tieto olisi kadotessaan merkityksellisintä yrityksesi liiketoiminnalle?



Kohta 1: Tiedon turvallinen säilytys

Merkityksellisimmän tiedon säilyttäminen on syytä järjestää niin, että ulkopuoliset eivät pääse siihen vahingossakaan käsiksi, eikä ole vaaraa menettää tärkeitä tietoja vaikkapa vesivahingon sattuessa ja tietokoneviruksen iskiessä. Tässä muutama vinkki tiedon turvalliseen säilyttämiseen:

Tiedon arkistointi

Aloitetaan perusasioista: Jos säilytät tietoja paperisina yrityksen tiloissa, muista huolehtia niiden turvallisesta säilyttämisestä. Lukittava arkistokaappi varmistaa, ettei kukaan epähuomiossa pääse selaamaan luottamuksellisia tai arkaluonteisia tietoja. Silppuri on yrittäjän ystävä, kun luottamuksellisia tietoja sisältäviä asiakirjoja on hävitettävä.

Jos yritykselläsi on arkistokaapeittain asiakastietoa sisältäviä papereita, on tietoturvasta huolehtimisen ohella myös hyvä aika ryhtyä pohtimaan tietojen digitalisointia. Esimerkiksi pilvipalvelussa asiakirjat ovat usein vielä arkistokaappia varmemmassa tallessa ja turvassa myös fyysisesti.

Turvallinen pilvipalvelu

Pilvipalveluiden avulla mahdollistat tiedostojen luotettavan säilyttämisen. Pilvipalvelu mahdollistaa esimerkiksi automaattisen varmuuskopioinnin ja varmuuskopioiden säilyttämisen eri sijainneissa. Automaattiset varmuuskopiot kaikista tiedostoista ja asiakirjoista varmistavat, että tietokoneen mennessä rikki tietosi ovat palautettavissa varmuuskopioista.

Pilvipalveluiden tietoturvassa, toimintavarmuudessa ja käyttöehdoissa on eroja, joista yrittäjän on hyvä olla tietoinen valitessaan palveluntarjoajaa. Huomioi pilvipalvelua valitessa esimerkiksi se, miten käyttäjiä hallinnoidaan. Turvallisessa pilvipalvelussa jokaisen käyttäjän on rekisteröidyttävä ja tunnistauduttava, jotta tietojen käsittelyä voidaan valvoa ja toisaalta estää sellainen tietojenkäsittely, mihin ei

ole oikeutta. Varmista myös, miten toimitaan odottamattomissa tilanteissa: esimerkiksi palveluntarjoajan toiminnan keskeytyessä syystä tai toisesta, sinun tulisi edelleen päästä käsiksi omiin tietoihisi.

Kiinnitä myös huomiota siihen, missä tietojasi säilytetään. Jos palveluntarjoaja säilyttää tietoja ympäri maailmaa, säilytykseen voidaan soveltaa kansainvälisiä ja kansallisia lakeja. Huolehdi siis siitä, että palveluntarjoaja säilyttää tiedon esimerkiksi Suomessa. Pilvipalvelut, joita me Lennulla tarjoamme, ovat sellaisia, joiden tietoturvallisuus ja -suoja ovat varmistettuja ja tarjoavat helpon käytettävyyden sekä saatavuuden.

Automaattiset päivitykset ja varmuuskopiointi

Yritystoiminnassa käyttämiesi ohjelmistojen päivitykset korjaavat mahdollisia löytyneitä haavoittuvuuksia sekä takaavat ohjelmistojen toimivuuden. Päivitykset ja varmuuskopiointi on hyvä automatisoida tapahtumaan säännöllisesti ja siten, että ne eivät haittaa käytettävyyttä.

Joskus varmuuskopioita on syytä säilyttää myös ulkoisilla kovalevyillä tai muistitikuilla. Jos teet varmuuskopioita ulkoisille muistilaitteille, suojaa laitteet aina salasanalla. Näin estät pääsyn tiedostoihin, jos laite joutuu vääriin käsiin.

