DIGI- JA VÄESTÖTIETO-VIRASTO

Digiturvan usein kysytyt kysymykset

VAHTI-hyvät käytännöt tukimate-riaali 31.5.2021

31.5.2021

Kommenttiversio 30.8.2021

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Dokumentinhallinta

Omistaja	Kimmo Rousku, Digi- ja väestötietovirasto
Laatinut	VAHTI-työryhmien jäsenet
Tarkastanut	VAHTI sihteeristö
Hyväksynyt	VAHTI sihteeristö

Version hallinta

versionro	mitä tehty	pvm/henkilö
0.42	Ensimmäinen luonnosversio muokattavana	18.11.2021 KR, JK
0.90	Luonnosversio kommenteille	31.5.2021 KR
1.00	Julkaisuversio	31.8.2021 KR

Sisällysluettelo

Digiturvan usein kysytyt kysymykset

1 Johdanto

Tämä tukimateriaali on laadittu julkisen hallinnon organisaatioille turvallisen työskentelyn ja toiminnan edistämisesi. Tukimateriaali pohjautuu julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) asiantuntijoiden kokoamiin riskienhallinnan, toiminnan jatkuvuuden ja valmiuden, tietoturvallisuuden ja tietosuojan hyviin käytäntöihin. Hyvien käytäntöjen mukaisesti toimimalla edistämme samalla kyberturvallisuuden toteutumista.

Toivomme, että annat meille palautetta tästä materiaalista. Saatuamme riittävästi parannus ja korjausehdotuksia, julkaisemme tästä päivitetyn version.
Linkki palautekyselyyn.

Mikäli organisaatio käyttää tässä materiaalissa olevia kysymyksiä ja vastauksia, jokainen organisaatio ja asiantuntija vastaa itse siitä, että vastaus sovitetaan tarkemmin organisaation omaan toimialaan ja sitä koskevaan lainsäädäntöön.

Kysymykset on jaoteltu digitaalisen turvallisuuden viitekehyksen viiden osa-alueen mukaisesti.

2 Riskienhallinta

2.1 Mitä riskienhallinnalla tarkoitetaan?

Riskienhallinta on toiminto, jolla johdetaan ja ohjataan organisaation riskejä. Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna.

Riskienhallinnan tarkoituksena on mahdollistaa organisaation menestyminen, toiminnan jatkuvuuden takaaminen ja tavoitteiden saavuttaminen. Riskienhallinta on järjestelmällistä ja tavoitteellista toimintaa, jolla tuetaan lisäksi organisaation johtamista ja kehittymistä. Usein sanaa riski käytetään uhka-sanan synonyyminä, mutta pohjimmiltaan riski voi olla myös positiivinen asia, mahdollisuus saada hyötyä jollain toimenpiteellä. Riskienhallinnan tarkoituksena on löytää organisaation menestymiseen ja tuloksellisuuteen sekä henkilöstön hyvinvointiin vaikuttavat tekijät.

Lähde: Ohje riskienhallintaan VM 22/2017
https://www.suomidigi.fi/sites/default/files/2020-06/VM_22_2017_1.pdf

"järjestelmällinen toiminta riskien rajoittamiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa. Riskien hallinta on jokaisen hallinnon tehtävää suorittavan henkilön vastuulla; erikseen organisoitu riskienhallintatoiminto tukee hallinnon johtamista.

Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän valinta, päätös riskien poistamisesta, alentamisesta tai pitämisestä omalla vastuulla, sekä riskienhallinnan organisointi.”

Lähde: Valtionhallinnon tietoturvasanasto
https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-82008-valtionhallinnon-tietoturvasanasto

Riskienhallinta on organisaation johdon ja muun henkilökunnan toteuttama organisaation johtamiseen ja toimintaan sisältyvä prosessi, jota sovelletaan strategian valinnasta lähtien kaikessa organisaation toiminnassa (yksiköt, prosessit, asiakassuhteet jne.). Riskienhallinnan tavoitteena on tunnistaa ja hallita organisaatioon vaikuttavia potentiaalisia tapahtumia ja pitää riskit sellaisissa rajoissa, ettei organisaation toiminta ole uhattuna, ja jotta voidaan vähentää epävarmuutta organisaation tavoitteiden toteutumisesta.

Riskienhallinta on työtä yrityksen toiminnan jatkuvuuden ja henkilöstön hyvinvoinnin turvaamiseksi. Riskienhallinnalla tarkoitetaan kaikkea yrityksessä tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.

Riskienhallinta on epäedullisten ja haitallisten tapahtumien välttämistä (vaikutetaan tapahtuman todennäköisyyteen) tai tapahtumien seurausten pienentämistä (vaikutetaan seurauksen suuruuteen). Riskienhallinta on myös potentiaalisten mahdollisuuksien tunnistamista, analysointia ja hyödyntämistä. Kaikki nämä toiminnat tähtäävät yrityksen tavoitteiden saavuttamiseen.

Lähde:
https://pk-rh.fi/riskienhallinta.html

2.2 Riskienhallinta on päätöksenteon työkalu

Riskienhallinnan pääasiallisena tarkoituksena on auttaa organisaatiota tekemään mahdollisimman hyviä ja informoituja päätöksiä, huomioiden näihin liittyvät epävarmuudet, jotta organisaation tavoitteet saavutetaan, tai jopa ylitetään, mahdollisimman todennäköisesti. Eli riskienhallinnan tarkoitus ei ole hallita/välttää vain negatiivisia epävarmuuksia, vaan pääasiallisesti lisätä positiivisten epävarmuuksien todennäköisyyttä/vaikutuksia. Tämä arvon luominen ja säilyttäminen on mm. ISO31000 keskeinen periaate, sillä se parantaa suorituskykyä sekä tukee innovointia ja tavoitteiden saavuttamista.

Riskienhallinnan vaikuttavuus riippuu sen sisällyttämisestä organisaation hallintotapaan ja päätöksentekoon. Riskienhallinta on siten sen sitomista organisaatoin kulttuuriin siten, että riskienhallinta on osa toimintaa joka päivä päätöstenteon yhteydessä. Riskienhallinta ei ole siis erillinen toimintonsa, joka suorittaa riskienhallintaa (neljännes)vuosittain, vaan osa kaikkea ja kaikkien tekemistä, päivittäin.

Lähteet:
https://riskacademy.blog/my-favourite-risk-management-books/ , ISO31000

2.3 Mikä on uhkan ja riskin välinen ero?

Uhka: “haitallinen tapahtuma, joka voi mahdollisesti toteutua, tai useampi mahdollinen häiriö, joka tapahtuessaan voi aiheuttaa sen, että tiedoille, muulle omaisuudelle tai toiminnalle tapahtuu ei-toivottua."

Riski: Epävarmuuden vaikutus tavoitteisiin, poikkeama odotetusta. Vaikutus voi olla positiivinen, negatiivinen tai molempia.

Keskeinen ero: Uhka on pääsääntöisesti vain negatiivinen tapahtuma. Riski taas voi olla myös positiivinen asia. Uhka voi olla myös riskin tekijä/aiheuttaja. Riski taas voi muodostua uhka/haavoittuvuus/suojattava kohde yhdistelmästä.

Lähteet: Tietoturvasanasto, ISO31000

2.4 Miten määritellään organisaatiolta edellytettävä turvallisuuden taso?

Kaikkialla toitotetaan, että ei ole olemassa 100% turvallisuutta. Mikä on se taso, joka sitten vaikka meidän meille kriittisessä ICT-palvelussa pitää saavuttaa ja kuinka määritän tämän tason?

Ensinnäkin, tavoiteltava taso tulee määritellä organisaatiot – toiminto – palvelukohtaisesti. Periaatteessa kaikkien ICT-palveluiden tuottamisessa tarvittavien kriittisten infrastruktuuriratkaisuiden osalta (palomuuri, hakemisto- ja nimipalvelut) taso tulee asettaa erityisen korkealle, koska ne ovat ratkaisevassa roolissa usein kaikkien käytettävissä olevien ICT-järjestelmien osalta.

Organisaation tavoitteisiin nähden tehty riskienarviointi auttaa määrittämään suuntaa antavan tason, johon pyritään tavoitteiden saavuttamisen varmistamiseksi, esimerkiksi kriittisten järjestelmien konfiguraatioiden ym. Taso/aste tulee määrittää niiden vaikuttavuuden osalta tavoitteisiin nähden.

Tasapaino pitää hakea sen välillä, mitä maksaa olla suojautumatta paremmin ja paljonko parempi suojaus maksaa. Suojausten toteuttaminen aiheuttaa yleensä helposti ennakoitavia kustannuksia (muista huomioida myös suojauksen käyttämisen vaikutukset organisaation toimintaan!). Suojautumatta jättämisessä pelataan ei-toivottavien tapahtumien todennäköisyyksien, ja niistä seuraavien kustannusten ja tappioiden maastossa. Eräs riskin määritelmä on, että se on epävarman tapahtuman hinnan odotusarvo (todennäköisyys kertaa hinta). Jos suojaus maksaa vähemmän kuin riski, niin suojaus kannattaa toteuttaa. Tarkka riskien arviointi on vaikeaa ja käytännössä tyydytään jonkinlaisiin approksimaatioihin. Tästä päästäänkin riskinottokykyyn ja -halukkuuteen.

