Rahoittaja

Jatkuvan oppimisen ja työllisyyden palvelukeskus

Tervetuloa koulutukseen!

Digitaaliset työkalut ja data yksinyrittäjän apuna

Euroopan unionin rahoittama – NextGenerationEU

Suomen kestävän kasvun ohjelma

Suomen Yrittäjäopisto

Suomen Yrittäjäopisto

Tietoturva ja tietosuoja yrityksessä

Digitaaliset työkalut ja data yksinyrittäjän apuna

JOTPA

Sisältö:

WEBINAARI 18.9. klo 12-15:00 (osa 2)

12:15 Tietoturva kokonaisuutena

12:30 Tietosuoja

13:00 Yrittäjän tietoturvan ABC

14:15 Tauko

14:30 Kriittiset toiminnot, riskien ja jatkuvuuden hallinta

14:45 Vapaat aiheet ja keskustelu

15:00 Päätös

Tänään äänessä

Kari Kananoja

IT-alalla n.30 vuotta

Kouluttajana 16 vuotta

- Ohjelmistotuotanto

- Tietoturva

Tietotekniikan ins,

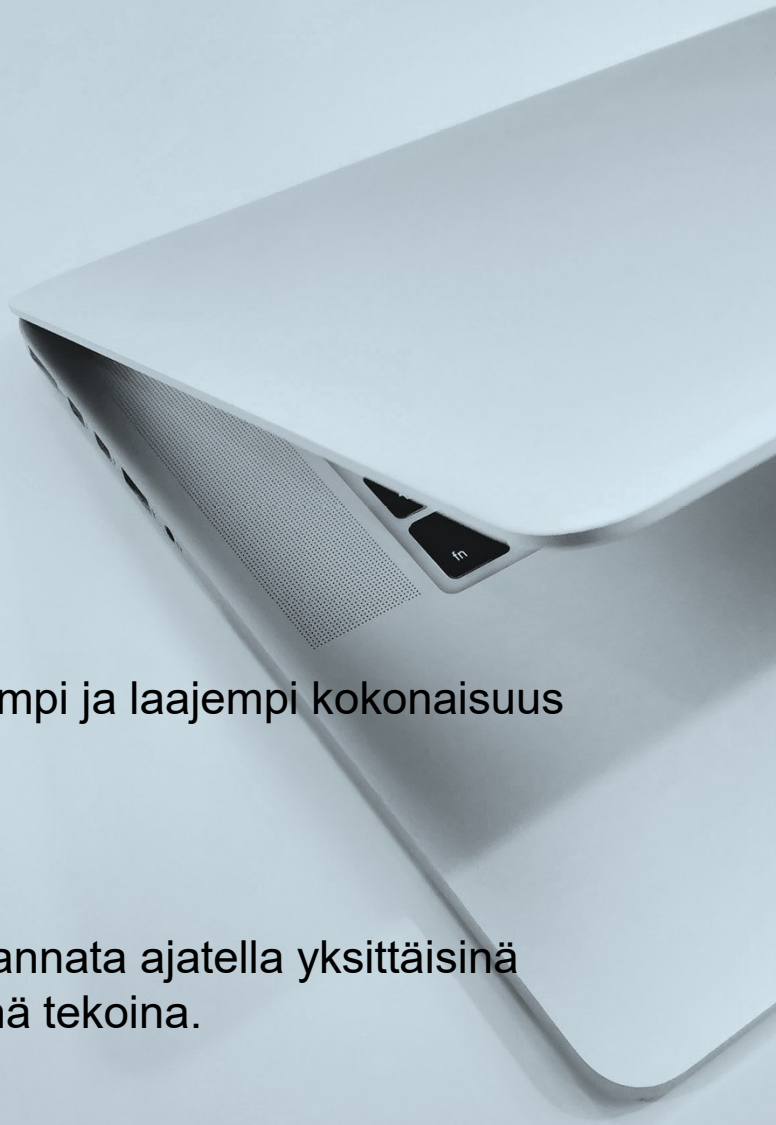
AmO,

Kyberturvallisuuden FM, työn alla

Tietoturva kokonaisuutena

Lähde: Digi- ja väestötietovirasto

- Tietoturvan voi jaotella monella tavalla, esimerkiksi:
- fyysinen tietoturva
  - mm. tilaturvallisuus ja fyysinen tiedon säilytys
- digitaalinen tietoturva, joka puolestaan on jaettavissa edelleen
  - - tekninen tietoturva
    - Ohjelmistot ja tekniikkaan perustuva suojaaminen
    - Tukee toiminnallista tietoturvaa
  - - toiminnallinen tietoturva
    - Oma toiminta ja päivittäisten toimintojen suojaaminen
    - Täydentää teknistä tietoturvaa, mutta on yrittäjän kannalta tärkeämpi ja laajempi kokonaisuus
  - - strateginen tietoturva



- Tietoturva ja siitä huolehtiminen ei ole kertaluontoinen prosessi, eikä sitä kannata ajatella yksittäisinä toimenpiteinä, vaan tulisi omaksua ajattelutapa, joka on läsnä jokapäiväisinä tekoina.