Turvallisessa pilvipalvelussa:

- Jokaisella käyttäjällä oma tunnuksensa (pääsyoikeudet ja niiden valvonta)
- Palvelu mahdollistaa monimenetelmäisen todentamisen (MFA)
- Tiedät, missä tietoa säilytetään (lainsäädäntö ja turvallisuus)
- Palvelu tukee yleisimpiä standardeja ja ohjelmistoja sekä laitteita
- Tieto salataan sekä säilytettäessä, että sitä siirrettäessä

Päätelaitesuojaus ja palomuurit

Tiedon säilytykseen liittyy myös laitteiden suojaaminen. Vaikka tiedot varmuuskopioidaan tai synkronoidaan automaattisesti pilvipalveluun, on yrittäjällä yleensä paljon tärkeää tietoa myös puhelimella, tietokoneella ja muilla laitteilla, jota ei synkronoida muualle tai synkronointi ei ole reaaliaikaista. Laitteet onkin hyvä suojata huolella jokaisella tasolla.

Palomuurit

Palomuuri suodattaa verkkoliikennettä sallien ainoastaan luvallisen liikenteen. Nykyaikaisella palomuurilla voidaan lisäksi havaita tai estää haittaohjelmia ja tunkeutumisia reaaliaikaisesti. Palomuuriratkaisua suunnitellessa tulisi huomioida eri laitteet ja verkot, jotta kaikki osa-alueet tulevat suojatuksi. Laitteilla tulisi olla oma ohjelmistopalomuurinsa, kun taas verkot tulee suojata erillisellä palomuurilla. Näin jokaisella laite- ja verkkotasolla tietoliikenne on suojattua ja valvottua, eikä yhden laitteen tai ohjelmiston pettäminen vaaranna kaikkea tietoa.

Laitteiden ohjelmistopalomuurit ovat usein osa päätelaitesuojaus-kokonaisuutta yhdessä virustorjunnan, selauksen suojan ja muiden tietoturvaominaisuuksien kanssa, jolloin yhdellä ratkaisulla saadaan aikaan erinomainen tietoturva, joka on ajantasainen.

Päätelaitesuojaus on ohjelmisto, jota voitaisiin kutsua vanhalla termillä virustorjunta. Päätelaitesuojaus on kokonaisvaltainen sovellus, joka mahdollistaa reaaliaikaisen uhkien torjunnan ja niihin reagoinnin, monitoroinnin, tietoliikenteen suojauksen ja muut laitteen turvallisuutta koskevat käytännöt.

Salauksella voidaan estää tiedon luvaton käyttö. Ilman salausta laitteiden kiintolevyt ovat helposti hakkeroitavissa, minkä vuoksi muistilaitteet ja kiintolevyt kannattaa salata.

Kohta 2: Tiedon turvallinen siirtäminen ja kuljettaminen

Suurin riski tiedon häviämiselle, muuttumiselle tai vääristymiselle on silloin, kun sitä siirretään. Tiedonsiirron turvaaminen onkin siis ensiarvoisen tärkeää, varsinkin kun siirrät tietoa yrityksen lähiverkosta pois. Tiedonsiirtoa tapahtuu lähes aina, kun laitteet kommunikoivat keskenään, minkä vuoksi kaikki verkkoliikenne on hyvä suojata. Yleensä hyökkääjät pyrkivät hyödyntämään heikointa laitetta tai ohjelmistoa, jonka välityksellä hyökätään muihin tai laitteiden väliseen liikenteeseen. Palomuureilla voidaan suojata verkkoliikennettä ja laitteita ohjelmistojen tarjoaman suojatun liikenteen lisäksi myös yrityksen sisäverkossa. Varmista siis tiedonsiirto turvallisesti esimerkiksi seuraavin keinoin:

Yrityksen verkon suojaus ja turvallisten verkkojen käyttö

Työskentelet sitten kotitoimistolla, yrityksesi tiloissa tai kahvilassa, on tärkeää varmistua siitä, että käyttämäsi verkko on riittävän turvallinen. Sekä kotona että yrityksen tiloissa oman verkon turvallisuudesta on helppo huolehtia asiantuntevan ICT-kumppanin neuvoja noudattaen. Lennun yritysmyynti auttaa löytämään juuri sinulle parhaan ratkaisun - ota yhteyttä vaikka heti!

