Tervetuloa koulutukseen

# KÄYTÄNNÖN TIETOTURVASUUNNITELMA HENKILÖTIETOJEN SUOJAAMISEKSI

22.9.2021, GDPR2DSM & Digiturvamalli

**Ismo Paananen**
CEO, Agendium Oy, CIPT

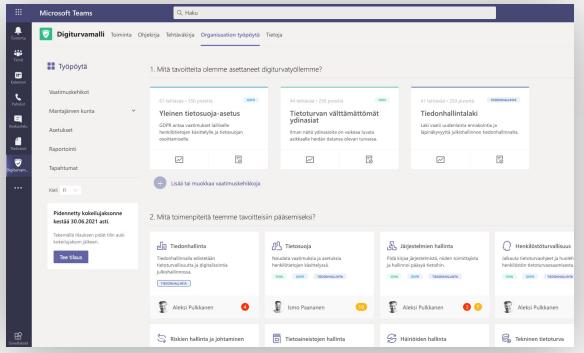
# Agendium Oy lyhyesti

- Digiturvaan ja vaatimustenmukaisuuden erikoistunut suomalainen ohjelmistoyritys
  - Sertifioitua ja koeteltua osaamista näissä teemoissa vuodesta 2013 alkaen
- Autamme organisoimaan digiturvatyön ja asiat lähelle ihmisten arkea
  - Palvelemme Digiturvamalli-sovelluksen kautta, Microsoft Teams -ympäristössä
- Asiakkaina 250+ suomalaista organisaatioita monilta aloita
  - Esimerkkejä asiakkaista…

# Aiheet tänään

1. Ymmärrä uhkat
2. Päätä tavoitteet
3. Luo oma suunnitelma
4. Varmista reagointi

- Mihin tietoturvalla varaudutaan?
  - Top 10 nykyajan tietoturvauhkat
  - Uutisia / case-esimerkkejä maailmalta
- Kuinka toimia digiturvan eteen?
  - ISO 27001 –standardin esittely
  - Nykytilan hahmottaminen ja tavoitetaso
  - Oma digiturvasuunnitelma


# Top 8 nykyajan tietoturvauhkat

Mihin tietoturvalla varaudutaan?

# 8 nykyajan suurinta tietoturvauhkaa

## Tietojen kalastelu

Phishingissä huijari yrittää hankkia arkaluontoisia tietoja (esim. salasanoja) esittämällä tuttua tahoa.

## Haittaohjelmat

Haittaohjelma on yleisnimitys ei-toivotuille ohjelmille. Virukset, botit, trojalaiset, rootkitit ja madot ovat eri tyyppisiä haittaohjelmia.

## Ransomware

Kiristyshaittaohjelma salaa uhrin tiedostot ja tarjoaa pääsyä lunnasmaksua vastaan.

## Business-email-compromise

Työntekijän sähköposti otetaan haltuun pyytääkseen kollegoja tai kumppaneita tekemään tekaistuja pankkisiirtoja.


## Salasanahyökkäykset

Tunnuksia on paljon ja samoja tunnistetietoja käytetään uudelleen ja uudelleen. Tosiasia, jota hyökkääjät hyödyntävät.

## Sisäpiirihyökkäykset

Tahalliset tai tahattomat. Ex-työntekijä suuttuu tai nykyinen työntekijä tekee huolimattomuusvirheen.

## Väärinkonfiguroitu pilvitallennustila

Avoimeksi jäänyt verkossa oleva tietokanta voi paljastaa arkaluontoisia tietoja.