Yrittäjä ja tietosuoja

- Yrityksen päättäjän tulee olla hevosen selässä eri järjestelmien osalta, siten että tietosuoja tulee kaikilta osin huomioitua.
- Tietosuojan eteen tulee nähdä vaivaa ja siihen liittyvät asiat tulee kuvata ja dokumentoida, yrittäjän siis tulee huolehtia tästä (vähimmillään kuvaus kerättävästä tiedosta ja sen käytöstä, tietosuojaseloste)
- Jos yrityksesi ei huolehdi riittävällä tasolla tietosuojasta ja vaatimustenmukaisuudesta, voi tietosuojaviranomaisten määräämä sakko olla moninkertainen verrattuna siihen, että hoitaisit asiat viranomaisen edellyttämällä tasolla.
- Markkinoilla on erilaisia ulkoisia palveluita ja järjestelmiä tietosuojan riittävään kuvaamiseen, ja oikea kumppani voi auttaa asiassa, mutta yrityksen tulee tehdä työ sen eteen. Tätä jaettua vastuuta et kuitenkaan voi päättäjänä paeta.
- Huolehtimalla tietosuojasta sekä vaatimustenmukaisuudesta, siivoat turhaa tietoa aktiivisesti, on tieto tällöin oikeellista ja toiminta käsittelyperusteen mukaista.

Tietosuoja

- Mitä eroa on tietosuojalla ja tietoturvalla? Tietoturva on yksi tietosuojan toteuttamisen keino. Sen tarkoitus on suojata tietoaineisto ja tietojärjestelmät.
- Tietosuojan osalta, yrittäjää velvoittavat lait ja määräykset
- Tietosuojalaki (1050/2018) (**http://www.finlex.fi/fi/laki/ajantasa/2018/20181050**) täsmentää ja täydentää EU:n yleistä tietosuoja-asetusta (**https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504**) ja sen kansallista soveltamista. Mikäli yrityksellä on työntekijöitä, heidän tietojensa käsittelemistä ohjaa työelämän tietosuojalaki. (laki yksityisyyden suojasta työelämässä (**https://www.finlex.fi/fi/laki/ajantasa/2004/20040759**)).
- Tietosuojavaltuutetun toimiston www-sivut (**https://tietosuoja.fi/organisaatiot**) antavat hyvän peruspaketin tietosuojaan ja sen vaatimuksiin. Jos tästä haluaa opiskelua laajentaa, edellisistä kannattaa jatkaa Eduhousen kurssisarjaan (**https://app.eduhouse.fi/palvelu/koulutukset/77489130-tietosuojan-perusteet-tietosuoja-kaytannossa-2?element=77491154**ja jos käyttää Microsoftin 365 –ympäristöä, niin siihen löytyy jälleen täydentävä opas (**https://lbproduction.s3.amazonaws.com/5f3535bcc424876f6f486604/extras/m365tietosuojaopas.pdf**)
- Tietosuojaseloste; esimerkkinä Verkkokauppa.com (**https://www.verkkokauppa.com/fi/ohjeet/tietosuojaseloste**), suppeampi pohja Innowiselta (**https://www.innowise.fi/fi/gdprn-mukainen-rekisteri-ja-tietosuojaselosteen-malli/**)

Pienyrittäjän tietoturvan ABC

- Mihin pienyrittäjän tulisi keskittyä, kun tietoturva kokonaisuutena kattaa tuhottomasti eri tekniikoita, standardeja ja tuotteita, puhumattakaan eroista eri it-ympäristöjen välillä?
- Mikä on olennaista ja tietoturvan parantamiseksi tehokkainta niin resurssillisesti kuin taloudellisestikin? Miten tehdä juuri sinun yritysympäristöstäsi mahdollisimman tietoturvallinen?
- Jokaisella yrittäjällä tilanne ja digitaalinen ympäristö vaihtelee -> toimenpiteitä ja tarpeita tulisi ajatella yrityskohtaisesti. Tärkeää on tasainen perustietoturva, ei niinkään mahdollisimman laaja ja kaiken kattava kokonaisuus. Keskittykää jokapäiväisten toimintojen turvaamiseen sekä yrityksenne kriittisiin toimintoihin ja pääomaan.