2.5 Mitä tarkoitetaan riskinottokyvyllä, entä riskinottohalulla?

Riskienottokyky tarkoittaa sitä, että on olemassa resilienssiä palautua, vaikka riski toteutuisi. Riskienottohalu on halukkuus toimia, vaikka riski on olemassa.

Riskienottohalukkuus ilmentää valmiutta/halua ottaa riskejä tehdessä päätöksiä tavoitteisiin nähden. Eli mitä riskejä ollaan halukkaita ottamaan, jotta tavoitteet mahdollisesti saavutetaan.

Riskienottokyky taas ilmentää riskien sietokykyä todellisuudessa suhteessa riskienottohalukkuuteen. Eli jos olet halukas ottamaan riskin tasolla x, niin kuinka sietokykyinen olet oikeasti, jos esim. x:n negatiiviset vaikutukset realisoituessaan ylittyvät.

2.6 Riskejä arvioidaan toteutuneen uhkan todennäköisyyden ja vaikutuksen tulona. Onko mahdollista saada mukaan vielä kolmatta näkökulmaa, aikaa?

Kyllä. Esim. palautumissuunnitelmaan on hyvä luonnostella myös palautumiseen käytettävä aika.

Riskejä, tai tarkemmin epävarmuuksia, tulisi aina tarkastella jotain aikahorisonttia vasten, koska jos sitä ei tehdä, niin kaikki on “mahdollista” riittävän pitkällä aikavälillä. Tyypillisesti tarkasteluväli on yksi vuosi tai esimerkiksi projektien osalta projektin (arvioitu) kesto.

Aika pitää ottaa huomioon todennäköisyyksien ja seurauksien arvioinnissa. Tapahtuman todennäköisyys riippuu tarkasteluhorisontista (esim. todennäköisyys, että tapahtuu *vuoden* aikana). Seurausvaikutuksissa voi olla tarpeen määritellä, kuinka kauas tulevaisuuteen seurauksia arvioidaan, varsinkin välillisten seurausten suhteen.

Sen lisäksi aikatekijä on tärkeä asia riskien vertailussa. Riskien vertailu on luontevinta samantyyppisten riskien välillä, ja samantyyppisissä riskeissä aikatekijä on yleensä samanlainen. Sen sijaan, jos vertaillaan ajallisesti erilaisia riskejä, vertailu voi olla huomattavasti hankalampaa ja tällöin joudutaan tekemään erilaisten riskien arvostuksia. Riskien luokittelu aikatekijöiden suhteen voi auttaa tällaisissa tilanteissa.

2.7 Minun pitäisi toteuttaa meidän organisaatiossa kyberriskien arviointi. Mistä kannattasi aloittaa, onko tähän jotain hyvää työkalua?

Yksinkertaisimmillaan riskiarvioinnin voi toteuttaa nelikenttänä. Nelikenttäanalyysi (SWOT) on yksinkertainen ja yleisesti käytetty yritystoiminnan analysointimenetelmä. Analyysin avulla voidaan selvittää yrityksen vahvuudet ja heikkoudet sekä tulevaisuuden mahdollisuudet ja uhat. Nelikenttäruudukon avulla yritys pystyy vaivattomasti arvioimaan omaa toimintaansa.
https://pk-rh.fi/tools/swot.html

Samoin Suomen Riskienhallintayhdistyksen sivuilta löytyvät:
https://pk-rh.fi/tools/haavoittuvuusanalyysi.html sekä
https://pk-rh.fi/tools/poa-analyysi.html

ISO31000 kuvaa riskienhallintaprosessin, jota voidaan soveltaa myös kyberriskien arviointiin. Eli tunnistetaan toimintaympäristö/arvioinnin kohde, arvioidaan riski (tunnista, analysoi, arvioi merkitys: tavoitteisiin), riskin käsittely(menetelmät), sekä näiden tallentaminen, viestintä ja seuranta. Riippuen organisaation kyvykkyyksistä ja resursseista, nämä voidaan tehdä Excelissä tai hankkia joku ohjelmisto. Ohjelmistoissa ei kuitenkaan usein voida tehdä kunnon mallintamista, jota taas mm. Excelissä voidaan tehdä. Excelissä taas ei ole varsinaisesti työkulkuja (workflow) tai niiden automatisointia, joita taas ohjelmistoissa yleensä on. Lisäksi ISO 27005 on standardi, joka on keskittynyt tietoturvariskien hallintaan.

Eräs tuore työkalu, josta on apua organisaation kyberriskien arvioinnissa, on Kybermittari (https://www.kybermittari.fi/). Se on Excelillä toteutettu itsearviointityökalu, jonka avulla voi hahmottaa organisaation kyberturvallisuuden hallinnan kypsyyttä ja kehitystarpeita.

2.8 Miten jäännösriski tunnistetaan ja määritetään?

Alkuperäistä riskiä, ilman kontrolleja, pienennetään riskienhallinnan keinoin, kunnes jäljelle jäävä riski, jäännösriski, on hyväksyttävällä tasolla tai ei ole syytä/järkevää pienentää enää.

Jäännösriski on se riskitaso, joka jää jäljelle, kun nykyiseen riskitasoon verrattuna toteutetaan *lisä*kontrolleja, jotta riski saadaan hyväksyttävälle tasolle tai sellaiselle tasolle, että ei ole syytä tai järkeä pienentää enempää.

2.9 Kaiken riskienhallinnan jälkeen meillä jää aina jäljelle iso määrä riskejä, joita ei saada mitenkään poistettua ja kyllä ne voi toteutua. Kenellä on vastuu hyväksyä ne?

Sen, jolla on päätöksentekovalta ja/tai sen, jolla on omistajuus ko. toimintoon (taloudellinen/rahoitus valta).

Organisaatiossa tulee olla päätetty ja kuvattu, ketkä ja mikä taso saa hyväksyä jäännösriskit sekä mitkä edellyttävät aina ylimmän johdon hyväksyntää. Ylin johto vastaa organisaation riskienhallinnan periaatteista ja päättää esimerkiksi heille tuotujen riskien osalta jäännösriskin määrän. Jäännösriski käytännössä tarkoittaa riskejä, joita ei saada poistettua tai joiden poistamisen kustannukset ovat suurempia kuin poistosta saatavat hyödyt.

2.10 Löytyykö jostain selkeää ohjetta, miten toteutan ja fasilitoin riskienhallintatyöpajan meidän johdolle ja sen jälkeen muulle henkilöstölle?

Työpajamenetelmä ei välttämättä ole paras tapa tehdä riskienarviointia, koska siinä ryhmädynamiikka saattaa vaikuttaa riskienarviointiin. Esimerkiksi ryhmäajattelu (group think) saattaa johtaa konsensukseen, joka ei ole validi. Joku saattaa pelätä auktoriteettia (authority bias), eli ei uskalla nostaa asioita esille auktoriteetin ollessa läsnä. Esim. näiden takia, kyselylomake riskeistä ja niiden tiedoista olisi parempi, koska saat anonyymisti kerättyä tietoja.

Kun tiedot on kerätty anonyymisti, voidaan käydä ne läpi palaverissa ja tarkentaa annettuja tietoja. Tämä ei myöskään syö osallistujien aikaa, kun arviot saa tehtyä erikseen silloin kun ajankohta sopii. Läpikäynti sitten auttaa tunnistamaan keskeiset epävarmuudet, joihin voidaan sopia hallintamenetelmät. Tässä myös hyvä huomioida, että tätä ei tule tehdä vain (neljännes)vuosittain, vaan kun päätöksiä tehdään ja/tai riskejä ilmenee. Eli joku ilmoituskanava riskeistä voisi olla olennainen (riski)indikaattoreiden osalta.

2.11 Miten tietosuojassa tehtävä riskienhallinta poikkeaa muusta riskienhallinnasta?

Tietosuoja-asetus edellyttää vaikutustenarviointia tietyissä tilanteissa. Vaikutustenarvioinnin yhtenä osana on henkilötietojen käsittelyyn liittyvien riskien arviointi. Periaatteessa toimintatapa on sama kuin muussakin riskienarvioinnissa eli riskit tunnistetaan, kuvataan, arvioidaan vaikutus ja todennäköisyys sekä määritetään hallintatoimenpiteet. Painopiste arvioinnissa on henkilötietojen käsittelyyn, prosessiin, järjestelmiin, ohjeistukseen jne liittyvien riskien havaitseminen, arvioiminen ja korjaavien toimenpiteiden hahmottaminen. Dokumentti liitetään yhteen muun vaikutustenarviointiin liittyvän dokumentaation kanssa.

