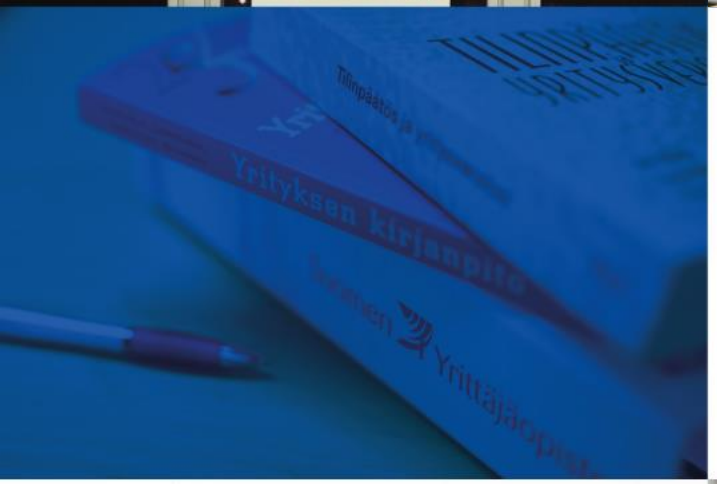
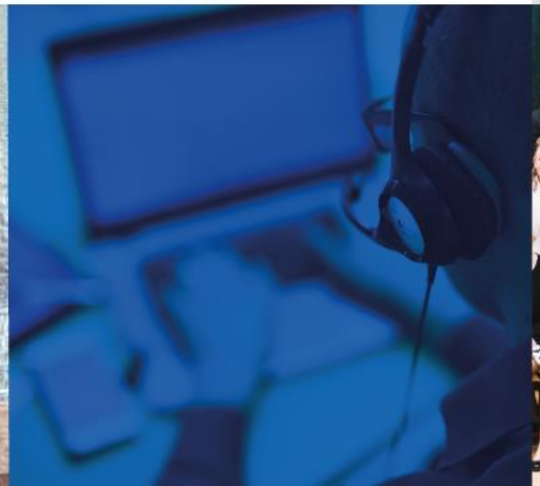


Suomen Yrittäjäopisto



Suomen Yrittäjäopisto

Yrityksen tietoturva

AJATUKSIA PIENEN YRITYKSEN TIETOTURVASTA

- **Pieni alustus ja termejä**
- Tarvitsenko tietoturvaa ja –suojaa?
- Lähtötilanteen pohdinta ja toimenpiteiden suunnittelu
- Mitä kannattaa suojata ja miksi?
- Esimerkkejä ja ajatuksia alustuksen pohjalta.

Yleistä

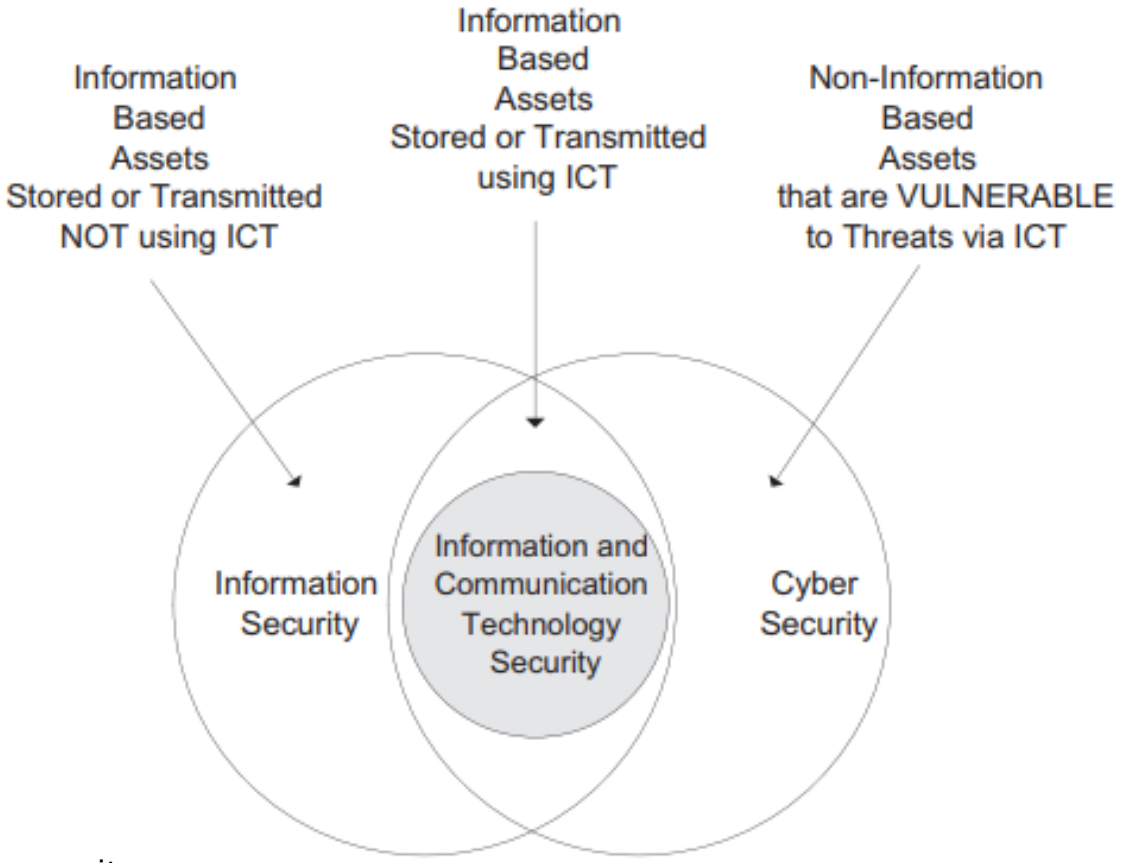
- Tietoturva ja –suoja on yhä korostuneempi asia yritysten ja organisaatioiden liiketoiminnassa ja strategiaratkaisuissa.
  - On huomattu, että data, automatisaatio ja teknistyminen aiheuttavat uudenlaisia riskejä toiminnan jatkuvuudelle ja katkottomuudelle.
- Erilaiset globaalit ilmiöt ovat tuoneet saman ajattelun myös valtioiden toimintaan.
  - On puhuttu jopa uudesta kylmästä sodasta tai hybridisodankäynnistä, joka näyttäytyy laaja-alaisena tietoturvauhkana yhteiskunnan ja sen osien toiminnalle.
- Koska julkinen verkko on globaali, ei uhka ole enää kokoluokkaan tai kohteeseen sidottu: se koskettaa meistä jokaista.

Tietoturvallisuus – Kyberturvallisuus

- Kaksi tuttua termiä, jotka vilahtelevat eri asiayhteyksissä ja eri lähteissä, ja viimeisen viiden vuoden aikana yhä useammin.
- Termejä, joiden ympärille mm. sanat ”haittaohjelma”, ”salasana”, ”mediavaikuttaminen”, ”tietovuoto”, ”murtautuminen” ja ”palomuuri” muodostavat erilaista uhkaähkyä.
- Media, IT-organisaatiot ja tekniset asiantuntijat kertovat, että
  - …jokainen yritys pienestä suureen tarvitsee erilaista ”turvaa”.
  - …jokaisen käyttäjän tulee olla varovainen kotona, kylillä ja varsinkin ulkomailla.
  - …mitään ei saa tehdä tarkistamatta tai harkitsematta.

Tietoturvallisuus – Kyberturvallisuus

- Laajoja käsitteitä, joista on tullut vielä laajempia digitalisaation ja IT:n muun kehityksen myötä.
- Ei yksiselitteisiä määritelmiä, eikä sellaisia edes tarvita.
- Ohessa tieteellinen kuvaus ja vieläpä englanniksi.



Kuva: Rossouw von Solms, Johan van Niekerk; From information security to cyber security

Tietoturvallisuus ihan lyhyesti

- Huomioidaan sana ”tieto”. Tästä johtaen tietoturva tarkoittaa yksinkertaisesti tietojen ja sen käyttöympäristön suojaamista.
- Pelkkä tieto on turhan ohut asia, joten laajennetaan hieman:
  - **Luottamuksellisuus**: käytännössä luottamuksellisen tiedon salassa pitämistä ja tiedon käytön rajoittamista vain niitä tarvitseville (oikeutetut henkilöt ja organisaatiot).
  - **Eheys**: tietojen pysyminen muuttumattomina ja tuhoutumattomana, käytännössä myös laadukkaana ja luotettavana (viitenumeron tai sotun tarkistus).
  - **Saatavuus/Käytettävyys**: tieto ovat nopeasti ja käytettävässä muodossa (esim. laadukas tietoliikenneyhteys, datan hakeminen varmuuskopiolta vikatilanteessa)

Kyberturva

- Kyberturvallisuus on tietoturvaa huomattavasti laajempi kokonaisuus, joka kattaa paljon muutakin kuin tietotekniikkaa.
- Yksi keskeinen asia on tiedon turvaaminen (vrt. kuva) ja toinen käyttöympäristöön/kokonaisuuteen liittyvän toiminnan jatkuvuuden takaaminen.

