# TIETOTURVA-KONSULTOINNIN OSTAJAN OPAS

# LAINSÄÄDÄNTÖ LUO RAAMIT TIETOTURVAN KEHITTÄMISELLE

Lisääntyvät tietoturvauhat ja lainsäädäntöön liittyvät vaatimukset lisäävät yritysten tarvetta tietoturvan arviointiin ja kehittämiseen. Tietoturvan nähdään usein perustuvan kahteen asiaan: virustorjuntasovellusten asentamiseen ja palomuurin konfigurointiin. Tosiasiassa tietoturvariskien hallinta on laajempi prosessi, jossa tärkeintä on ymmärtää kokonaistilanne ja johtaa tietoturvaa tietyn prosessoidun toimintamallin mukaisesti.

# VALMISTAUDU PITKÄJÄNTEISEEN PROSESSIIN

Tehdäkseen tietoturvansa hallinnoinnista mahdollisimman kevyttä, yritykset havittelevat usein valmiiksi paketoitua tietoturvaratkaisua, jossa dokumentit saadaan valmiina nippuna. Periaatteessa dokumentit voitaisiinkin generoida valmiina pakettina ja myydä sellaisenaan. Haasteena tässä on kuitenkin toiminnan lyhytnäköisyys, joka laskee ratkaisun kannattavuutta. Yritys toki saisi kaiken vaadittavan dokumentaation, mutta todellisuudessa mikään ei muuttuisi.

Tietoturva ei ole tuote. Se on prosessi. Prosessi ei lopu missään vaiheessa, vaan vaatii jatkuvaa ylläpitoa. Se on implementoitava pysyväksi osaksi yrityksen toimintatapoja. Parhaimmallaan koko tietoturva muuttuu täysin läpinäkyväksi, jolloin sitä ei edes huomaa yrityksen normaalien toimien ohella.

Tietoturvaa tai tietosuojaa ei voi ostaa vilkkuvilla valoilla ja hienoilla kuorilla. Molemmat perustuvat ymmärrykseen siitä, mitä yrityksen tulee olla ja mitä tavoitteiden saavuttaminen vaatii.

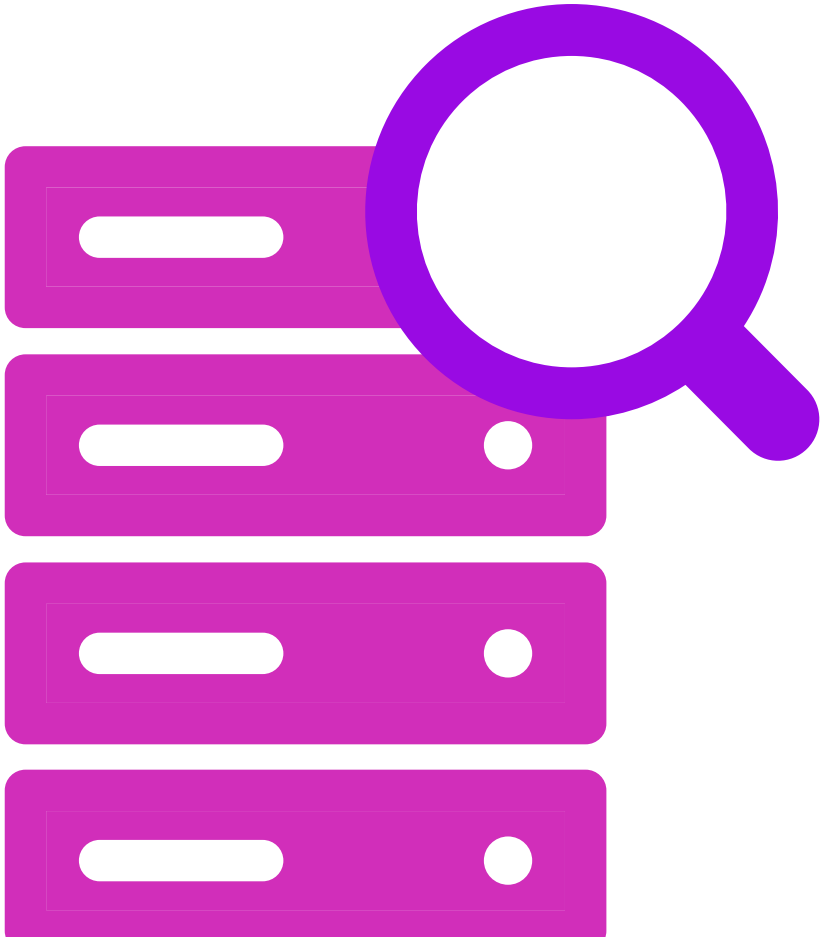
# ENNEN TOIMENPITEITÄ TOTEUTETAAN ALKUKARTOITUS