Tietosuojan puolella tulee myös muistaa tarvittava vaikutustenarviointi. Vaikutustenarvioinnin tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Vaikutustenarvioinnissa kuvataan henkilötietojen käsittelyä, arvioidaan käsittelyn tarpeellisuutta, oikeasuhteisuutta ja henkilötietojen käsittelystä aiheutuvia riskejä sekä tarvittavia toimenpiteitä, joilla riskeihin puututaan. Tavoitteena on sen arviointi, onko jäljelle jäänyt riski oikeutettu ja hyväksyttävissä käsillä olevissa olosuhteissa. Vaikutustenarviointi auttaa rekisterinpitäjää tietosuojalainsäädännön vaatimusten noudattamisessa, sen dokumentoinnissa ja osoittamisessa.
Lisätietoja: https://tietosuoja.fi/vaikutustenarviointi

3 Toiminnan jatkuvuus ja varautuminen

3.1 Mitä toiminnan jatkuvuus ja varautuminen tarkoittavat?

Jatkuvuuden hallinta on ydintoimintojen varmistamista ennalta määriteltyjen mallien mukaan normaalioloissa, normaaliolojen häiriötilanteissa ja poikkeusoloissa.

Varautumisella tarkoitetaan toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen kaikissa tilanteissa. Varautumistoimenpiteitä ovat esimerkiksi riskien arviointi, jatkuvuus- ja valmiussuunnittelu, tekniset ja rakenteelliset etukäteisvalmistelut, koulutus, harjoitukset sekä tilojen ja kriittisten resurssien varaukset. Varautuminen jakaantuu suunnitteluun, sen edellyttämiin käytännön valmistelutoimenpiteisiin, näiden toteuttamiseen ja kehittämiseen sekä harjoitteluun.

Lähde:
VAHTI 2/2016 Toiminnan jatkuvuuden hallinta - https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2016_pdf.pdf

3.2 Tarvitsemmeko valmiussuunnitelmaa, missä tämä määritellään?

Valmiussuunnitelman tarve määritellään valmiuslaissa:
https://www.finlex.fi/fi/laki/ajantasa/2011/20111552

3.3 Miten varmistan meidän hankinnoissa, että toimittaja huolehtii riittävästi palvelun jatkuvuudenhallintaan ja saatavuuteen liittyvistä meidän vaatimuksista?

Jatkuvuudenhallinta ja saatavuus on määriteltävä jo hankintavaihessa ja myös kirjattava sopimuksiin.

Sovittujen asioiden toteutumista ja hallintaa on myös valvottava. Jatkuvuudenhallinnan ja poikkeamanhallinnan harjoittelu ovat yksi keino valvoa asiaa.

3.4 Mitkä ovat yleisimmät skenaariot, joihin tulisi olla varauduttu?

Jos meidän pitäisi tunnistaa kymmenen yleisintä sellaista skenaariota tai tilannetta, joka vaarantaa meidän organisaation toiminnan, mitkä ne mahtaisivat olla? Siis varmasti sellaisia, joihin eniten on käytännössä törmätty.

1. Sähkönjakelun aiheuttamat häiriöt eri kohteissa

   Esimerkiksi oma konesali, palvelutoimittajan konesali, organisaation toimitila tai muut kriittiset toimisto- ja tuotantotilat. Sekä paikallisesti, mutta myös laajemmalla alueella.

2. Tietoliikenneyhteyksien toimimattomuus

   Alkaen yksittäisestä toimipisteestä laajentuen laajavaikutteiseen ja pitkäkestoiseen alueelliseen häiriöön.

3. Tietoverkkorikollisten aiheuttama uhka

   - esimerkiksi kyberhyökkäykset, kiristyshaittaohjelmat ja muu toiminnan tarkoituksellinen häirintä

   Tietoverkkorikolliset ovat ottamassa käyttöön entistä agressiivisempia menetelmiä esimerkiksi lunnaiden vaatimisen osalta. Tämän ohella organisaation tulee varautua uudenlaisiin huijauksiin sekä muihin menetelmiin, joilla henkilöstöltä yritetään kalastella tietoa tai informaatiovaikuttamisen keinoin vaikuttaa heihin.

4. Henkilöstön saatavuus

   Eräs perinteinen skenaario liittyy siihen, että henkilöstö ei pääse työpaikalle. Nyt käynnissä oleva koronaviruspandemia on aiheuttanut osin käänteisen ilmiön, henkilöstö on ohjattu työskentelemään etänä. Tällöin korostuu etätyön osalta kaikki ne uhat ja riskit, jotka normaalisti tulisi tunnistaa ja hallita työskenneltäessä työpai

5. Toimimattomat järjestelmät tai prosessit

   Esimerkiksi teknisissä ongelmissa tuen puute (toimittajan puolelta); ei ole sovittu, mitä tehdään ongelmatilanteissa ongelmallisina aikoina, vaan oletetaan korjausten hoituvan samalla tavalla tavallisena tiistaina ja jouluyönä. Tässä on iso vastuu myös palvelun tilaajalla: vaadittavien päätösten tekijä on oltava tavoitettavissa tai päätösvaltaa on uskallettava delegoida palveluntuottajalle. [Onko tämä sitä, mitä edellisessä kohdassa tarkoitetaan toimimattomalla prosessilla?]

6. Järjestelmien vanheneminen tai poistaminen saatavilta

7. Jatkuvat muutokset, osaaminen ei pysy samalla tasolla muutosten kanssa

8. Lainsäädännön muutokset – toimintaa ei pystytä saattamaan lain vaatimalle tasolle

9. Fyysinen tuho (tulipalo, tilojen tuhoutuminen)

10. Tietojen menettäminen muun kuin tahallisen häirinnän tuloksena. (Laiterikot, vahingot jne).

11. Ei ole rahaa, tai ei ole budjetoitu tietylle oleelliselle toiminnalle riittävästi rahaa (taloudelliset ongelmat).

12. Ei ole riittävästi henkilökuntaa (henkilöstö ongelmat, ei tekijöitä).

3.5 Harjoitus lunnashaittaohjelmahyökkäystä vastaan

Esimieheni pyysi minut toteuttamaan yksinkertaisimman mahdollisen harjoituksen siltä varalta, että lunnashaittaohjelma pääsee meidän verkkoon ja tietokoneisiin, miten tällainen kannattaisi toteuttaa?

Harjoitus voidaan toteuttaa esim. ruutupaperiharjoituksena, jossa käydään läpi johtaminen, viestintä, teknisen ylläpidon tehtävät ja muut toimintaskenaariot.

Harjoituksena tämä on myös siinä mielessä “aito”, että haittaohjelman ollessa verkossa koneita ei kannata käyttää.

3.6 Osallistuimme vuosina 2018 ja 2019 TAISTO-harjoituksiin, mutta viimevuonna jäi väliin. Kai noita tulee vielä jatkossa?

Digi- ja väestötietovirasto on sitoutunut vuoden 2018 ensimmäisen harjoituksen jälkeen toteuttamaan niitä ainakin 2019-2022. Tämän jälkeen tarve arvioidaan uudelleen. Löydät lisätietoa harjoituksista https://dvv.fi/taisto. Sivustolta löytyy myös linkki uuteen TAISTOmaatti-harjoitusautomaatti-palveluun, joka on digitalisoitu, organisaation oman aikataulun mukaisesti toteutettava TAISTO-harjoitus. Tämä ensimmäinen TAISTOmaatti-harjoitus pohjautuu vuoden 2019 TAISTO19-harjoitukseen.

3.7 Meillä ei ole resursseja hoitaa kaikkia mahdollisia asioita kuntoon, mitkä on yleensä ne kriittisimmät asiat, joiden jatkuvuudesta meidän tulisi huolehtia. Olemme ulkoistaneet kaiken paikalliselle yritykselle.

Sopimusten tärkeys korostuu ulkoistustilanteissa. On avainasia hoitaa sopimukset siihen kuntoon, että jatkuvuus on varmistettu. Sopimuksen hinta varmasti nousee sitä mukaa, kun sopimukseen lisätään vaatimuksia palveluntuottajalle. Jatkuvuuden hallinta maksaa, mutta sen hallitsemattomuus se vasta maksaakin.

3.8 Käytämme lähes kokonaan pilvipalveluita, onko meidän tarvetta miettiä näitä jatkuvuusasioita, koska “pilvifirma” hoitaa kaikki häiriötilanteet?

On tarvetta miettiä. Tähän vaikuttaa erittäin paljon organisaation toiminnan luonne eli palveluiden ja tietojen kriittisyys. Tätä kautta organisaatiolle syntyy velvoitteet huolehtia esimerkiksi tietojen saatavuudesta, jonka tulisi ohjata kaikkia digiturvan osa-alueita.

Esimerkiksi jatkuvuus voidaan varmistaa käyttämällä kahta tai useampaa pilvitoimijaa joihinkin tarkoituksiin. Joskus myös netti ei vain toimi. Silloin ei auta, että pilvipalveluntarjoajalla on konesaleja kolmella mantereella ja aurinkoa seuraava SOC-toiminto (turvallisuusoperointikeskus). Jatkuvuusasioiden miettiminen voi siis tarkoittaa muun muassa sen miettimistä, että millä keinoilla edes jonkinlainen internetyhteys saadaan varmistettua. Pitäisikö hankkia satelliittipuhelin yrityksen kriittisten toimintojen internetyhteyttä varten siltä varalta, että netti on koko Suomesta pari tuntia poikki? Vai hyväksytäänkö se, että yrityksen toiminta seisoo sen pari tuntia?