## Laiton henkilötietojen käsittely

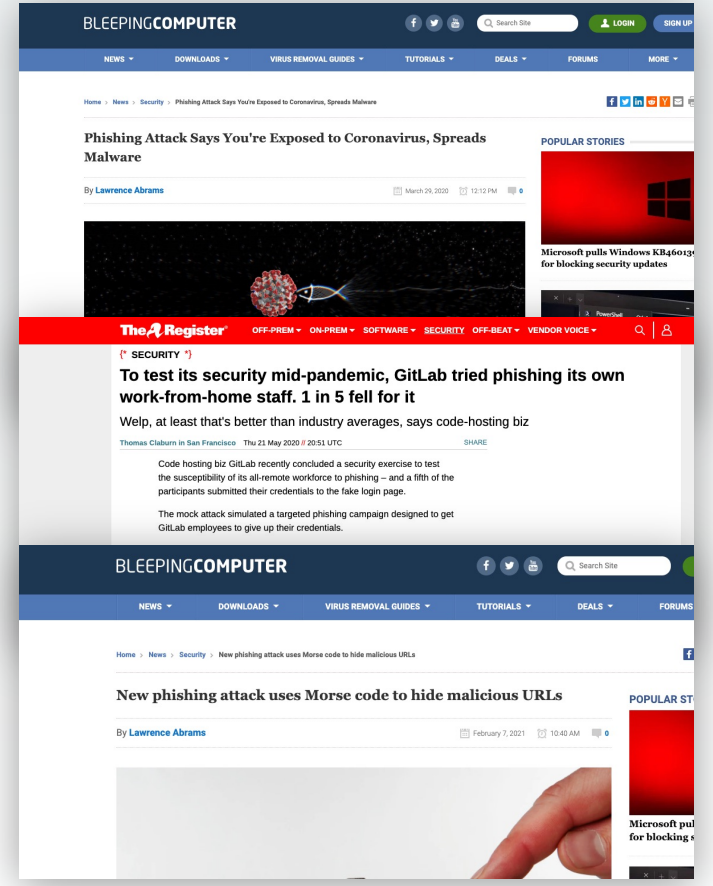
GDPR vaatii tietosuojan perusasioiden raportointia selosteessa käsittelytoimista ja sen osoittamista, kuinka takaamme käsittelyn turvallisuuden.

# Case-esimerkki

- Tietojenkalastelu ajankohtaisilla teemoilla
  - Phishing email says you’re infected with Corona virus, and spreads Malware
- Phishing toimii tuloksekkaasti
  - To test its security mid-pandemic, GitLab tried phishing its own work-from-home staff. 1 in 5 fell for it
- Tavat kehittyvät
  - New phishing attack uses Morse code to hide malicious URLs

## Tietojen kalastelu

Phishingissä huijari yrittää hankkia arkaluontoisia tietoja (esim. salasanoja) esittämällä tuttua tahoa.



# Case-esimerkki

**Ransomware**
Kiristyshaittaohjelma salaa uhrin tiedostot ja tarjoaa pääsyä lunnasmaksua vastaan.

- Ransomwaressa yhä useammin mukana myös tietojen julkaisulla kiristäminen
  - Why Paying to Delete Stolen Data is Bonkers
- Ramsomware-tapauksia eri aloilla päivittäin
  - Campari hit by Ragnar Locker Ransomware, $15 million demanded
- Haittaohjelmia uusia reittejä
  - Hugely Popular 'The Great Suspender' Chrome Extension Contains Malware

