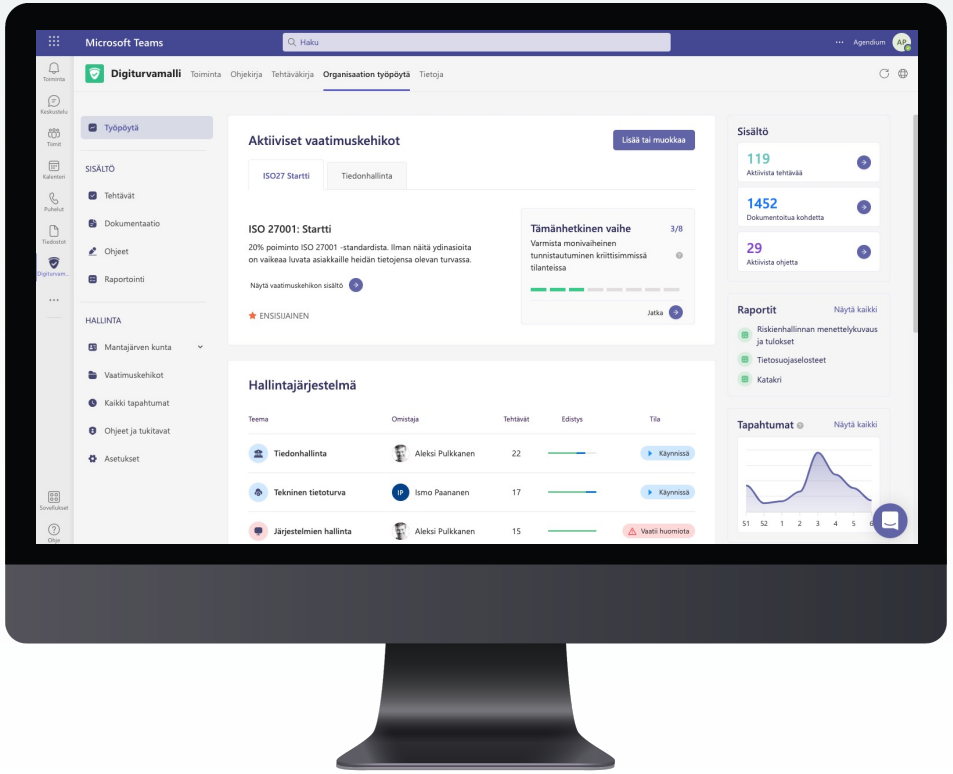
Kohti turvallista henkilötietojen käsittelyä

Tietoturvan hallintajärjestelmän rakentaminen

Ismo Paananen

CEO, Agendium Oy,
CIPT

Agendium Oy lyhyesti



1

Agendium Oy

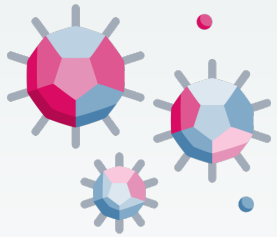
- Digiturvan johtamiseen ja hallintaan erikoistunut ohjelmistoyritys
- Pääpaikka Tampereella, n. 10 hengen tiimi
- Missiomme on tarjota paras mahdollinen alusta digiturvan hallintaan, joka selkeyttää työtä

2

Digiturvamalli

- Digiturvan hallintajärjestelmä, suoraan MS Teamsin sisällä
- Tiimimme dedikoitu tämän kehittämiseen ja auttamaan asiakkaita onnistumaan
- 300+ asiakasta kaikkien eri alojen organisaaioista

Tietosuojan kaksi pääkuoppaa



Ei laillista perustetta käsittelyyn

Relevantti ”ei-normaalissa käytössä”

Esimerkkejä

- Puutteellinen viestintä / suostumus (Google)
- Ei oikeusperustetta (H&M, TIM)
- Yleistä myös käsittelyperiaatteiden rikkominen (esim. tietojen minimointi, ParkkiPate)

Käsittelyn turvallisuus pettää

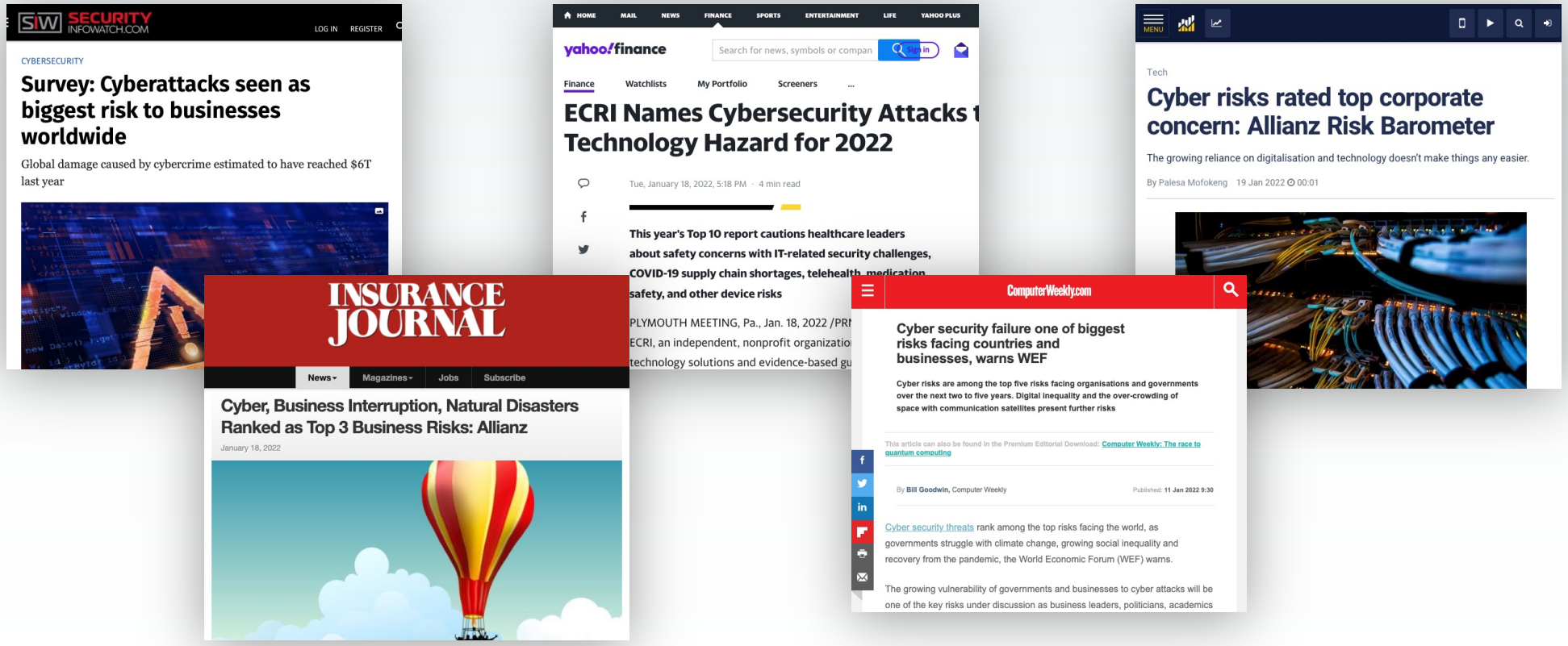
Relevantti kaikilla organisaatioilla

Esimerkkejä

- Puuttuva 2FA
- Riittämätön turvallisuustestaus
- Riittämätön ohjeistus
- Puutteelliset lokitiedot

01

Riskejä on monenlaisia, mutta nykyaikaisessa organisaatiossa **tietoturvariskit** alkavat dominoida



Mitä tietoturvariskit ovat?

Vihollisriskit

Kolmannen osapuolen toimittajat, sisäpiiriuhat, luotetut sisäpiiriläiset, vakiintuneet hakkerikollektiivit, etuoikeutetut sisäpiiriläiset, yritysvakoilut ja kansallisvaltiot.

Inhimilliset virheet

Käyttäjä voi vahingossa ladata haittaohjelmia tai joutua huijatuksi tietojenkalastelulla. Myös vaikkapa väärä tallennuspaikka voi paljastaa arkaluontoisia tietoja.

Järjestelmävirheet

Kun järjestelmässä tapahtuu virhe, se voi aiheuttaa tietojen menetyksen ja johtaa myös liiketoiminnan jatkuvuuden häiriintymiseen.

Luonnonkatastrofit

Hurrikaanit, tulvat, maanjäristykset, tulipalot ja salamat voivat aiheuttaa yhtä paljon vahinkoa kuin ilkeä kyberrikollinen

Mitä niiden realisoituessa tapahtuu?

Luvaton pääsy

Voi aiheutua haitallisista hyökkääjistä, haittaohjelmista tai työntekijöiden virheistä

Tietojen vuotaminen

Hyökkäykset tai virheelliset pilviasetukset voivat johtaa henkilötietojen (PII) ja muun tyyppisten arkaluontoisten tietojen vuotamiseen.

Tietojen väärinkäyttö

Sisäpiiriläinen voi käyttää tietoja väärin muuttamalla, poistamalla tai käyttämällä tietoja luvatta

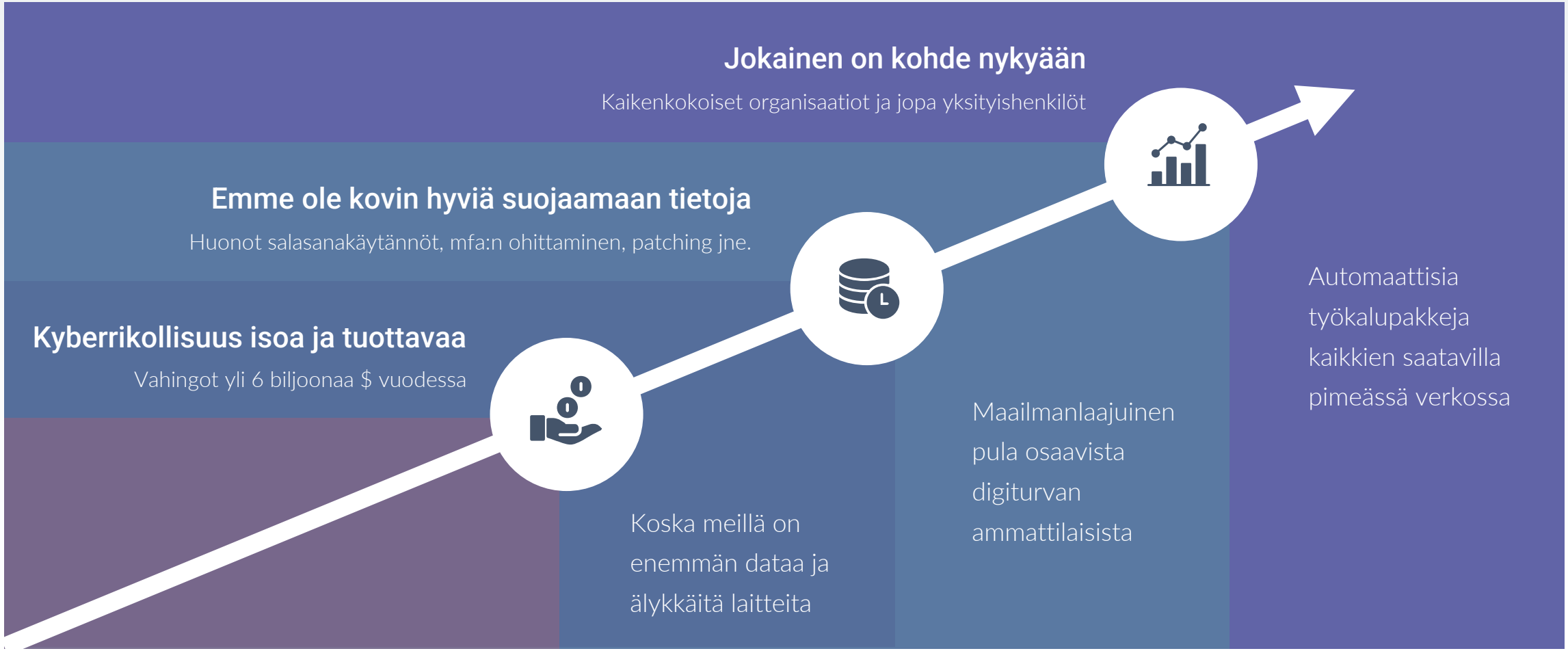
Tietojen katoaminen

Huonosti konfiguroidut replikointi- ja varmuuskopiointiprosessit voivat johtaa tietojen menetykseen tai vahingossa tapahtuvaan poistamiseen.

Toiminnan keskeytyminen

seisokit voivat aiheuttaa mainevaurioita ja tulonmenetyksiä. Ne voivat olla seurausta vahingosta tai esim. palvelunestohyökkäyksestä (DDoS).

Kyberhyökkäyksiin liittyvät **riskit** kasvavat jatkuvasti...



Nykyajan isoimpia tietoturvauhkia...

Tietojen kalastelu
AKA: Email spoofing, Social engineering, Identity theft

Haittaohjelmat
AKA: Viruses, Trojan Horses, Spyware, Worms

Ransomware
AKA: Encryption ransoms, CryptoWalls

Laiton henkilötietojen käsittely
AKA: Data procetion compliance, GDPR compliance

Salasanahyökkäykset
AKA: Compromised credentials, Password cracking

Sisäpiirihyökkäykset
AKA: Malicious employees, Internal cyber attacks

Toimitusketjuhyökkäykset
AKA: Third-party attacks, Watering hole attacks

Henkilöstön rooli digiturvassa on **jatkuvasti korostunut**

01 Liikkuva työ

Enemmän laitteita ja dataa aina ulottuvilla, joiden suojaaminen on haastavampaa.

02 Digitalisaatio

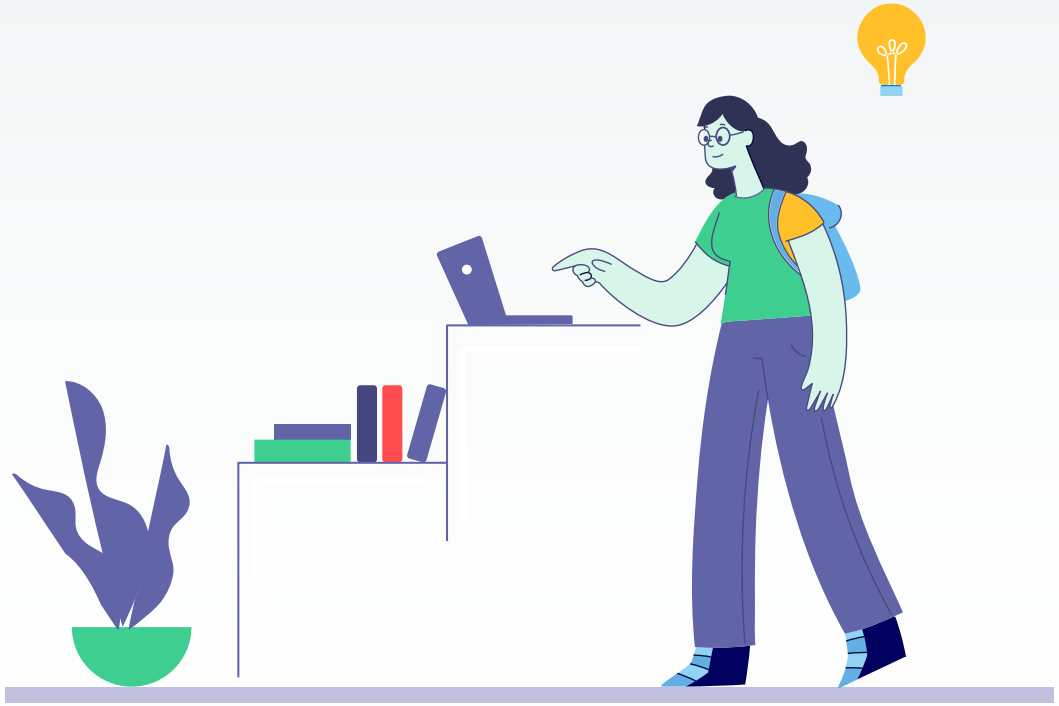
Jokainen tietotyöläinen tarvitsee yhä useampaa järjestelmää ja useampia tunnistetietoja päivittäin.

03 Etätyö

Pandemia on ajanut ihmiset yhä enemmän etätöihin – perinteisten suojausten ulkopuolelle.

04 Huijaukset

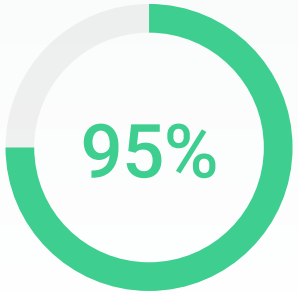
Tietojenkalastelu ja muut huijaukset ovat valtava riski, etenkin jos turvallisia toimitapoja ei ole sisäistetty.



Hyökkäysten **kohdistaminen ihmisiin** on tehokasta **kyberrikollisille**

hyökkäyksistä vaatii inhimillisen virheen

Hyökkäykset alkavat joko makron mahdollistamisesta, tiedoston avaamisesta, linkin klikkaamisesta...



hyökkäyksistä inhimillinen virhe on tärkeä mahdollistaja

Inhimillistä virhettä voidaan sitten eskaloida eteenpäin laajemmin mm. teknisiä haavoittuvuuksia hyödyntämällä.

Mitä ovat **inhimilliset virheet** tietoturvassa? (1/2)

Inhimilliset virheet näkyvät monin eri tavoin…

Työntekijän toimet…

- Myös tahtomattomat toimet tai tekemättä jättäminen

mahdollistavat häiriön.

- Aiheuttaa häiriön
- Laajentaa häiriötä
- Mahdollistaa häiriön tapahtumisen

Mitä ovat **inhimilliset virheet** tietoturvassa? (2/2)

Huijauksiin lankeaminen

Haittaohjelman lataaminen, luottamuksellisten tietojen luovutus tietojenkalastelijalle, väärän linkin klikkaaminen...

Päivitysten lykkääminen

Haavoittuvuutta päästään hyödyntämään, koska henkilöstö ei ole päivittänyt puhelintaan, läppäriään, tablettiaan...

Huono pääsynhallinta

Järjestelmien tai tietojen jakaminen liian suurelle joukolle, pääsyoikeuksien päivittämisen laiminlyönti...

Fyysisen turvallisuuden laiminlyönti

Toimiston kulunvalvonnan tai vierailijavalvonnan tukeminen, salakatselu tai salakuuntelu...

Huono salasanahygienia

Heikot salasanat, huono varastointi, salasanojen jakaminen, ei reagointia vuotamiseen...

Varomaton sähköpostin käyttö

Väärään osoitteeseen lähettäminen, BCC-ongelmat...

Huolimaton tietojen käsittely

Tietojen lataaminen paikallisesti, tulostaminen ilman turvallista hävittämistä, julkaisu vahingossa...

Tarvitaan systemaattista toimintatapaa

Mikä on tietoturvan hallintajärjestelmät (ISMS)?

- Organisaation on luotava itselleen tietoturvan hallintajärjestelmä
  - Määrittää, kuinka tietoturvaa toteutetaan organisaation päivittäisessä toiminnassa
- Tarvitaan johdettu kokonaiskuva
  - Ei hahmotonta kasaa piilossa olevaa tekemistä
  - Standardi ei anna muotovaatimuksia, mutta hyviä käytäntöjä on tarjolla

Mikä on ISO 27001?

ISO 27001 on kansainvälisesti tunnetuin tietoturvastandardi

Hallintajärjestelmä

Organisaatio ylläpitää ja jatkuvasti parantaa tietoturvan hallintajärjestelmää (ISMS)

01

Johtamisen toimintatavat

Organisaatio johtaa tietoturvaa systemaattisesti ja uskottavin toimintatavoin

02

Tietojen suojaustavat

Organisaatiolla on riittävät tavat tiedon suojaamiseen ja näiden jatkuvaan arviointiin

03

114 hallintakeinoa käsiteltäväksi tiedon suojaamiseksi

5. Tietoturvapolitiikat

6. Tietoturvallisuuden organisointi

7. Henkilöstöturvallisuus

8. Suojattavan omaisuuden hallinta

9. Pääsynhallinta

10. Salaus

11. Fyysinen turvallisuus

12. Käyttöturvallisuus

13. Viestintäturvallisuus

14. Järjestelmien hankinta ja kehitys

15. Toimittajasuhteet

16. Häiriöiden hallinta

17. Jatkuvuuden hallinta

18. Vaatimustenmukaisuus

Mitä tietoturvan hallintakeinot ovat?

- Esim. kannettavan tietokoneen jättäminen autoon

Ohje

Organisaation sääntö, jota on noudatettava

Koulutus

Ymmärtää syyt ohjeiden takana, motivoituu

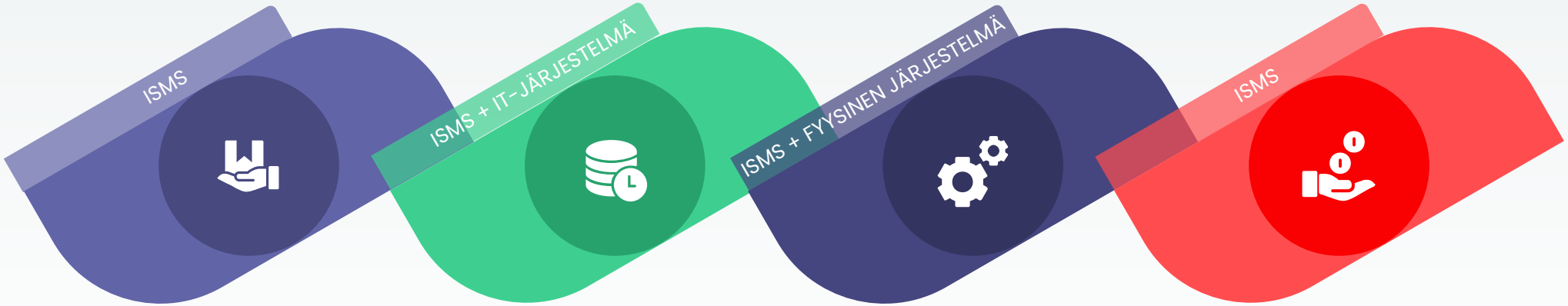
Tekninen kontrolli

Pakollinen koneen lukitus, levyn salaus

Omaisuuden hallinta

Kannettavien seuranta ja tietopääsyn valvonta

Tarvitaan monenlaisten keinojen yhdistelmä



Organisaatio

Omaisuuden hallinta, vastuut, jatkuvuuden suunnittelu

Tekninen

Varmuuskopiot, salaus, haavoittuvuuksien hallinta

Fyysinen

Pääsynhallinta, laitteiden suojaus ja huolto

Ihmiset

Ohjeet, koulutus, sopimukselliset keinot

Ensimmäisiä keinoja

01	**Tietojärjestelmät**	Kerää tiedot kaikista tietojärjestelmistä, ja kirjaa ylös niiden tärkeimmät tiedot kuten toimittaja ja tallennettavat tiedot, muista ylläpitovastuu!
02	**Tietovarannot**	Selvitä millaisia kokonaisuuksia tietoaineistoista syntyy, ja käy läpi tiedot huolella. Tätä tietoa tarvitaan myös tietosuojaviestinnässä.
03	**Ohjeistaminen**	Etätyö, tietojenkalastelu, salasanojen huolellinen käyttö, henkilötietojen käsittelyn ymmärtäminen – mm. näistä tulisi ohjeistaa
04	**Suojaaminen**	Tekniset suojauskeinot ovat tärkeässä roolissa, joista monivaiheinen tunnistautuminen on tärkeimpiä

Muita tärkeitä tietoturvan peruspilareita

Mobiililaitteet

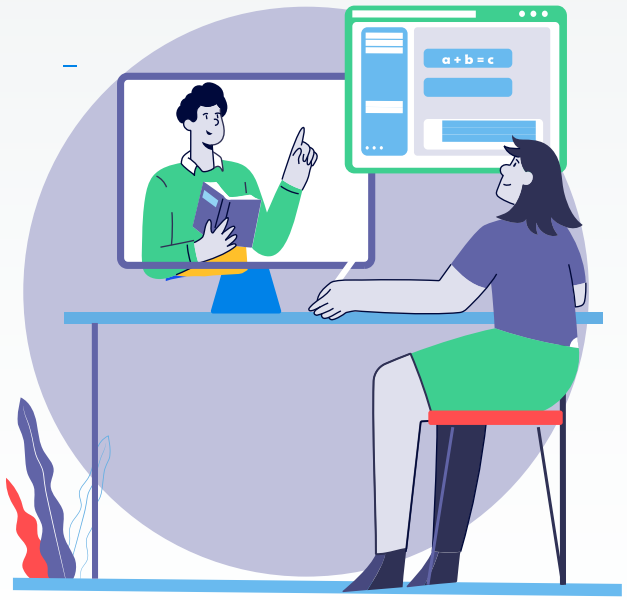
PIN-koodi ja varautuminen laitteen katoamiseen

Salaaminen

Salataan kovalevyllä olevat tiedot koneen katoamisen varalle

Häiriöön varautuminen

Mieti miten ilmoitetaan talon sisällä ja kehen otetaan yhteyttä



Varmuuskopiointi

Muistettava myös varmentaa että voidaan palauttaa

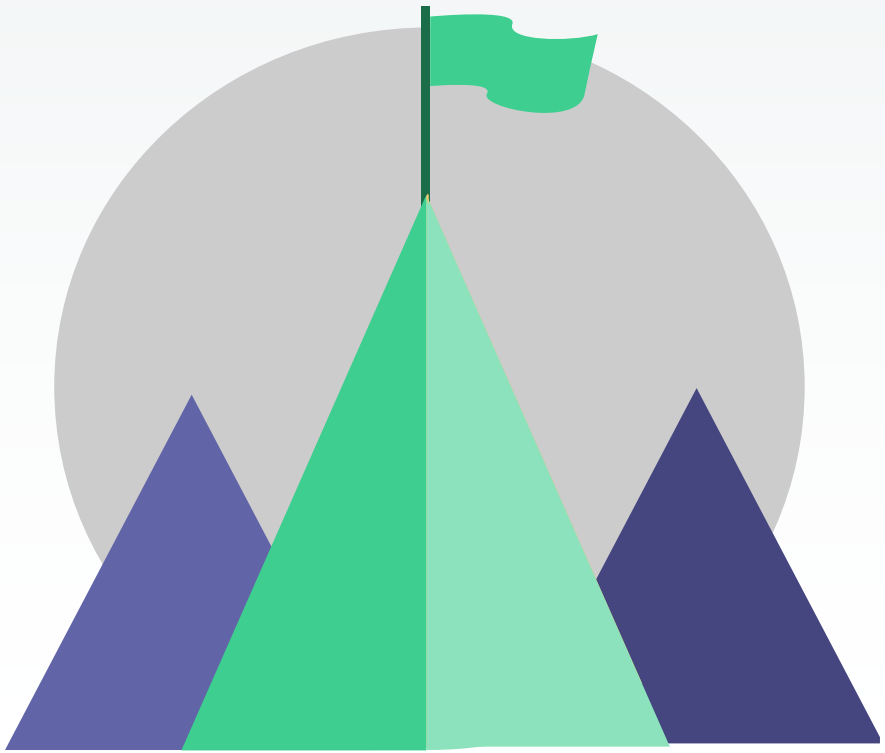
Haittaohjelmasuojaus

Virustorjunta auttaa jonkin verran, mutta ei saa luottaa liikaa

Häiriöiden käsittely

Tietoa häiriön hoidosta tarvitaan usein jälkikäteen

Toimivan hallintajärjestelmän hyödyt



01 Parantunut tietoturva

Suojaudu kyberhyökkäyksiltä ja vähennä riskejä selkeällä tietoturvatyöllä.

02 Helpompi asiakashankinta

Helpota myyntiä näyttämällä, että tietoturva otetaan vakavasti ja parhaat käytännöt ovat käytössä.

03 Vältä sakkoja ja ongelmia

Näytä vahvojen todisteiden avulla, että tietoturva oli otettu vakavasti ja työtä oli tehty.

04 Vahvuutta sertifioinnista

Vahva ISMS-toteutus on pakollinen sertifioinnin saamiseksi.

Kiitokset!

Ismo Paananen

CEO, Agendium Oy, CIPT

+358 40 7288 299

ismo.paananen@agendium.com

Lisäoppia: digiturvamalli.fi/webinarit