3.9 Eihän tietosuoja-asiat liity mitenkään jatkuvuus ja varautumisasioihin?

Kyllä liittyy. Tietosuojan tulee olla sisäänrakennettu muuhun toimintaan. Asiakkaiden tietosuojan loukkaus on monella tapaa riski organisaation maineelle ja sitä myötä asiakkaiden luottamukselle ja sitä myötä asiakkaiden halulle jatkaa asiointia. Miettikää esimerkiksi Psykoterapiakeskus Vastaamon tapausta.

3.10 En ole varma, mutta voi olla, että meidän firman kaikki tiedot sijaitsevat jossain pilvessä ulkomailla. Tuli vain mieleen, että jos kaikki tietoliikenneyhteydet menee poikki maailmalle, mitä me silloin tehdään?

Tämä tulisi olla mietittynä ennakolta ja otettuna huomioon sekä riskienhallinnan että toiminnan jatkuvuuden ja varautumisen näkökulmasta. Mikä on se aika, kuinka kauan organisaatio tulee toimeen ilman palveluita ja tietoja, jotka pilvessä sijaitsevat. Onko olemassa jotain keinoa, jolla tiedot saadaan tällaisessa tilanteessa käyttöön myös Suomesta?

4 Tietoturvallisuus

4.1 Mitä tietoturvallisuudella tarkoitetaan?

Tietoturvallisuus koostuu kolmesta osa-alueesta, joita voidaan edellyttää käsiteltävänä olevien tietojen tai niiden käsittelyssä tarvittavien palveluiden, tilojen osalta.

Tietoturvallisuus kattaa järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus Saatavuus tarkoittaa tietoturvallisuuden yhteydessä sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvallisuus on riskienhallintaa.

https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-82008-valtionhallinnon-tietoturvasanasto

4.2 Nyt kun tiedonhallintalaki on astunut voimaan 1.1.2020, saisinko yksinkertaiset ohjeet siitä, milloin tiedot pitää luokitella turvallisuusluokitelluksi?

Tiedonhallintalakiin liittyvä kattava ohjeistus löytyy osoitteesta:
https://vm.fi/tiedonhallintalautakunta

Esimerkiksi tähän liittyen sivustolta löytyy:
Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

4.3 Pelkään hakea töihin sellaiseen työpaikkaan, jossa tehdään turvallisuusselvityksiä, koska nuoruudessa vähän hölmöilin. Eikö musta koskaan tule virkahenkilöä?

Kyllä voit päästä töihin sellaiseen organisaatioon, joka tekee henkilöstöstä turvallisuusselvityksen. Mikäli selvityksessä löytyy jotain historiatietoja, ne käydään huolella läpi ja arvioidaan, kuinka kauan tapahtumasta on kulunut aikaa ja voiko se vaikuttaa tehtävien hoitamiseen.

Löydät vastauksia näihin kysymyksiin Suojelupoliisin sivuilta:
https://supo.fi/usein-kysyttya-turvallisuusselvityksista

Sivulla on esimerkiksi kysymys: Voiko menneisyyden maksuhäiriömerkintä estää turvallisuusselvityksen läpäisyn:

”Kyllä ja ei. Turvallisuusselvitys ei ole yksittäinen päätös, vaan siinä selvitetään haettavan työn kannalta merkitykselliset asiat. Turvallisuusselvityksen hakija (esimerkiksi työnantaja) päättää itsenäisesti, millaisilla asioilla on merkitystä rekrytoinnin kannalta. Menneisyyden maksuhäiriöt, kuten ulosottoon menneet perinnät, voivat joissakin tapauksissa tulla turvallisuusselvityksessä ilmoitettaviksi. Maksuhäiriömerkinnät käydään siis läpi tapauskohtaisesti. Suojelupoliisi ei koskaan tee päätöstä rekrytoinnista, vaan päätöksen tekee aina työnantaja.”

4.4 Salasanaturvallisuus on digitaalisen turvallisuuden kulmakiviä, koska kaikki palvelut eivät vielä tue monivaiheista kirjautumista. Mitä menetelmää tai palvelua suosittelette turvalliseen ja kätevään salasanojen hallintaan työ- tai yksityiselämässä?

Suosittelemme salasanan hallintaohjelman käyttöönottoa. Tästä löytyy kysymys ja vastaus tämän materiaalin lopusta.

4.5 Voiko salasanani olla esimerkiksi AkuAnkkahevolintukukka ja se on turvallisempi kuin H4&gD2”(?

Voi ja on turvallisempi. Merkittävimmät tekijät salasanoissa on sen “pituus” eli merkkien määrä ja se että salasana on “yksilöllinen” eli ei esiinny omana sananaan jossakin. Lisäksi samaa salasanaa ei kannata käyttää useissa palveluissa vaan yksi salasana/palvelu.

Katso esimerkiksi https://pidempiparempi.fi/.

4.6 Kuulin joskus väitettävän, että voin kirjoittaa salasanan paperille tai vaikkapa kännykkääni selväkielisenä, jos samassa ei ole käyttäjätunnusta tai palvelua, johon niitä voi käyttää?

Tällaisenaan ei kannata. Joka ilkeämielinen, joka saa haltuusi salasanasi, voi selvittää käyttäjätunnuksesi jollain toisella keinolla. Sen sijaan, jos lisää salasanaan jotain sellaista, jonka sinä vain tiedät, tätä voidaan pitää hyvänä käytäntönä. Eikä tätä kannata tehdä niin, että jokaisen salasanan alkuun lisää vaikkapa *poista* vaan se voi olla esimerkiksi joka salasanan alkuun ja loppuun vaikkapa kaksi satunnaista kirjainta/merkkiä tai salalauseessa jokin sana. Itse tiedät ja muistat, että tämä pitää poistaa, jos joudut kaivamaan salasanan esille.

Lisäksi monissa salasanojen hallintaohjelmissa ei ole mahdollisuutta palauttaa unohtunutta pääsalasanaa, joten jos pääsalasana pääsee unohtumaan eikä sitä ole missään muualla tallella, niin silloin et voi käyttää mitään hallintaohjelmaan tallentamiasi tietoja. Kaikkien käyttämiesi palveluiden unohtuneiden salasanojen palauttaminen palvelu kerrallaan voi vaatia valtavan työmäärän. Siksi tällainen erittäin tärkeä salasana voi olla perusteltua kirjoittaa paperille tai osia salasanasta usealle paperille ja säilyttää papereita turvallisissa paikoissa, joihin murtautumisen voit helposti havaita. Turvallinen paikka voi olla esimerkiksi henkilökohtainen lokero työpaikkasi turvakaapissa.

4.7 Miksi ei kannata käyttää edes vapaa-ajalla Facebookin, Googlen tai vastaavien some-palveluiden kautta tapahtuvaa kirjautumista johonkin uuteen palveluun?

Mikäli jostain syystä kyseisen palvelun salasana päätyy ulkopuolisille henkilöille, hän saa samalla pääsyn kaikkiin niihin palveluihin, joihin olet tällä samalla tunnistautumisella sallinut pääsyn. Suosittelemme käyttämään jokaiseen palveluun sen omaa tunnistautumismenetelmää.

4.8 Kuka oikeasti lukee noiden älypuhelimien sovellusten käyttöehdot?

Minä. Ja se on tuskallista.

Käytännössä noiden seikkaperäinen lukeminen on mahdotonta. Sen sijaan huomattavasti suositeltavampaa on katsoa, mitä oikeuksia kyseinen sovellus ottaa käyttöön ja poistaa sellaiset, joita ei salli puhelimellaan käytettävän. Tärkeimmät ovat mikrofoni ja kmera, paikkatieto sekä pääsy laitteella oleviin tietoihin kuten valokuviin, paikkatieto ja kaiutin.

4.9 Millainen vaara tulee siitä, jos liityn Suomessa johonkin julkiseen wifi-verkkoon, joka ei ole salasanalla suojattu?

Verkkoliikennettäsi voidaan mahdollisesti vakoilla ja sinut saatetaan saada ohjattua käyttämään palvelimia, joita ei ollut tarkoitus käyttää (esim. harhauttaa kirjautumaan oikealta näyttävään palveluun)

4.10 Voitteko avata, mitä VPN tarkoittaa ja miksi se pitäisi olla tietokoneessa käytössä?

Salattu tiedonsiirtoyhteys kahden laitteen välillä. Kun se on käytössä, tiedon luottamuksellisuus ja eheys säilyy sinun käyttämän laitteen ja sen VPN:n toisen pään välillä. VPN on lyhenne sanoista Virtual Private Network eli virtuaalinen yksityisverkko, joka muuttaa esimerkiksi muuten avoimen internet-verkon käytön paljon turvallisemmaksi.

4.11 Kimmo Rousku on mainostanut palvelua, josta voi tarkistaa, onko oma salasana ollut jossain palvelussa, josta se olisi päätynyt rikollisille? Voiko tällaiseen palveluun luottaa.