Kyberturvallisuus käytännössä

- Se varsinainen ”ICT” eli informaatio- ja kommunikointiteknologiat (verkot, laitteet ja niiden sisältämät ohjelmistot ja järjestelmät)…
- Ns. kapasiteetti-käsite, joka voi olla muodoltaan mm. erilaisia palveluja (esim. sähkö, vesi, junaliikenne), abstraktia/aineetonta omaisuutta (data eri muodoissa) tai laajassa mittakaavassa yhteiskunnallinen toiminto (esim. vesilaitokset). Ylipäätään mikä tahansa kokonaisuus, johon ns. kyberavaruuden avulla voidaan vaikuttaa aina puolustusvoimia myöten.
- Sekä tietenkin edellä mainittujen käyttäjäkunta, joka puolestaan on kovinkin laaja käsite: yksittäinen ihminen, kunta/kaupunki, maatila, teollisuuslaitos tai jopa kokonainen kansakunta.

- Pieni alustus ja termejä
- **Tarvitsenko tietoturvaa ja –suojaa?**
- Lähtötilanteen pohdinta ja toimenpiteiden suunnittelu
- Mitä kannattaa suojata ja miksi?
- Esimerkkejä ja ajatuksia alustuksen pohjalta.

Tarvitsenko tietoturvaa?

- Isommissa organisaatioissa tietoturva katsotaan välttämättömäksi toimintaedellytykseksi ja bisneksen selkärangaksi, jopa kilpailutekijäksi.
- Tämän lisäksi laatujärjestelmät, asiakkaiden vaatimukset, monihyväinen lainsäädäntö, huoltovarmuustekijät, asetukset ja normit ja monet säädellyt asiat pakottavat tietoturvan laadukkaaseen hallintaan.
- Itsestäänselvyyksiä isoissa organisaatioissa, mutta mikä on asian laita pienissä yrityksissä ja yhteisöissä?

Pieniä on paljon (2017)

Yritykset 2017				
Toimiala (TOL 2008)	**Yrityksiä**		**Henkilöstöä**	
		%	**1 000**	**%**
Maatalous, metsätalous ja kalatalous	77 580	21,3	49	3,4
Teollisuus	20 246	5,6	293	20,2
Rakentaminen	41 114	11,3	166	11,4
Tukku- ja vähittäiskauppa, moottoriajoneuvojen ja moottoripyörien korjaus	41 911	11,5	235	16,1
Kuljetus ja varastointi	20 132	5,5	121	8,3
Majoitus- ja ravitsemistoiminta	12 059	3,3	59	4,1
Informaatio ja viestintä	10 553	2,9	85	5,8
Rahoitus- ja vakuutustoiminta	7 996	2,2	42	2,9
Kiinteistöalan toiminta	29 327	8,0	20	1,4
Ammatillinen, tieteellinen ja tekninen toiminta	36 662	10,1	103	7,1
Hallinto- ja tukipalvelutoiminta	14 230	3,9	133	9,2
Terveys- ja sosiaalipalvelut	18 387	5,0	76	5,2
Muut toimialat	34 317	9,4	71	4,9
Kaikki toimialat	**364 514**	**100**	**1 453**	**100**

Henkilöstön määrä		
0–4	325 643	89,3
5–19	29 333	8,0
20–99	7 926	2,2
100–499	1 342	0,4
500–	270	0,1
Yhteensä	**364 514**	**100**

Lähde: Tilastokeskus (https://www.tilastokeskus.fi/tup/suoluk/suoluk_yritykset.html)

Tarvitsenko tietoturvaa?

Tietoturvan tarve ja merkitys tiedostetaan usein kiitettävästi.

Pienissä organisaatioissa asiaa ei kuitenkaan välttämättä mielletä tärkeäksi. Syyt ovat ilmeisiä:

1. Riskit arvioidaan niin pieneksi, ettei asia ole merkityksellinen.
2. Päivittäinen työ ja ansaitseminen vievät kaiken ajan, jolloin asiaa ei ehditä pohtia.
3. Psykologisen inhimilliset syyt: emme pelkää uhkia, joita emme näe, havaitse, tiedosta tai mistä emme yksinkertaisesti tiedä.

Vähäisen tarpeen syitä

- ”Meillä ei ole mitään arvokasta tai merkityksellistä”
- ”Meidän asiat eivät kiinnosta ketään, voi tulla lukemaan jos huvittaa”
- ”Mitään ei ole tapahtunut ennenkään, eikä tapahdu jatkossakaan”
- ”Maksaisin turhasta” ja ”Raha käytetään siellä, missä sitä oikeasti tarvitaan”

On täysin mahdollista, että näin asia myös on. Jatko vanhaan malliin on oikeutettu ratkaisu.

Koska olettaminen on myös virheiden lähtökohta, kannattaa asia kuitenkin miettiä yhden kerran vähän tarkemmin. Tietoturvan tarpeen aliarvioiminen on kuitenkin henkilö- tai organisaatiokohtainen virhe.

Tarvitsenko tietoturvaa?

- Jos yritys, yhdistys tai yksityishenkilö käyttää arkipäivän tietojenkäsittelyssään tietokonetta tai mobiililaitetta, tietoturvaa tarvitaan melko todennäköisesti.
- Jos em. laite on kytketty julkiseen verkkoon ja sen tietolähteisiin tai jos käyttäjät osallistuvat yhä laajentuviin digitalisaatiokekkereihin, ei asiasta ole enää mitään epäselvyyksiä.
- Myös pienen organisaatioon toimintaan voi liittyä lainsäädäntöä, jolloin tietoturva muuttuu merkityksellisemmäksi ja usein sen lisäpiirteeksi muotoutuu esim. tietosuoja-asetuksen tai vastaavan vaatimukset.

- Pieni alustus ja termejä
- Tarvitsenko tietoturvaa ja –suojaa?
- **Lähtötilanteen pohdinta ja toimenpiteiden suunnittelu**
- Mitä kannattaa suojata ja miksi?
- Esimerkkejä ja ajatuksia alustuksen pohjalta.

Ihan aluksi…

- Tietoturvan osalta kannattaa olla itselleen armollinen.
- Edes ICT-osaajat eivät ole perille kaikista tarpeellisista tekniikoista tai vaikkapa tietoturva-aukoista. Tiedämme, että joku tietää ja osaa aina enemmän.
- Loppukäyttäjän tasolla (yksityisyrittäjät, mikroyritykset) tekniikan ymmärtämisellä ja hyödyntämisellä on rajansa. Maalaisjärki, ohjeiden noudattaminen, koulutus ja sopiva itsensä valistaminen riittävät varmasti.

Kaikilla on oikeus historiaan…

- Yritysten sovellus- ja tietotekniikkaympäristö on koostettu yleisesti pitkällä aikavälillä, niin pienten kuin vähän suurempienkin.
- On siis mahdollista, että ympäristöä ei ole koskaan mietitty kokonaisuutena: teknistyminen ja mahdollinen laajentuminen on tapahtunut tarvehakuisesti sen mukaan, kuinka paljon investointivaraa on ollut. Hyvänä esimerkkinä tästä vaikkapa maatilat.
- Tekninen ja toiminnallinen kokonaisuus saattaa olla hajanainen paketti, jota on haastava ymmärtää, kehittää ja päivittää, vaikka keinoja olisikin olemassa.

Riskien kartoitus ja riskianalyysi

- Riskianalyysissa selvitetään uhat, todennäköisyydet ja mahdollisten vahinkojen suuruus sekä laatu (vakavuus).
  - Mitä ovat oikeat ja realistiset riskitekijät?
  - Voidaanko menettää dataa, rahaa, mainetta ja kunniaa?
  - Vakavimmat asiat tulee miettiä ja suhteuttaa todennäköisyyteen.
- Pienessä yrityksessä pohdinta ja dokumentointi on maltillista, perustuen harkintaan.
- Toimenpiteiden ja tekniikan määrä tulee suhteuttaa riskiin. Tämä on myös yleensä suorassa suhteessa rahankäyttöön.

Riskin koko vs. toimenpiteet

- Tietoturvaa voi ostaa, parantaa ja miettiä loputtomasti. Mikä sitten on riittävä taso ja kuka sen voi määritellä?
- Viime kädessä omistajataho määrittelee sen, miten paljon tietoturvaan voi ja kannattaa uhrata aikaa, rahaa ja resursseja.
- Apua löytyy:
  - Paikalliset IT-yrittäjät ymmärtävät tarpeet hyvin, koska ovat samassa liemessä
  - Laite- ja sovellustoimittajat auttavat ainakin jossakin määrin ilmaiseksi ja rahalla loppuun asti.
  - Operaattorilta voi kysyä ja tietenkin myös ostaa tukea ja tekniikkaa.
  - Konsultit ja tietoturvaan keskittyneet yritykset auttavat luonnollisesti mielellään, tosin hinta on vaihteleva käsite.