Lähde: Lounea

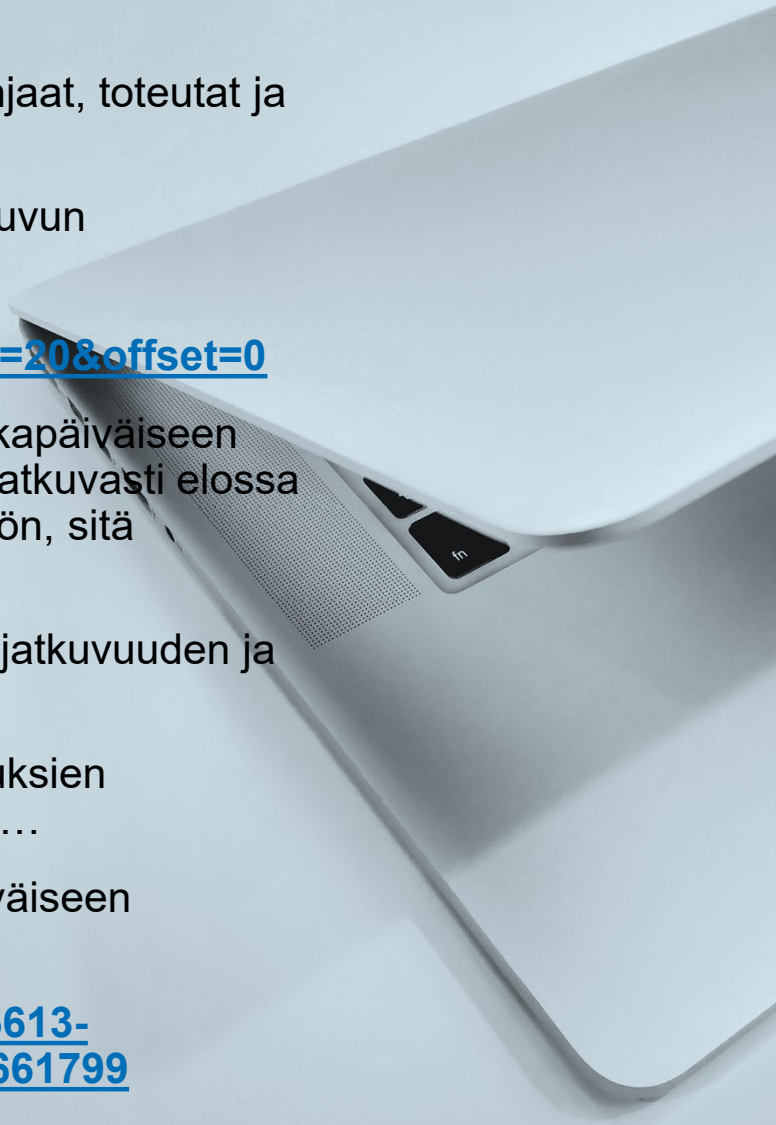
Pienyrittäjän tietoturvan ABC

- (linkit ovat osia Eduhousen Tietoturvan perusteet ja sen osa-alueet webinaareista)
  - Jokapäiväiset toiminnot; Linkki:Näin suojaudut yleisimmiltä uhilta (**https://app.eduhouse.fi/palvelu/fi-digiskills/koulutuskokonaisuudet/39555613-tietoturvan-perusteet-2/39517137-tutustuminen-tietoturvaan?element=53661885**)
    - Muista:
      - Salasanat, niiden muodostaminen ja tallennus
      - Palomuuri, liikenteen rajoittaminen
      - Virusten torjunta
      - VPN ja tietokoneen käyttäminen yleisissä verkoissa
      - Tiedon varastointi ja muistilaitteet
      - Varmuuskopioinnit
  - Haittaohjelmilta suojautuminen; Linkki: Haittaohjelmien leviäminen (**https://app.eduhouse.fi/palvelu/fi-digiskills/koulutuskokonaisuudet/39555613-tietoturvan-perusteet-2/39517137-tutustuminen-tietoturvaan?element=53660999**)
  - Tietojen kalastelu; Linkki: Tietojenkalastelun keinot (**https://app.eduhouse.fi/palvelu/fi-digiskills/koulutuskokonaisuudet/39555613-tietoturvan-perusteet-2/39517137-tutustuminen-tietoturvaan?element=53661743**)
  - Fyysinen tietoturva; tilaturvallisuus ja ei-digitaalisen tiedon suojaaminen
  - Ulkoisten palveluitten tietoturvasta huolehtiminen
  - Tietosuoja ja sen toteuttaminen