# Seuraamuksia

**Laiton henkilötietojen käsittely**
GDPR vaatii tietosuojan osoittamista sekä käsittelyn turvallisuuden varmistamista

## Sakkoja annettu 300M€ edestä (lähteenä enforcementtracker.com, 20.1.2021)

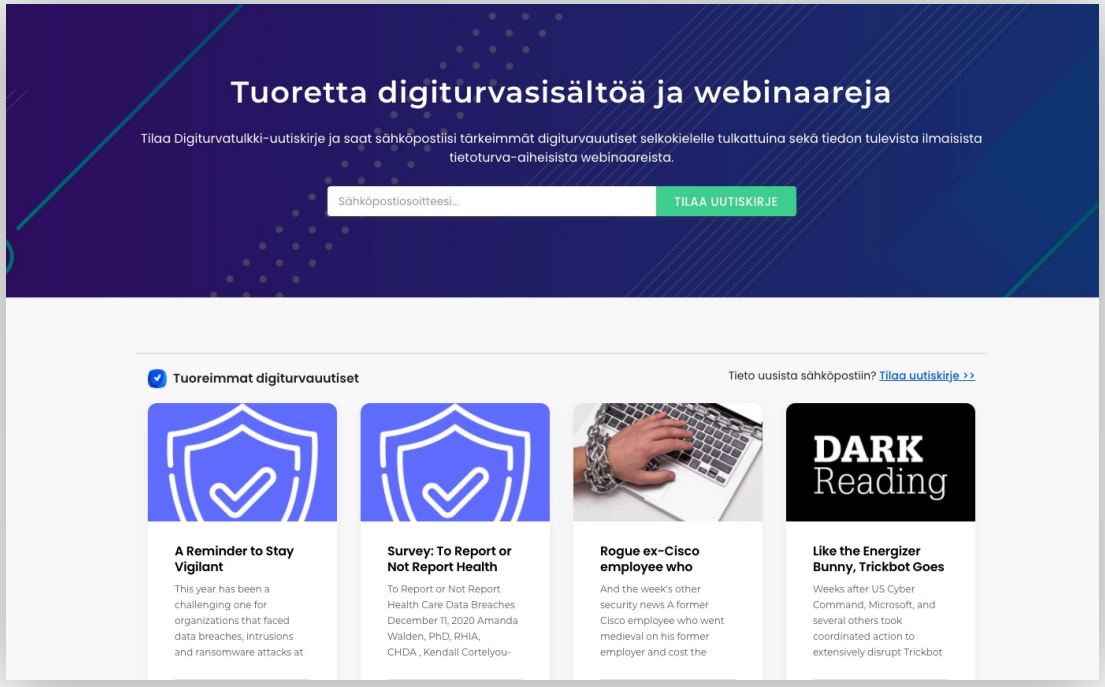
| Violation | Sum of Fines |
|---|---|
| Insufficient legal basis for data processing | **€ 163,902,598** (at 201 fines) |
| Insufficient technical and organisational measures to ensure information security | **€ 63,782,532** (at 112 fines) |
| Non-compliance with general data processing principles | **€ 33,076,164** (at 84 fines) |
| Insufficient fulfilment of data subjects rights | **€ 7,667,725** (at 49 fines) |
| Insufficient fulfilment of information obligations | **€ 5,630,445** (at 29 fines) |
| Insufficient fulfilment of data breach notification obligations | **€ 714,291** (at 14 fines) |
| Lack of appointment of data protection officer | **€ 186,000** (at 5 fines) |
| Insufficient cooperation with supervisory authority | **€ 151,779** (at 22 fines) |
| Insufficient data processing agreement | **€ 14,380** (at 2 fines) |
| Unknown | **€ 500** (at 1 fines) |

# Yhteenvetona

- Erityiset henkilötietojen käsittelyn tarkoitukset tärkeää tiedosta ja hoitaa huolella
    - Oikeusperusteena suostumus tai oikeutettu etu
- Iso osa tietosuojaongelmista lähtee tietoturvaongelmista
    - Kaikille tietoturvaongelmat voivat johtaa tietosuojasakkoihin

# Pysy kärryillä?

- Julkaisemme viikottain Digiturvatulkki-uutiskirjettä
  - Tärkeimmät uutiset selkokielellä tulkattuina
  - https://digiturvamalli.fi/tulkki




# ISO 27001 - tietoturvastandardi

Pikaesittely

# ISO27001

- Johtava kansainvälinen standardi tietoturvallisuudesta
  - ISO ja IEC julkaisijat
  - Kaikille toimialoille
  - Sertifioituminen mahdollista
- Auttaa suojaamaan tietoja systemaattisesti ja kustannustehokkaasti
  - Ottamalla käyttöön tietoturvallisuuden hallintajärjestelmä
    - Järjestelmä, jossa kuvattu toimintaympäristö, riskit, hallintakeinot, tavoitteet
    - Valvotaan, mitataan, jatkuvasti parannetaan


# Hallintakeinojen osa-alueet ja ISO27002

ISO27001-tietoturvastandardi

# ISO27001:n osa-alueet

**"Millaisilla menettelyillä varmistetaan tietoturvan järjestelmällinen johtaminen ja hallinta organisaatiossa?"**

### 4. Organisaation toimintaympäristö

Tietoturvan kannalta tärkeiden sisäisten ja ulkoisten asioiden ymmärtäminen


### 6. Suunnittelu

Riskien arvioinnin ja käsittelyn toteuttaminen, soveltuvuuslausunto, tavoitteet

### 8. Toiminta

Riskien arvioinnin ja käsittelyn tarkempi toteutus sekä tavoitteiden saavuttaminen