- Pieni alustus ja termejä
- Tarvitsenko tietoturvaa ja –suojaa?
- Lähtötilanteen pohdinta ja toimenpiteiden suunnittelu
- **Mitä kannattaa suojata ja miksi?**
- **Esimerkkejä ja ajatuksia alustuksen pohjalta**

Mietintään

- Älä oleta, että vain tieto olisi suojattava tai ainoa vastapuolelle merkittävä kohde. Kuten totesimme edellä, tiedon lisäksi mm. käyttöympäristö ja ihmiset kuuluvat suojauksen piiriin. Kun liiketoiminta siirtyy verkkoon, tulevat väärinkäyttäjät seuraavat perässä.
- Muutama perushaaste pohdittavaksi:
  - Suojautujalle arvottomalta tuntuva tieto tai kapasiteetti voi olla toiselle käyttökelpoinen asia, osa jotakin suurempaa ja vakavampaa. Miten tunnistat ne ja arvotat nämä asiat?
  - Suojautuja joutuu varautumaan moneen uhkaan ja riskiin. Vastapuoli taas tarvitsee vain yhden heikon kohdan ja tällä osapuolella VOI OLLA käytössään osaamista, kapasiteettia (pilvi), automaatiota (robotteja) ja erityisiä välineitä. Miten tämä epäedullinen tilanne käännetään voitoksi?

Esimerkkejä suojautumiselle

- Luottokortti- ja pankkitietojen varastaminen, tietojen kalastaminen, henkilöllisyyden varastaminen eli identiteettivarkaus
- Tiedon kryptaaminen tai tuhoaminen → Suora haitanteko tai kiristys
- Laitteiden ja automaatiojärjestelmien vikaannuttaminen
  - Räätälöity tai muuten kohdennettu uhka.
- Laitteille murtautuminen vaihtelevista syistä johtuen
- Erilaisen datamateriaalin varastaminen, henkilön/ henkilöiden kuvaaminen/videointi ja levittäminen nettiin => Intimiteettisuojaan kajoaminen.
- Tekijän omien jälkien peittäminen ja naamioituminen toiselle identiteetille
  - Huijaukset, roskaposti, väärät rekisteröitymiset, muu potentiaalinen käyttökohde
- Kapasiteetin käyttäminen (tietokoneet, kamerat, ilmalämpöpumput, jääkaappi)
  - Virtuaalivaluutan louhinta, nettiyhteyden hyödyntäminen palvelunestoissa

Tietoturvaa koetellaan…

Suomen Yrittäjäopisto

UUTINEN Talouselämä 7.2.2018

Hyppönen: Koteihin vyöryy vakoilulaitteita - käyttäjät eivät ymmärrä, ongelmiin olisi tartuttava - Tivi

Adoben Flash Playerista löytyi viime viikolla jälleen uusi haavoittuvuus, jonka avulla hakkeri voi ladata tietokoneelle haittaohjelman. Tivi 7.2.2018

TIETOMURROT | Olli Vänskä 26.9.2017 klo 17:41 Tivi 09/2017

Equifaxin toimitusjohtajalle kenkää - 143 miljoonan ihmisen tietomurto oli liikaa

Petya- ja NotPetya-nimillä tunnettu haittaohjelma levisi kesäkuussa laajalle ja tuli kalliiksi esimerkiksi konttialuksistaan tunnetulle logistiikkayhtiö Maerskille. Hyökkäys sulki useita konttiterminaalien järjestelmiä aiheuttaen yli 230 miljoonan euron vahingot. Kotimikro.fi

Asiantuntijoiden mukaan kiristyskampanjalla peitettiin Petya-haittaohjelman todellista tarkoitusta, joka oli kyberhyökkäys Ukrainaa vastaan.

Mirai-bottiverkko on ottanut haltuunsa tuhansien suomalaisten modeemeja

Viestintavirasto.fi

29.11.2016 klo 17:41

SUURI määrä Helsingin Uusyrityskeskuksen asiakkaiden tietoja on varastettu tietomurron yhteydessä. Tiedot vietiin Liiketoimintasuunnitelma.com-palvelusta.

HS: 6.4.

Oikeus tuomitsi 20-vuotiaan miehen ehdolliseen vankeuteen palvelunestohyökkäyksistä – Kohteina pankit ja mediat Yle.fi-uutiset 12/2017

TIETOTURVA | Teemu Laitila 5.2. klo 11:42

…nteen uudenvuodenaattona 2014.

Nyt se tapahtuu: jo yli 130 haittaohjelmaa hyödyntää Spectreä ja Meltdownia TIVI 5.2.2018

Identiteetti varastetaan Suomessa useammin kuin pyörä – "Varkaat kalastelevat tietoja paperinkeräyksestä" Aamulehti 05/2017

KYBER | TIVI 4.10.2017 klo 19:00

Vuosi sitten verkkohyökkäys kylmensi kerrostalon - Yle: hyökkäys voi iskea vaikka lypsykoneeseen Tivi 10/2017

Teollisuusyrityksillä on syytä katsella tarkasti, miten ne ovat suojautuneet kyberhyökkäyksiltä. Suomessa tunnustetaan, että ei ainakaan riittävästi. Kuitenkin esimerkiksi järjestelmiin iskenyt kiristyshaitake aiheuttaa äkkiä valtavia menetyksiä. Tivi 6.2.2017

Tunnus, salasanat ja tunnistautuminen

- Ehkä eniten keskusteltu asia tietoturvassa?
- Pelkän salasanan rakenteen ja vaikeuden sijasta kannattaa keskittyä sen käyttöön, toisteisuuteen, muistamiseen ja kohdennukseen.
- Salasanan laatu ja rakenne on tärkeä asia, mutta se ei ole tietoturvan selkäranka.
  - Vaikea salasana voi aiheuttaa muistamisen tuskan ja kääntää ajatuksen päinvastaiseksi: tietoturvasta tulee turvattomuutta.
  - Salasana voi olla sisällöltään melko yksinkertainen, mutta kuitenkin toimiva. Suomenkielinen salasana on maailmalla aina melko vaikea tai eksoottinen.
  - Älä käytä salasanassa samoja, toistuvia osia tai komponentteja, jotka ovat arvattavia.

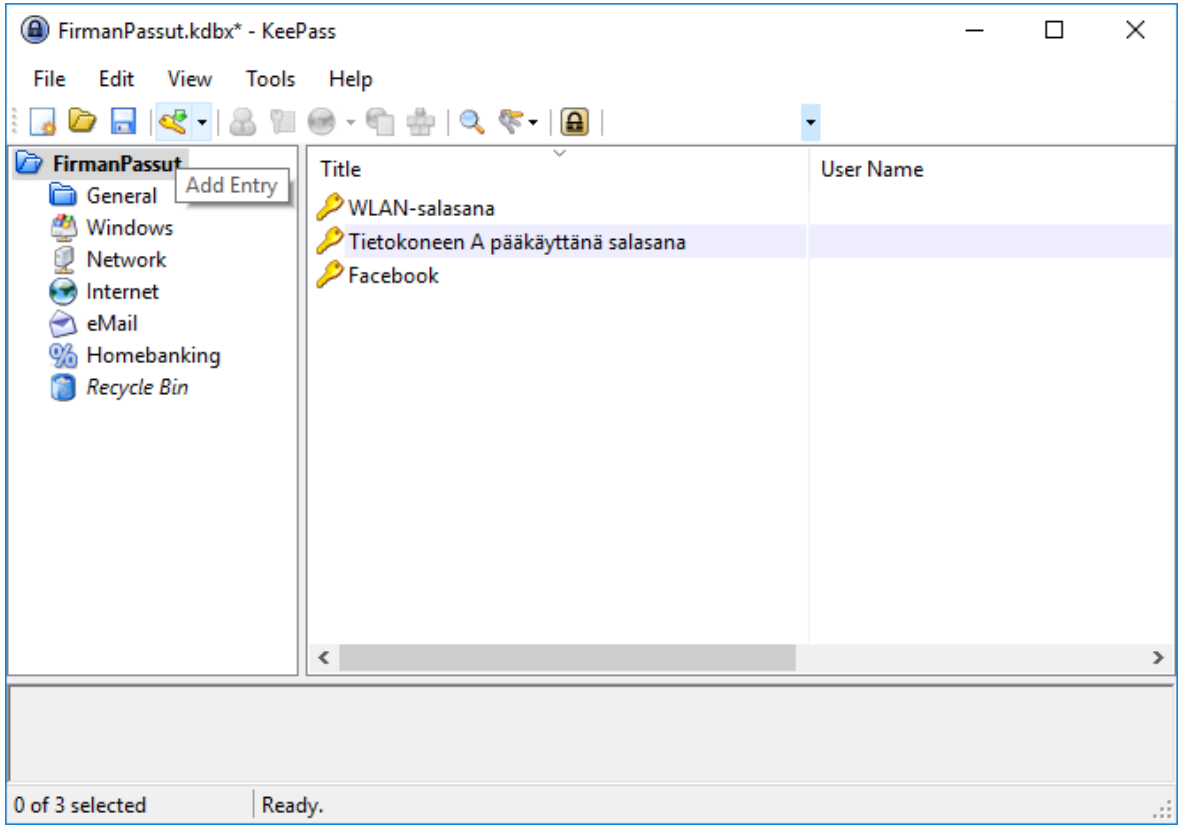
Tunnus, salasanat ja tunnistautuminen

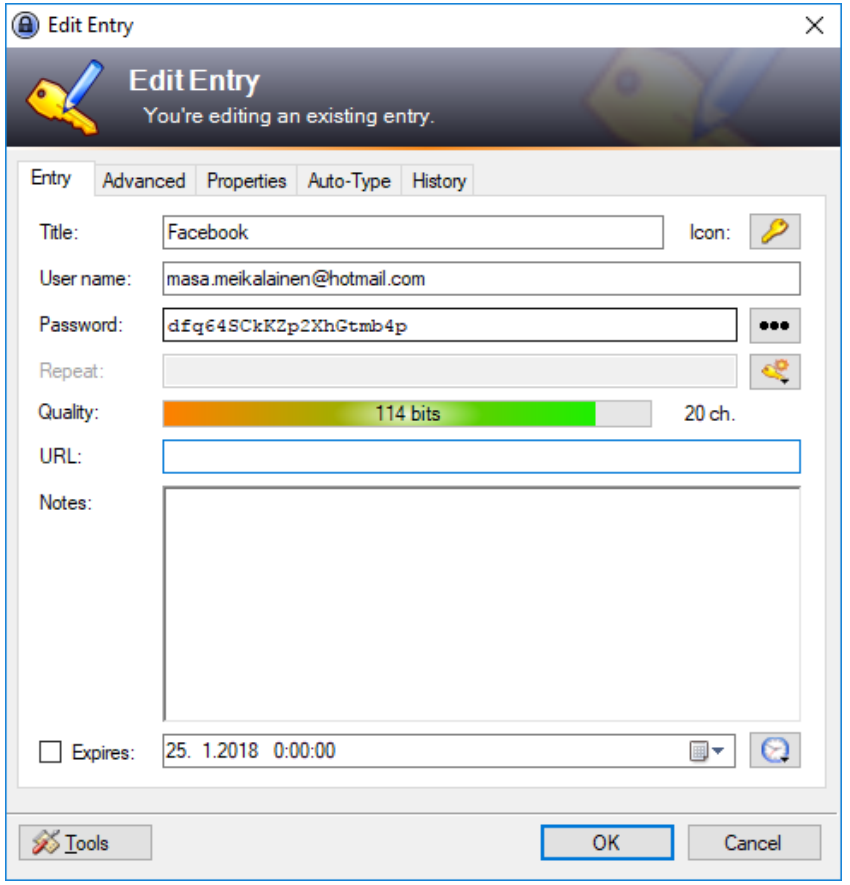
- Ei kaikkia munia samaan koriin: Käytä aina eri salasanaa niissä palveluissa, joissa on oikeasti kriittistä sisältöä.
  - Sama ”yleissalasana” voi olla ns. kevyempiä palveluita yhdistävä tekijä.
- Älä turhaan varo salasanan kertakäyttöisyyttä ja vaihtoja: jos käytät palvelua kerran kesässä, on sama jos keksit pitkän salasanan ja unohdat sen saman tien. Ensi kesänä sitten unohtuneen salasanan vaihto ja homma jatkuu…

Salasanat ja tunnistautuminen

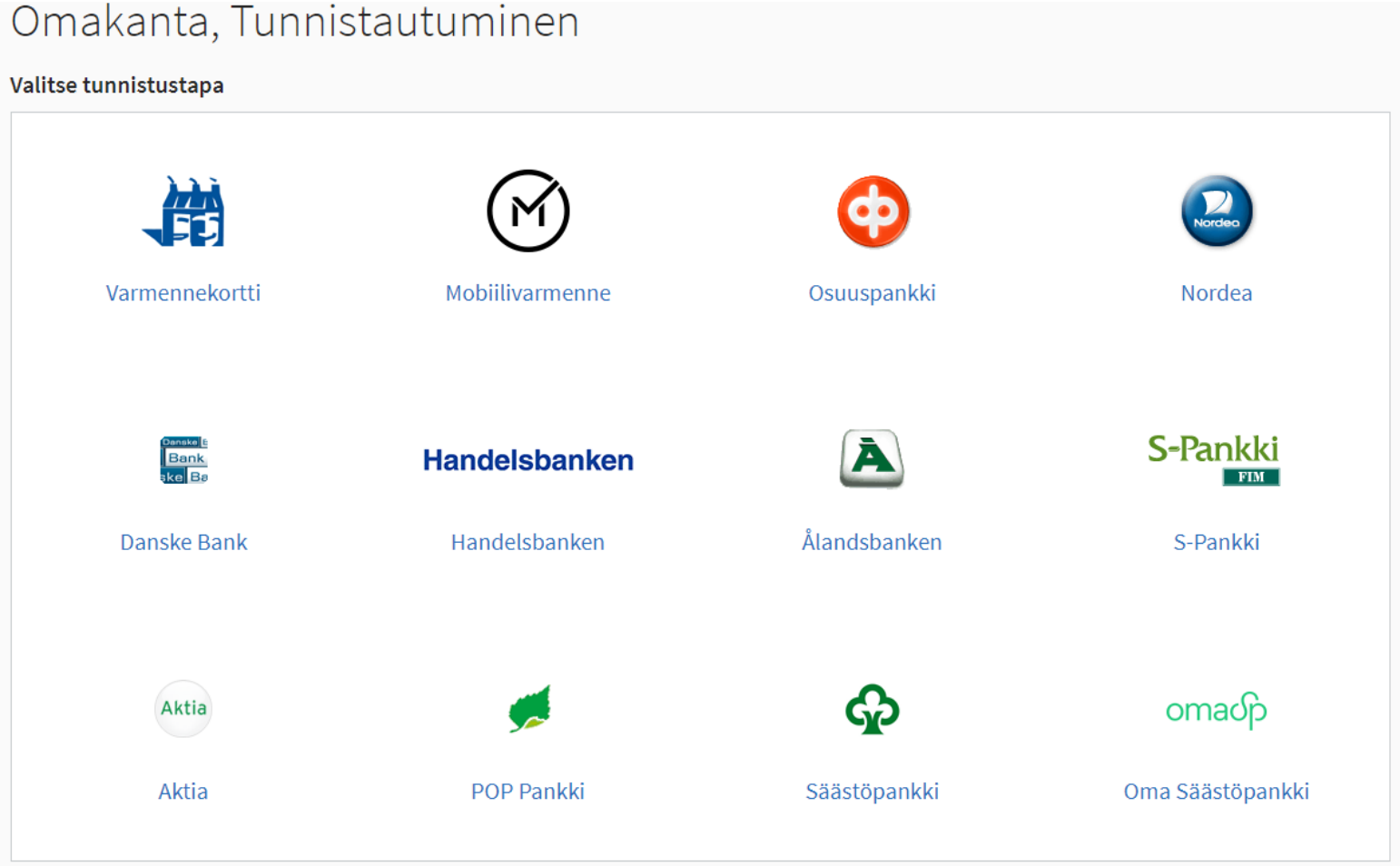
- Jos palveluita/tunnuksia/salasanoja on paljon, älä muistele niitä turhaan, vaan käytä salasanatietokantaa (password manager), hyvin suojattua sähköistä salasanalistaa (onko sellaista?), mobiilivarmenteita ja -tunnisteita.
- Käytä kaksivaiheista tunnistautumista niissä palveluissa, joissa hyödynnät luottokortti- tai pankkitietoja.