Yleisin ja varmin tapa varmistaa yhteyden suojaus on käyttää VPN-yhteyttä. VPN-yhteys mahdollistaa salatun ja turvallisen yhteyden sekä internetiin että yrityksen lähiverkkoon. Ilman yksityistä, salattua yhteyttä verkon sisällä (VPN) muut samassa verkossa olevat toimijat ja laitteet kykenevät näkemään liikenteesi ja tunnistamaan laitteesi. Pahimmillaan joku voi yrittää murtautua laitteeseen.

Turvalliset viestintäkanavat

On hyvä harkita, mitä jakaa ja missä viestintäkanavissa. Vaikka iloinen kesälomatoivotus ja -tiedote yrityksen kiinniolosta vaikuttaa rennolta, voi se hakkerille olla suora kutsu ja tieto siitä, että yritykseen on helpompi tunkeutua. Tärkeää on myös ymmärtää tiedon suojaaminen siten, että luottamuksellista tietoa ei välity kolmansille osapuolille tai sellaisille palveluntarjoajille, jotka eivät käsittele tietoa luottamuksellisesti tai siirtävät tiedon muualle kuin mihin asiakas


VPN
CONNECTED

Mikä on VPN-yhteys? Milloin sitä tarvitaan?

VPN eli “virtual private network” on tuttu monelle, joka on tehnyt etätöitä. VPN-yhteys mahdollistaa turvallisen, suojatun verkkoyhteyden muodostamisen palomuurin kautta sekä internetiin että yrityksen lähiverkkoon ja verkkoasemiin. VPN muodostaa “putken”, jota pitkin tietoliikenteesi kulkee salattuna ja suojattuna.

Miten saat VPN-yhteyden käyttöösi?
Esimerkiksi kun tilaat yrityksellesi Lennulta palomuurin, voit samalla kertaa ottaa käyttöösi VPN-yhteyden. Ota yhteyttä yritysmyyntiimme ja kysy lisää!

Varo rogue-wifiä julkisella paikalla!
Julkisessa tilassa, kuten kahvilassa, ravintolassa tai hotellissa, voi vaania yllättävä uhka: rogue-wifi. Rogue-wifillä tarkoitetaan oikeaksi tekeytyvää verkkoa, jonka huijari tai hakkeri on rakentanut. Tarkoitus on huijata oikealta vaikuttavalla verkolla tai verkon nimellä ihmiset yhdistämään laitteensa rogue-verkkoon, jolloin kaikki verkkoliikenne kulkee todellisuudessa huijarin verkon kautta.

Miten välttyä rogue-wifiltä?
Kun käytät etätyössä VPN-sovellusta, kulkee tieto salattuna, vaikka vahingossa yhdistäisitkin väärään verkkoon. Kuitenkin laitteesi on edelleen alttiimpi hyökkäyksille, jolloin on hyvä olla päätelaitesuojaus kunnossa. Käyttämällä vain omia tai tunnettuja yhteyksiä ja sovelluksia, varmistut riittävästä suojasta.

tai sidosryhmä on antanut luvan. Suositeltavaa onkin siis tutustua palveluiden ehtoihin ja siihen, minkä maan lainsäädäntöä tietojen käsittelyyn sovelletaan sekä miten palveluntarjoaja käsittelee palvelun sisällä lähetettävää tietoa.

Keskustele asiakkaiden ja sidosryhmien kanssa turvallisista viestintäkanavista. Erityisesti, kun yritysten ja sidosryhmien välillä siirretään luottamuksellisia tietoja, on hyvä ottaa puheeksi, mitä viestikanavia on turvallista käyttää. Hyvä tapa on esimerkiksi luottamuksellisen tiedon lähettämiseen käyttää salattua sähköpostia tai niin kutsuttua turvapostia.

Työyhteisössä kannattaa myös sopia pelisäännöistä sen suhteen, millaista tietoa ei ole turvallista lähettää esimerkiksi sähköpostitse tai pikaviestipalvelussa. Osana hallinnollista tietoturvaa onkin siis hyvä määrittää yrityksessä käytettävät sovellukset ja viestintävälineet jotta tietosuoja ja -turva ovat varmistettu.