Pienyrittäjän tietoturvan ABC

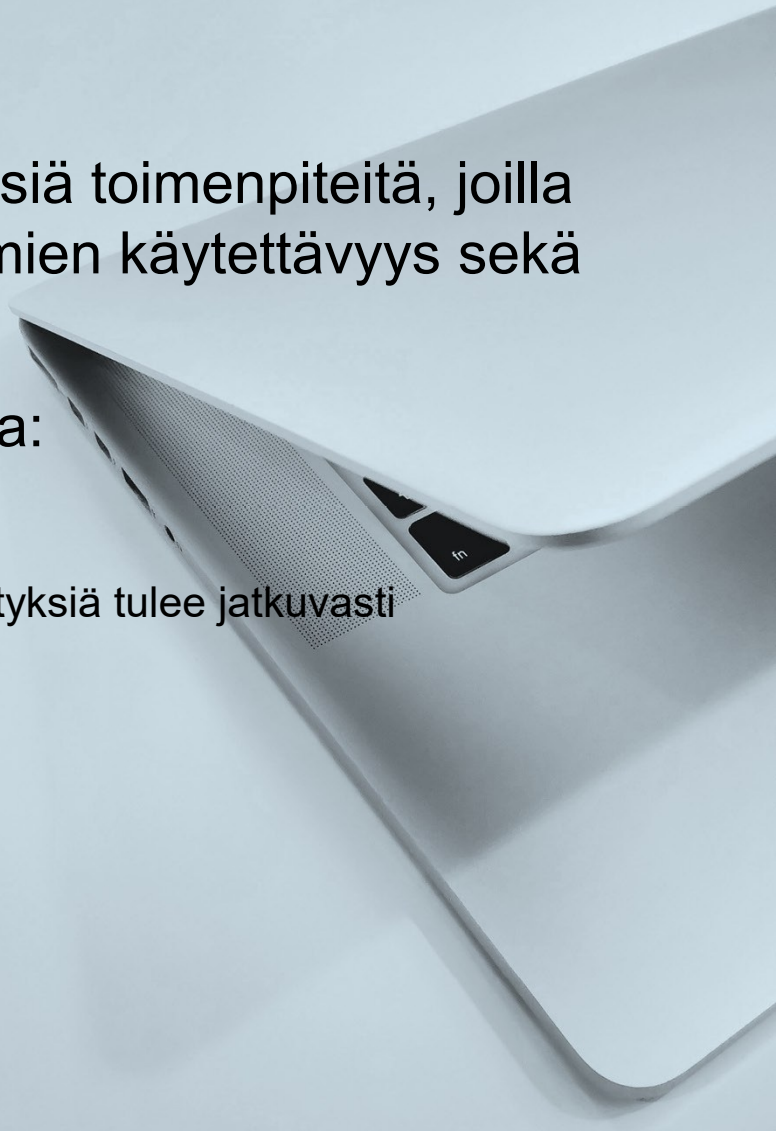
- Ajan tasalla pysyminen ja kouluttautuminen; Koska pienyrittäjänä käytännössä ohjaat, toteutat ja myös kehität yrityksesi tietoturvaa, tee seuraavasti
  - Kouluttaudu ja seuraa tietoturvauutisia. Ota tavaksi vaikkapa sähköpostien luvun yhteydessä käydä lukemassa viimeiset tietoturvauutiset (esim. viikoittainen kyberturvauutiset) **https://www.kyberturvallisuuskeskus.fi/fi/viikkokatsaus?active=0&limit=20&offset=0**
  - Tee tietoturva-ajattelusta osa jokapäiväistä toimintaa, sisällytä periaatteet jokapäiväiseen työhösi. Tietoturvan toteuttaminen ei ole kertaluontoista, vaan pikemminkin jatkuvasti elossa oleva prosessi. Mitä paremmin liität tämän prosessin kaikkeen muuhun työhön, sitä paremmin se on kunnossa ja ajan tasalla.
  - Yrityksen toiminnan turvaamiseksi, tee tietoturvan hallinnasta osa yrityksesi jatkuvuuden ja riskien hallintaa
  - Varaudu tietoturvan pettämiseen suunnittelemalla korjaavat ja riskien seurauksien vaikutusten vähentämisen toimet. Suunnittelu säästää kallisarvoista aikaa……
  - Käy Linkki: Eduhouse videosarja läpi (n. 4 tuntia), paras sijoituksesi jokapäiväiseen tietoturvaan

https://app.eduhouse.fi/palvelu/fi-digiskills/koulutuskokonaisuudet/39555613-tietoturvan-perusteet-2/39517137-tutustuminen-tietoturvaan?element=53661799



Tietoturva

- Tietoturva tarkoittaa muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen.
- Yrityksen kannalta, tietoturva sisältää monia eri osa-alueita:
  - Tietosuoja ja sen alaiset tiedot, niiden käyttö ja säilytys
  - Ohjelmistoturvallisuus; pidä laitteittesi päivitykset kunnossa, tietoturvapäivityksiä tulee jatkuvasti
  - Laiteturvallisuus; tietokoneen ja verkon suojaaminen
  - Palveluiden suojaaminen
  - Tietoturvasäännöt ja niiden koulutus/ylläpito
  - Huijaukset ja niiden tunnistaminen
  - Oman webbisivun ja/tai verkkokaupan suojaaminen
  - Varautuminen, esim.varmistukset ja toiminnot vahingon sattuessa



Kriittiset toiminnot ja niihin kohdistuvat riskit

- Yrittäjä joutuu pohtimaan jatkuvasti yrityksensä toimintaedellytyksiä, niiden kehittämistä ja olemassa olevan toiminnan turvaamista
- Kun puhutaan toiminnan turvaamisesta, käsite jatkuvuuden hallinta on olennainen osa toimintaa
- Jatkuvuuden hallinnan keskiössä on yrityksen toimintojen varmistaminen kaikissa tilanteissa, myös yllättävien toimintaympäristön muutoksien kohdatessa.
- Toisin sanoen tulee selvittää ja arvioida
    - yrityksen kriittiset toiminnot ja niihin kohdistuvat riskit
    - kriittisten toimintojen suojaaminen
    - toimintatavat ja –vastuut muutostilanteissa
- Tämän päivän alati kehittyvässä tietoteknisessä ympäristössä, tietoturva (myös kyberturva) on olennainen osa toimintojen suojaamista ja turvaamista, varsinkin jos liiketoiminta on pääosin digitaalisten ympäristöjen varassa.