Salasanatietokanta: Keepas

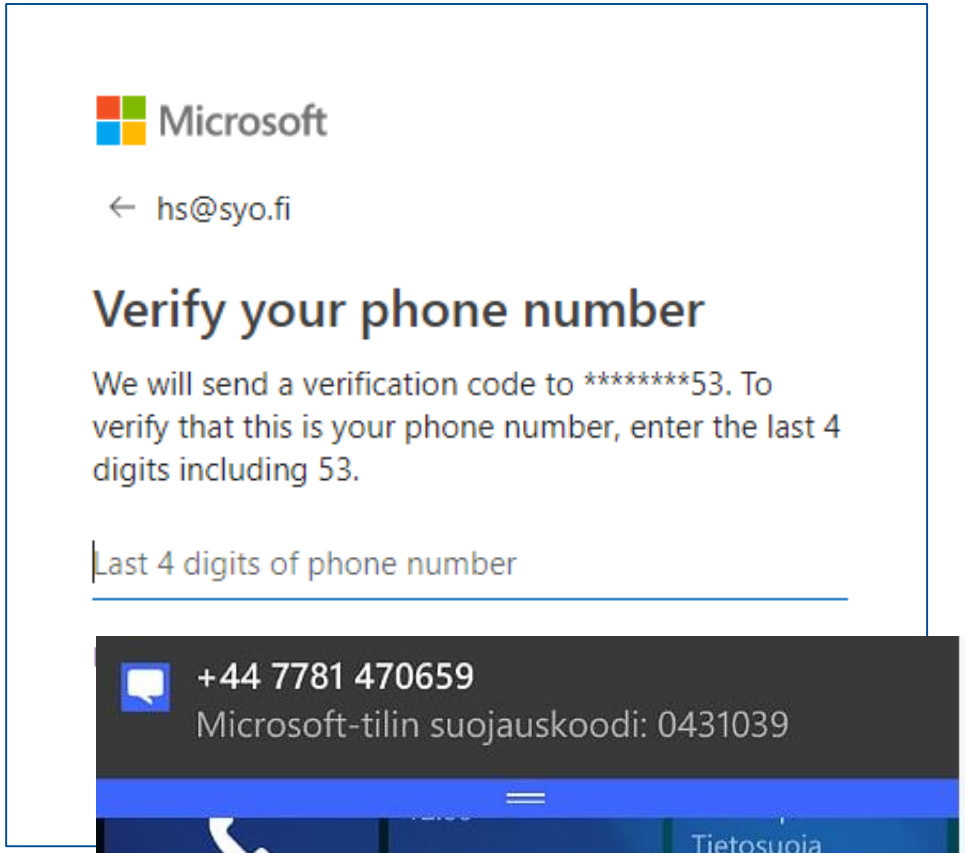


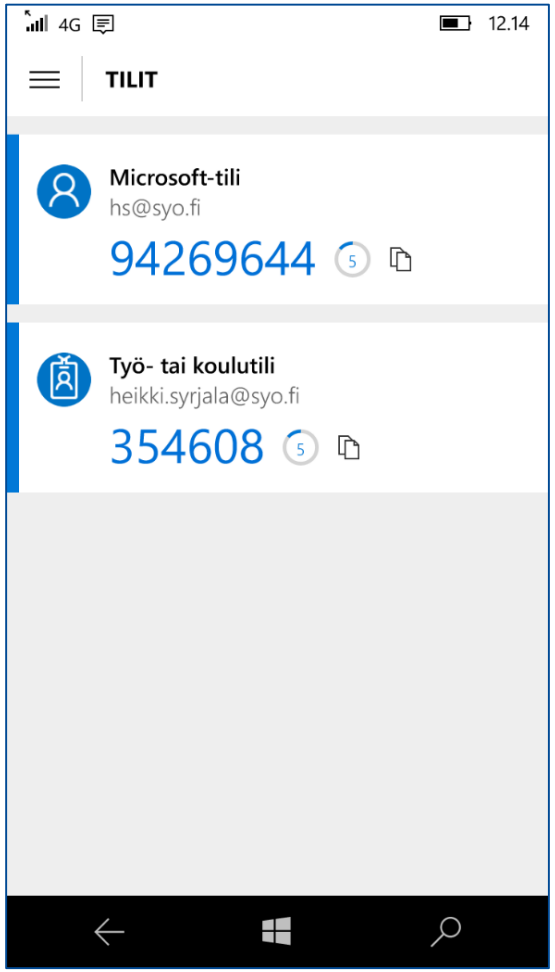


Mobiilivarmenne; Pankkitunnistus

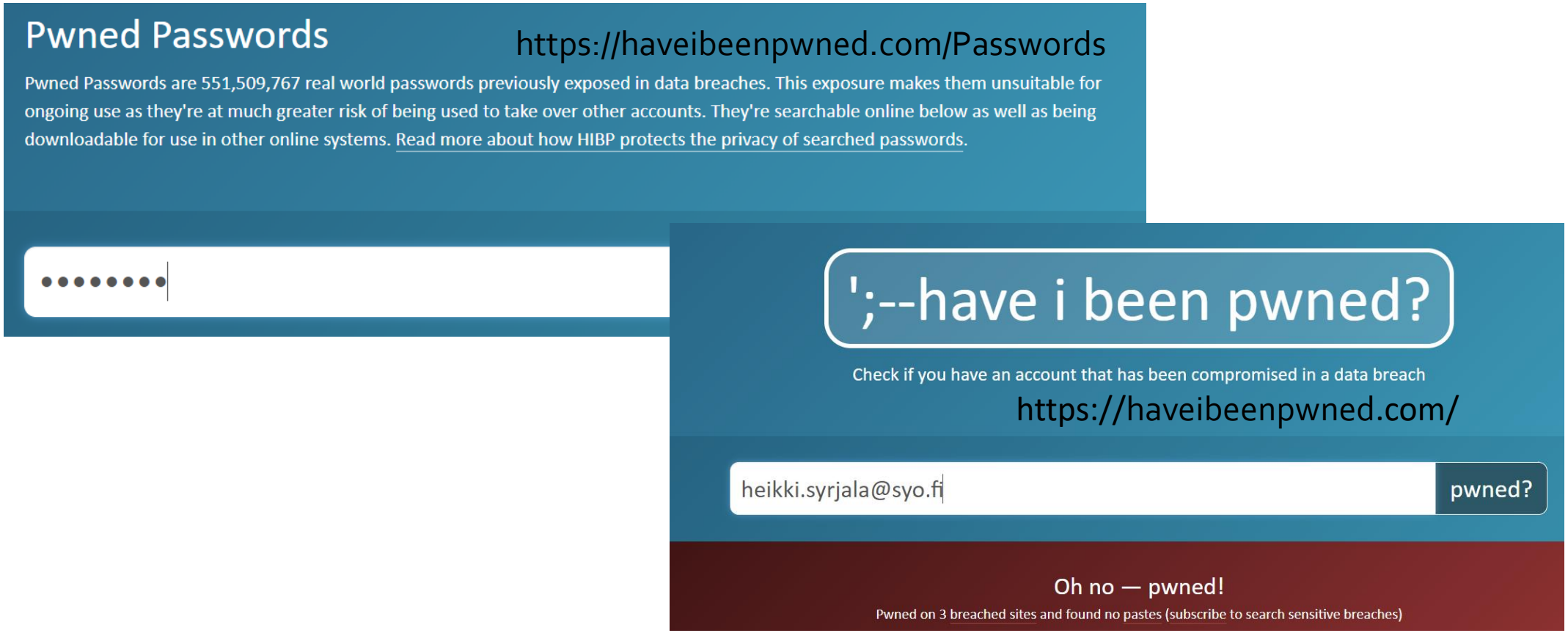


Kaksivaiheinen tunnistautuminen





Esimerkki


Pwned Passwords
https://haveibeenpwned.com/Passwords
Pwned Passwords are 551,509,767 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
https://haveibeenpwned.com/
heikki.syrjala@syo.fi
pwned?
Oh no — pwned!
Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)

Esimerkki

TIETOVUODOT | Jori Virtanen 17.1. klo 10:35

Valtava tietovuoto jättää kaikki aiemmat katastrofit varjoonsa – 773 miljoonaa uhria, näin katsot olet[illegible]

Kokoelmasta löytyy 772 904 991 nimeä.

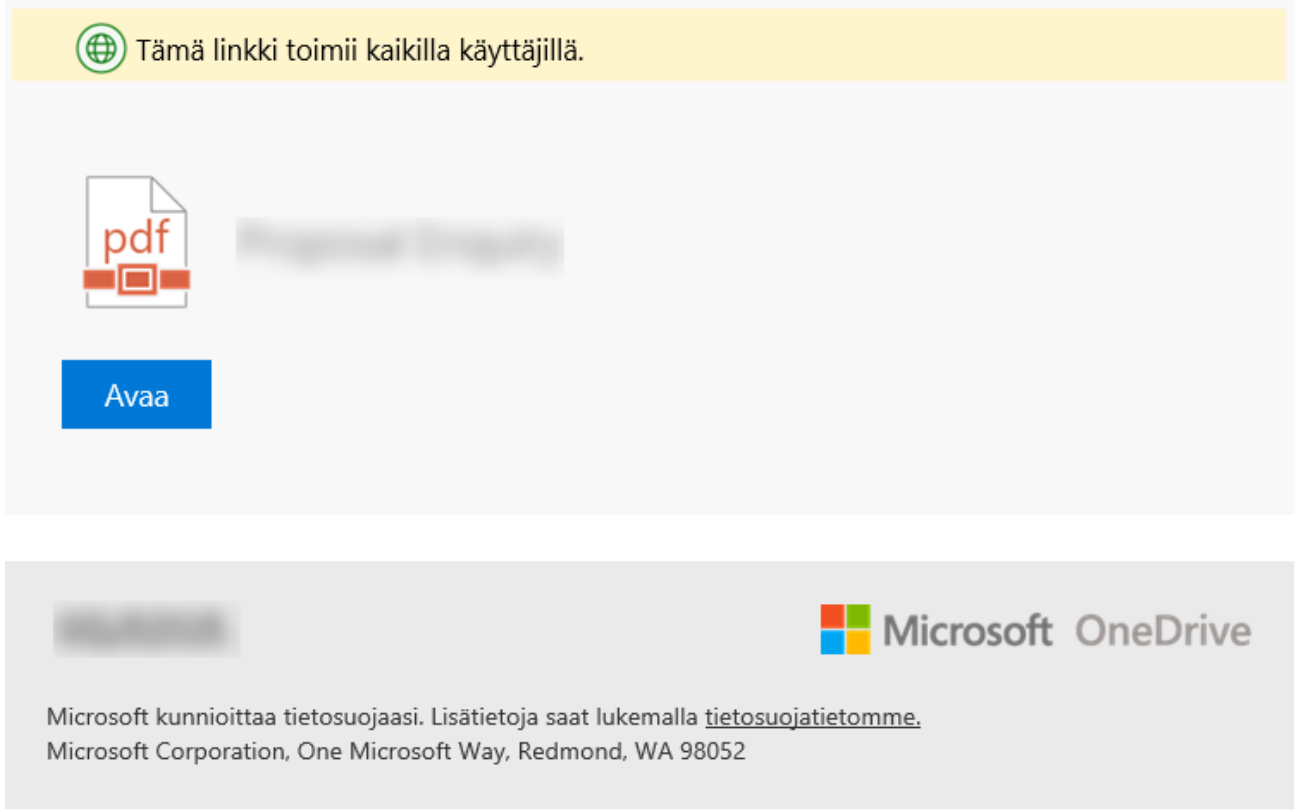
Hakkerit sanovat saatteessaan, että datapaketti on koostettu yli 2000 hakkeroidusta tietokannasta.

Kokoelman löytänyt tietoturvatutkija **Troy Hunt** kertoo blogissaan, että 773 miljoonaa uhria itse asiassa vähättelee tietovuodon laajuutta. Hunt nimittäin siivosi datapakettia. Raakamuodossaan siitä löytyy 2,7 miljardia riviä sähköpostiosoitteita ja salasanoja, joita on yhdistelty yli miljardilla eri tavalla.

Käyttäjän sähköpostiosoite on yhä useammin myös palveluiden käyttäjätunnus. Jos ja kun moni meistä on käyttänyt historian aikana samaa email-tunnusta eri palveluissa, samoin kuin yhtä ja samaa salasanaa, ovat nämä saattaneet vuotaa tietomurtojen yhteydessä vääriin käsiin. Viisainta olisikin lähteä muuttamaan tilannetta palvelu kerrallaan.

Esimerkki

[redacted] jakoi kanssasi tämän asiakirjan.



Ns. aito tilanne, jossa organisaation A henkilön varastetulla identiteetillä lähetettiin jakolinkin sisältävä sähköposti organisaation B henkilölle.

Jakolinkin avaaminen aikaansai kirjautumisen, jonka yhteydessä käyttäjän salasana ja tunnus päätyivät vääriin käsiin.

Koska linkin lähettäjä ja vastaanottaja tunsivat toisensa ja posti näytti aidolta & tuli todellisesta lähteestä, meni myös vastaanottaja vipuun, jolloin dominoefekti jatkui…

Esimerkki

Suojaustoimia Office 365 -tunnusten tietojenkalastelua vastaan

11.06.2018 klo 14:18 - Päivitetty 29.06.2018 klo 14:20

Useiden suomalaisten yritysten työntekijöiden ja johtajien sähköpostiviesteihin on kevään 2018 aikana varastettu ja heidän käyttäjätunnuksillaan on tehty useita petoksia ja petosten yrityksiä. Kyberturvallisuuskeskus kehottaa kaikkia Office 365 -tuotteita käyttäviä yrityksiä rajoittamaan sähköpostin edelleenlähetyssääntöjen tekemistä ja ottamaan käyttöön kaksivaiheinen tunnistautuminen.

Koska sähköpostit ovat jo väärissä käsissä, yritetään niihin lähetettyjen huijausviestien avulla harhauttaa käyttäjiä luovuttamaan myös salasanansa ja mahdolliset muut tunnistetiedot ”kaupan päälle

Sääntö nro 1: älä käytä samaa salasanaa ERI palveluissa, koska altistat kaikki palvelut vaaraan salasanan mahdollisen murtamisen jälkeen.

Sääntö nro 2: käytä kaikissa rahaan liittyvissä palveluissa kaksivaiheista tunnistusta. Vähäpätöisissä palveluissa tämä ei ole niin ”nöpön nuukaa”

Sääntö nro 3: Jos vähänkään epäilet saamasi sähköpostiviestin tarkoitusperää tai todenmukaisuutta, älä avaa sitä.

Esimerkki

Yläkoulun Wilma-järjestelmässä epäily väärinkäytöksestä Kauhavalla – luvattomia viestejä opettajien nimissä, oppilaiden tietoja muokattu

Eteläpohjalaiskoulun Wilmaan on päästy luvatta joulun aikaan.

Tietosuoja 18.1.2019 klo 13:30 | päivitetty 18.1.2019 klo 13:33

Oheinen esimerkki oli melko mitätön tapahtuma loppujen lopuksi. Huomioitavaa onkin tapauksen saama julkisuus, eräänlainen mainetappio ja jälkityö. Viranomaiset ovat asiassa mukana pienellä kynnyksellä, koska asia on vielä uusi ja ennakkotilanteita on toistaiseksi vähän.

Osaltaan myös uutisointi mutkistaa tilannetta. Yksi media puhuu tietojen vääriin käsiin joutumisesta, toinen tietomurrosta, kolmas tietosuojasta ja -turvasta.

"Tietoturvan peruskysymyksiä"

Pohjanmaan poliisista kerrotaan, että ilmoituksia tietomurroista tulee tämän tästä. Yleensä kyse on salasanoihin ja käyttäjätunnuksiin liittyvästä huolimattomuudesta.

Päätelaitteet ja käyttöoikeudet

- Nykyisin puhumme tietokoneiden sijasta päätelaitteista, koska data makaa pilvipalveluiden ja muuttuneiden tottumusten sijasta yhä enemmän mobiililaitteilla.
- Kaikki päätelaitteet tulisi suojata ja turvata useammalla tavalla – riippuen hieman siitä, miten ja missä sitä käytetään.
- Laitteet suojataan vahvalla salasanalla, PIN-koodilla tai biometrisellä tunnisteella (kasvot; sormenjälki; iris-tunnistus).
- Laitteita päivitetään säännöllisesti tietoturvapäivitysten osalta. Samalla pyritään välttämään laitteita, joiden päivitysmahdollisuudet ovat huonot.

Päätelaitteet ja käyttöoikeudet

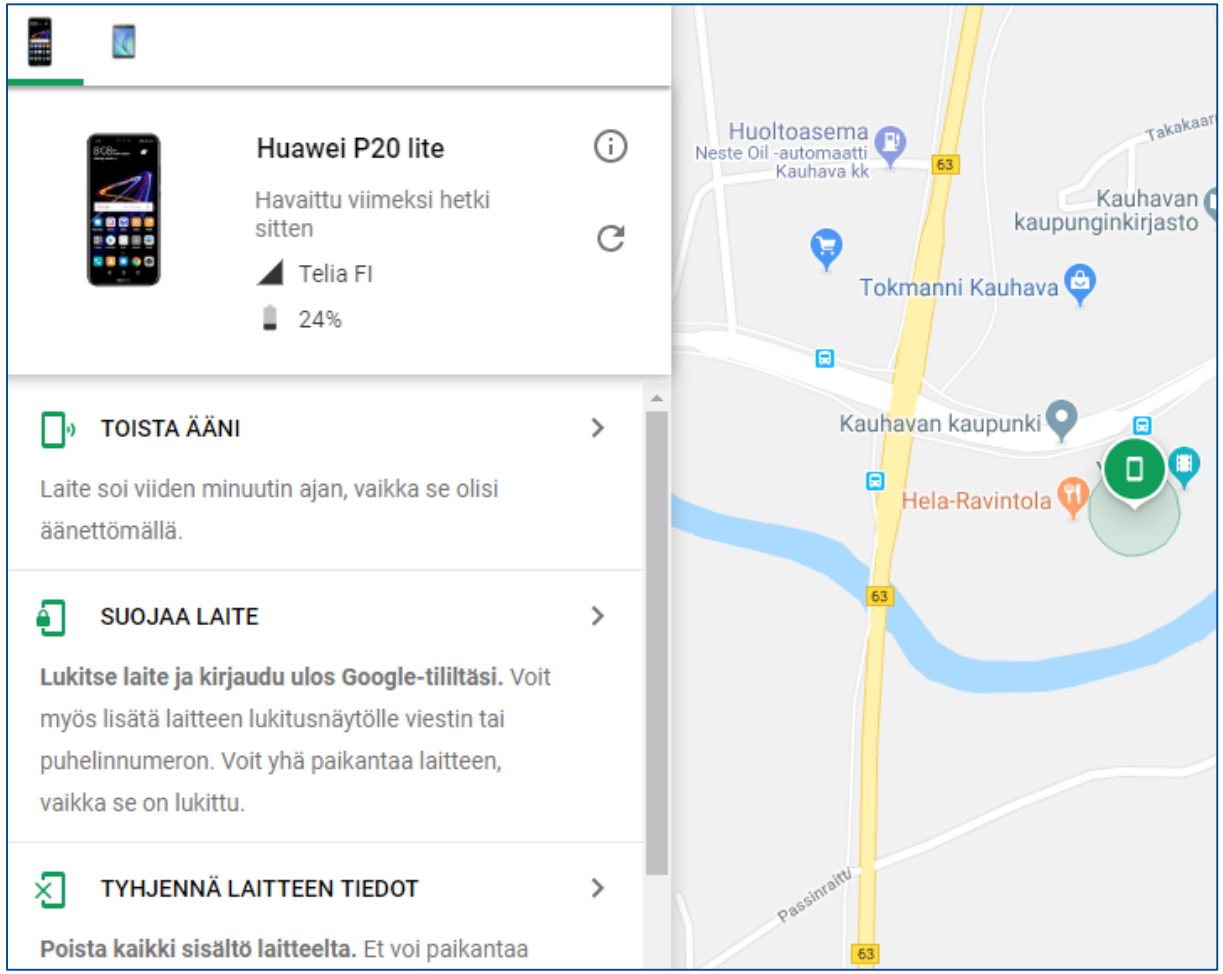
- Laitteisiin asennetaan tunnettu haittaohjelmasuojaus, palomuuri ja mahdollinen seurannan ja paikallistamisen esto.
  - Tämä ei aina riitä, mutta pienentää riskiä merkittävästi.
- Ns. kyseenalaisia verkkosivustoja vältetään. Lisäksi käytetään selaimen privaattitilaa vieraissa kohteissa, jotta tallentuvan datan määrä edelleen minimoituu.
- Tärkeä asia: tietokoneita ei käytetä turhaan pääkäyttäjän (administrator) tunnuksella ja selainkäyttöä tällä tunnuksella ei suoriteta ollenkaan.
  - Pääkäyttäjän oikeuksilla mahdollinen haittaohjelman toiminta ja koneen saastuminen on täysin mahdollista web-käytön yhteydessä.

Päätelaitteet ja käyttöoikeudet

- Laitteen massamuistit voidaan suojata/salata, mikäli laite liikkuu paljon (etenkin älypuhelin, joka sisältää ”koko elämän”). Tällä estetään myös unohduksien jälkeinen katastrofi tehokkaasti.
  - Nykyisin jo oletuksena osassa laitteita
- Laitteissa on mahdollisuus paikallistamiseen, lukitsemiseen ja mahdollisesti myös etäpyyhkimiseen.
  - Koskee myös yksityishenkilöitä ja heidän laitteitaan.
- Vielä yksi asia: kannattaako oman yritystoiminnan tietoa sisältäviä laitteita käyttää henkilökohtaiseen viihdekäyttöön?

Esimerkki: haittaohjelmatilanne tänä aamuna

Laitteen paikannus ja toimenpiteet



Laitteiden ja ohjelmistojen päivittäminen

- Päivittämisen merkityksestä on kerrottu niin monessa mediassa pitkään ja runsaasti, että kaikille lienee selvää, että laitteita ja sovelluksia pitää päivittää ainakin tietoturvan osalta?
  - On olemassa myös toiminnallisia päivityksiä, joka on eri asia.
- Muista kuitenkin perussääntö:
  - Kaikki päivitykset eivät ole hyväksi ja voivat jopa aiheuttaa ongelmia. Päivityskin voidaan nimittäin päivittää toimivaksi.
  - Jos päivitys on kriittinen, sitä ei pidä tietenkään lykätä loputtomasti.
- Kuka ehtii seurata tätä? Kenellä on asiantuntemusta tähän? Tiedätkö, kuinka usein ja miten laitteita/sovelluksia päivitetään?

Laitteiden ja ohjelmistojen päivitettävyys

- Yritysten laitteiden ja sovellusten ikä ja päivittämisen mahdollisuus vaihtelevat. Yleinen termi on elinkaari ja elinkaariajattelu.
- Laitteen päivityssykli voi loppua jo parissa vuodessa, mutta hyödyntäminen jatkuu edelleen hyvinkin pitkän aikaa. Päivitysten jatkuminen vaihtelee:
  - Mobiililaitteiden (puhelin, tabletti tms.) kestoikä on n. 3 vuotta, päivityksiä tulee vaihtelevasti.
  - Tietokoneen käyttöikä voi olla kymmenen vuotta, mutta sen käyttöjärjestelmä on mahdollisesti lyhytikäisempi päivityksiltään.
  - Rakennusten ja niiden automaation kestoikä voidaan ajatella kymmeniksi vuosiksi.
- Päivitettävyys VOI olla ongelma, jos laite toimii verkossa päivittämättömänä ennen tai jälkeen elinkaarensa loppua. Säännöllisiä tietoturvapäivityksiä pitäisi tehdä, ettei komponentti aiheuta tietoturvauhkaa verkossa.

Tietoverkot

- Tämä osuus riippuu paljolti siitä, millainen käyttötilanne ja –tarve on, ja puhutaanko omasta vai muiden omistamasta verkosta. Käsitellään asiaa siis yleisellä tasolla:
- Pyri välttämään avoimia, suojaamattomia verkkoja, mikäli oman luotetun verkon (esim. kännykältä jaetun mobiiliyhteys) käyttäminen ei onnistu.
  - Ulkomailla varsinkin, kotimaassa harkinnan mukaan.
- Verkossa toimiminen edellyttää haittaohjelmasuojausta ja mahdollisesti sen kyljessä olevaa ohjelmallista palomuuria, mikäli käytät tietokonetta. Mobiililaitteella selailtaessa tilanne on moniulotteisempi.
- Erilaisia seurannanestoon ja verkkoidentiteetin häivyttämiseen tarkoitettuja sovelluksia on saatavilla, mikäli haluat pysyä seurannan ulkopuolella (jota on toki monen tyyppistä).

Tietoverkot

- Vältä sivustoja, joiden sisältö tai erillisen ”rankkaussovelluksen” arvioima maine on kyseenalainen.
- Erota työkäyttöön ja viihdekäyttöön tarkoitetut laitteet, sovellukset ja toiminnot toisistaan verkkoselausten osalta, mikäli mahdollista.
  - Esim. työkannettavalla työasiat, tabletilla viihdekäyttö
  - Esim. lapset eivät käytä vanhempien työkannattavia viihdekäytössää
- Älä käytä mobiililaitteilla sovelluskauppojen ulkopuolisia latauskohteita ja käytä harkintaa eksoottisempien sovellusten asennuksessa.
  - Esim. Google Play-kaupasta on saatavilla vähän sitä sun tätä ja huonolla tuurilla napsahtaa.