Kohta 3: Tiedon turvallinen käyttäminen

Tiedon tulee olla saatavissa ja käytettävissä juuri silloin, kun sitä tarvitaan. Miten voit varmistaa, että tietosi pysyvät tallessa ja turvassa myös päivittäisessä arjessa? Tiedon turvalliseen käyttöön liittyvät sekä tunnukset ja käyttöoikeudet että hyvät yhteiset käytännöt. Näillä tarkoitetaan sitä, miten tietoturvaa hallinnoidaan ja johdetaan yrityksessä. Hyvä hallinnollinen tietoturva antaa yrityksen toiminnalle selkeät käytännöt ja toimintatavat.

Käyttöoikeudet ja käyttäjän tunnistus

Ensimmäinen askel tiedon turvallisessa käytössä on varmistaa, kenellä on pääsy yrityksen laitteisiin, palveluihin ja sovelluksiin. Pääperiaatteena voi pitää, että esimerkiksi työntekijän tulisi päästä yrityksen järjestelmiin vain omalla käyttäjätunnuksella ja salasanalla.

Useissa ohjelmistoissa voit myös määritellä erilaisia rooleja tai ryhmiä, jotka määrittävät, mitä kukin käyttäjä pystyy muokkaamaan tai tarkastelemaan. Esimerkiksi verkkosivujen hallinnoinnissa tai asiakasrekisterin ylläpidossa jokaisella työntekijällä ei ole tarve olla kaikkia oikeuksia. Yhdellä työntekijällä voi olla oikeus muokata sivuston rakennetta ja koodia, toisilla taas vain mahdollisuus muokata sivun tekstejä.

Monivaiheinen tunnistautuminen

Kaikissa yrityksen käyttämissä järjestelmissä, palveluissa, ohjelmistoissa ja sosiaalisen median tileillä on syytä ottaa käyttöön monivaiheinen tunnistautuminen eli MFA (Multi Factor Authentication). Monivaiheinen tunnistautuminen varmistaa käyttäjän tunnistamisen kahden tai useamman tekijän avulla.

Jos esimerkiksi käyttäjän salasana murretaan tai se paljastuu, ei hyökkääjä pääse kirjautumaan, koska käytössä on salasanan lisäksi jokin toinen tekijä jolla vahvistetaan käyttäjä. Vahvistus voi olla puhelinnumero tai vahvistus sovellus, joista sovellus on suositeltavin ja helppokäyttöisin eikä vaadi välttämättä työntekijälle omaa puhelinnumeroa.

Turvallisten tunnusten resepti:

1. Samaa salasanaa ei saa käyttää useassa eri paikassa
2. Salasanan tulisi olla monimutkaisempi kuin yksi lyhyt sana ja numero
3. Vältä yksittäisiä sanoja.

Katso tästä lisäksi Kyberturvallisuuskeskuksen ohjeet turvallisen salasanan keksimiseen:
www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan


2FA
******
Username
****
Remember Me
Forgot Password?
LOGIN

Vahvat salasanat ja salasanan hallintaohjelma

Salasanoilla on väliä, sillä ulkopuolisen tahon on helppo arvata tai löytää kokeilemalla liian yksinkertainen salasana.

Turvallisten ja riittävän monimutkaisten salasanojen luomiseen voi käyttää salasanageneraattoria. Yrityksen tunnukset voi lisäksi tallentaa salasanan hallintaohjelmaan eli niin kutsuttuun salasanapankkiin. Salasanapankkiin voit lisätä myös työntekijäsi ja opastaa heitäkin käyttämään turvallisia salasanoja.

Turvalliset salasanat voivat tuntua hankalilta ja monimutkaisilta muistaa. Lisäksi yrityksen käytössä on usein monen monta eri järjestelmää, joista jokaiseen tulisi olla eri salasana. Tästä syystä salasanapankki helpottaa niin yrittäjän kuin työntekijöidenkin arkea.

Tietoturvakäytännöt: varmista, että henkilöstö tietää turvalliset toimintatavat

Yhteiset tietoturvakäytännöt on hyvä kirjata ylös ja säilyttää näkyvillä. Kerro käytännöt aina uusille työntekijöille ja muistuta käytännöistä säännöllisesti. Näytä myös itse esimerkkiä noudattamalla yhteisiä käytäntöjä!

Tietoturvakäytännöt kannattaa suhteuttaa yrityksen tarpeisiin. Yksinyrittäjän tai muutaman henkilön pienyrityksen ei kannata lähteä rakentamaan liian monimutkaista kokonaisuutta. Yksinkertaiset yhteiset toimintatavat riittävät usein pitkälle ja ovat kaikkein varmimpia.

Pohdi ensin, missä järjestelmissä yritykselle tärkeää tietoa, joka ei saa joutua ulkopuolisten käsiin, säilytetään. Sitten voit poimia juuri läpikäydyistä keinoista sopivat tietoturvatoimet juuri sinun yrityksellesi.

Tietojen kalastelu – miten välttää huijaukset ja kalasteluyritykset yritystoiminnassa

Huijauksilta ja tietojen kalastelun yrityksiltä välttyy parhaiten noudattamalla tavanomaista varovaisuutta. Pienessäkin yrityksessä kannattaa ohjeistaa myös henkilöstöä noudattamaan varovaisuutta ja suhtautumaan varauksella vaikkapa sähköpostitse saapuviin erikoiselta kuulostaviin pyyntöihin.

Epäilyttävän viestin tuntomerkit voi liittää esimerkiksi yrityksen tietoturvaohjeistukseen. Työntekijöitä

Esimerkki pienen yrityksen yhteisistä tietoturvaohjeista:

1. Varmista, että toimitilat lukitaan aina, kun ketään ei ole paikalla
2. Käytä kaksivaiheista tunnistautumista aina, kun se on mahdollista
3. Lukitse tietokone aina, kun poistut työpisteeltä
4. Käytä vain vahvoja salasanoja ja tallenna ne salasanapankkiin
5. Varmistu henkilöistä, jotka ilmoittavat tekevänsä muutoksia yrityksen järjestelmiin
6. Älä käytä samoja tunnuksia ja laitteita sekä työhön että vapaa-aikaan.

voi ohjeistaa ottamaan yhteyden suoraan esihenkilöönsä, jos heiltä pyydetään viestissä esim. yrityksen maksutietoja, tunnuksia tai salasanoja. Liitetiedostoja, jotka tulevat entuudestaan tuntemattomalta lähettäjältä, pyytämättä tai ovat muuten epäilyttäviä, ei kannata avata.

Jos sattuisi kuitenkin käymään niin, että yrittäjä itse tai joku henkilöstön jäsen on klikannut epäilyttävää linkkiä tai antanut tietoja epäilyttävälle taholle, kannattaa ensimmäisenä ottaa yhteys omaan IT-palveluntarjoajaan. Esimerkiksi Lennun asiantuntijat auttavat ja neuvovat näissä tilanteissa mielellään, ja Lennu tarjoaa myös kattavia tietoturvapalveluita kaiken kokoisille yrityksille.

Tietoturva etätyössä

Yleistyvä etätyö luo uudenlaisia haasteita tietoturvaan. Työntekijällä ei välttämättä ole kotonaan samanlaisia tietoturvajärjestelmiä kuin työpaikalla. Miten huolehditaan turvallisesta tiedonsiirrosta ja kommunikaatiosta?

Oli kyseessä sitten työntekijä tai yrittäjä itse, esimerkiksi kotona ja julkisilla paikoilla voi olla yllättäviä vaaratilanteita. Kahvilassa ulkopuolinen näkee näytöltä asiakastietoja, tai läppäri varastetaan repusta.