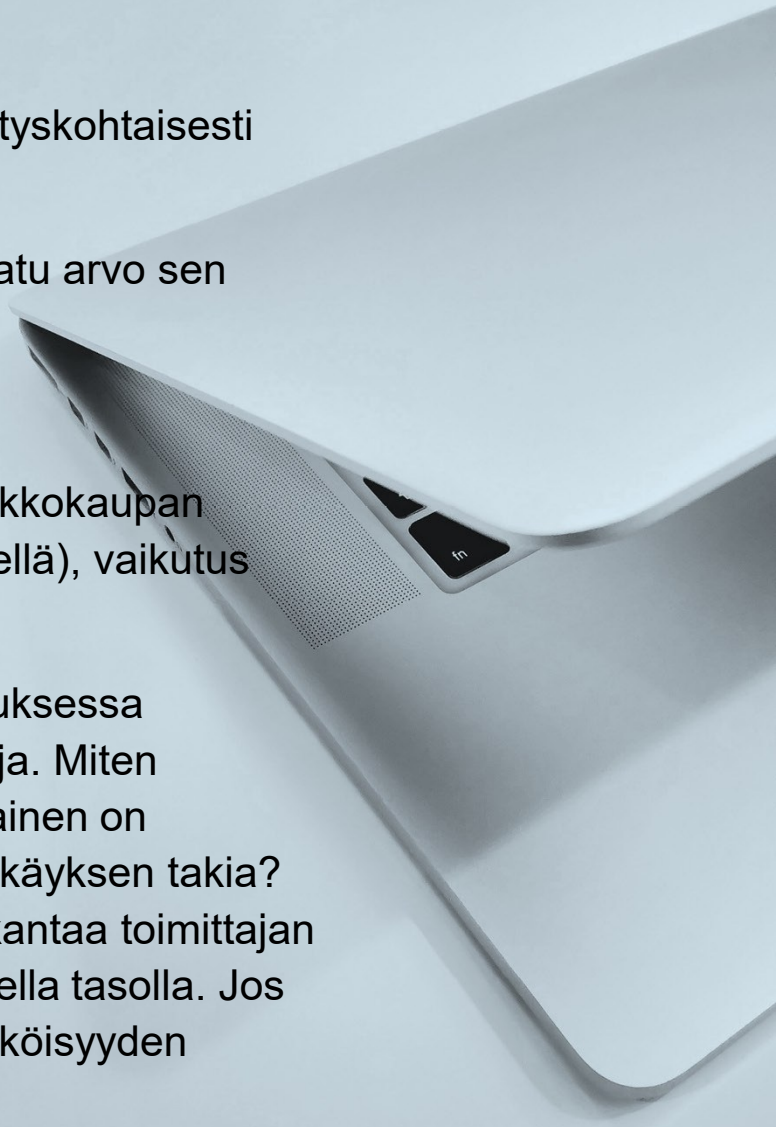
Lähde: PK-RH riskienhallinta

Jatkuvuuden hallinta / riskien hallinta

- Toimintoja ja niiden kriittisyyttä voidaan arvioida monella tasolla, riippuen siitä, mikä kunkin toiminnon osalla ajatellaan olevan yritystoiminnan kannalta merkitsevintä. Miten ja millä tavoin, ei ole merkityksellistä, pääasia on löytää liiketoiminnan kannalta kriittiset osat ja asettaa ne tärkeysjärjestykseen.
- Jokaisen yrittäjän tulee omalta kohdaltaan pohtia, mikä on tärkeää, minkä suojaamiseen/riskin hallintaan kannattaa panostaa ja miten (taloudellisesti tai ajallisesti)
- Arviointia voidaan suorittaa esim. seuraavista näkökulmista:
    - Taloudelliset seikat, aikakriittisyys, vaikutukset yrityksen muihin toimintoihin
    - Mitä muuta?
- Esimerkki
    - Jos yritys on verkkokauppa, mitkä seikat voivat vaarantaa verkkokaupan toimintaa?
        - Logistiset ongelmat; tavaran saanti (toimitukset, kuljetukset, varastointi jne)
        - Kilpailulliset ongelmat (hintataso, toimitusvarmuus ja –nopeus jne)
        - Tietotekniset ongelmat (verkkopalvelun saatavuus ja toimintavarmuus, tiedon hallinta jne)
        - Mitä muuta?