Kimmo Rousku: Olen mainostanut kahta palvelua, tunnetun Australialaisen tietoturva-asiantuntija Troy Huntin palvelua https://haveibeenpwned.com/ sekä F-Securen vastaavanlaista palvelua https://www.f-secure.com/fi/home/free-tools/identity-theft-checker. Itse käytän niitä vapaa-ajan sähköpostin turvallisuuden varmentamiseen.

Tällaisen palvelun tuottajan tulee itse varmistaa, onko palvelu voimassa olevan lainsäädännön mukainen. Samoin näissä ei tule käyttää mitään sellaista palvelua, jonka turvallisuudesta ei voi varmistua.

4.12 Jos en luota täysin kotikoneeni virustorjuntaohjelmaan, voinko käyttää jotain palvelua esimerkiksi yksittäisen, sähköpostin kautta tulleen liitetiedoston skannaamiseen?

Itse olen vastaavissa tilanteissa käyttänyt https://www.virustotal.com/gui/ -palvelua, joka skannaa tiedoston yli 70 erilaisella haittaohjelmien tunnistamiseen tarkoitetulla ohjelmistolla.

Tätä ***ei saa käyttää*** työtehtävissäsi käsittelemiesi tiedostojen tarkastamiseen. Huomaa, tänne ei saa lähettää kuin julkisia tiedostoja, joissa ei ole esimerkiksi henkilötietoja. En käytä tätä kuin poikkeustilanteissa vapaa-ajan postiini tuleviin epäilyttävien tiedostojen tarkastamiseen. Kannattaa huomata, että edes tämä palvelu ei tunnista ns. uutta, toistaiseksi tuntematonta haittaohjelmaa, esimerkiksi kohdistettua APT-uhkaa.

4.13 Miksi läheskään kaikki kotonani olevat nettiin liitetyt laitteet eivät osaa päivittä omaa ohjelmistoaan automaattisesti? Esimerkiksi meidän älytelkkarin päivittäminen on hirveän hankalaa.

Kulutuselektroniikassa hintakilpailu on kovaa ja valmistajien katteet pieniä. Kuluttajat ostavat tuotteita niiden uusien ominaisuuksien ja nopeuden perusteella. Nopeasti markkinoille päässyttä tuotetta myydään enemmän kuin hitaammin markkinoille päässyttä tuotetta.

Koska ohjelmistopäivityksen tekeminen ei ole kuluttajalle näkyvä eikä usein kuluttajaa kiinnostavakaan ominaisuus ostohetkellä, niin valmistajien ei kannata panostaa päivityksen tekemisen kehittämiseen helposti käytettäväksi.

Tähän ongelmaan esimerkiksi Traficomin Tietoturvamerkki (https://www.tietoturvamerkki.fi/) tuo helpotusta sekä valmistajille että kuluttajille.

4.14 Salakuunteleeko puhelimessani oleva Facebook ohjelma minua? Niin monesti käy niin, että kun juttelen mieheni kanssa jostakin, pian siitä löytyy jommankumman Facesta heti mainoksia?

Tästä on ollut paljon keskustelua. Nyytietojen perusteella, normaali some-palvelut eivät kuuntele käyttäjiä ilman lupaa. Totuutta on vaikea tietää ja laitteilla on muitakin

ohjelmia sekä keinoja, jotka voivat siirtää tietoja mainostajille. Sen sijaan jos käytössäsi on ns. älykaiutin tai laitteen digitaalinen assistentti (esimerkiksi Apple Siri), se kuuntelee ja odottaa ääniohjeita, joka kannatta erityisesti etänä kotona ja muualla työskenneltäessä huomioida.

4.15 Onko laitonta käyttää avointa wifi-verkkoa, josta en tiedä, kenen se on? Esimerkiksi meidän kerrostalossa on parikin sellaista ja toimivat nopeasti.

Jos wifi-verkon käyttämiseen ei tarvita salasanaa, sen käyttämiselle ei ole laillista estettä. Vaikeampi kysymys on, saako käyttää wifi-verkkoa, joka ei mainosta SSID:tään (verkkotunnustaan eli ”verkon nimeä”. Kannattaa varmaan jättää käyttämättä sellaista verkkoa, jos ei ole saanut omistajalta lupaa sen käyttöön. Wifin sijaan voit jakaa turvallisemmin oman älypuhelimesi 4- tai 5G-yhteyden omaan käyttöösi.

4.16 Onko todella niin, että nämä puhelimien sirit ja muut tai amazonin älykaiuttimet kuuntelee päällä ollessaan kaikkea? Ja kaikki kiertää jonkin pilvipalvelun kautta?

Tässä on varmasti laitekohtaisia eroja. Eivät välttämättä kaikkea, yleensä laitteet aktivoituvat avainsanan kuultuaan, asetuksilla voi vaikuttaa toimivuuteen. Toisinaan laitteet voivat vahingossa mennä kuuntelutilaan. Jokaisen, joka ottaa kotonaan tai puhelimessaan tällaisen käyttöön, tulee ymmärtää tähän liittyvät riskit, erityisesti työtehtäviin liittyviä asioita hoitaessaan, myös puhelimella puhuessaan.

4.17 Jos haluan käyttää älypuhelinta, mutta en halua lainkaan vaarantaa yksityisyyttäni, voinko käyttää sitä ilman kirjautumista minnekään vaikkapa pelkästään selaimella?

Riippuu käytettävästä älypuhelimesta ja sen käyttämästä ekosysteemistä. Yleensä puhelimen www-selaimen käyttäminen ei edellytä kirjautumista. Sen sijaan jos haluat käyttää appseja, sovelluksia, tämä edellyttää kirjautumista.

4.18 Olen törmännyt välillä sanoihin TOR ja darknet tai darkweb. Mitä noi ovat, miten niihin pääsee?

Osa Internetiä, joka ei löydy ns. tyypillisillä hakukoneilla. Ideana on turvata käyttäjien anonymiteetti mahdollisimman hyvin. Tarvitset TOR-selaimen (tai lisäosan).

Emme suosittele näiden palveluiden käyttöä, ellet tiedä, mitä olet tekemässä. Näissä ympäristöissä voit törmätä sellaiseen materiaaliin, jota et toivo saavasi nähtävillesi.

4.19 Onko hirveästi väliä, jos asennan tietsikkaani tulevat päivitykset aika myöhässä, joskus menee muutama viikko ennen kuin buuttaan koneeni?

Riippuu mitä koneella tekee ja kuinka kriittisestä päivityksestä on kyse ja mille verkkosivustolle tai vastaavaa palvelua käyttää. Haavoittuvuuksia voi hyödyntää monella tavalla.

Käytännössä siis on! Kyberrikolliset kehittyvät yhä paremmiksi siinä, miten nopeasti ne kehittävät tunnettujen haavoittuvuuksien hyväksikäyttömenetelmiä. Suosittujen ohjelmistojen vakaviin haavoittuvuuksiin rikolliset saattavat kehittää hyväksikäyttömenetelmän alle vuorokaudessa päivityksen julkaisemisesta. Etenkin organisaatioiden ICT-palvelininfrastruktuurista vastaavien tulee jatkossa kyetä entistä nopeammin testaamaan ja ajamaan tulleet kriittiset päivitykset. Maaliskuussa 2021 merkittävä Microsoft Exchange-palvelinohjelmiston haavoittuvuus on aiheuttanut myös Suomessa merkittävän määrän tietomurtoja.

Rikolliset liittävät hyväksikäyttömenetelmiä osaksi haittaohjelmia, joita he levittävät esimerkiksi sähköpostin välityksellä. Lisäksi rikolliset muuntelevat jatkuvasti haittaohjelmatiedostoja, jotta virusskannerit eivät tunnistaisi niitä. Aina jossakin joku saa ensimmäisenä uuden version haittaohjelmasta, jota mikään virusskanneri ei tunnista. Silloin tietokoneen suojaus on pitkälti kiinni siitä, onko sen ohjelmistot päivitetty vai onko niissä haavoittuvuuksia, joiden avulla haittaohjelma pääsee salaa pureutumaan koneeseen.

4.20 Mikä on hakkerin ja krakkerin ero?

Hakkeri on tietotekniikan osaava harrastaja, krakkeri on pahantahtoinen murtautuja. On puhuttu myös valkoisia, harmaita tai mustia hattuja käyttävistä hakkereista sen mukaan, miten eettisesti hakkeri käyttää taitojaan, mutta värien käyttäminen toimijan eettisyyden kuvaamiseen on arveluttavaa ihmisten yhdenvertaisuuden kannalta (miksi muka musta on paha ja valkoinen hyvä?). Puhukaamme siis enintään hyvis- ja pahishakkereista. Pahishakkeri ja krakkeri ovat siis sama asia.

4.21 Miten tunnistan sähköpostista helpoiten, että se on mahdollisesti jokin huijaus? Mitkä olisivat hyviä tuntomerkkejä?

