fordione

TIETOTURVALLISUUSKOULUTUS

”Ihan tunnepohjalla mennään...”

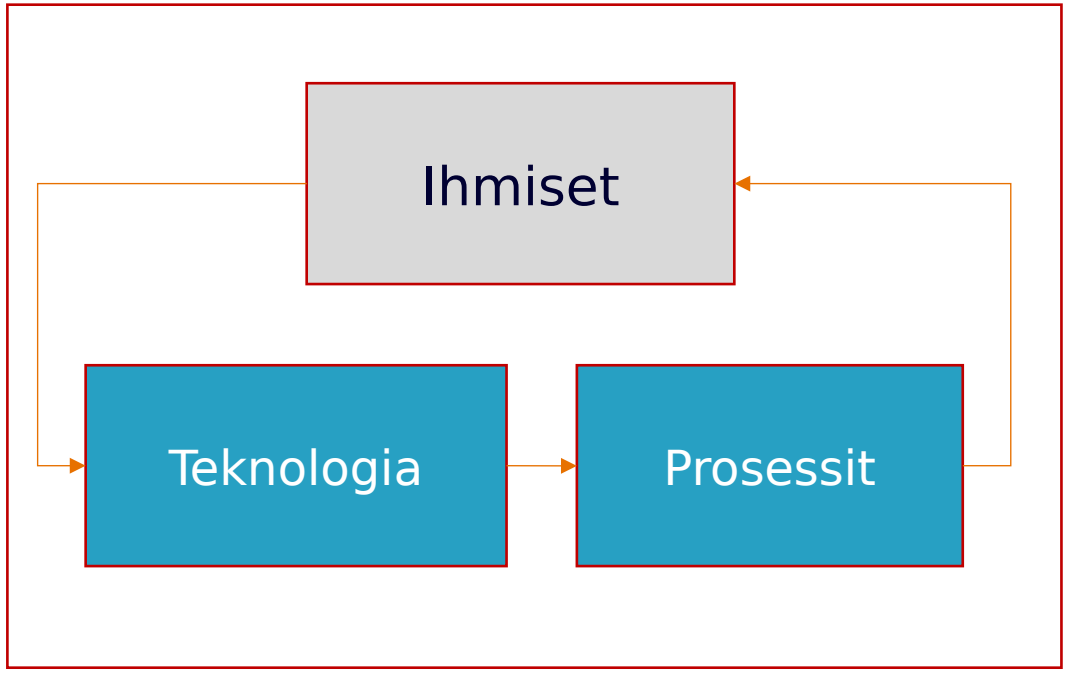
Turvallisuus on tunne

96 %
ihmisistä kokee
henkilökohtaisen
turvallisuutensa hyväksi *)

Tunne on jonkin tuntemuksen, kuten mielihyvän tai mielipahan, sävyttämä tietoinen elämys