Tietoturvariskeihin varautuminen

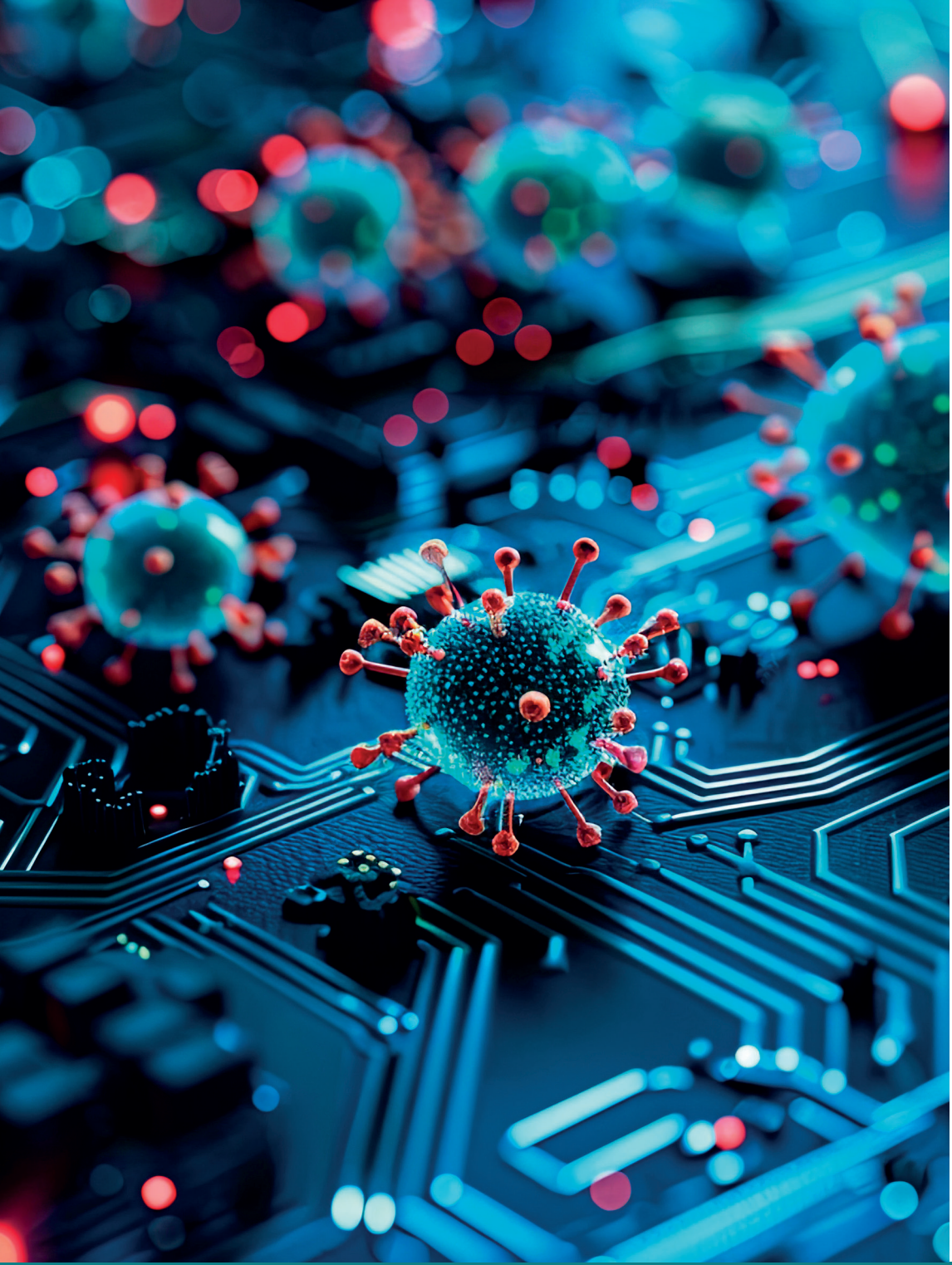
Tietoturvan lähtökohtana voidaan pitää, että tietoturvalla varaudutaan tilanteeseen, jossa riski toteutuu. Tämän vuoksi uhkia tunnistaessa hyvä lähtökohta on usein aloittaa siitä, miten tällaiseen tilanteeseen varaudutaan. Suunnitelman ei tarvitse olla monimutkainen, mutta sen on hyvä olla selkeä ja tallennettuna tai tulostettuna paikkaan, josta myös työntekijät löytävät sen ja voivat noudattaa ohjeita.

Erilaisten tilanteiden varalle kannattaa tutustua esimerkiksi Kyberturvallisuuskeskuksen sivuihin ja sieltä erityisesti tietoturvapoikkeamia varten olevaan toimintaohjeeseen (www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TietomurtoToimintaohje.pdf).
Usein henkilö, organisaatio tai yritys ei edes huomaa mitään epäilyttävää tai huomaa suoraan sitä, että heillä olisi haittaohjelma verkossaan. Yleisimmin tietoturvapoikkeamat huomataan ulkopuolisen tahon, kuten palveluntarjoajan tai esimerkiksi Kyberturvallisuuskeskuksen toimesta.

Tämän lisäksi tilanteissa saattaa yleensä olla monta rautaa tulessa ja tietoturvapoikkeaman sattuessa samaiselta sivulta löydät lomakkeen (www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toimi-nain-jos-havaitset-tietoturvapoikkeaman), joka ohjaa selkeästi mitä tulee tehdä.