Omituinen lähettäjäosoite tai vastaavasti hyvin aidon näköinen lähettäjäosoite, jossa saattaa olla yhden merkin ero aitoon. Vaikka niin, että kirjain o on korvattu nollalla tai kirjain m korvattu kahdella n kirjaimella. Kiireessä näitä on huono havaita.

Viesti saattaa tosin tulla ihan aidostakin osoitteesta, joka on kaapattu. Myös kiireelliset pyynnöt rahansiirtoon tai kiireellinen pyyntö kirjautua lähetettyyn linkkiin ovat vaaran merkkejä. Siirtämällä hiiren kursorin linkin päälle, voit usein varmistaa minne, linkki oikeasti on viemässä. Myös se, että henkilö, jonka kanssa viestit normaalisti suomeksi, yhtäkkiä lähettää sinulle viestin englanniksi tai viesti muuten vaikuttaa siltä, että henkilö ei normaalisti kirjoita viestin tyylillä. Myös ns. Luottamukselliset pyynnöt, joissa vedotaan sinuun, ettet kerro kenellekään ja hoidat jonkun asian ohi virallisten prosessien ovat yleinen tapa huijauksissa.

Saat “johtajalta” viestin, jossa hän kertoo, että on kuullut, että sinä olet luotettava henkilö. “Johtaja” pyytää sinua siirtämään rahaa (tai tekemään jonkun toimenpiteen) puolestaan koska ei juuri nyt pääse sitä itse tekemään. Kyseessä on tietysti hätätilanne ja äärimmäisen kiireellisesti tarvitsee juuri sinun apuasi. Tässä vaiheessa hälytyskellojen pitäisi soida aika lujaa. Viestintä saattaa siirtyä myös käyttämäänne pikaviestimeen, jos aito tili on saatu kaapattua.

Huijauksissa vedotaan usein inhimillisiin tekijöihin kuten kiire, tärkeys, salaisuus, raha/ahneus/halpuus, kertaluonteisuus, auktoriteetti, jne. Jos asia tuntuu uskomattomalta –se todennäköisesti sellainen onkin. Kannattaa aina epäilyttävissä tapauksissa kysyä asiaa muualta.

4.22 Nettihuijari sai huijattua minua nettikirppiksellä ja tavarat jäivät tulematta, mutta eurot meni. Ei kai kannata muuta kuin kääriytyä vilttiin ja mennä piiloon häpeämään mokaani ☹.

Tästä koitui se oppi, että seuraavalla kerralla et ole niin helposti huijattavissa! Pienistäkin petoksista kannattaa tehdä rikosilmoitus. Kyllä poliisi selvittää niitäkin. Jos ei heti, niin ehkä vuoden tai parin päästä huijari tekee ratkaisevan virheen ja jää kiinni. Ilman rikosilmoitusta poliisi ei tutki.

4.23 En ole varma, mistä asioista kannattaa tehdä rikosilmoitus, milloin pitäisi ottaa yhteyttä Tietosuojavaltuutetun toimistoon tai Kyberturvallisuuskeskukseen.

Rikosilmoitus kannattaa tehdä aina kun on kyseessä taloudellinen tappio, muu vahinko, jota voi mitata, tai kunnian tai kotirauhan loukkaus. Kun teet rikosilmoituksen, poliisi voi selvittää tekijän ja hänet voidaan saattaa vastuuseen teostaan.

Tietosuojavaltuutetun toimistoon ilmoitetaan henkilötietojen loukkauksista ja sellaisten epäilyistä. Tietosuojavaltuutetun toimistossa toimiva seuraamuskollegio voi määrätä hallinnollisia seuraamusmaksuja tietosuojaa rikkoneille.

Kyberturvallisuuskeskukseen voi ilmoittaa tietomurroista, haittaohjelmatartunnoista ja haittaohjelmien levittämisestä, tietojen kalastelusta ICT-välineillä, palvelunestohyökkäyksistä ja yleisten viestintäpalveluiden toimivuushäiriöistä, sekä tällaisten epäilyistä.

Kaikista em. paikoista voi myös kysyä, onko ilmoituksen teko aiheellista.

5 Tietosuoja

5.1 Mitä tietosuojalla tarkoitetaan?

Jokaisella on oikeus henkilötietojensa suojaan. Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.
https://tietosuoja.fi/tietosuoja

5.2 Mitä tietovuodolla tarkoitetaan?

Tietovuoto tarkoittaa salassa pidettävän tai yksityiseksi tarkoitetun tiedon levittämistä ulkopuolisille tahoille.

Tietovuodossa julkaistut tiedot voivat olla esimerkiksi tunnuksia, salasanoja, henkilötunnuksia, osoitteita tai maksukorttitietoja. Useimmiten tietovuodon tarkoituksena on rahallinen hyötyminen. Tietovuodon aikaansaava henkilö yleensä murtautuu yrityksen tai palvelun tietokantaan.

5.3 Nyt jos tapahtuu joku hakkerointi ja meidän palvelusta vuotaa jonnekin tietoja, siitä pitäisi käsittääkseni ilmoittaa jonnekin 72 tunnin sisällä, minne ja miten?

Henkilötietojen tietoturvaloukkauksesta pitää ilmoittaa 72 tunnin sisällä tietosuojavaltuutetun toimistolle (paitsi jos loukkauksesta ei aiheudu rekisteröidyille minkäänlaista riskiä). Ilmoituksen voi tehdä tietosuojavaltuutetun toimiston nettisivujen lomakkeella (https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta). Löydät lisätietoa aiheesta https://tietosuoja.fi/tietoturvaloukkaukset

5.4 Organisaatiomme työntekijältä katosi usb-tikku, jossa oli noin 20 meidän organisaation henkilöstön hr-tietoa, mukaan luettuna henkilötunnus. Muistitikku on kuitenkin salattu monimutkaisella salasanalla. Onko tämä kuinka iso riski ja mitä kannattaisi tehdä?

Riski riippuu kyseessä olevien henkilötietojen laadusta ja salauksen laadusta. Kannattaa tutusta edellä mainittuun lisätietosivustoon.

5.5 Meillä on pohdittu sitä, että jos meidän henkilötietoja sisältävään verkkopalveluun a) kohdistuu palvelunestohyökkäys tai b) iskee lunnashaittaohjelma, joka estää tietojen saatavuuden, onko tämä silloin henkilötietojen tietoturvaloukkaus?

On. Myös henkilötietojen saatavuuteen ja eheyteen vaikuttavat tietoturvaloukkaukset ovat henkilötietojen tietoturvaloukkauksia.

5.6 Miksi henkilötietojen luovuttamisesta EU-alueen ulkopuolelle kohkataan niin paljon? Matkustettiinhan me ennen koronaa kaikkialla maailmassa!

EU:n tietosuojasääntelyn ajatuksena on taata tietty tietosuojan taso ja varmistua siitä, että tiedot on suojattu riittävästi myös silloin, kun niitä siirretään EU:n ulkopuolelle sellaisiin maihin, jossa lainsäädäntö ei välttämättä takaa samanlaista tasoa. Matkustaessa henkilö tietää itse, mihin maahan matkustaa ja mitä tietoja antaa, mutta ympäri maailmaa tuotettavien verkkopalveluiden osalta tilanne ei monestikaan ole yhtä selkeä – siksi sääntelyllä on pyritty varmistamaan, että EU-alueella voi luottaa siihen, että tiedot on suojattu myös silloin, kun tietoja siirretään EU:n ulkopuolelle.

5.7 Nyt on tullut valtavasti kaikenlaisia kivoja teknisiä härpättimiä markkinoille, joista osa on tosi halpoja, mutta niiden mukana tulee joku kiinalainen appsi. Hieman olen miettinyt, uskaltaako tuollaisia laitteita ostaa ja miten niiden tietoturvasta ja tietosuojasta on huolehdittu?

Katso vastaus kysymykseen 4.13.

Miksi ihan julkiset tiedot kuten nimi ja osoite, puhelinnumero yms ovat henkilötietoja? Niitähän käsitellään koko ajan kaikkialla. Eikös ne voisi julkista vapaasti käytettäväksi ilman mitään sen ihmeempää?

Lue lisää:
https://tietosuoja.fi/mika-on-henkilotieto:

5.8 Tietosuoja-asetuksessa hehkutettiin tietojen siirrettävyyden helpottumista. Itse en ole vielä törmännyt kertaakaan siihen, että olisin voinut hyödyntää tätä?

Voit käyttää oikeutta esimerkiksi siihen, että saat selville, mitä tietoja sinusta on järjestelmään kirjattu. Tai jos olet siirtymässä yksityisestä palvelusta toiseen, tämä voi joissakin tilanteissa helpottaa siirtymistä.

5.9 Löysin nettipalvelusta vääriä tietojani ja palvelu ei suostu korjaamaan niitä, mitä kannattaisi seuraavaksi tehdä?

“Jos rekisterinpitäjä kieltäytyy oikaisemasta tietojasi, sen täytyy kertoa sinulle kieltäytymisen syyt. Kieltäytymisen on aina perustuttava lakiin. Jos kieltäytymiselle ei mielestäsi ole perusteita, voit tarvittaessa ottaa yhteyttä tietosuojavaltuutettuun.” Lähde: https://tietosuoja.fi/kun-haluat-oikaista-tietojasi

5.10 Sain sähköpostiini kokonaan toiselle henkilölle tarkoitetun sähköpostiviestin, jossa oli mielestäni arkaluonteisia tietoja. Tämä selvisi vasta luettuani koko viestin. Miten tällaisessa tilanteessa tulisi toimia?

Kerro tapahtuneesta viestin lähettäjälle. Voit myös ilmoittaa asiasta Tietosuojavaltuutetun toimistoon. Jos epäilet viestin saamisen johtuvan rikoksesta, tee rikosilmoitus asuinkuntasi poliisille. Liitä viesti täydellisenä otsaketietoineen rikosilmoitukseen. Näiden toimenpiteiden jälkeen poista erheellisesti saamasi viesti. Älä ilmaise minnekään muualle viestin sisältöä tai sitä, että olet ylipäänsä saanut viestin, äläkä käytä viestin sisältöä mitenkään hyväksesi (katso laki sähköisen viestinnän palveluista (917/2014) 136 §).

6 Kyberturvallisuus

6.1 Mitä kyberturvallisuudella tarkoitetaan?

Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia.

Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot.

Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.

Keskeiset tavoitteet ja toimintalinjat, joiden avulla Suomi vastaa kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistaa sen toimivuuden, määritellään Suomen kyberturvallisuusstrategiassa (valtioneuvoston periaatepäätös 24.1.2013).

Lähde: Kyberturvallisuuden sanasto - https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

6.2 Mitä tarkoittaa kyberhyökkäys?

Tietoverkon kautta tehtyjä toimenpiteitä, joilla pyritään vaikuttamaan kohteen toimintakykyyn.

6.3 Mitä on kyberdiplomatia?

Esimerkiksi valtioiden välistä yhteistyötä, jossa käsitellään kansainvälistä oikeutta ja normeja, kyberturvallisuutta, muita luottamusta lisääviä toimia ja internetin hallintaa. Toiminnan tarkoituksena on lisätä luottamusta ja keskinäistä yhteisymmärrystä, luoda yhteisiä pelisääntöjä, joiden avulla vähennetään erilaisten konfliktien uhkaa.

6.4 Miten hybridivaikuttaminen ja hybridiuhat liittyvät kyberturvallisuuteen?

Kyberhyökkäykset ja muu ICT-järjestelmien kautta tehtävä vaikuttaminen (esimerkiksi informaatiovaikuttaminen somessa) voivat olla eräitä hybridivaikuttamisen keinoja. Suurin osa kyberhyökkäyksistä ei kuitenkaan ole hybridivaikuttamista.

6.5 Mitä tarkoittaa informaatiovaikuttaminen?

Informaatiovaikuttamisella yleisesti ottaen tarkoitetaan toimintaa, jossa yleensä väärällä ja harhaanjohtavalla tiedolla pyritään vaikuttamaan ihmisten mielipiteisiin, käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintaan.

Toisaalta vaikuttaminen voi pohjautua myös tosiallisen tiedon käyttöön omien tarkoituksien edesauttamiseksi.

6.6 Kenen vastuulla kyberturvallisuus meidän työpaikalla on? Onko se ICT-ylläpitäjän vai toimitusjohtajan asia?

Kyberturvallisuus on viime kädessä ylimmän johdon vastuulla. Ylimmän johdon (yrityksen hallitus, ylin toimiva johto) tehtävä on linjata, miten organisaation tulee hallita kyberturvallisuuden riskejä ja poikkeamia ja minkälaisia riskejä organisaatio sietää. Ylimmän johdon tulee delegoida tehtäviä ja osoittaa organisaatiolle riittävät resurssit tekemiensä linjausten toteuttamiseen. Sitä myötä kyberturvallisuus on koko organisaatiolle kuuluva asia, mutta sen johtamisen on lähdettävä liikkeelle ylimmästä johdosta niin kuin muidenkin laatuasioiden. Kyberturvallisuus ei ole itseisarvo vaan keino varmistaa organisaation digitaalisesta maailmasta riippuvien ydintoimintojen jatkuvuus. Käytännössä sen toteuttaminen edellyttää meidän kaikkien turvallista toimintaa esimerkiksi annettuja ohjeita noudattamalla, työtehtävien ohella myös vapaa-ajalla.

7 Muita edellisten osa-alueiden ulkopuolella esitettyjä kysymyksiä?

Digi- ja väestötietoviraston Digiturvaviikolla 26.-30.10.2020 esitettyjä kysymyksiä

7.1 Mikä olisi paras tapa päästä verkostoitumaan kyberturva-ammattilaisten kanssa, jos ei ennestään ole mukana vahti-toiminnassa?

Tervetuloa mukaan VAHTI-toimintaan!

Lisätietoa VAHTI-toiminnasta:
https://dvv.fi/vahti

Ilmoittaudu VAHTI-toimintaan:
https://www.lyyti.fi/reg/vahtityoryhmat

7.2 Ovatko älypuhelimet tietoturvallisia?

Ne ovat jatkuvasti verkkoon kytkettyjä, sisältävät paljon yksilöivää henkilötietoa (omaa ja muiden: esim. yhteystiedot, valokuvat ja keskustelut) ja käyttäjän on vaikea tietää mitä kaikkea dataa puhelimen taustajärjestelmät liikuttavat. Meneekö yksilöivien henkilötietojen käsittely puhelimissa ja sen eri sovelluksissa sääntöjen mukaan? Miten saan selville onko minua yksilöiviä henkilötietoja vuotanut jollekin kolmannelle osapuolelle kaverin älypuhelimesta?

Älypuhelimiin kannatta suhtautua samalla tavalla kuin muihin tietokoneisiin. Käyttäjän tulisi itse arvioida käyttöön ottamiensa sovellusten (Apps) turvallisuus, joka onnistuu esimerkiksi katsomalla, mitä oikeuksia sovellus tarvitsee toimiakseen. Kaverin puhelimen toiminnasta ja sitä kautta tietojen päätymisestä palveluihin on käytännössä melkein mahdoton saada selvyyttä. Tiedossamme on useita esimerkkejä, joissa nimenomaan käyttämäsi verkoston muiden henkilöiden kautta tietoja on päätynyt ulkopuolisille tahoille.

7.3 Mistä voi johtua, että tietokonetta avatessa jo ennen verkkoon kirjautumista näytöllä näyttäisi sulkeutuvan joku ikkuna ?

Jos epäilee, että joku on päässyt omiin tietoihin, kannattaako vaihtaa samalla sekä tietokone että kännykkä, jos tiedot on synkronoitu molempiin? Miten kannattaa ottaa varmuuskopiot yhteystiedoista, sähköposteista, viesteistä ja kuvista?

Erilaiset ikkunan tietokoneeseen kirjauduttaessa saattavat johtua siitä, että organisaation ylläpito suorittaa tietokoneella joitakin automaattisia toimenpiteitä. Vapaa-ajan tietokoneessa tällaisia harvemmin esiintyy. Aina jos epäilee omien laitteiden turvallisuutta, kannattaa tällöin suorittaa laitteisiin haittaohjelmatarkistus. Tämä tapahtuu

joko asentamalla haittaohjelmien tarkistusohjelma (markkinoilla myös maksuttomia tuotteita) tai ajaa tällainen tarkastus verkon ylitse.

Jos epäilee omien laitteiden turvallisuutta, eräs keino on resetoida ja ottaa laite käyttöön uutena laitteena ja tehdä se erikseen tietokoneen ja kännykän osalta. Varmuuskopiointi on helpointa vapaa-ajan laitteilla käyttäen laitteiden tarjoamaa pilvipalvelua, mutta eräs suositeltava keino etenkin tietokoneiden osalta on ulkoinen usb-muisti. Ja joka tapauksessa tulee huolella varmistua siitä, että varmuuskopiossa ovat varmasti kaikki tarvittavat tiedostot.

Organisaation käyttöösi antamien laitteiden osalta noudata tai pyydä tarkempia ohjeita, edellä olevat suositukset koskevat ennen kaikkea vapaa-ajan laitteita.

7.4 Pitäisikö kaupallisiin nettisivuihin/yhteisöjen sivuihin/someen kirjautuessaan käyttää käyttäjätunnuksena jotain erillistä tunnusta eikä sähköpostiosoitettaan, kuten yleensä on?

Kysyn, koska olen oppinut, että jos meiliosoite päätyy vääriin käsiin, niin salasanatkin on helppo saada tietoonsa.

Tämä on erittäin hyvä kysymys. Voimme suositella sitä, että jos palvelu mahdollistaa muun kuin sähköpostiosoitteen käyttämään tällaista tunnusta. Toinen suositus on se, että harvemmin tarvittaville, ei niin kriittisille palveluille perustaa oman sähköpostitunnuksen ja muun kriittisemmän asioinnin keskittää varsinaiseen käyttämäänsä vapaa-ajan sähköpostiosoitteeseen.

7.5 Kysymys koskee USB-laitteiden tietoturvaa. Millaisia riskejä sisältyy muistitikkujen käyttöön tai vaikkapa kännykän latureihin?