*) Lähde: TUOVI, eli sisäisen turvallisuuden portaali

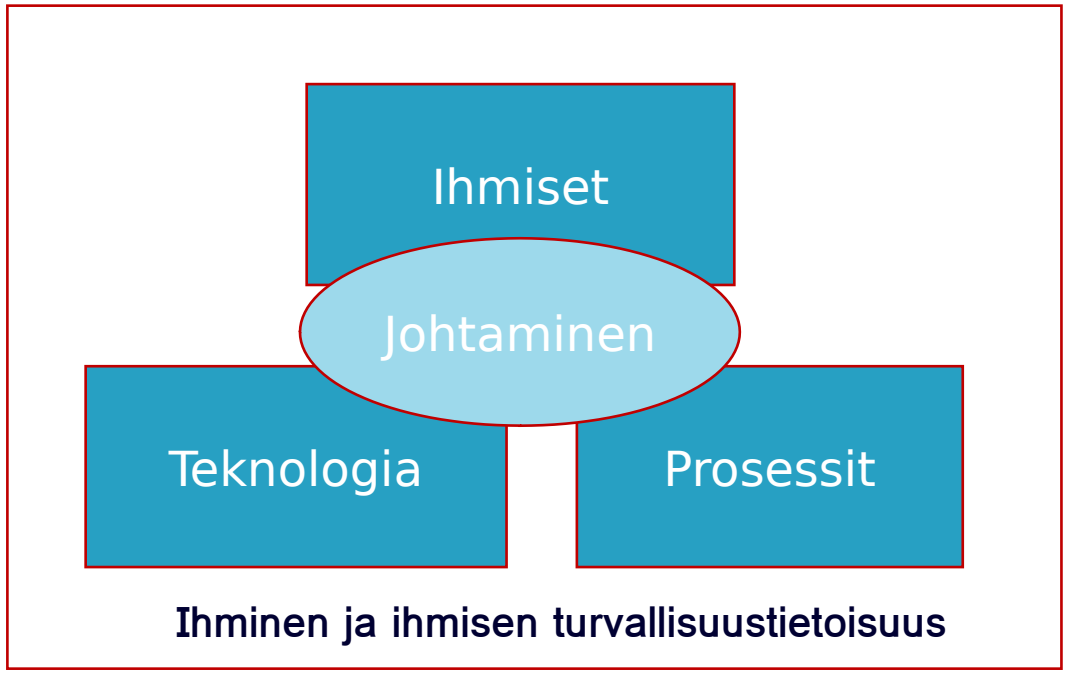
Kasvavat uhat pakottavat kuitenkin panostamaan turvallisuuteen aina vain enemmän – ja tässä yhteydessä turvallisuustietoisuuden lisäämiseen tulee kiinnittää erityistä huomiota



- Ihmiset eivät välttämättä suhtaudu tietoturvaan välinpitämättömästi, mutta he eivät aina ymmärrä omaa tärkeää rooliaan esimerkiksi organisaation tietoturvaan kohdistuvien riskien minimoimisessa
- Meidän tulisi kuitenkin pystyä tunnistamaan erilaisia tietoturvallisuuteen liittyviä poikkeustilanteita ja toimimaan oikein niiden mahdollisesti tapahduttua
- Oikein toimimista edistetään parhaiten tietoturvallisuusosaamista ja digiturvakulttuuria vahvistamalla

Kyberturvallisuus..

..tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja tämän vaikutusta niiden toimintoihin



- Ihmiseen kohdistuu jatkuvasti haasteita niin teknologian kuin ympäristönkin kautta
- Teknologian tulee olla luotettavaa ja skaalautuvaa ja sen tulee suojata organisaation ydintoiminnot
- Prosessien tulisi olla tunnistettuja, kuvattuja sekä turvattuja turvallisen toiminnan kehittämistä ja poikkeaman hallintaa varten

Kaikkea tätä pitäisi pystyä myös johtamaan.

Ihmisten kohdalla olemme harmaalla alueella.
Niinpä olisikin syytä keskittyä ihmiseen
ja ihmisen käyttäytymiseen

Kytkeydymme tietoturvallisuuteen pääsääntöisesti sosiaalisen kerroksen kautta

Tietoturvallisuus ja sen toteuttaminen voidaan jakaa kolmeen osaan

1) Fyysinen kerros
   - Kerros, jossa data liikkuu ja sen suojaaminen
2) Tekninen kerros
   - Laitteet ja ohjelmistot ja niiden suojaaminen
3) Sosiaalinen kerros
   - Eli miten yksilö tuntee ja toimii

Sosiaalista kerrosta ohjaa usein *tunne*, sillä, kuten todettua, yksilön kokema turvallisuus on pohjimmiltaan tunne. Tunteitamme taasen ohjaavat vahvasti ***arvot***. Siksi onkin tärkeää, että turvallisuuden ohjeistamisessa ja kouluttamisessa huomioidaan myös yksilön arvot.

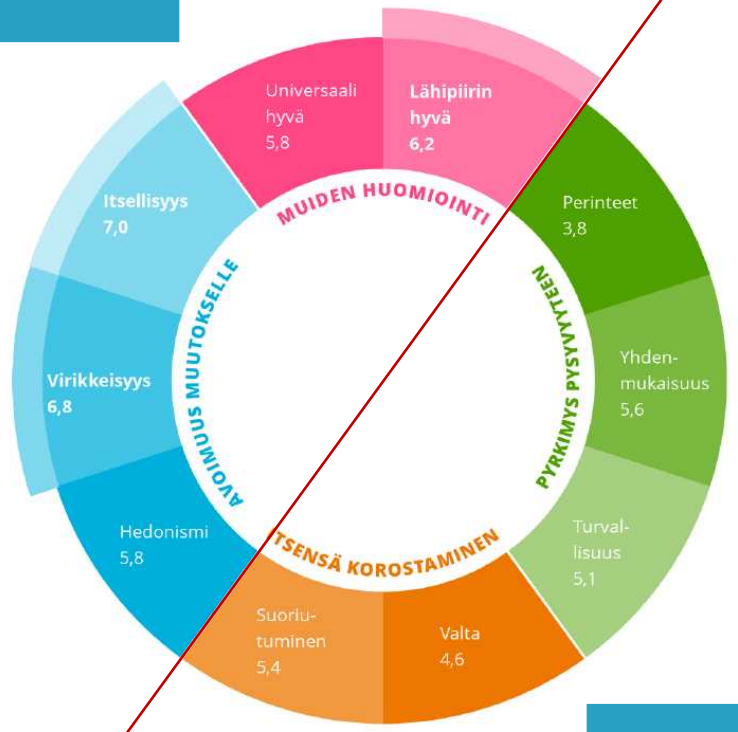
Tietoturvallisuus edellyttää yksiselitteistä määrittelyä. Ihmisiä taasen ohjaavat arvot - ja siksi me näemme myös turvallisuuden toteuttamisen eri tavoilla

Tunnistetut arvot auttavat luomaan kulttuuria

- Arvot ilmentävät käsitystä siitä, miten asioiden mielestämme pitäisi olla
- Kulttuuri on aina kollektiivinen, ei yksilöllinen ilmiö ja se jaetaan ainakin osittain niiden ihmisten kanssa, jotka elävät tai työskentelevät samassa sosiaalisessa ympäristössä
- Jokainen ihminen luo omalta osaltaan arvojensa kautta kulttuuria
- Kulttuuria voidaan kuvata siten, että se kattaa yhteisön jakamat arvot, merkityksellistämisen, viestimisen ja tekemisen tavat sekä todellisuutta jäsentävät käsitykset ja uskomukset
- Näin ollen myös tietoturvallisuuden toteuttaminen edellyttää yhteisistä arvoista johdettua kulttuuria

Arvomme saattavat ohjata meitä myös turvallisuuden toteuttajina

Tietoturvaa toteutetaan itselle kulloinkin parhaiten soveltuvalla tavalla



Tietoturvaa toteutetaan ohjeiden mukaisesti

Suorittamamme toiminnan perusteella, olemme havainneet että tietoturvan toteuttamisen suhteen ihmiset voidaan jakaa neljään eri ryhmään:

- **Henkilö toteuttaa tietoturvakäytänteitä hyvin vaihtelevasti = *tuuliviiri***
- **Henkilö toteuttaa tietoturvakäytänteitä vaihtelevan innokkaasti = *innokas***
- **Henkilö toteuttaa tietoturvakäytänteitä mallikkaasti = *mallikas***
- **Henkilö on tunnollinen tietoturvan toteuttaja = *tunnollinen***

Tietoturvapoikkeama on yleensä monen asian summa.
Niihin on muutamia tunnistettavia seikkoja.

Suojaus voi pettää monella tavalla.

Tunnistetaanpa niistä muutamia.

Monen asian summa – jolla on usein yhteinen nimittäjä

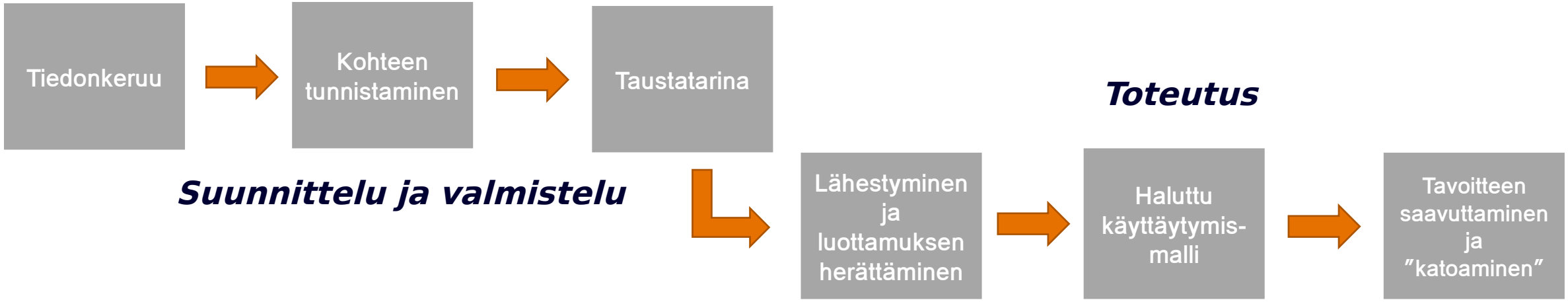
Tietoturvallisuuden johtaminen
Organisaation johto ei ole kiinnittänyt tietoturvallisuuteen ja sen johtamiseen riittävästi huomiota
Olennaisimpia toimintoja ja tietoja ei ole priorisoitu
”IT-asia”
”Luotamme työntekijöihimme 100 prosenttisesti”
Ymmärryksen puute

Teknologia
Verkon ja muun teknisen infrastruktuurin puutteet suojauksessa
Tietokantojen ja palveluiden huono suojaus
Huonosti suojatut laitteet ja huonosti hallinnoidut salasanat

Henkilöstö
Tietoturvallisuuteen liittyvä kouluttamattomuus
Ohjeiden noudattamattomuus
Huono tietoturvallisuusosaaminen
Omasta työnkuvasta johdetun koulutuksen puute
Erilainen arvomaailma

Ihminen on helppo kohde, koska meidän manipulointimme on lähtökohtaisesti helpompaa kuin suojausteknologioiden murtamien

- Käyttäjän manipuloinnin (Social Engineering) tavoitteena on vaikuttaa uhriin ja saada hänet tekemään asioita, jotka eivät ole hänen etunsa mukaisia. Tyypillisesti avuksi käytetään ihmisen heikkouksia.
- Manipulointi jakautuu kahteen osaan
  - Suunnittelu ja valmistelu
  - Toteutus



Kalastelua harrastetaan myös somessa, kuten tapaus Robin Sage osoittaa

Vuodesta 1974 lähtien Robin Sage -harjoitus on ollut SFQC:n (= USA:n armeijan erityisjoukkojen pätevyyskurssi) huipentuma ja näytönpaikka sotilaille, jotka pyrkivät ansaitsemaan himoitun vihreän baretin.

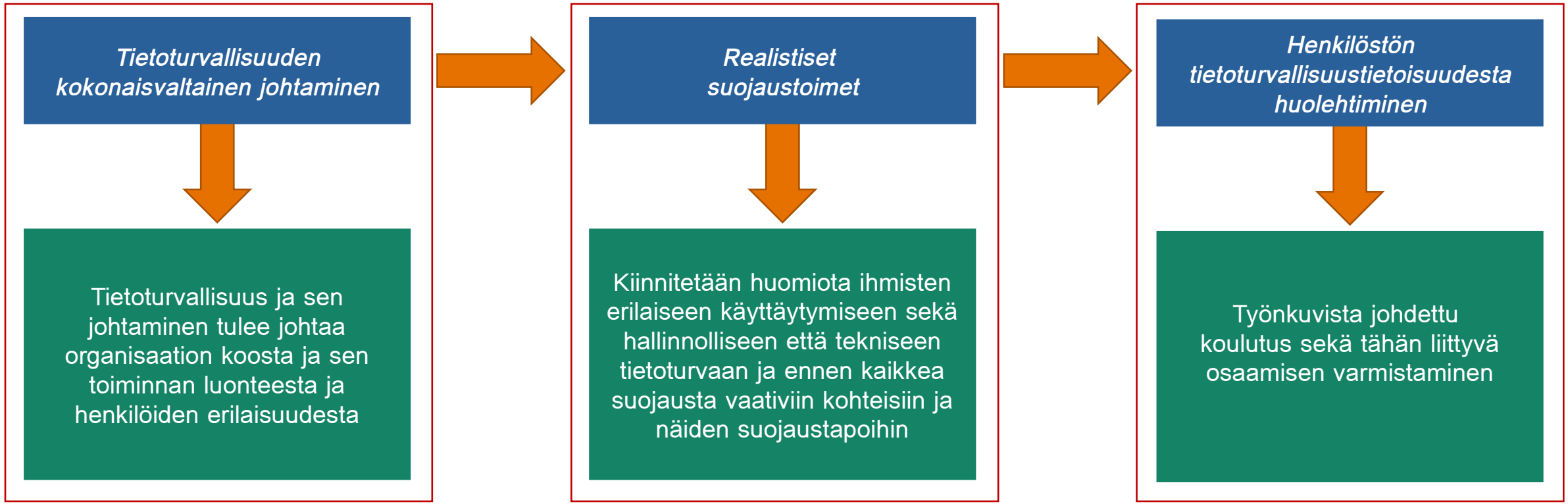
”Eräiden valkohattuhakkereiden onnistui soluttautua Yhdysvaltojen sotilas- ja tiedusteluorganisaatioihin luomalla valeprofiilit Facebookiin, LinkedIniin ja Twitteriin. Profiili sai nimen Robin Sage. Tekoälyn avulla hänelle luotiin profiilikuva ja ammatiksi ilmoitettiin ”kyberturvallisuusanalyytikko”.

Muutaman viikon sisään hänellä oli satoja ystäviä ja seuraajia mm. USA:n puolustushallinnosta, puolustusteollisuudesta, NSA:sta sekä Iso-Britannian asevoimista. Hänen onnistui verkostonsa kautta saada käsiinsä nimiä, osoitteita, sähköpostiosoitteita, pankkitilejä ja muita arkaluontoisia tietoja. Tämän lisäksi hän sai lukuisia illallis- ja esiintymiskutsuja sekä työtarjouksia mm. sellaisilta tahoilta kuin Google ja Lockheed Martin.

Profiili sai edellä kuvattuja kutsuja ja tarjouksia vielä senkin jälkeen, kun sen oli paljastettu olevan alusta loppuun valhetta.”

Tarinan opetus.
Älä hyväksy kaveripyyntöjä henkilöiltä, joita et tunne!

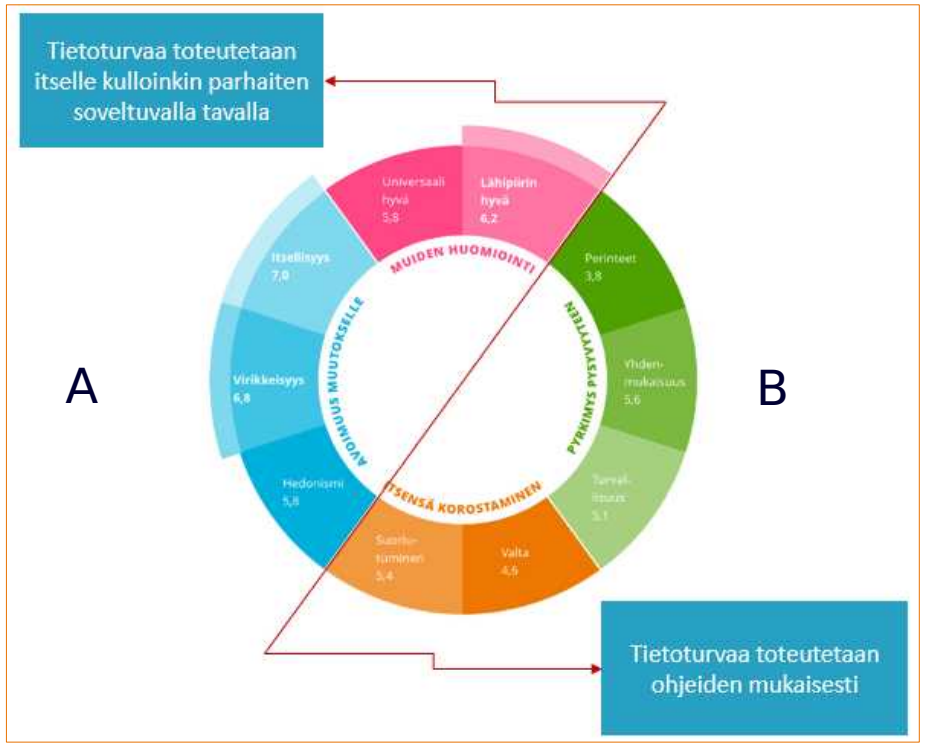
Mitä organisaatiot sitten voivat tehdä tietoturvallisuuden lisäämiseksi?



Ollako vai ei? Siinä pulma.

Pitääkö jatkossa puhua tietoturvallisuudesta,
tietoturvasta tai kyberturvasta?
Vaiko vain turvallisuudesta?

Pohdintaa



Alkuasetelma: Henkilön lukitsematon kännykkä on päätynyt vääriin käsiin.

Pohdinta 1: Mitä uhkia se saattaa aiheuttaa

a) Henkilölle itselleen

b) Hänen edustamalleen organisaatiolle

c) Läheisille ja ystäville

Pohdinta 2: Mitä henkilön tulisi tehdä, jotta mahdolliset seuraamukset jäisivät mahdollisimman vähäisiksi

Pohdinta 3: Miten kuvittelisitte vasemmalla esitettyjen ryhmien A:n ja B:n kohdalla suojaustoimien eroavan toisistaan?

Huomioita

Uhat itselle

Pankkiyhteydet

Sosiaalisen median tilien kaappaaminen

Verkko-ostokset, esim. Amazon

Kotiin liittyvät uhat

Identiteettivarkaus

Uhat organisaatiolle

Pääsy järjestelmiin

Tietovuodot

Esiintyminen organisaation nimissä

Mainehaitta

Uhat läheisille ja ystäville

- Sosiaalisen median aiheuttamat uhat

Suojautuminen

- Mahdollisimman lyhyt lukitusaika
- Mahdollisimman vähän appeja ja mieluusti vain oikeasti tärkeitä
- Joka palveluun eri salasana
- Ei arvattavat salasanat
- Sosiaalisen median etiketti
- Tieto siitä, miten toimia, jos kännykkä häviää
- Toimi heti, kun huomaat tilanteen
- Etähallinta

Pohdintoja tapahtuneesta

Uhat henkilölle itselleen

- Pääsy Some-tilille
- Puhelimeen tallennettujen salasanojen hyödyntäminen
- Verkkokauppatilaukset
- Mahdollinen henkilötietojen löytyminen
- Kännykän sisältämien tietojen hyödyntäminen
  - Esim. sijainti
- Kiristys (Esim. hakuhistorian pohjalta)
- Identiteettivarkaus

Uhat organisaatiolle

- Sähköpostitilin kaappaus

Uhat läheisille ja ystäville

- Kalasteluviestit
- Case Messenger

Suojautuminen

- Ilmoitus hävinneestä puhelimesta
- Korttien sulkeminen
- Tietosuojavastaavalle ilmoitus, mikäli tarpeen
- Kännykkään asennettujen tilien lukitseminen

Osallistuminen vapaehtoiseen tutkimukseen

Kirjaudu sivulle

https://tacitco.com/aloita/

Kirjoita käyttäjätunnukseksi

14120

Valitse salasana seuraavasti

Vaihteleva123	= Toteutat tietoturvakäytänteitä mielestäsi hyvin vaihtelevasti
Innokas123	= Toteutat tietoturvakäytänteitä mielestäsi vaihtelevan innokkaasti
Mallikas123	= Toteutat tietoturvakäytänteitä mielestäsi mallikkaasti
Tunnollinen123	= Toteutat tietoturvakäytänteitä mielestäsi tunnollisesti

FORDIONE

Matti Timonen
matti.timonen@fordione.fi
+358 400 137 136