Prosessi vaatii aina ymmärrystä vallitsevasta tilanteesta. Tähän selkeä toimintamalli on ennen käyttöönottoa läpikäytävä alkukartoitus. Tyypillisesti alkuvaiheessa yrityksen tietoturvallisuuden tila arvioidaan ISO 27001 ja CIS -kriittisiin kontrolleihin sekä EU:n tietoturvasuoja-asetukseen pohjautuvalla tietoturva-arvioinnillamme.

Ensimmäisessä vaiheessa kartoitetaan, mitä tietoa yrityksellä on suojattavana. Yleensä suojattava tieto on asiakasrekistereitä, tuotekehitystietoa, sisäisiä hinnastoja ja sopimuksia sekä tietoa, jota yritys käyttää liiketoimintansa pyörittämiseen.

Seuraavaksi pitäisi ymmärtää miksi jotain suojataan. Yritystiedon suojaamista ohjaa riskiajattelu. Mikäli tieto menetetään, siitä seuraa taloudellisia seuraamuksia. Myös erilaiset lait ja asetukset putoavat miksi-kysymyksen alle.

Alkukartoituksen jälkeen voidaan siirtyä toimenpiteiden suunnitteluun ja käyttöönottoon, jotka esitellään oppaan seuraavassa osiossa.



# TIETOTURVAKONSULTOINNIN KÄYTTÖÖNOTTAMISEN OSA-ALUEET

## JOHTAMISMALLIN RAKENTAMINEN

Tietoturvan monikerroksisen, sipulimaisen toimintamallin rakentaminen alkaa johtamismallin rakentamisesta. Tämän yhteydessä tietoturvariskejä arvioidaan tietoturvallisuuden riskienhallinnan viitekehyksellä.

## KÄYTTÄJIEN KOULUTTAMINEN

Kun johtaminen on kunnossa, keskitytään käyttäjien kouluttamiseen laatimalla ja jalkauttamalla ohjeistuksia. Tähän osioon kannattaa panostaa, koska yrityksesi työntekijät toimivat tärkeimpänä porttina tietoturvasi varmistamisessa.

## TEKNISET KONTROLLIT

Johtamismallin rakentamisen ja käyttäjien kouluttamisen jälkeen rakennetaan yrityksesi tarpeisiin soveltuvat tekniset kontrollit, kuten palomuurit ja kovennuskäytännöt.

# JOHTAMISMALLIN RAKENTAMINEN

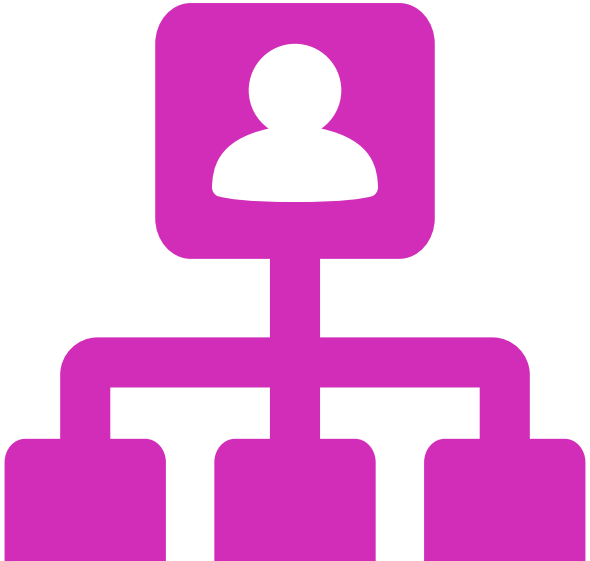
# JOHTAMISMALLIN RAKENTAMINEN

Johdon tuki mahdollistaa käytännössä koko tietoturvaprosessin. Mikäli tukea ei ole, myöskään resursseja ei ole. Ilman resursseja prosessit eivät toteudu.

**Olemme on rakentanut erityisesti pk-yrityksille sopivan tietoturvan arviointi- ja johtamismallin, ja koska kaikkien yritysten suojaustarpeet ovat erilaisia, mallit räätälöidään aina yrityksesi tarpeiden mukaisesti. Asiakas saa projektin jälkeen tietoturvan tilannekartan, tarkemmat arviot eri tietoturvallisuuden osa-alueista ja kehityssuunnitelman jatkoa varten. Tämän jälkeen yritykselle rakennetaan räätälöity tietoturvallisuuden johtamisen viitekehys, sisältäen esimerkiksi riskienhallinnan periaatteet sekä tietoturvapolitiikan, -periaatteet ja -ohjeistukset.**

Jatkossa yritykselle voidaan rakentaa tietoturvatietoisuuden ohjelma henkilöstön osaamisen ylläpitämiseksi ja luoda teknisempiä, esimerkiksi haavoittuvuuksienhallinnan tai lokienhallinnan prosesseja teknisen tietoturvan tehostamiseksi. Kaikki edellä mainitut muodostavat yhdessä yrityksen tietoturvallisuuden viitekehyksen, jota yrityksen tietoturvasta vastaava henkilö johtaa. Jos yrityksellä ei ole halua tai resursseja johtaa tietoturvaansa itse, voimme myös osallistua säännölliseen, vuosikellon mukaiseen tietoturvatyöhön.

Jotta prosessi tietoturvan rakentamiseksi pysyisi kasassa, toimia on suoritettava siis kaikilla osa-alueilla. Johtaminen pitää kasassa prosessin muita osa-alueita. Tästä johtuen tietoturvaprosessi aloitetaan johtamismallin rakentamisesta.



# KÄYTTÄJIEN KOULUTTAMINEN JA SITOUTTAMINEN

# KÄYTTÄJIEN KOULUTTAMINEN JA SITOUTTAMINEN

Tietoturvan heikoin lenkki on usein yrityksen oma henkilöstö. Teknologialla voidaan tukea ihmisten toimintaa, mutta pelkällä teknisellä suojauksella ei voida rakentaa toimivaa ympäristöä. Vaikka periaatteessa teknologialla voidaan luoda tietoturvaa tukeva ympäristö kokonaisuudessaan, ympäristöllä on aina käyttäjä. Tietoturvaan muodostuvat aukot riippuvat sen käyttäjien toiminnasta ja tavoista hyödyntää teknisiä työkaluja. Tästä johtuen tietoturvaprosessissa keskitytään johtamismallin rakentamisen jälkeen käyttäjien kouluttamiseen.

Useimmiten henkilöstö jää teknologiahuuman pyörteissä huomiotta – kohtalokkain seurauksin. Koulutuksen kautta henkilöstölle voidaan muun muassa avata, minkälaisia liitetiedostoja voi avata, voiko kadulta löydettyä USB-muistitikkua liittää yrityksen koneeseen ja minkälaisilla sivustoilla voi surffata turvallisesti.

Hyvässä tietoturvapolitiikassa henkilöstön tietoisuuden lisääminen on huomioitu, mutta paremmassa politiikassa toiminta on myös jalkautettu ja otettu käyttöön. Valveutunut henkilöstö havainnoi esimerkiksi jatkuvasti yrityksen tiloissa liikkuvia henkilöitä. Tietoisuuden lisääminen vaatii aikaa sekä johdonmukaista toimintaa ja johtamista. Kaiken pohjalla on sovitut käytännöt ja tietoturvapolitiikka, mieluiten kirjallisena ja yrityksen johdon hyväksymänä.

# TEKNISET KONTROLLIT

# TEKNISET KONTROLLIT

Nykytila-arvion, johtamismallin rakentamisen ja käyttäjien kouluttamisen jälkeen voidaan luoda teknisempiä, esimerkiksi haavoittuvuuksienhallinnan tai lokienhallinnan prosesseja tietoturvan tehostamiseksi. Tämä on tietoturvan ja -suojan tekninen osio. Mitä paremmin alkukartoitus on toteutettu eli ymmärretään, mitä yrityksessä suojataan ja miksi valittuja osa-alueita on suojattava, sitä tarkemmin voidaan investoida teknologiaan ja sijoittaa tekniset ratkaisut oikeisiin kohtiin, jolloin ne tukevat toimintaa mahdollisimman tehokkaasti.

Seuraavalla sivulla oleva kuvio havainnollistaa tietoturvan ja -suojan neljää peruspilaria, joiden varaan tietoturvan malli rakennetaan. Alkukartoituksen yhteydessä määritellään mitä ja miksi yrityksessä tulee suojata. Tämän jälkeen rakennetaan johtamismalli, joka pitää kasassa tietoturvan muita osa-alueita. Lopuksi suunnitellaan käytännön ratkaisut, joihin lukeutuu tekniset kontrollit ja käyttäjien eli henkilöstön koulutus.


MITÄ?
MIKSI?
JOHTAMINEN
MITEN?

# MUISTA VARAUTUA MYÖS PERINTEISIN KEINOIN

Yritysten huomion kiinnittyessä pitkälti verkkosivujen hakkerointiin, perinteisten keinojen estäminen saattaa unohtua. Perinteisistä keinoista esimerkkinä toimii yritysvakoilu, joka viittaa tilanteeseen, jossa ulkopuolinen henkilö tunkeutuu yrityksen tiloihin ja urkkii tietoa. Yritysvakoilu ei ole myytti, vaan yleisesti käytetty menetelmä.

Yritysvakoilun kautta tunkeutujat voivat päästä tiloihin, joissa käsitellään luottamuksellisia asioita. Mikäli niin sanottu puhtaan pöydän politiikka ei ole yrityksessä käytössä, vakoilurikolliset pääsevät todennäköisesti käsiksi luottamuksellisiin dokumentteihin. Puhtaan pöydän politiikka tarkoittaa periaatetta, jossa kaikki materiaali pidetään visusti kaapissa piilossa. Lukitsemattomien ovien lisäksi lukitsemattomat tietokoneet voivat olla uhka, sillä niille voidaan varsin huomaamattomasti ja nopeasti asentaa erilaisia seurantasovelluksia.

Laitteiden pienentyessä ja hintojen laskiessa teknologian kehitys virtaviivaistaa rikollista vakoilutoimintaa tuomalla kuuntelu- ja tallennuslaitteet kaikkien ulottuville. Laitteet ovat nykyisin erittäin kehittyneitä ja hyvin suunniteltuja, jolloin niitä on helppo jättää myös hyvinkin näkyville paikoille, kuten esimerkiksi neuvotteluhuoneeseen tai jopa toimitusjohtajan pöydälle.

Nebulan toimintamallissa otetaan huomioon myös perinteiset tietoturvauhat. Näin tietoturva jalkautetaan kokonaisvaltaisesti yritykseen.

# TIETOTURVAN LOPUTTOMALTA TUNTUVAA KÄSITESUMAA PELÄTÄÄN TURHAAN

Viime vuosina tietoturvan saralla on ollut lukuisia erilaisia hype-sanoja. Tämän hetken hype-sana on ehdottomasti GDPR (General Data Protection Regulation) eli EU:n uusi tietosuoja-asetus. Johtuen alkuvuoden laajoista hyökkäyksistä, hyväksi kakkoseksi sijoittuu RansomWare. Muutama vuosi sitten hypetyksen kohteena oli Kyber. Näiden termien yhteydessä puhutaan usein myös digitalisaatiosta ja IoT:sta (Internet of Things).

**Loppujen lopuksi GDPR:n ja kyberin takana on aivan perus tietoturva, tietoturvapolitiikat ja käytänteet.** Tietoturvapolitiikka luo rungon, jonka pohjalta rakennetaan myös tietosuojapolitiikka. Tietoturvapolitiikka taas käsittelee koko yrityksen tapaa ja asennetta luottamuksellisen tiedon käsittelyssä.

IT-maailma on pullollaan erilaisia lyhenteitä, ja jokaisella osa-alueella on oma lyhenneavaruutensa. Tietoturva taiteilee hallinnollisen ja teknologisen maailman välimaastossa, pitäen sisällään myös liiketoiminallisia käsitteitä. Toisin sanottuna yllä olevaa sanalistaa voisi jatkaa vielä ties kuinka pitkälle.

Lyhenteiden ja termien määrä voi olla yksi tekijä, joka aiheuttaa epävarmuutta tietoturvan suhteen. On ymmärrettävää, että termien vierauden johdosta voi olla vaikeaa hahmottaa, mistä tietoturvaprosessi kannattaa aloittaa. Loppukädessä kaiken taustalla vaikuttavat kuitenkin samat tietoturvakäytännöt, jotka on liitettävä kokonaisvaltaisesti osaksi yrityksen toimintaa.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ISMS | Compliance | IAM | PIA | Secret | Data Breach | C-level Fraud | Access Control | IPS |
| GDPR | ISO 27000 | HASH | DRP | ST III | DDoS | Malware | Token | BCM |
| CERT | VAHTI | PKI | CIA | VPN | X.509 | RansomWare | RSA | Classification |
| NSA | KATAKRI | Palomuuri | NIST | CISSP | Phishing | Key logger | PGP | Cyber |
| CISM | Ciso | AV | HSM | NDA | White Hat | BotNet | IDS | BYOD |
| Sertifikaatti | AES-256 | DLP | Confidential | ATP | Sniffing | Trojan | SIEM | |

# PARHAIMMILLAAN TIETOTURVA ON YRITYKSEN KILPAILUVALTTI

Oikotietä onneen ei ole olemassa. Tavoitteita ei saavuteta, mikäli tietoturva nähdään vanhan tavan mukaan ainoastaan IT-osaston asiana. Tietoturvan tulisi olla luonnollinen osa koko normaalia toimintaa, ei päälleliimattua toimintaa.

Parhaimmillaan tietoturva ja tietosuoja ovat yrityksen kilpailuvaltteja. Hyvästä tietoturvasta kannattaa kertoa ulos, ja vaikka yrityksellä ei olisikaan sertifikaattia tietoturvan osoittamiseksi, oman toiminnan avaamisella voidaan luoda luottamusta. Ylipäätään tietoturva on yrityksen prosessi, ei nippu paperia ja dokumentteja. Toimiva kokonaisuus heijastuu myös yrityksen ulkoisille sidosryhmille, kuten yhteistyökumppaneille ja asiakkaille, luoden yrityksestä kuvaa luotettavana palveluiden ja tuotteiden tarjoajana.

# TIETOTURVAKONSULTOINNIN MARSSIASKELEET TIIVISTETTYNÄ

## ALKUKARTOITUS JA NYKYTILA-ANALYYSI

Yrityksen nykytila arvioidaan ISO 27001 ja CIS -kriittisiin kontrolleihin sekä EU:n tietoturvasuoja-asetukseen pohjautuvalla tietoturva-arvioinnillamme. Tarkoituksena on selvittää, mitä yrityksessä suojataan ja miksi. Tässä yhteydessä laaditaan myös kehityskartta, jota yritys voi käyttää toimenpiteiden suorittamiseen itse tai vaihtoehtoisesti ostaa ne kolmannelta osapuolelta.

## JOHTAMISMALLIN RAKENTAMINEN

Tietoturvan käytännön toteutus aloitetaan johtamismallin rakentamisesta. Tähän sisältyy myös vastuualueiden määrittely. Johtaminen luo pohjan tietoturvan muille osa-alueille ja mahdollistaa prosessin onnistumisen.

## HENKILÖSTÖN KOULUTTAMINEN JA SITOUTTAMINEN

Henkilöstö on oleellisessa osassa tietoturvan rakentamista. Näin ollen henkilöstön kouluttaminen ja sitouttaminen on ratkaisevassa asemassa tietoturvaprosessin onnistumiselle.

## TEKNISET KONTROLLIT

Tekniset kontrollit rakennetaan vasta viimeisessä vaiheessa. Prosessin aiemmat vaiheet tukevat teknisten ratkaisujen sijoittamista oikeisiin kohtiin. Teknisten kontrollien lisäksi on huomioitava myös perinteiset keinot suojautua tietomurroilta.

**TELIA INMICS-NEBULA**

myynti@inmicsnebula.fi
www.inmicsnebula.fi