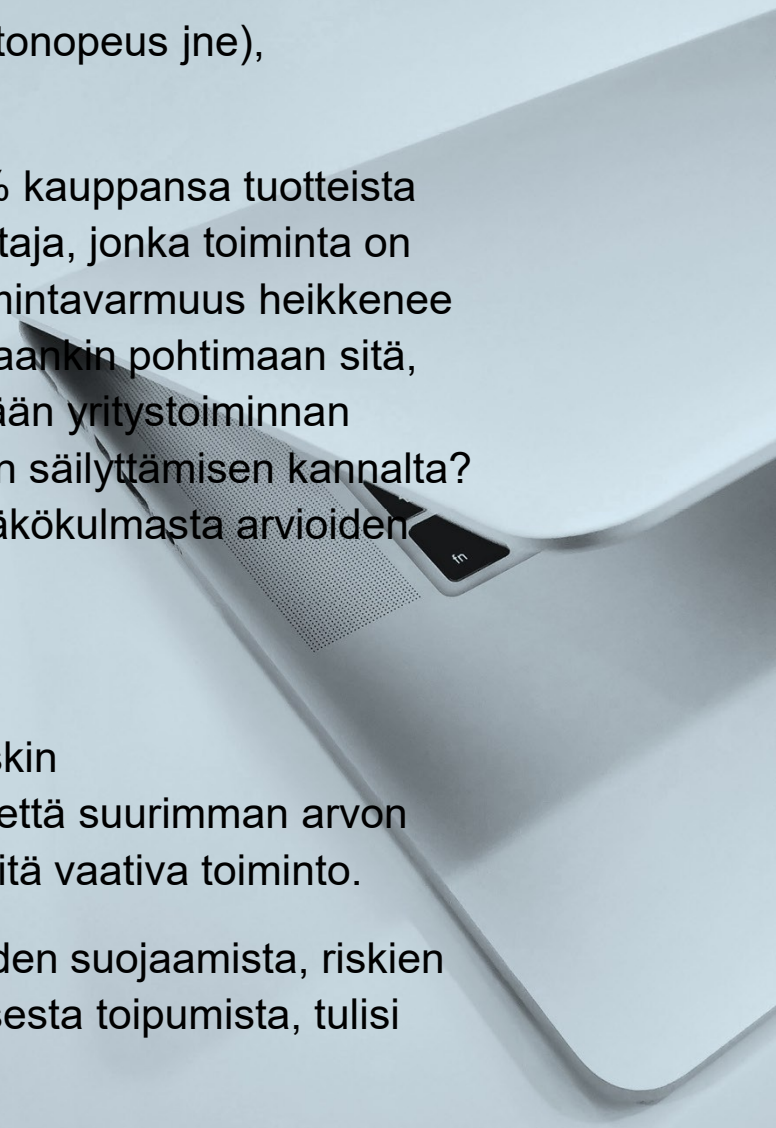
Toimintojen arviointi

- Kyse on siis pohjimmiltaan riskien hallinnasta
- Koska kaikkia riskejä ei voida (tai ole taloudellisesti kannattavaa) hallita, ne täytyy yrityskohtaisesti arvottaa
- Yksinkertaisin tapa arvottaa riskejä, on päätellä riskin vaikutus toimintaan ja kertoa saatu arvo sen toteutumistodennäköisyydellä, esimerkiksi:
    - Molemmissa tekijöissä voidaan käyttää vaikkapa numeroita, esim. 0 – 5
    - Jos ajatellaan yksi verkkokauppayrityksen kriittisistä toiminnoista olevan verkkokaupan saavutettavuus (ellei sivusto ole pystyssä, liiketoiminta loppuu samalla hetkellä), vaikutus toimintaan tällä riskillä on siis 5
    - Mikä on todennäköisyys riskin toteutumiselle? Verkkokauppa on tässä tapauksessa kolmannelta osapuolelta hankittu palvelu, jonka tietoturvasta vastaa toimittaja. Miten todennäköisesti toimittajan jatkuvuuden hallinta on hyvässä kunnossa? Millainen on toimittajan vastuu, jos kaikesta huolimatta palvelu kaatuu, esim. verkkohyökkäyksen takia? Tässä tapauksessa, toimitus- ja palvelusopimuksessa ei ole otettu tarkasti kantaa toimittajan vastuuseen eikä ole voitu varmistua toimittajan riskien hallinnasta kohtuullisella tasolla. Jos painotetaan toimintojen aikakriittisyyttä, voidaan arvioida toteutumistodennäköisyyden olevan esim. 4.