Tuttava on kertonut löytäneensä kadulta Helsingin keskustasta kullanvärisen kännykän laturin. Ilmeisesti rikolliset voivat pyrkiä levittämään haittaohjelmia myös siten, että viaton ohikulkija poimii löytämänsä laitteen mukaansa ja ryhtyy sitä käyttämään. Onko tällaisesta kokemusta Suomessa?

Tuntemattomiin USB-laitteisiin, erityisesti tikkuihin kannattaa suhtautua varauksella, sillä niiden kautta voi levitä ja levittää haittaohjelmia. Periaatteessa laturiinkin voinee tehdä muutoksen, jolloin sen kautta voi levittää haittaohjelmia, mutta se vaatii hieman teknistä osaamista tekijältä.

7.6 Kaikille kausityöntekijöille ei voida työn puolesta jakaa älypuhelimia. Osalla heistä on kuitenkin tunnukset ja pääsy pöytäkoneelta organisaation verkkoon.

Omalta älylaitteeltaan he voivat myös jakaa kuvia ja muita - työhön liittyviä tiedostoja – organisaation verkon kautta. Millaisia riskejä tähän sisältyy digiturvan kannalta?

Yleensä olisi hyvä tapa olisi, jos organisaation verkkoon liitettäisiin ainoastaan organisaation omistamia laitteita. Organisaation omistamilla laitteilla on todennäköisemmin suojausohjelmistot ja ne ovat todennäköisimmin ajan tasalla. Sama koskee myös älypuhelimia, sillä niillekin on tehty haittaohjelmia tai ne voivat levittää haittaohjelmia eteenpäin organisaation työasemiin.

Riippuen käsiteltävän tiedon (esim. henkilötiedot) laadusta, omien laitteiden käyttämisessä työasioissa saattaa piillä vaara, koska tiedostot saattavat päätyä henkilökohtaisista laitteista helposti väärään paikkaan, esimerkiksi ulkomaiseen pilvipalveluun. Tämä saattaa olla voimassa olevan tietosuojasäädöstön vastaista. Yksi vaihtoehto pienentää tilanteen riskiä on eriyttää organisaation verkko siten, että organisaation omistuksessa ovat laitteet ovat eriytetyssä verkossa ja muut laitteet ovat esimerkiksi vierasverkossa.

7.7 Jos epäilen että joku on nähnyt työpaikalla tai julkisessa tilassa kun näpyttelen salasanani kirjautuessani koneelle (kurkkinut selän takana) miten pystyn vaihtamaan sen?

Henkilökohtaiset salasanat koneelle vaihdetaan itse silloin kun tietty käyttömäärä salasanalle tulee täyteen, mutta voinko tehdä sen myös muulloinkin?

Voit kaikissa laitteissa vaihtaa käyttämäsi salasanan milloin haluat. Tapa vaihtelee käyttämäsi laitteen käyttöjärjestelmästä tai käyttämästäsi verkkopalvelusta. Esimerkiksi Windows-laitteessa se tapahtuu painamalla ctrl + alt+ del -näppäimiä yhtä aikaa. Tämän jälkeen valitaan vaihda salasana. Sitten tulee syöttää vanha salasana, keksiä uusi salasana ja vahvistaa se. MacOs:ssä tulee mennä asetukset-kohtaan, käyttäjät ja ryhmät. Sitten valitaan käyttäjä, jonka salasana halutaan vaihtaa ja sitten Vaihda salasana.

7.8 Kannattaako aina käyttää VPN ohjelmistoa nettiyhteyksissä sekä kotona että työpaikalla? VPN SWOT, mahd. ja uhat?

VPN:n uhkat ja mahdollisuudet

Mahdollisuus:
Estää verkkopalveluita jäljittämästä käyttäjää IP-osoitteiden perusteella. Jos työnantaja tarjoaa VPN-yhteyden, se usein on toteutettu niin, että voidaan käsitellä työpaikan ulkopuolisesta verkosta lähes yhtä turvallisesti kuin työnantajan verkossa.

Uhka:
Voi joissain tapauksissa antaa valheellisen turvallisuuden tunteen, sillä palvelut voivat seurata käyttäjää esimerkiksi evästeiden avulla. VPN ei myöskään suojaa käyttäjäänsä haittaohjelmatartunnoilta, joten sen kanssakin kannattaa edelleen olla tarkkana, mitä klikkaa. VPN-palvelutarjoajan valintaan kannattaa käyttää aikaa ja valita joku tunnettu alan toimija, sillä kaikki käyttäjän data menee palveluntarjoajan kautta.

Jos palvelu on maksuton, saattaa olla, että palvelu käyttää käyttäjästään keräämästä tiedosta kaupallisiin tarkoituksiin.

7.9 Millä tavoin organisaation pitäisi varmistaa omien kriittisten palveluiden toimittajiensa tietoturvaa?

Riittääkö vain sopimuslause, jossa kumppani lupaa kautta kiven ja kannon että ovat huolellisia, vai pitäisikö pyytää kumppanilta tarkempi selvitys tietoturvatoimenpiteistä ja ehkäpä vielä vahvistus vuosittain että hommat on hoidossa?

Kuvausten vaatiminen on hyvä tapa, samoin sopimusten laatiminen, jossa on määritetty SLA:t missä ajassa esim. häiriöistä ilmoitetaan ja korjataan, samoin tulee myös sopia sanktiosta. Sopimuksessa kannattaa myös sopia mahdollisen auditoinnin tekemisestä. Tämän ohella tulee sopia, miten toimittajan kanssa käytävissä säännöllisissä yhteistyökokouksissa käsitellään säännöllisesti palveluiden turvallisuutta. Myös se, missä tilanteissa toimittaja on yhteyksissä ja ilmoittaa erikseen mahdollisista havaituista uhkista tai riskeistä. Voit tutustua myös Huoltovarmuuskeskuksen laatimiin Sopiva-mallilauseisiin.

7.10 Miten näette WhatsAppin käytön työasioihin, onko täysin ongelmaton vai pitäisikö käyttöä välttää? Entä mikäli käytetään, niin pitäisikö henkilöstöä ohjeistaa tarkemmin sen käyttöön?

Voiko työasioita keskustella whatsupissa? Tiedän, ettei luonnollisesti turvaluokiteltua mutta ihan ylipäätään jos ihan tavalliseenkin työasioiden hoitoon käyttää whatsuppia? En itse käytä mutta monelle tuntuu olevan käytössä.

Lainaus WhatsApp:n käyttöehdoista: (f) involve any non-personal use of our Services unless otherwise authorized by us. Suomeksi tarkoittaa sitä, että Whatsapp lähtökohtaisesti kieltää kaiken muun kuin sovelluksen yksityisen käytön, joten sitä ei voida suositella viralliseen työkäyttöön. Whatsapp:lla on olemassa Whatsapp Business pienten organisaatioiden käyttöön https://www.whatsapp.com/business/ .

Whatsapp:n käyttö työympäristössä on parhaimmillaan esimerkiksi tiimin epäviralli-sessa ja sisäisessä viestinnässä. Käytettäessä sitä tulee ehdottomasti huolehtia, että salassa pidettävää tai henkilötietoa ei päädy viesteihin. Sovellusta voidaan käyttää esimerkiksi herätteiden lähettämiseen, ”Sinulla on sähköpostia”, jolloin varsinainen asia toimitetaan turvallisemmalla sähköpostilla.

Kuten kaikkien organisaatioiden tarjoamien palveluiden osalta, organisaation pitää ohjeistaa henkilöstölle sen käyttöön tarjoamien tai sallimien palveluiden ja sovellusten turvallinen käyttö.

Yleisesti ottaen Signal-sovellusta pidetään tietoturvallisempana vaihtoehtona, jonka käyttäminen myös työtehtävien hoitamiseen on ohjelmiston valmistajan mukaan sallittua.

7.11 Salasanaturvallisuus on digitaalisen turvallisuuden kulmakiviä, koska kaikki palvelut eivät vielä tue monivaiheista kirjautumista. Mitä menetelmää tai palvelua suosittelette turvalliseen ja kätevään salasanojen hallintaan työ- tai yksityiselämässä?

Salasananhallinta sovelluksen käyttö on suositeltavaa, koska sen avulla voidaan helposti varmistaa pitkät ja ainutkertaiset salasanat. Salasanojenhallintaohjelman valintaan ja salasanoihin liittyviä neuvoja löytyy täältä:

Neuvoja salasanan hallintasovelluksen käyttöönottoon
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon

Salasanat haltuun - Kuka käyttää tiliäsi?
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/salasanat-haltuun

Pidempi parempi - Näin teet hyvän salasanan
https://www.kyberturvallisuuskeskus.fi/fi/pidempi-parempi-nain-teet-hyvan-salasanan

Muistutus:

Muistathan tutustua 4T-malliin eli **T**unnista **T**iedot | **T**ilat | **T**yökalut ja työskentele sen mukaisesti:

TTTT-malli digiturvalliseen työskentelyyn, 19.5.2021 (pdf)

TTTT-mallin koulutusvideo (5:43)