### 5. Johtajuus

Ylimmän johdon sitoutuminen tavoitteiden asettamiseen ja resurssien takaamiseen

### 7. Tukitoiminnot

Resurssien, osaamisen, tietoisuuden viestinnän ja dokumentoinnin varmistaminen

### 9. Suorituskyvyn arviointi

Oman toiminnan valvonta, mittaaminen, sisäinen auditointi ja johdon katselmukset

### 10. Parantaminen

Poikkeamien käsittely ja korjaaminen ja muu jatkuva parantaminen

# ISO27002:n osa-alueet (1/2)

**"Millaisilla hallintakeinoilla tietojen turvallisuutta konkreettisesti parannetaan?"**

### 5. Tietoturvapolitiikat

Kuinka tietoturvapolitiikat määritellään, hyväksytään, jalkautetaan


### 7. Henkilöstöturvallisuus

Rekrytointi, sopimukset, työsuhteen muutoshetket, koulutus, ohjeistus

### 9. Pääsynhallinta

Pääsyn rajaaminen ja käyttäjien hallittu tunnistaminen

### 11. Fyysinen turvallisuus

Estetään pääsy fyysisille alueille ja suojataan laitteistoa yms. haitalta

### 6. Tietoturvallisuuden organisointi

Roolien ja vastuiden määrittely ja organisationaaliset näkökulmat (projektinhallinta, etätyö)

### 8. Suojattavan omaisuuden hallinta

Tiedon, tietojärjestelmien, laitteiston, kumppanien, tunnistaminen, luokittelu ja vastuuttaminen

### 10. Salaus

Salauksen ja salausavainten oikeaoppinen käyttö tietojen suojaamiseen

### 12. Käyttöturvallisuus

Varmistetaan tietojärjestelmien turvallisuus monipuolisesti (ohjeet, varmuuskopiot, lokit, haavoittuvuudet…)

# ISO27002:n osa-alueet (2/2)

**“Millaisilla hallintakeinoilla tietojen turvallisuutta konkreettisesti parannetaan?”**

### 13. Viestintäturvallisuus

Suojataan verkkoa ja siellä liikkuvaa tietoa


### 15. Suhteet toimittajiin

Varmistetaan kumppanien riittävä tietoturvataso

### 17. Liiketoiminnan jatkuvuus

Varaudutaan ongelmiin järjestelmien ja tiedon saatavuudessa

### 14. Järjestelmien hankinta ja kehitys

Huomioidaan tietoturva uusia järjestelmiä hankittaessa ja ohjelmistokehityksessä

### 16. Tietoturvahäiriöiden hallinta

Asiallinen viestintä ja käsittely häiriöiden tapauksissa ja häiriöistä oppiminen

### 18. Vaatimustenmukaisuus

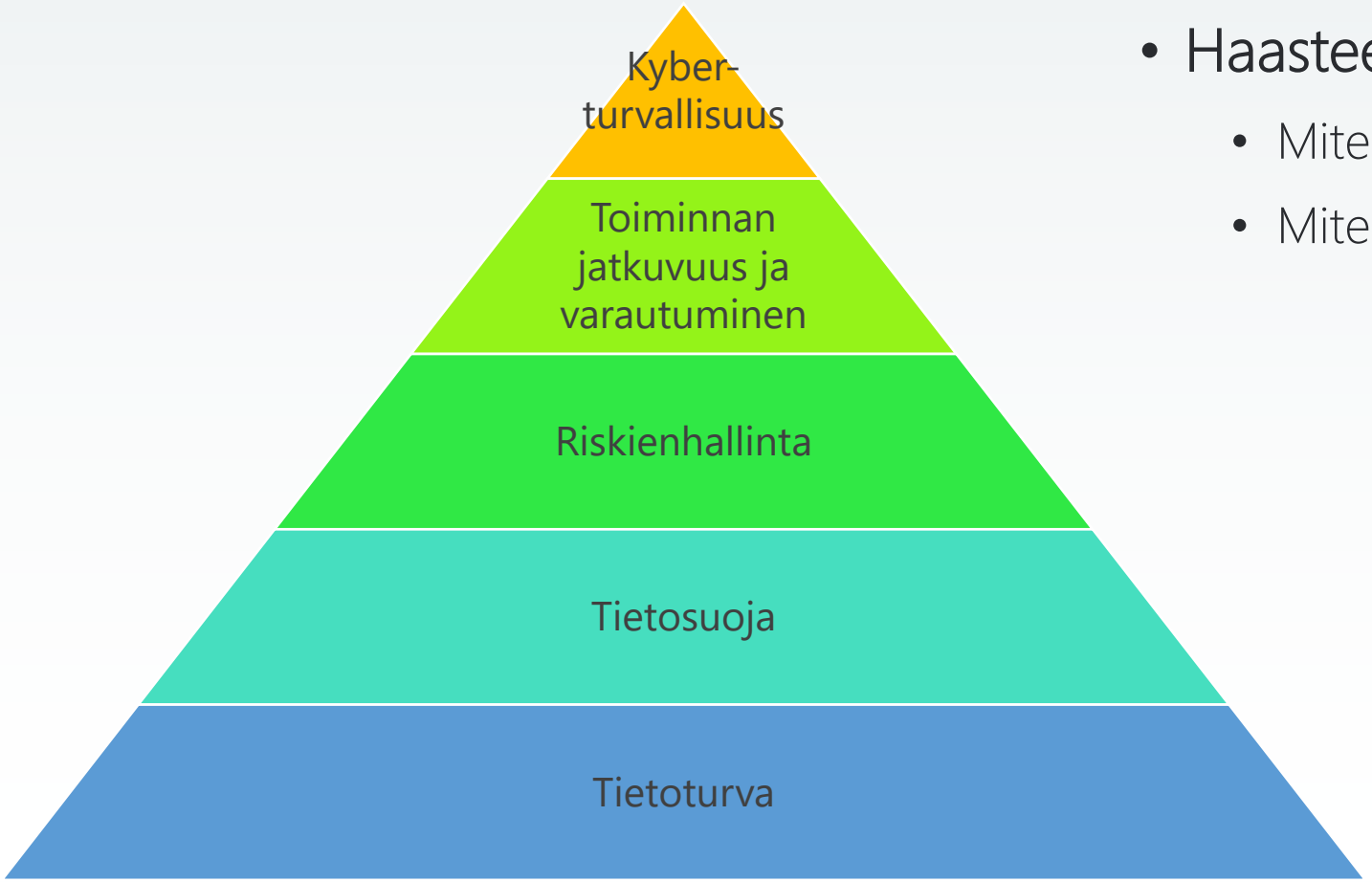
Huomioidaan muut lakien, sopimusten yms. vaatimukset ja auditoidaan omaa toimintaa

1. Ymmärrä uhkat | 2. Päätä tavoitteet | 3. Luo oma suunnitelma | 4. Varmista reagointi

# Nykytilan hahmottaminen ja tavoitetaso

Kuinka toimia digiturvan eteen?

# Digitaalinen turvallisuus

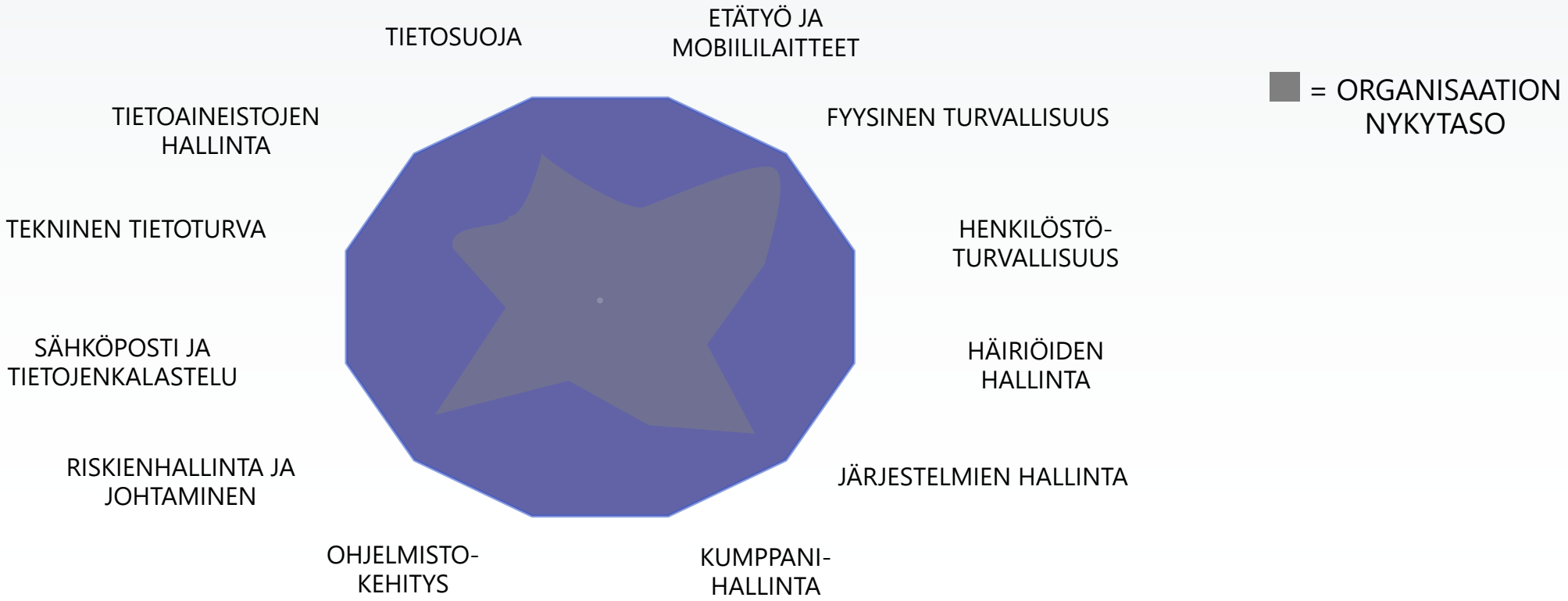



- Haasteena tämän vienti konkretiaan
  - Miten näkyy organisaation arjessa?
  - Miten **tietoturva** tässä ymmärretään?

Mukaillen Kimmo Rousku, Digi- ja väestövirasto

# Digiturvan 12 pääteemaa

- Digiturva on laaja, muttei loputon kokonaisuus
  - Työssä haasteena on osaoptimointi sekä vaihtoehtojen mereen hukkuminen



# Yhteenvetona

- Tietoturvassa kannattaa tukeutua yleisiin hyviin käytäntöihin
  - Näitä tarjoavat mm. ISO 27001
- Standardit sisältävät sekä perusasioita, että haastavampia kohtia
  - Helpoin aloittaa ”välttämättömistä ydinasioista”
  - Riskilähtöistä työskentelyä ja jatkuvaa kehittämistä voi parantaa myöhemmin
- Kun oma nykytaso ymmärretään ja tavoitetaso päätetään, työssä voidaan onnistua
  - Tarvittavien organisaation roolien sitoutuminen


# Oma digiturvasuunnitelma

Kuinka toimia digiturvan eteen?

# Mille tasolle pyritään?

## Ydin

Tietoturvan ydinasiat: toimintaympäristön kartoitus, tärkeimmät vastuut ja tekniset toimenpiteet, henkilöstön ohjeistamista

20 %

## Laajennettu

Laajennetut tehtävävastuut, teknisen suojauksen tehostaminen, kokonaisvaltaisempi suojaus esim. fyysisten tilojen suhteen

50 %

## Täysi

Sertifioinnin mahdollistava, uskottavasti johdettu ja valvottu hallintajärjestelmä

100 %

# Oma digiturvasuunnitelma

## Tietoturvatyön käynnistämisen askeleet

| Järjestäydy | Ydin | Laajennettu | Täysi |
|---|---|---|---|
| ✓ Tavoitetason asettaminen<br><br>Tarvittavan tiimin tunnistaminen<br><br>Työkalujen valinta | Oleellisin dokumentaatio<br>- järjestelmät<br>- kumppanit<br>- tieto ja tietovarannot<br><br>Oleellisimmat ohjeistukset<br>- tietojenkalastelu<br>- etätyö<br>- salasanat | Tietoturvan tärkeimpiä tehtäviä avainhenkilöille<br>- pääsynhallinta<br>- lokitukset<br>- sopimukset<br>- haittaohjelmat<br>- … | Riskilähtöinen työskentely<br><br>Oman tietoturvatason valvonta<br>- sisäiset auditoinnit<br>- katselmukset<br>- poikkeamat ja parannukset |

# Digiturvatyön pakolliset roolit

- Rajusti yksinkertaistaen…

## Johto

Organisaation ylin johto

Vastuina

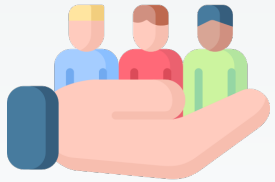
- Asettaa tavoitteet
- Resursoi
- Valvoo ja varmistaa tavoitteiden saavuttamisen

## Digiturvatiimi

Minimissään tietohallinto ja tietosuoja

Vastuina

- Toteuttavat työn vaatimia tehtäviä
- Laativat ohjeita
- Varmistavat vaatimusten täyttämisen



## Henkilöstö

Kaikki tietoa käsittelevät ihmiset

Vastuina

- Tuntevat omat ohjeet
- Noudattavat ohjeita
- Auttavat organisaatiota parantamaan

# 1. Tietojärjestelmien dokumentointi

*Organisaation on ylläpidettävä listaa käytetyistä tietojärjestelmistä sekä tietojärjestelmille nimetyistä omistajista. Omistaja vastaa järjestelmän tietojen täydentämisestä sekä mahdollisista muista tietoturvatoimenpiteistä, jotka liittyvät tiiviisti järjestelmään.*

- Järjestelmään liittyvät vastuut ja sen käyttötarkoitus
- Järjestelmän tietojen sijainti
- Kuvaus järjestelmän ylläpito- ja kehitysvastuista sekä tähän mahdollisesti liittyvät toimittajat
- Tarvittaessa tietojärjestelmän pääsyoikeusroolit ja tunnistautumistavat

# 2. Tietovarantojen dokumentointi

*Organisaation on ylläpidettävä listaa hallinnoimistaan tietovarannoista sekä nimetyistä omistajista. Omistaja vastaa varannon tietojen täydentämisestä sekä mahdollisista muista digiturvatoimenpiteistä, jotka liittyvät tiiviisti tietovarantoon.*

- Tietovarantoon liittyvät vastuut
- Tietojen käyttötarkoitukset
- Tietoaineistot, joista tietovaranto muodostuu
- Tietojen säännönmukaiset luovutukset
- Tarvittaessa tieto tietovarannon sidoksesta toimintaprosesseihin

# 3. Henkilöstön ohjeistaminen

- Etätyöhön liittyvät ohjeistukset henkilöstölle
  - *Etätyötä tekevälle henkilöstölle on luotu omat toimintaohjeet, joiden noudattamista seurataan. Lisäksi henkilöstölle järjestetään säännöllisesti koulutusta, jossa selvitetään mobiililaitteiden käytöstä ja etätyöstä aiheutuvia uhkia tietoturvallisuudelle ja kerrataan toimintaohjeita.*
- Ohjeistukset henkilöstölle tietojenkalasteluun liittyen
  - *Organisaatio on muodostanut henkilöstölle toimintaohjeet, joilla määritellään eri viestintäpalvelujen hyväksyttävä käyttö ja joiden avulla pyritään estämään luottamuksellisen tiedon paljastaminen esimerkiksi tietojenkalastelijalle tai muille ulkopuolisille.*
- Hyväksyttävän käytön ohjeet tärkeille tietojärjestelmille
  - *Tärkeäksi luokitellun tietojärjestelmän omistaja määrittelee, dokumentoi ja jalkauttaa hyväksyttävän käytön säännöt tietojärjestelmälle. Säännöt kuvaavat mm. tietoturvavaatimukset, jotka järjestelmän sisältävään tietoon liittyvät. Omistaja vastaa sääntöjen toimittamisesta käyttäjille. Käyttäjät ovat itse vastuussa omasta sekä heidän vastuullaan suoritetusta käytöstä.*
- Ohjeistukset henkilöstölle henkilötietojen käsittelyyn liittyen
  - *Tietosuojan vastuuhenkilö on muodostanut toimintaohjeet henkilötietoja käsittelevälle henkilöstölle. Lisäksi tietosuojan vastuuhenkilö on valmiina antamaan neuvoja rekisterinpitäjälle, henkilötietoja käsitteleville kumppaneille tai omalle henkilöstölle tietosuojaan liittyen tietosuoja-asetuksen tai muiden tietosuojavaatimusten noudattamiseen.*

# 4. Monivaiheinen tunnistautuminen

- Monivaiheisen tunnistautumisen käyttö tärkeiksi määriteltyihin järjestelmiin
  - Tärkeää tietoa sisältäviin järjestelmiin olisi kirjauduttava useita tunnistamiskeinoja käyttävällä kirjautumisella, jota kutsutaan englanniksi joko "two-factor", ”multi-factor” tai ”dual factor” tunnistautumiseksi.
  - Esimerkiksi kirjautuessaan ensin salasanalla, käyttäjälle voidaan lähettää lisäksi kertakäyttöinen tunnistautumiskoodi tekstiviestinä. Tällöin hänet on tunnistettu kahden tekijän avulla (salasanan tietäminen ja puhelimen omistajuus).
- Monivaiheisen tunnistautumisen käyttö pääkäyttäjille
  - Organisaation tärkeimmissä järjestelmissä pääkäyttäjinä toimivilta vaaditaan useita tunnistamiskeinoja käyttävää kirjautumista (engl. multi-factor authentication, MFA).

# 5. Käsittelyprosessien ymmärtäminen

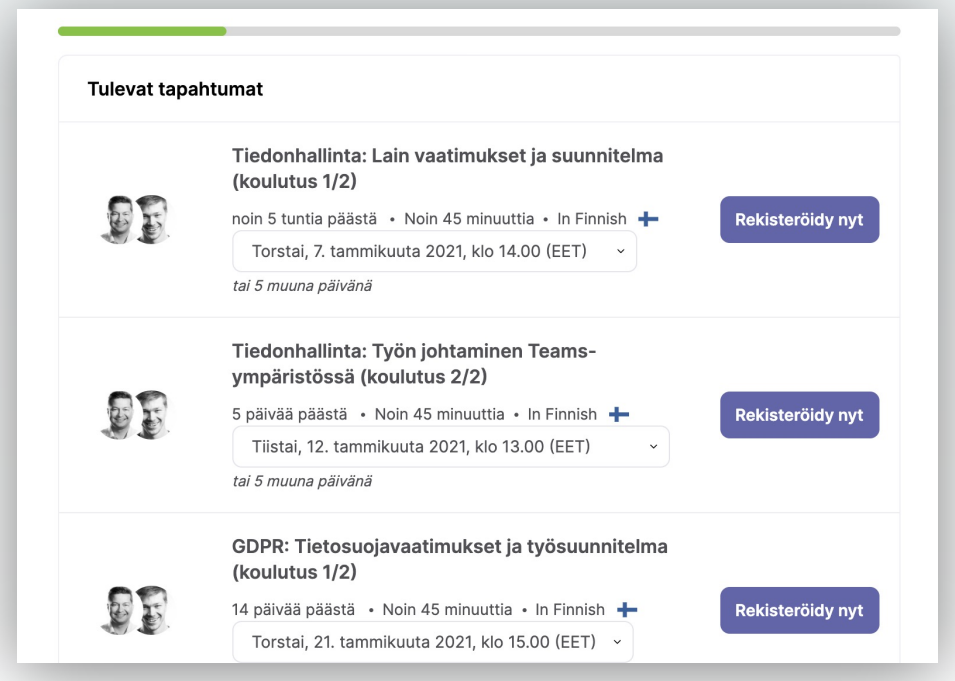
- Organisaatiomme ylläpitää listaa tietovarantoihin sisältyvistä tietoaineistoista. Listaus sisältää mm. seuraavat tiedot
  - Aineiston käsittelyyn käytetyt tietojärjestelmät ja muut keinot
  - Keskeiset tietoryhmät aineistossa (ja sisältääkö henkilötietoja)
  - Tietojen säilytysaika
  - Tarvittaessa tieto aineistojen arkistoinnista / hävittämisestä
- Henkilötietojen käsittelyperusteet on dokumentoitu. Dokumentaation on sisällettävä vähintään
  - käsittelyn oikeusperuste sekä tarvittavat lisätiedot
  - tahot, joille käsittelyä on ulkoistettu
  - liittyvät tietoaineistot

# Muita steppejä

- Suojaa sähköpostin ja mobiililaitteiden käyttöä
  - Mobiililaitteiden PIN-suojaus ja automaattinen lukitus
  - Prosessi mobiililaitteiden katoamisen tai varastamisen varalle
  - Mobiililaitteiden käyttöön liittyvä ohjeistus ja koulutus henkilöstölle
- Tarkenna toimintatavat ja työnjako teknisen suojauksen laajemmalle toteutukselle
  - Haittaohjelmasuojaus
  - Varmuuskopiointi ja sen varmentaminen
  - Laitteiden salaaminen ja sen hallinta
- Suunnittele häiriöiden hallinnan toimintatavat
  - Häiriöiden ilmoitusprosessi ja -ohjeet henkilöstölle
  - Tietoturvahäiriöiden käsittely ja dokumentointi

# Lisää digiturva-asiaa?

- Järjestämme webinaareja eri digiturvateemoista viikottain
  - Aikataulu ja ilmoittautuminen > https://digiturvamalli.fi/webinarit
- Webinaareja kannattaa jatkossakin hyödyntää
  - Uuden kehityksen ja tulkintojen seuraaminen
  - Uusien käyttäjien perehdytys työkalun pariin
  - Seuraavat vaatimuskehikot tai työn laajennus



Digiturvamalli

# ASKEL ASKELEELTA KOHTI PAREMPAA DIGITURVAA

**Ismo Paananen**

CEO, Agendium Oy, CIPT

+358 40 7288 299

ismo.paananen@agendium.com

**Aleksi Pulkkanen**

COO, Agendium Oy, CIPP/E

+358 44 3581 817

aleksi.pulkkanen@agendium.com