Toimintojen arviointi

- Seuraavaksi, pohditaan vaikkapa logistista riskiä tavaratoimituksissa. Jos tavaraa ei saada verkkokauppaa varten toimittajalta (aikakriittisyys arvioitava, oma varasto, kiertonopeus jne), liiketoiminta pysähtyy. Riskin vaikutus toimintaan voisi olla tässäkin 5.
- Mikä on todennäköisyys riskin toteutumiselle? Verkkokauppayritys hankkii 70% kauppansa tuotteista yhdeltä ja samalta toimittajalta. Toimittaja on vakavarainen ja vakiintunut toimittaja, jonka toiminta on kuitenkin pienyritystoimintaa. Mikä on todennäköisyys sille, että toimittajan toimintavarmuus heikkenee olennaisesti tai toimituksiin tulee huomattavia viiveitä? Tässäkin kohtaa joudutaankin pohtimaan sitä, miten sopimuksissa on tällaiseen varauduttu. Riittääkö 30% tuoteosuus pitämään yritystoiminnan elossa? Kuinka suuri vaikutus tällä olisi taloudellisesti, tai asiakaskunnan ja sen säilyttämisen kannalta? Vaikutukset kilpailutilanteeseen? Todennäköisyys riskin toteutumiselle talousnäkökulmasta arvioiden voisi arviona olla esim. 3, olettaen että sopimusasiat ovat pääosin kunnossa.

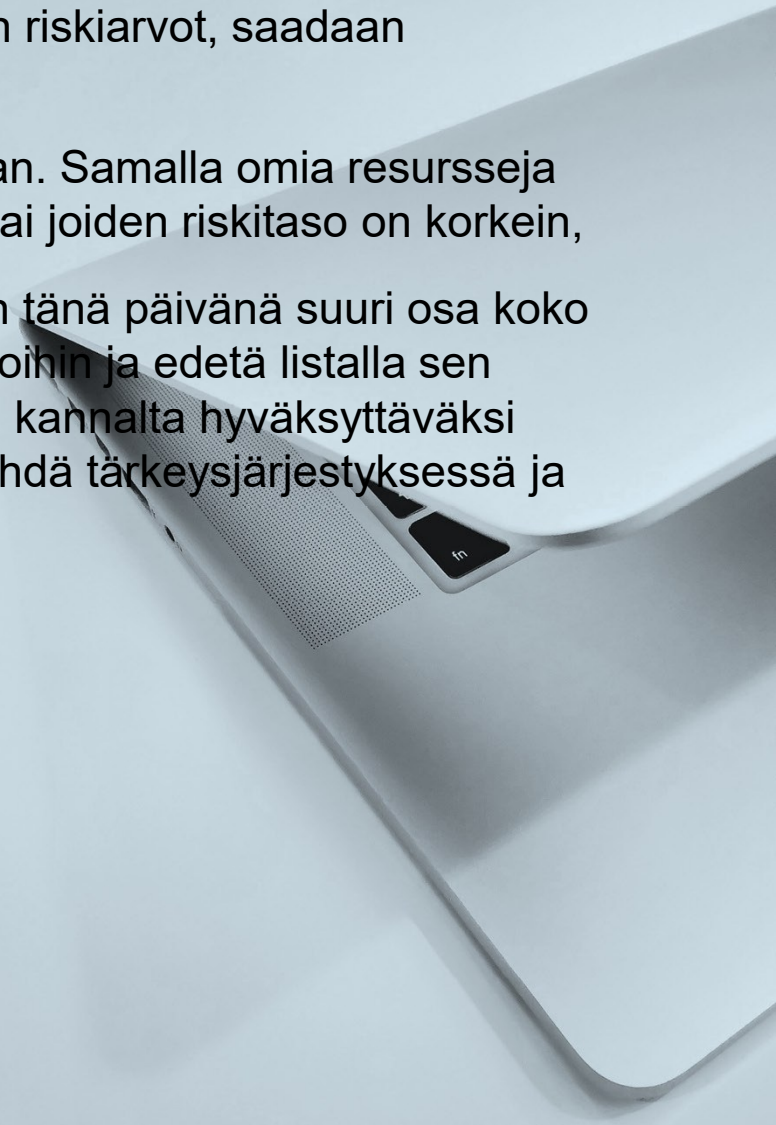


Edellä käsitellyllä tavalla toiminnot arvottamalla, kertomalla riskin vaikutusarvo riskin toteutumistodennäköisyyden arvolla, saamme toiminnot arvojärjestykseen siten, että suurimman arvon saanut toiminto on yrityksen toiminnan kannalta tärkein ja siten eniten toimenpiteitä vaativa toiminto.

Näin saamme selville yrityksen kannalta ne toiminnot (tärkeysjärjestyksessä), joiden suojaamista, riskien pienentämistä (tai niiden vaikutuksen minimointia) ja esimerkiksi riskin toteutumisesta toipumista, tulisi pohtia ja kehittää.