Yritystoiminnan verkot

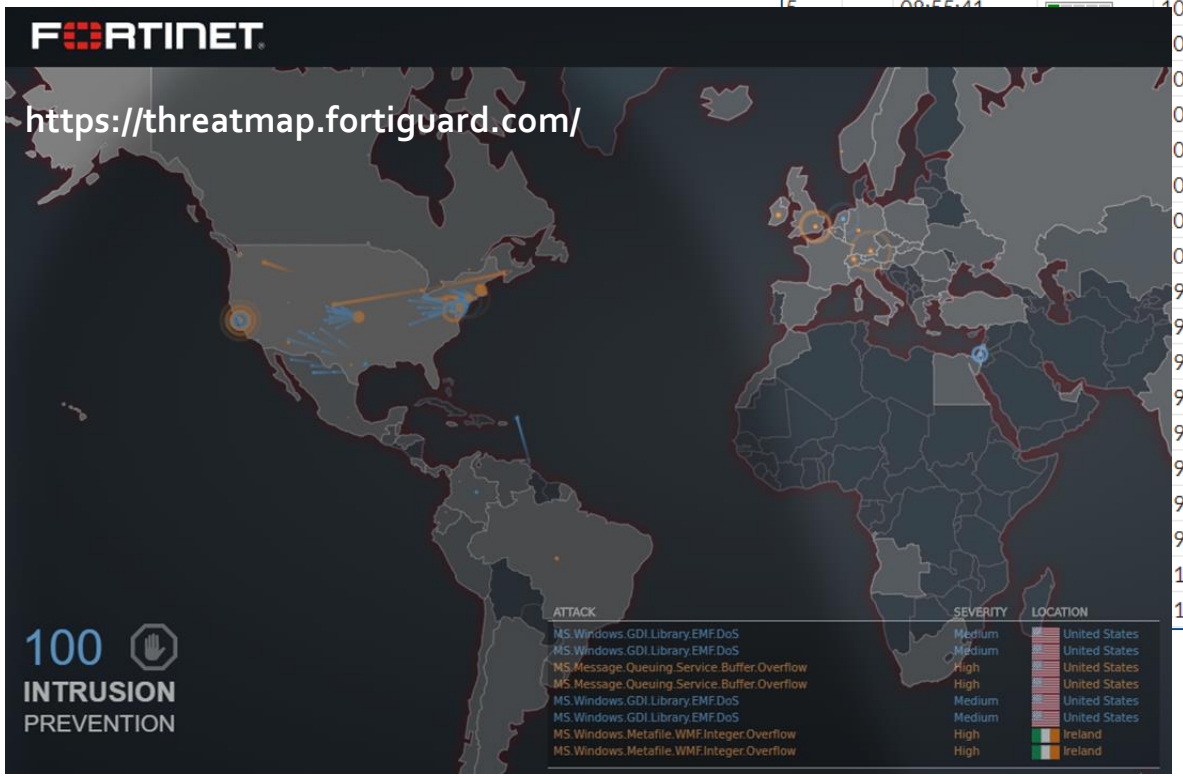
- Yrityksessä saattaa olla useampi langaton ja langallinen yhteys. Verkkoratkaisu voi olla monipuolisempi kuin äkkiseltään voisi kuvitella.
- Käytännössä verkon pitäisi olla eritasoinen ja suhteutettu toimintaan. Pyri siis välttämään tilanne, jossa kaikki liikenne siirtyy samassa verkossa.
  - Yrityksen data oman verkkoonsa.
  - Automaatio- ja hallintajärjestelmät pois julkisesta ja viihdekäyttöverkosta.
  - Viihdeliikenne kokonaan omaan verkkoonsa, samoin vierasverkot vierasliikennettä varten.
- Jos verkon takana oleva tekniikka on oikeasti tärkeää ja edellyttää varmaa toimintaa, harkitse palomuurin hankintaa ja verkon tietoturvan kevyttä arviointia – mieluusti palveluna toki.

Tietoverkon laitteet

- Salasana ja käyttäjätunnukset heti pois oletuksista. Juuri näitä jokainen robotti etsii pitkin poikin Internet-verkkoa.
- Tietoturva- ja firmwarepäivitykset ajan tasalle ainakin verkon rajapinnassa olevilla laitteilla (ADSL-laitteet, mokkulat, palomuurit).
- Onko laite hallittava tai ”näkyykö” laite julkiseen verkkoon (Internet)? Miksi ja onko tämä pakollista?
  - Erilaiset IoT-laitteet ovat tietoturvaltaan niin ja näin. On tunnettu tosiasia, että myös tunnettujen laitteiden valmistajilla on heikot kohtansa.
- Tiedätkö mitä laitteita verkkosi sisältää? Kotiverkossa voi olla niitä paljon enemmän kuin oletatkaan.

Esimerkki: tietoverkot

#		Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1		09:03:48		172.104.6.206	tcp		detected		Cisco.Smart.Install.Feature.Enable.Scanner
2		08:58:07		112.217.106.50	tcp		detected		MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow
3		08:55:41		10.10.1.80	tcp		detected		SSL.Anonymous.Ciphers.Negotiation
4		08:55:41		10.10.1.80	tcp		detected		SSL.Anonymous.Ciphers.Negotiation
				10.10.1.80	tcp		detected		SSL.Anonymous.Ciphers.Negotiation
				0.10.1.80	tcp		detected		SSL.Anonymous.Ciphers.Negotiation
				0.10.1.80	tcp		detected		SSL.Anonymous.Ciphers.Negotiation
				0.10.1.80	tcp		detected		SSL.Anonymous.Ciphers.Negotiation
				0.10.1.80	tcp		detected		SSL.Anonymous.Ciphers.Negotiation
				0.10.1.80	tcp		detected		SSL.Anonymous.Ciphers.Negotiation
				06.189.73.122	tcp		detected		ZmEu.Vulnerability.Scanner
				06.189.73.122	tcp		detected		ZmEu.Vulnerability.Scanner
				9.127.238.44	tcp		detected		Joomla!.Core.Session.Remote.Code.Execution
				9.127.238.44	tcp		detected		Joomla!.Core.Session.Remote.Code.Execution
				9.127.238.44	tcp		detected		ThinkPHP.Request.Method.Remote.Code.Execution
				9.127.238.44	tcp		detected		PHP.Diescan
				9.127.238.44	tcp		detected		PHP.Diescan
				9.127.238.44	tcp		detected		PHP.Diescan
				9.127.238.44	tcp		detected		PHP.Diescan
				9.127.238.44	tcp		detected		PHP.Diescan
				18.25.71.119	tcp		detected		Joomla!.Core.Session.Remote.Code.Execution
				18.25.71.119	tcp		detected		ThinkPHP.Request.Method.Remote.Code.Execution



Varmuuskopiointi

- Yritystoiminnan tietoteknisiin oletusarvoihin kuuluu olennaisena osana datan varmuuskopiointi. Sama totuus ulottuu myös henkilökohtaiseen dataan, mutta sen kriittisyys ei ehkä valokuvia ja videoita lukuun ottamatta ole aivan samalla tasolla.
- Varmuuskopioinnin idean ymmärtää jokainen: data tallennetaan useaan kertaan eri kohteeseen, jotta laiterikot, tulipalot tai mahdolliset haittaohjelmien toiminnot eivät tuhoaisi ainutlaatuista dataa.
- Tekniikkaa on paljon, ja varmuuskopiointia kannattaa oikeasti miettiä hieman laajemmin.

Varmuuskopiointi

- Ensisijaisin asia ei ole mediavalinta, vaan se, että varmuuskopiointia tehdään säännöllisesti ja sitä myös testataan aika ajoin luotettavuuden nimissä.
- Jos kohteena on tuotantojärjestelmä ja varmuuskopiointi on saatavavilla palveluna, tartu siihen, mikäli hinta on asiallinen.
- Älä kavahda pilveä: tunnettu pilvipalvelu on hyvä vaihtoehto monen asian laite- ja tekniikkariippumattomaan varmuuskopiointiin (tietokannat, tiedostot, valokuvat…). Hinta voi olla ilmainen tai jotakin muuta eli suhteuta tämä tarpeeseen.
  - Pilven luotettavuus ja toimintavarmuus on vähintään hyvä, jos kyseessä on tunnettu palvelu.
  - Pilven tietoturva on hyvällä tasolla ja varmasti parempi kuin käyttäjän oma tietoturva, jos kohteena on edelleen tunnettu pilvipalvelu.
- USB-levyt on suhteellisen hyvä media, mutta vielä parempi, jos mukana on edes auttava automaatio varmistuksen suoritukseen.

Automaatio- ja laitejärjestelmät

- Yrityksillä on tai voi olla erilaista automaatiota ja tietoliikennettä:
  - Tuotantotiloissa
  - Säätöjärjestelmissä
  - Valvontalaitteissa
  - Roboteissa
  - Erilaisissa anturijärjestelmissä
  - Työkoneissa ja traktoreissa ja niin edelleen…

Automaatio- ja laitejärjestelmät

- Suurin osa näistä lukuisista laitteista ja antureista on tietoverkkoon kytkettyjä, koska järjestelmätoimittaja tai muu vastaava taho edellyttää näin tapahtuvan.
- Järjestelmien toiminta, päivitystilanne, ylläpito ja huolto vaihtelevat näissä suuresti.
- Omaehtoisen toiminnan ja itse sovelletun tietoturvan ulottaminen näihin järjestelmiin voi olla luvatonta tai jopa haitallista, joten näitä järjestelmiä emme voi tässä yhteydessä käsitellä kuin yleisellä tasolla.

Linkkejä

- https://www.yksityisyydensuoja.fi/salasanat
- https://crackstation.net/
- https://www.md5online.org/
- https://worldmap3.f-secure.com/

Kysymyksiä