Tarkistuslista etätyön tietoturvaan:

1. Käytä näytönsuojakalvoa suojataksesi tiedon, jota käsittelet
2. Lukitse koneesi poistuessasi sen ääreltä, tai ota mieluiten mukaasi anastamisen välttämiseksi
3. Käytä etätyössä aina VPN-yhteyttä
4. Jos mahdollista, vältä julkisia verkkoja ja käytä vain yrityksen tarjoamia yhteyksiä (työpuhelimen yhteyspiste, sim-kortti).



Suunnitelma tietoturvapoikkeaman varalle voi näyttää esimerkiksi tältä:

1. Mitä on tapahtunut? Selvitä tilannekuva ja informoi esihenkilöä.
2. Jos on selvää, että tietoturvapoikkeama on tapahtunut tai haittaohjelma on saastuttanut laitteen tai verkon, on sellaiset laitteet hyvä kytkeä irti verkosta ja muista laitteista, mutta niissä on hyvä pitää virrat päällä ellet ole saanut muuta ohjeistusta.
3. Jos sidosryhmääsi liittyvä järjestelmä, ohjelmisto tai tiedot ovat vaarantuneet, ilmoita heille asiasta.
4. Mikäli laite on yhteydessä muihin laitteisiin tiettyjen tunnuksien avulla, on nämä syytä poistaa käytöstä.
5. Älä poista, tuhoa tai muuta laitteella tai verkossa olevia tietoja - usein näistä on apua silloin, kun poikkeamaa selvitetään.
6. Ota yhteys IT-palveluntarjoajaan, niin saat asiantuntijoilta neuvoja ja apua.
7. Jos epäilet maksuliikennetietojesi vaarantuneen, estä niiden käyttö.
8. Älä tee muutoksia järjestelmiin ilman ohjeistusta.
9. Tee tarvittaessa rikosilmoitus.
10. Tee tarvittaessa ilmoitus kyberturvallisuuskeskukseen.
11. Ota yhteyttä palveluntarjoajaan, jos epäilet tietoturvapoikkeaman tapahtuneen.

Tarkistuslista pienyrittäjän tietoturvaan

Nyt olemme käyneet läpi kaikki pienyrittäjän tietoturvan tärkeimmät kohdat. Auttaaksemme sinut alkuun oman tietoturvasi kokonaisuuden rakentamisessa, kokosimme tähän vielä lyhyen tarkistuslistan pienyrittäjän tietoturvasta.

Tarkistuslista tietoturvaan

- [ ] **Tiedän, mikä yrityksessäni on sellaista tietoa, joka ei saa joutua ulkopuolisten käsiin.**
  Näitä voivat olla esimerkiksi asiakastiedot, yrityksen luottokorttien numerot ja kirjanpidon tiedot.

- [ ] **Säilytän yritykseni tärkeitä tietoja turvallisessa sijainnissa ja tiedän, miten ne on suojattu.**
  Onko käytössä pilvipalvelu vai arkistokaappi? Tiedäthän, missä tietojasi säilytetään?

- [ ] **Yritykseni verkko ja laitteet on suojattu salasanoin ja palomuurein.**
  Kysy Lennun asiantuntijoilta hyvistä turvallisista ratkaisuista!

- [ ] **Tiedän, kenellä on pääsy yritykseni tietoihin sekä ketkä kaikki voivat lukea ja muokata tietoja.**
  Onhan kaikilla työntekijöillä omat tunnukset käyttämiisi palveluihin, vahvat salasanat ja kaksivaiheinen tunnistautuminen käytössä?

- [ ] **Yritykselleni on määritetty yhteiset tietoturvakäytännöt.**

Tietoturvakartoitus

Haluatko, että asiantuntijamme tekee tietoturvakartoituksen puolestasi?

Lue lisää verkkosivuiltamme: lennu.fi/yrityksille/muut-palvelut/tietoturvakartoitus

Yrityksesi turvallinen kiitotie kasvuun

lennu it

Lennusti vaan.

Soita tai laita viestiä
yritysasiakaspalveluumme (ark. 8–16):

03 450 5590

yritysmyynti@lennu.fi

lennusti lennunet lennu-it