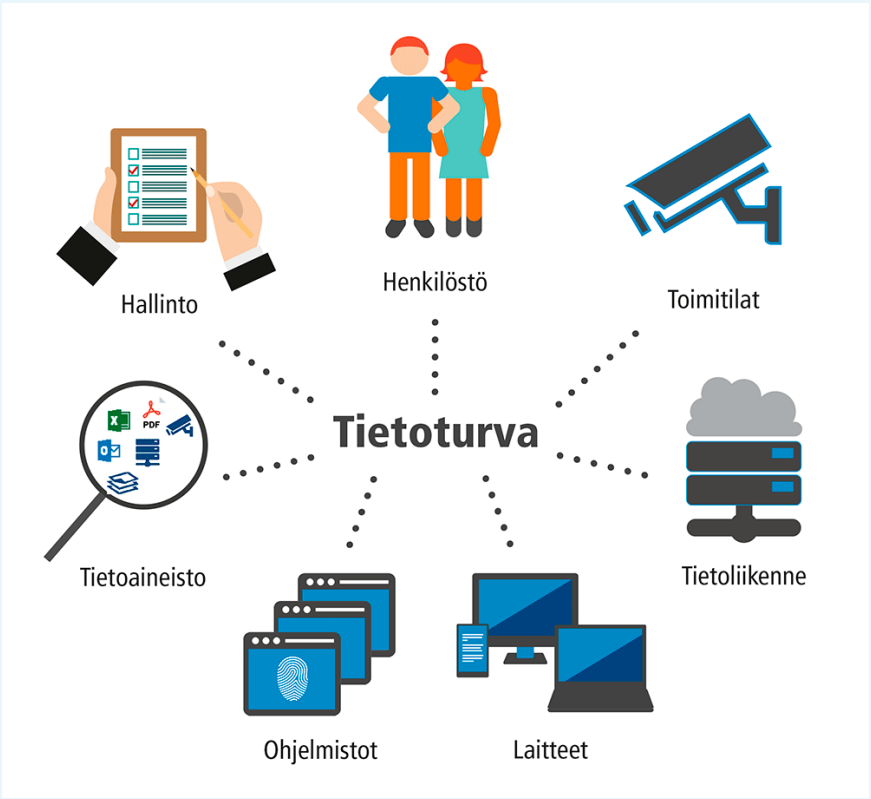
Toimintojen arviointi

- Kun on saatu arvotettua mahdollisimman kattavasti yrityksen eri toimintojen riskiarvot, saadaan aikaseksi arvojen perusteella luokiteltu toimintojen järjestys
- Mitä korkeampi arvo, sitä tärkeämpää on kiinnittää huomiota riskin hallintaan. Samalla omia resursseja kohdistetaan luonnollisella tavalla niihin toimintoihin, jotka ovat tärkeimpiä tai joiden riskitaso on korkein,
- Tällä tavoin voidaan aloittaa toimet myös tietoturvan osalta (joka tosiaan on tänä päivänä suuri osa koko jatkuvuuden hallintaa). Samalla voidaan keskittyä aluksi tärkeimpiin toimintoihin ja edetä listalla sen mukaan, mihin on resursseja ja mikä on nähtävä yrityksen riskien hallinnan kannalta hyväksyttäväksi tasoksi. Tällä tavoin, mahdollisesti isoksikin kasvava arviointityö voidaan tehdä tärkeysjärjestyksessä ja siinä vauhdissa kun resurssit antavat myöden.
- Riskien minimoiminen
  - Riskin poistaminen
  - Riskin vähentäminen
  - Riskin vaikutuksen ulkoistaminen
  - Riskin vaikutusten vähentäminen



Yhteenveto

- Pohdi toimintasi kannalta kriittisimmät toiminnot
- Mieti, minkä verran juuri sinun yrityksesi voi käyttää tietoturva-asioiden hoitamiseen, älä sorru ylilyönteihin. Monet asiat voi hoitaa ihan itsekin, jotkut voi ja kannattaa ostaa ulkopuolisilta.
- Laita perusasiat kuntoon (muistilista/ABC aiemmissa sivuilla)
- Pysy asioista tietoisena, jotta voit liittää osaamisesi jokapäiväisiin toimintoihin
- Jos käsittelet henkilötietoja, laita tietosuojan edellyttämät asiat kuntoon
- Alkuvaiheessa tarvitaan hiukan enemmän aikaa, mutta
    - Riskien hallinta (ja tietoturva) on jatkuvaa toimintaa, ei kertaluontoinen projekti
    - Mitä paremmin teet alkuvaiheen, sitä luontevampaa ja etenkin resurssien kannalta tehokkaampaa on pitää niin tietoturva kuin riskien hallinta ja varautuminenkin osana jokapäiväistä toimintaa
- Muista pitää yllä kokonaisuutta, ketju on yhtä vahva kuin heikoin lenkki ja heikoin lenkki on (valitettavasti) useinkin käyttäjä/ihminen



Lähde: DataGroup

Tämä materiaali on tuotettu Digitaaliset työkalut ja data yksinyrittäjän apuna koulutuksessa.

Palvelukeskus edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta. Palvelukeskuksen toimintaa ohjaavat opetus- ja kulttuuriministeriö sekä työ- ja elinkeinoministeriö.

Euroopan unionin rahoittama – NextGenerationEU

Suomen kestävän kasvun ohjelma

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus