

Pienyritysten kyberturvallisuusopas



Sisällys

Johdanto	3
1 Yleisimmät kyberuhat pienyritysten haittana	4
1.1 Tietojenkalastelu	4
1.2 Haittaohjelmat	7
1.3 Kiristyshaittaohjelmat	8
2 Suojautumiskeinoja	10
2.1 Automaattiset päivitykset	10
2.2 Automaattiset kopiot	11
2.3 Monivaiheinen tunnistautuminen	12
3 Kohti parempaa kyberturvaa	13
3.1 Käyttöoikeuksien hallinta	14
3.2 Salalause	15
3.3 Harjoitus- ja koulutustoiminta	16
4 Muistilista	17
5 Sanasto	18

Osiot täydentävät toisiaan ja asioita käsitellään kattavammin sille varatun otsikon alla. Esimerkiksi uhka-osion alla ei avata suojautumiskeinoja otsikkotasoa enempää. Näitä on avattu enemmän Suojautumiskeinoja-osion alla. Olemme koonneet ohjeeseen myös erillisiä lisäohjeita,

jotka löytyvät esimerkiksi Kyberturvallisuuskeskuksen sivuilta. Pääset linkkien kautta lisäohjeisiin.

Jos et ehdi lukea koko opasta nyt, niin olemme koneet lyhyen muistilistan, jonka avulla pääset alkuun:



Pidä laitteet, järjestelmät ja ohjelmistot päivitettyinä.



Riittävän pitkä salasana tai lause ja monivaiheinen tunnistautuminen palveluihin.



Rajaa käyttäjiltä oikeudet tarpeen mukaan.



Maltilta on valttia.



Jos joudut tietoturvapoiikkeaman tai sen yrityksen kohteeksi, ilmoita Kyberturvallisuuskeskukselle.

Johdanto

Tämä opas auttaa pienyrittäjiä ja pienyrityksiä – alle 50 työntekijän yrityksiä – suojautumaan yleisimpiä kyberuhkia vastaan. Pienyrityksiin kohdistuvat kyberuhkat voivat toteutuessaan aiheuttaa yritystoiminnalle merkittävää haittaa ja pahimmillaan johtaa liiketoiminnan keskeytymiseen. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus saa päivittäin ilmoituksia, joissa kerrotaan kyberturvallisuuden vaarantumisesta. Kyberuhkat koskettavat kaikenlaisia organisaatioita – isoja ja pieniä.

Kun yrityksen arki pyörii normaalisti, kaikki toimii ja työntekijät voivat esimerkiksi käyttää työ sähköpostia ja tarvitsemiaan toimisto-ohjelmistoja sujuvasti. Tilanne muuttuu vakavaksi, kun yritys joutuu yllättäen tietoturvaloukkauksen uhriksi. Voivatko sähköpostin käyttäjätunnus ja salasana päätyä väärin käsiin? Miten toimitaan, jos yrityksen tietokoneelle tulee kiristyshaitta-ohjelma, joka lukitsee koneen ja estää sen käytön? Mitä jos tietoja ei ole varmuuskopioitu, ja niiden palauttaminen ei ole mahdollista? Taloudellisten tappioiden lisäksi tilanteesta voi kärsiä yrityksen maine.

Onneksi kyberturvallisuuden ei tarvitse olla vaikeaa. Monilla pienillä teoilla omasta toiminnastaan voi tehdä turvallisempaa ja välttää yleisimmiltä uhilta. Sen lisäksi, että huolehdit omasta kyberturvallisuudestasi, vaikuttavat tekemäsi toimenpiteet positiivisesti myös asiakkaiden ja sidosryhmien kyberturvallisuuteen. Lukemalla tämän oppaan pääset jo pitkälle. Olemme keränneet tähän oppaaseen muutamia yleisimpiä yritysten kyberturvallisuutta vaarantavia tekijöitä, sekä keinoja suojautua niitä vastaan.

Jos organisaatiosi joutuu tietoturvaloukkauksen kohteeksi, kannattaa tapahtuneesta ilmoittaa heti Kyberturvallisuuskeskukselle.

Kyberturvallisuuskeskus neuvoo:

- tilanteen hahmottamisessa
- lisävahinkojen estämisessä
- tilanteesta toipumisessa.

Ilmoitusten kautta saamiensa tietojen avulla Kyberturvallisuuskeskus voi esimerkiksi varoittaa muita organisaatioita. Kyberturvallisuuskeskus ei paljasta yksilöiviä tietoja ilman tietoturvaloukkauksen kohteen lupaa.

Voit ottaa yhteyttä

Kyberturvallisuuskeskukseen:

- Ilmoitus tietoturvaloukkauksesta -lomakkeella <https://www.kyberturvallisuuskeskus.fi/fi/ilmoita>
- Sähköpostilla osoitteeseen cert@traficom.fi
- Puhelimella numeroon 0295 345 630 (pvm/mpm) (arkisin kello 9-15)

Kyberturvallisuuskeskuksen palvelut ovat maksuttomia ja kuuluvat kaikille. Lisätietoa kaikista Kyberturvallisuuskeskuksen palveluista löydät osoitteesta <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme>

Opas perustuu Australian kyberturvallisuusviranomaisen tuottamaan materiaaliin Small Business Cyber Security Guide. Oppaassa käytetyt termit on avattu hyödyntäen TEPA-termipankin termejä. Lisää tietoa termeistä <https://termipankki.fi/tepa/fi/>

1 Yleisimmät kyberuhat pienyritysten haittana

Pienyrityksille vähäisestäkin kyberturvallisuustapahtumasta voi aiheutua merkittäviä, ei-toivottuja vaikutuksia. Tässä osiossa kerromme yleisimmistä kyberuhkista ja mitä voit tehdä turvataksesi yrityksesi toiminnan.

1.1 Tietojenkalastelu



Mitä?

Aidolta näyttävä viesti, jonka tarkoituksena on huijata viestin vastaanottajalta rahaa tai tietoa tai saada pääsy vastaanottajan järjestelmään.

Tietojenkalasteluviestit näyttävät tulevan yleensä henkilöltä tai organisaatiolta, jonka tiedät tai tunnet. Viestit jäljittelevät oikeiden organisaatioiden ulkoasua, esimerkiksi logoa, jotta viesti olisi mahdollisimman todentuntuinen. Rikollisen on myös mahdollista murtaa kokonaan jonkun toisen käyttäjän tili. Tällöin viestit saattavat tulla suoraan tuntemasi henkilön tai organisaation sähköpostista.

Haitallisia linkkejä liikkuu sähköpostin lisäksi myös sosiaalisessa mediassa ja internetsivustoilla. Niitä saatetaan levittää myös tekstiviesteillä ja erilaisten pikaviestimien kautta.

Kuka?

Uhriksi kelpaa kuka tahansa, jolta voi saada esimerkiksi rahaa tai arvokasta tietoa – riittää, että pieni osa kohteista haksahtaa.

Kalasteluviestejä lähetetään tavallisesti massapostina tuhansille eri ihmisille ja organisaatioille. Vaikka prosentuaalisesti vain pieni osa viestin vastaanottajista avaa haitallisen liitteen tai klikkaa linkkiä, voivat rikolliset saada haltuunsa paljon erilaista tietoa sekä sievoisen summan rahaa.

- **Tietojenkalastelu** (Phishing) avulla pyritään vaikuttamaan käyttäjään ja saamaan hänet antamaan sähköpostin tai verkkosivun

välityksellä luottamuksellista tietoa. Tietojenkalastelu voi tapahtua esimerkiksi niin, että käyttäjältä pyydetään pankin nimissä sähköpostitse luottokortin numeroa ja tunnuslukua.

- **Kohdennettu tietojenkalastelu** (Spear Phishing) on tiettyyn henkilöön tai tietyn organisaation henkilöstöön kohdistuvaa verkkourkintaa, joka vaikuttaa tulevan tutulta taholta. Kohdennettu verkkourkinta voi tapahtua esimerkiksi siten, että kohteelle lähetetään sähköpostiviesti, joka näyttää tulevan pankilta, työtoverilta tai esimieheltä, jolloin urkinnan kohde ei osaa olla varovainen ja saattaa lähettää luottamuksellista tietoa urkkijalle.
- **Toimitusjohtajahuijaus** (CEO Fraud) rikollinen esiintyy yleensä yrityksen johtajana ja lähestyy yrityksen rahaliikenteestä vastaavaa työntekijää. Viestin lähettäjän tiedot saattavat näyttää hyvin aidolta, jolloin lähettäjän viestiä ei osata heti epäillä huijaukseksi. Tarkoituksena on saada työntekijä maksamaan valesuku tai tekemään muu, usein kiireellinen tilisiirto tai palkanmaksu, joka päättyy huijarille.

Missä?

Sähköposti, tekstiviesti, pikaviestit, sosiaalinen media

Tietojenkalastelua tehdään useissa eri kanavissa ja kohteena voivat olla myös erilaiset palvelut. Esimerkiksi sosiaalisen median tilit voivat tietojenkalastelun seurauksena päätyä väärin käsiin. Tietojenkalastelu on kehittynyttä ja joistakin huijausviesteistä on erittäin vaikea päätellä, että kyseessä on huijaus. Myös taitavasti tehtyjä suomenkielisiä huijausviestejä on liikkeellä. Viesteissä saatetaan vedota inhimilliseen tekijään kuten tunteisiin tai kiireeseen, jotta huijaus saadaan onnistumaan.



Ole erityisen tarkkana

- kun saat kiireellisen tilisiirtopyynnön.
- kun saat ilmoituksen tilitietojen muutoksesta.
- kun avaat sähköpostiliitteitä.
- mikäli viestissä pyydetään tarkistamaan tai varmistamaan kirjautumistiedot palveluun.
- mikäli avaat liitteen kirjautumalla tunnuksillasi palveluun. Tarkista linkin todenmukaisuus ja se, että kirjaudut oikeaan paikkaan.



Suojautuminen

- Jos saat linkin palveluntarjoajalta ja pyynnön kirjautua sivuille nopeasti, suosittelemme lähetetyn linkin sijaan kirjautumaan palveluntarjoajan oman verkkosivun kautta ja siten varmistamaan, onko viesti aito.
- Jos et ole varma vastaanottamasi viestin lähettäjästä tai sen sisällöstä, varmista asia esimerkiksi soittamalla viestin lähettäjälle. Katso yhteystiedot muualta kuin lähetetystä viestistä (esim. virallisilta verkkosivuilta).
- Jos epäilet linkin aitoutta, älä klikkaa.
- Ole terveen epäluuloinen. Epäilyksen tulisi herätä, jos saat pikaisen pyynnön kirjautua palveluntarjoajan sivuille, maksaa lasku tai muuttaa tilitietoja.



Esimerkki Microsoft Office 365 -huijausviestistä.



Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta:

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/suojautuminen-microsoft-office-365-tunnusten-kalastelulta-ja>

Näin suojaudut tietomurroilta:

<https://www.kyberturvallisuuskeskus.fi/fi/nain-suojaudut-tietomurroilta>

Neuvoja epäilyttävien sivujen tunnistamiseksi:

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-epailyttavien-sivujen-tunnistamiseksi>



1.2 Haittaohjelmat

Mitä?

Ohjelmisto, jonka tarkoituksena on aiheuttaa harmia

Haittaohjelma on yleiskäsite ohjelmalle, joka tarkoituksella aiheuttaa koneen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Olet saattanut törmätä esimerkiksi mediassa sanoihin virus, vakoiluohjelma, troijalainen tai mato. Nämä ovat nimiä erilaisille haittaohjelmatyypeille.

Miksi?

Häirintä. Vahingonteko. Huijaaminen.

Usein syy haittaohjelman asentamiselle on taloudellinen hyöty. Haittaohjelma voidaan esimerkiksi asentaa varastamaan tärkeää tietoa, kuten pankkitunnuksia tai salasanoja, louhimaan luvatta virtuaalivaluutta tai seuraamaan tietokoneen käyttäjän toimintaa.

Haittaohjelman avulla rikollisen on mahdollista esimerkiksi vakoilla tai ottaa tietokone haltuunsa. Haittaohjelman avulla rikollinen voi esimerkiksi

- varastaa tietoa
- salata tiedostoja
- vakoilla
- tehdä muuta vakavaa rikollista toimintaa.

Kuka?

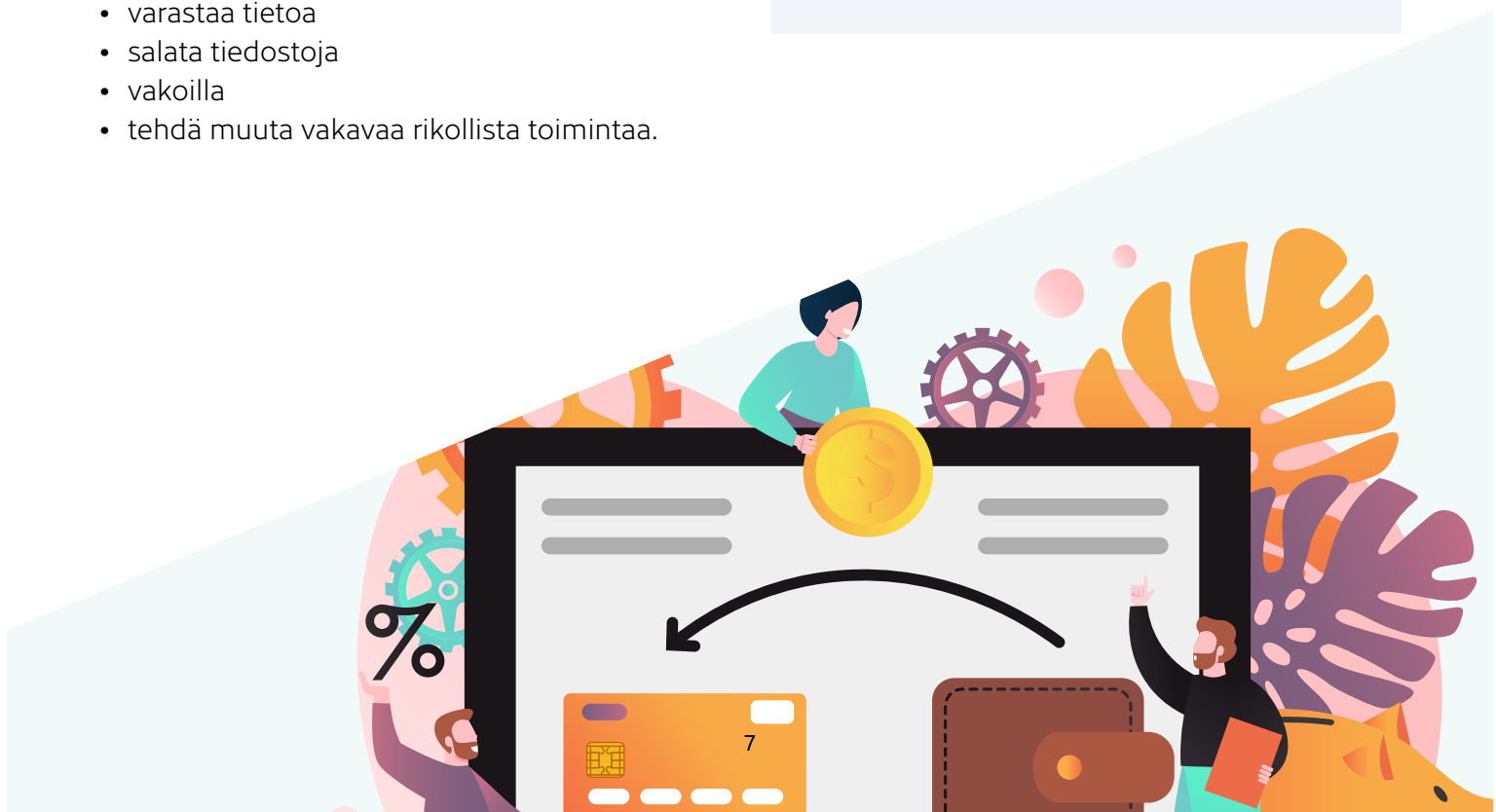
Uhriksi voi joutua kuka tahansa, missä tahansa

Haittaohjelman tekijä voi olla mistä päin maailmaa tahansa. Tarvitaan vain tietokone, teknistä osaamista ja pahat aikeet. Kohde on valittu useimmiten siksi, että sen tietoihin on päästy tunkeutumaan helposti.



Suojautuminen

- Pidä käyttöjärjestelmät päivitettyinä.
- Pidä ohjelmistot päivitettyinä.
- Ota varmuuskopiot.
- Suhtaudu sähköpostiliitteisiin ja linkkeihin terveellä epäluulolla.
- Älä käytä järjestelmiä pääkäyttäjänä. Luo käyttäjille omat tilit, joilla ei ole pääkäyttäjien oikeuksia. Vähemmän oikeuden periaatteesta kerrotaan lisää myöhemmin.





1.3 Kiristyshaittaohjelma

Mitä?

Kiristyshaittaohjelma, joka lukitsee tietokoneesi ja tiedostot, ja vaatii lunnaita

Kiristyshaittaohjelma pääsee tietokoneelle useissa tapauksissa aidolta näyttävän sähköpostin välityksellä, jossa viestin mukana tulee linkki tai liitetiedosto. Kun liite avataan tai linkkiä klikataan, kiristyshaittaohjelma pääsee koneelle ja estää tietokoneen käytön salaamalla tietokoneen tiedostot. Tällä tarkoitetaan sitä, että kiristyshaittaohjelma esimerkiksi muuntaa joitakin tiedostoja salakirjoitetuun muotoon. Näitä tiedostoja ei voi avata ilman oikeaa salauksenpurkuavainta. Usein rikollinen lupaa, että maksamalla tietyn summan salaus poistetaan tai uhri saa salauksenpurkuavaimen. Summa pyydetään usein virtuaalivaluuttana (esim. bitcoin). Tällaisessa tilanteessa ei ole takeita, että tiedostot palautetaan lunnaiden maksun jälkeen. Tiedot voidaan myös jakaa myöhemmin, vaikka lunnaat olisi maksettu.

Oman digitaalisen ympäristön tunteminen on tärkeää. Verkkoon voi olla liitettyä erilaisia laitteita, joita ei ole suojattu esimerkiksi salasalla tai ne näkyvät tarpeettomasti julkisena. Laitteessa voi olla esimerkiksi langaton internet-yhteys, johon laite on liitetty. Jos laitetta ei ole suojattu salasalla tai laitteen oletussalasanaa ei ole muutettu, rikollinen pääsee helposti laitteelle käsiksi myös etänä. Tällainen laite, kuten tulostin, voi suojaamattomana tarjota reitin rikolliselle sisälle yrityksen verkkoon.

Tee poliisille rikosilmoitus, jos epäilet joutuneesi tai olet joutunut onnistuneen tietomurron, tietojenkalastelun tai kiristyshaittaohjelman uhriksi.

www.poliisi.fi

Miksi?

Taloudellinen motiivi

Erilaisia lunnasvaatimuksia on esitetty kautta aikojen rikosten yhteydessä. Nyt rikokset ja lunnasvaatimukset ovat siirtyneet verkkoon. Kiristyshaittaohjelma on rikolliselle tuottoisa tapa toteuttaa rikos ja sen riskit ovat vähäiset. Kiristyshaittaohjelma on helppo toteuttaa ja kohdentaa kerta toisensa jälkeen eri vastaanottajille.

Kuka?

Pienet, keski- ja suuret yritykset

Kuka tahansa voi joutua rikollisten uhriksi. Rikollisten näkökulmasta pienyritykset ovat helppo kohde, sillä ne eivät yleensä ole varautuneet kyberhyökkäyksiin hyvin. Monet pienet yritykset eivät ole yhtä tietoisia omasta tietoturvas- taan kuin suuremmat yritykset, ja pienempien resurssien vuoksi ne toteuttavat todennäköisesti vähemmän tietoturvatointimenpiteitä.



Suojautuminen

- Pidä käyttöjärjestelmät päivitettyinä.
- Pidä ohjelmistot päivitettyinä.
- Ota varmuuskopiot.
- Suhtaudu sähköpostiliitteisiin ja linkkeihin terveellä epäluulolla.
- Älä käytä järjestelmiä pääkäyttäjänä. Luo käyttäjille omat tilit, joilla ei ole pääkäyttäjien oikeuksia. Vähemmän oikeuden periaatteesta kerrotaan lisää myöhemmin.
- Tunne ympäristösi ja tarkista, ettei tarpeettomia palveluita näy julkisena internetiin.



Jos koneellesi tulee kiristyshaittaohjelma ja saat lunnasvaatimuksen, älä maksa lunnaita!

Kyberturvallisuuskeskus ei suosittele maksamaan lunnaita, jotka rikollinen käskää maksamaan ongelman ratkaisemiseksi. Ei ole mitään takeita, että ongelma ratkeaa

maksun jälkeen. Lisäksi on mahdollista, että rahavaatimusten määrä kasvaa tai rikollinen tekee toisen hyökkäyksen, eikä palveluita saada takaisin omaan käyttöön. Lisäksi lunnaiden maksaminen kannustaa rikollisia jatkamaan vastaavaa toimintaa muuallakin – et kai halua rahoittaa rikollista toimintaa?

2 Suojautumiskeinoja

On erittäin tärkeää pitää järjestelmien ja laitteiden päivitykset ajan tasalla. Suuri osa ohjelmistopäivityksistä sisältää haavoittuvuuksien korjauksia, joiden avulla korjataan edellisen version turvallisuuspuutteita. Päivitykset on syytä asentaa pian niiden julkaisemisen jälkeen. Ohjelmistopäivitykset ovat saatavilla sovelluskaupasta, palveluntarjoajan sivuilta tai automaattisen päivityksen kautta, josta tietokoneesi ilmoittaa. Päivittämättömillä järjestelmillä on aina suurempi riski joutua tietomurron kohteeksi, koska rikolliset hyödyntävät vanhentuneissa ohjelmistoissa olevia turvallisuuspuutteita. Pitämällä päivitykset kunnossa pidät myös rikolliset loitolla.

Esimerkiksi käyttöjärjestelmä on tärkeä ohjelmisto tietokoneessasi. Se hallitsee tietokoneesi laitteistoa ja kaikkia sen ohjelmia. Siksi se on tärkeä päivittää ja pitää ajan tasalla. Lisäksi on tärkeä tehdä säännöllisesti varmuuskopiointi tietokoneesi tiedostoille.

Seuraavien vinkkien avulla voit lisätä omien laitteiden ja käyttämiesi järjestelmien turvallisuutta.

2.1 Automaattiset päivitykset



Mitä?

Ohjelmiston päivitykset

Useimmat ohjelmat tarjoavat automaattisia päivityksiä, jolloin sinun ei itse tarvitse etsiä uusinta päivitystä ja tietää itse milloin sellainen on saatavilla. Samalla voit olla varma, että käyttämäsi ohjelmistot ovat ajantasaisia eivätkä päivitykset unohdu. Yleensä automaattinen päivitys otetaan käyttöön ohjelman asetuksista.

Päivitystä vaativat esimerkiksi käyttöjärjestelmä sekä erilaiset sovellukset, kuten sähköposti, toimisto-ohjelmat ja PDF-lukija.

Miksi?

Turvallisemmin, nopeammin, paremmin

- Parempi tietoturva.
- Parempi suoja rahan ja tiedon menetykseltä tai identiteettivarkaudelta.
- Parannetut ominaisuudet ja tehokkaammat järjestelmät.

Milloin?

Päivittäin

- Ota automaattiset päivitykset käyttöön ohjelman asetuksista.
- Tee tietoturvasta rutiinia: asenna manuaaliset päivitykset välittömästi, jos automaattisia päivityksiä ei ole saatavilla.
- Jotta työnteke ei keskeydy päivitysten takia, voit ajastaa ne sinulle sopivaan ajankohtaan.
- Varmista myös, että haittaohjelman torjuntaohjelmistoon on aktivoituna automaattiset päivitykset.

Huom!

Kun ohjelmisto tai laite tulee elinkaarensa päähän (end-of-life, EOL), valmistaja ei enää tuota siihen päivityksiä. Tässä vaiheessa laite tai ohjelmisto pitää vaihtaa päivitettyyn versioon tai täysin uuteen, jonka kehitystä ja turvallisuutta valmistaja tukee. Elinkaari kannattaa huomioida jo hankintahetkellä. Katso ohjeesta lisää:

<https://www.kyberturvallisuuskeskus.fi/ajankohtaista/kaytosta-poistuvien-palveluiden-alasajo-tulee-tehda-huolella>



2.2. Automaattiset varmuuskopiot

Mitä?

Tietojen varmuuskopiot

Varmuuskopio on digitaalinen kopio yrityksesi toiminnalle keskeisistä tiedoista ja palveluista kuten asiakastiedoista. Tee tärkeimmistä tiedoista sekä palveluista varmuuskopiot. Säilytä varmuuskopiot erillään suojattavista järjestelmistä ja tiedoista, esimerkiksi fyysisesti verkosta irti olevalla kiintolevyllä (kovalevy), ettei esimerkiksi kiristyshaittaohjelma tee myös varmuuskopioista käyttökelvottomia.

Testaa varmuuskopioiden palauttamista säännöllisesti, esimerkiksi neljännesvuosittain. Näin varmistut, että varmuuskopioiden palauttaminen onnistuu ja tarvittavat tiedot on varmuuskopioitu.

Miksi?

Turvallisemmin ja nopeammin

- Tietojen palauttaminen onnistuu nopeasti ja helposti, jos niistä on tehty varmuuskopiot. Näin tietojen palautus on mahdollista, mikäli ne ovat kadonneet, varastettu tai tuhoutuneet.
- Varmuuskopiointi suojaa yrityksesi uskottavuutta ja auttaa täyttämään mahdolliset lailliset velvoitteet.
- Saat mielenrauhaa siitä, että yrityksesi tiedot ovat suojattu ja käytettävissä, jotta voit keskittyä työn tekemiseen.

Milloin?

Tänään ja joka päivä

- Valitse yrityksellesi sopiva palvelu tai ohjelma, jonka avulla saat otettua varmuuskopiot tärkeistä tiedoista.
- Varmista säännöllisesti, että saat palautettua tiedot käyttöösi.
- Talleta fyysinen varmuuskopio (esim. kovalevy, jonne tiedot on tallennettu) johonkin turvalliseen paikkaan, joka ei ole samassa paikassa tietokoneen kanssa.

Huom!

Joillakin toimialoilla on velvoite säilyttää dokumentaatioita tietty aika (esimerkiksi verotus- ja laskutustiedot). Tarkistathan tietojen tallennusajan oman yrityksesi osalta ja huomioit asian varmuuskopioita tehdessä, jotta tarvittava tieto on tallessa ja palautettavissa.





2.3 Monivaiheinen tunnistautuminen

Mitä?

Turvallisuustoimenpide, joka vaatii kahden tai useamman todennustekijän käytön, jotta kirjautuminen järjestelmään on mahdollista.

Monivaiheinen tunnistautuminen tarkoittaa sitä, että henkilön identiteetti varmistetaan useampaa eri tunnistautumistapaa käyttämällä. Sähköinen tunnistaminen perustuu kolmelle pilarille, jotka ovat:

1. Jotain mitä tiedän (esim. salasana)
2. Jotakin mitä omistan (esim. matkapuhelimeen lähetettävä muuttuva koodi, kuten mobiilivarmenne)
3. Jotakin mitä olen (esim. sormenjälki tai muu käyttäjän yksilöivä ominaisuus)

Kahden kolmesta todennustavasta on toteutettava, jotta tunnistus on riittävä.

Mikäli käyttäjätunnus ja salasana päätyvät rikollisen haltuun, tulee hänen saada haltuunsa vielä monivaiheisen todentamisen kertakäyttökoodi tai vastaava tieto onnistuakseen tietomurrossa.

Miksi?

Parantaa turvallisuutta

Kaksivaiheinen tunnistautuminen (Two-factor Authentication, 2FA) on yleisin monivaiheisen tunnistautumisen muoto. Sen käyttöönotto hankaloittaa merkittävästi rikollisten mahdollisuuksia hyödyntää tietojenkalastelua. Rikolliset voivat saada käsiinsä esimerkiksi salasanan palveluun, mutta eivät pääse kirjautumaan, koska heillä ei ole toista todentamiseen vaadittavaa tietoa käytössään.

Missä?

Ota monivaiheinen tunnistautuminen käyttöön kirjautuessasi tärkeisiin yrityksen sisäisiin ja ulkoisiin palveluihin.

Pienyritysten on suositeltavaa käyttää monivaiheista tunnistautumista aina kun se on mahdollista. Monivaiheinen tunnistautuminen, joka pohjautuu vähintään kahteen todennustekijään voi pitää sisällään:

- salasanan
- todennuslaitteen (esim. tunnuslukulaite, joita pankeilla on käytössä) tai suojaus-avaimen (ns. token)
- sormenjälkitunnisteen
- vahvistusviestin sähköpostiin tai tekstiviestillä
- muuttuvan PIN-koodin
- todennussovelluksen.



3 Kohti parempaa kyberturvaa

Yrityksen pitää koosta riippumatta olla tietoinen omasta tietoturvastaan.

Pienissä yrityksissä yksi ihminen vastaa useasta eri asiasta ja on samaan aikaan yrityksen toimitusjohtaja, myyjä ja tietoturvastaa-va. Yhden ihmisen ollessa vastuussa monesta asiasta, aika on kortilla eikä kaikkea ehdi tehdä. Tässä osiossa kerromme, mitä toimia voit tehdä hallitaksesi paremmin yrityksesi tietoturvaa.

Ennaltaehkäisevillä toimilla tavoitellaan tilannetta, jossa organisaatio on hyökkääjän näkökulmasta kannattamaton kohde. Tällöin hyökkäys on hankala toteuttaa, koska organisaatio kykenee estämään, havaitsemaan ja tarvittaessa reagoimaan kyberturvallisuus-uhkiin juuri oikealla tavalla.





3.1 Käyttöoikeuksien hallinta

Mitä?

Käyttö- ja pääsyoikeuksien hallinta: Kenellä on oikeus päästä yrityksen käyttämissä järjestelmissä olevaan tietoon.

Käyttöoikeuksien antaminen erilaisille käyttäjäryhmille on tapa rajoittaa tiedon saamista sellaisilta henkilöiltä, joilla ei ole tarvetta saada kyseistä tietoa työtehtävänsä puitteissa.

- Päättää kuka tarvitsee mitään tietoa ja kenelle pääsyoikeus halutaan myöntää.
- Mikäli yrityksessä on useampi työntekijä, määrittele eritasoisia käyttöoikeuksia järjestelmiin ja niissä oleviin tietoihin.
- Valvo käyttäjäoikeuksien toteutumista.

Miksi?

Riskien vähentäminen – henkilöstö, jolla ei ole tarvetta tietoon, ei tarvitse pääsyoikeutta siihen.

Usein pienyritykset ovat ulkoistaneet osan palveluistaan ulkoisille toimijoille, esimerkiksi verkkosivustojen ylläpitoyrityksille. Onkin hyvä pohtia, millaiset käyttöoikeudet omilla työntekijöillä tai ulkoistetuilla palveluntarjoajilla on yrityksen hallussa olevaan tietoon, kuten:

- tietoverkkoihin
- kansioihin
- sovelluksiin
- yrityssalaisuuksiin tai muihin arkaluonteisiin tietoihin.

Huomioi yllä olevat esimerkit yrityksen omalla palvelimella ja/tai pilvipalvelimella.

Kuka?

Vähemmän oikeuden periaate

Riippuen yrityksesi koosta ja luonteesta, on aihetta hyvä lähestyä rajatun käyttöoikeuden periaatteen kautta. Sen tarkoituksena on, että työntekijöiden tulee voida tehdä työnsä, mutta käyttöoikeuksien ei tarvitse olla laajat vaan kattaa ne osa-alueet, jotka mahdollistavat työn tekemisen tehokkaasti. Samalla voidaan vähentää ihmisten aiheuttamaa riskiä esimerkiksi sellaisessa tilanteessa, jossa organisaation sisältä tuleva henkilö haluaa vahingoittaa yrityksen toimintaa.

Mikäli yritykseesi kohdennetaan tunnusten kalastelua ja rikollinen onnistuu yrityksessään, vähemmän oikeuden periaate voi suojata yritystäsi. Jos oikeudet ovat rajattuja, ei väärissä käsissä olevalla tilillä pystytä aiheuttamaan niin suuria vahinkoja.



Tarkista

- Rajoita pääkäyttäjaoikeuksia – pääkäyttäjaoikeuksia ei tarvita päivittäisessä työssä.
- Älä jaa kirjautumistietoja.
- Älä käytä yhteiskäyttötunnuksia.
- Muista poistaa käyttöoikeudet henkilöiltä, joilla ei ole niille enää tarvetta, kuten entiset työntekijät ja palveluntarjoajat.

3.2 Salalause



Mitä?

Pidempi on parempi – käytä salasanan sijaan salalausetta.

Salalausetta käytetään salasanan tavoin, mutta se on pidempi. Salalausetta käytetään erilaisiin palveluihin ja järjestelmiin. Salalause on erityisen tehokas, kun sitä käytetään yhdessä monivaiheisen tunnistautumisen kanssa.



Hyvä salalause on:

- **Yksilöllinen** – Samaa salalauseetta ei käytetä useissa eri palveluissa eikä sitä ole otettu tunnetusta kappaleesta tai sanonnasta.
- **Pitkä** – Salalause on vaikeampia arvata, jos siinä käytetään yksittäisten sanojen sijaan kokonaista lausetta.
- **Monimutkainen** – Salalause sisältää erikokoisia kirjaimia, sekä erikois-merkkejä ja numeroita.
- **Helppo muistaa** – Salalause on helpompi muistaa, jos sen taustalle kehittää itselleen helposti muistettavan systeemin tai käytä apuna salasanojen hallintaohjelmaa.

Lue lisää:

<https://www.kyberturvallisuuskeskus.fi/fi/ajan-kohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-tee-hyvan-salasanan>

Miksi?

Turvallisuus parantuu käyttämällä salalausetta.

- Vaikeampi murtaa kuin tavallinen salasana.
- Helpompi muistaa kuin salasana, jossa on käytetty satunnaisesti erilaisia merkkejä.
- Täyttää erilaiset salasanavaatimukset vaivattomasti.

Missä?

Kaikissa palveluissa, joissa salasanaa käytetään

Moneen internetissä käytettyyn palveluun on kohdistunut suuria salasanavuotoja. Jopa miljoonia käyttäjätunnus-salasana-pareja on vuodettu yleisesti saataville. Käyttämällä eri salasanoja jokaisessa eri palvelussa voit estää vuotaneiden tunnusten laajemman väärinkäytön. Suosittelemme käyttämään salasanojen muistamista helpottavaa salasanan hallintaohjelmaa sekä kaksi- tai monivaiheista tunnistautumista niissä palveluissa, joissa se on mahdollista.

Kaksivaiheista tunnistautumista tukevat yhä useammat palvelut, kuten monet sosiaalisen median kanavat (esim. Facebook, LinkedIn ja Twitter) ja sähköpostiohjelmat (esim. Gmail ja Microsoft Office 365). Voit katsoa, onko käyttämälläsi palvelulla kaksivaiheista tunnistautumista menemällä palvelun asetuksiin ja katsoamalla mitä yksityisyys- tai turvallisuusasetuksia palvelusta löytyy.





3.3 Harjoitus- ja koulutustoiminta

Mitä?

Tarjota henkilöstölle koulutusta, jotta he osaat toimia työssään tietoturvalisest.

Tee yrityksellesi suunnitelma tietoturvapoiikkeamien hallitsemiseksi. Suunnitelmasta tulisi käydä ilmi ainakin seuraavat asiat

- miten tietoturvahäiriöihin varaudutaan
- miten vahinkoja rajoitetaan, jos yritys joutuu tietoturvaloukkauksen uhriksi
- miten yritys toipuu tietoturvahäiriöstä.

Yrityksen kannattaa luoda jokin prosessi, jonka avulla sen käyttämät järjestelmät sekä henkilöstö voivat ilmoittaa tietoturvapoiikemista yrityksen toimintaympäristössä. Tietoturvapoiikema-ilmoituksen teko opettaa henkilökuntaa

- tunnistamaan
- välttämään
- raportoimaan
- poistamaan
- toipumaan.

Miksi?

Työntekijällä on tärkeä rooli yrityksen tietoturvan edistämisessä

Me kaikki teemme virheitä, mutta niistä voi ottaa myös opiksi. Jokainen henkilöstöön kuuluva voi vaikuttaa yrityksen kyberturvallisuuteen. Yrityksen tulee tarjota työntekijöilleen koulutusta, jotta henkilöstöllä on tarvittavat taidot toimia oikein, kun yrityksen kyberturvallisuus on uhatuna. Koulutuksen avulla parannetaan kyberturvallisuutta ja turvataan tärkeiden tietojen, kuten asiakastietojen salassapysyminen.

Milloin?

Tee kyberturvallisuudesta jokapäiväistä ja harjoittele säännöllisesti.

Kyberturvallisuus kehittyy jatkuvasti. Pitämällä henkilöstön tietotaidot ajan tasalla voidaan vaikuttaa siihen, onko yritys helppo vai haastava kohde rikollisille.

Tee kyberturvallisuudesta osa päivittäistä työntekoa.

- Ota kyberturvallisuuteen liittyvät asiat osaksi jokapäiväistä toimintaa, päivitä tietoja ja harjoittele tasaisin väliajoin.
- Tee tietoturvapoiikkeamien hallintamalli, esimerkiksi tapa, jolla tietoturvapoiikkeamista ilmoitetaan.
- Palkitse työntekijöitä siitä, että he raportoivat poiikkeamista.

Harjoittelua on jo sekin, että yritystä uhkaavia tilanteita mietitään vaikka kahvikupin äärellä.

Katso lisää vinkkejä ja käytännön esimerkkejä harjoitteluun alla olevista oppaista tai

<https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta>

Kyberharjoitusohje. Käsikirja harjoituksen järjestäjälle. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf>

Kyberharjoitusskenaariot 2020. Skenaarioesimerkkejä harjoituksen järjestäjälle <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusskenaariot2020.pdf>

4 Muistilista

Ohjelmistot ja käyttöjärjestelmät

- Ota käyttöjärjestelmien ja ohjelmistojen automaattiset päivitykset käyttöön.
 - Valitse sinulle sopiva aika päivityksen käynnistymiselle.
- Tee säännöllisin väliajoin varmuuskopiot.
 - Säilytä varmuuskopiot erillisessä paikassa ja erillisellä laitteella, joka ei ole koko ajan yhdistettynä tietokoneeseesi.
- Testaa varmuuskopioiden palauttamista esimerkiksi kerran kuussa tai kvartaalissa.
- Ota käyttöön monivaiheinen tunnistautuminen aina kun se mahdollista.

Henkilöstö ja prosessit

- Päätä, kuka pääsee käsiksi mihinkin tietoon.
 - Rajoita järjestelmänvalvojan oikeudet tarpeen mukaan. Normaalikäytössä ei tarvita pääkäyttäjaoikeuksia. Käytä perusoikeuksilla ja kirjaudu erikseen/korota oikeuksia vain, kun ylläpitotoimiin on tarvetta ja palauta käyttöoikeus sen jälkeen perusoikeuksiin. Huomioi myös pilvipalveluiden oikeudet.
 - Älä käytä yhteisiä käyttäjätunnuksia – jokaisella tulisi olla omat tunnukset.
 - Muista sulkea ja poistaa tunnukset, kun käyttäjä ei ole enää työsuhteessa yrityksessä tai hänellä ei ole tarvetta tai oikeutta tietoon.
- Käytä salalauseetta yksittäisen sanan sijaan. Käytä monivaiheisen tunnistuksen kanssa.
- Hyvä salasana on:
 - yksilöllinen
 - pitkä
 - monimutkainen
 - helppo muistaa.
- Kouluta ja harjoittele riittävän usein. Lisää henkilöstön tietoisuutta kyberturvallisuudesta.
- Tee yrityksellesi suunnitelma tietoturvapoikkeamien hallitsemiseksi ja palkitse työntekijät, jotka raportoivat kyberturvallisuuspoikkeamasta.
- Luo kyberturvallisuuden kulttuuria ja ota asiat osaksi keskustelua.
- Ole erityisen tarkkana, jos saat seuraavanlaista sähköpostia:
 - Saat pyynnön pikaisen tilisiirron tekemiselle.
 - Tilitiedot halutaan päivittää.
 - Viestissä on liitetiedosto, jonka on lähettänyt tuntematon toimija, tai viesti poikkeaa tutun toimijan tavallisesti lähettämistä viesteistä.
- Saat pyynnön tarkistaa kirjautumistiedot palveluun ja mahdollisen kirjautumislinkin viestin mukana.

5 Sanasto

Tähän osioon on koottu oppaan termejä sekä muutamia sellaisia yleisiä sanoja, joita saatat kuulla, kun puhutaan kyberturvallisuudesta.

Digitaalinen turvallisuus

Käytetään usein kyberturvallisuuden synonyymina. Digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita. Terminä uusi ja vakiintumaton.

Haavoittuvuus

Mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa.

Haittaohjelma

Aiheuttaa tahallisesti tietojärjestelmän tai laitteen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa.

Identiteettivarkaus

Toisen ihmisen henkilötietojen tai muiden luottamuksellisten tietojen luvaton haltuunotto ja käyttäminen taloudellisen tai muun hyödyn saamiseksi.

Kiintolevy tai kovalevy

Tietokoneeseen kiinteästi asennettu levymuisti, jota käytetään tietokoneen massamuistina. Siihen tallennetaan ohjelmat ja muut tiedostot.

Kiristyshaittaohjelma

Salaa tai manipuloi laitteella olevia tietoja ja tyypillisesti vaatii käyttäjältä lunnaita salauksen purkamisesta.

Kohdennettu tietojenkalastelu

Tiettyyn henkilöön tai tietyn organisaation henkilöstöön kohdistuvaa verkkourkintaa.

Kryptovaluutta

Salaukseen perustuva digitaalinen virtuaalivaluutta. Sitä voi ostaa tai hankkia louhimalla (engl. mining) eli käyttämällä tietokoneen laskentatehoa valuuttasiirtojen käsittelyyn ja verkon toiminnan turvaamiseen. Kryptovaluuttoja eivät yleensä hallitse pankit, valtiot tai muut yksittäiset tahot, vaan niiden olemassaolo perustuu kryptovaluuttaohjelmia ajavien tietokoneiden vertaisverkossa ylläpitämään laskentatehoon.

Kyberrikollisuus

Viestintäverkkoja ja tietojärjestelmiä hyödyntäen tehdyt sekä niihin kohdistuvat rikokset. Kyberrikoksia ovat esimerkiksi tietojen kalastelu, identiteettivarkaudet ja kiristyshaittaohjelmat.

Kyberturvallisuus

Tavoitetilä, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.

Käyttöjärjestelmä

Ohjelmakokonaisuus, joka huolehtii käyttämäsi tietokonelaitteiston ja siihen asennettujen ohjelmien yhteistoiminnasta. Tyypillisimpiä käyttöjärjestelmiä ovat Windows-, Linux- ja MacOS-käyttöjärjestelmät.

Laskutushuijaus

Organisaatioon tulee yhteydenotto, joka on olevinaan tavarantoimittajalta/ palveluntarjoajalta, ja jossa pyydetään muutosta laskutustietoihin.

Monivaiheinen tunnistautuminen

Henkilön identiteetti varmistetaan useampaa eri tunnistautumistapaa käyttämällä.

Nollapäivähaavoittuvuus

Tietojärjestelmässä oleva haavoittuvuus, johon ei ole saatavilla korjausta.

Pilvipalvelu

Hajautettu verkkopalvelu, jossa tietokoneita, ohjelmia, tallennustilaa ja muita tietoteknisiä palveluja käytetään verkon kautta.

Pääkäyttäjä (eng. administrator, admin)

Tietojärjestelmän käyttäjätunnus, jolla on tavallisia käyttäjiä suuremmat oikeudet tehdä muutoksia järjestelmään ja asentaa laitteelle ohjelmia.

Salasanan hallintaohjelma

Tuttavallisemmin salasanamanageri. Auttaa salasanojen turvallisessa käytössä eri palveluissa. Sovelluksen avulla pidät salasanasi suojattuna yhden pääsalasanan takana ilman, että joudut muistamaan kaikkia salasanvoja.

Salasana tai salalause

Tunniste, jota käytetään usein yhdessä siihen liittyvän käyttäjätunnuksen kanssa. Se on usein henkilökohtainen ja tarkoitettu vain käyttöoikeuden haltijan tietoon.

Tietojenkalastelu (phishing)

Käyttäjältä pyritään saamaan luottamuksellista tietoa kuten henkilötietoja, sähköpostin tai verkkosivun välityksellä.

Tietokoneohjelma

Tietokoneen käsiteltäväksi ja suoritettavaksi tarkoitettu (digitaalisesti koodattu) ohjelma. Esimerkiksi taulukkolaskentaohjelma Excel.

Tietomurto

Luvaton tietojärjestelmään, palveluun tai laitteeseen tunkeutuminen tai sovelluksen, kuten esimerkiksi sähköpostitilin luvaton käyttö haltuun saatujen tunnusten avulla.

Tietoturva

Järjestelyt, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus.

Tietoturvapoikkeama

Yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti.

Tietoturvapoikkeaman hallinta

Toimenpiteet, joilla varaudutaan ja reagoidaan tietoturvahäiriöihin vahinkojen rajoittamiseksi ja niistä toipumiseksi.

Tietoturvauhka

Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu tietoturvaan ja toteutuessaan vaarantaa sen.

Tietovuoto

Tietomurron seurauksena haltuun saadut suojattavat tai salassa pidettävät tiedot leviävät ulkopuolisille.

Toimitusjohtajahuijaus

Rikollinen tekeytyy organisaation johtajaksi ja pyrkii saamaan työntekijän tekemään rahansiirron omalle huijaustililleen.

Varmuuskopio

Tarkoitettu käytettäväksi, jos alkuperäinen tallenne menetetään esimerkiksi vian tai vahingon takia. Varmuuskopioita voi tallentaa esimerkiksi ulkoisille kiintolevyille tai verkkotallennuspalveluun.

Vähemmän oikeuden periaate

Tietojärjestelmän käyttöoikeudet tulee rajata suppeimpiin mahdollisiin oikeuksiin, joilla käyttäjä tai prosessi kykenee suoriutumaan sille määrätystä tehtävästä.



**Heräsikö oppaan sisällöstä tai
kyberturvallisuudesta kysymyksiä?**

Voit olla yhteydessä Kyberturvallisuuskeskukseen
sähköpostitse: kyberturvallisuuskeskus@traficom.fi

**Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus**

PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi