Moduuli 1: Tietoturva ja johdon vastuut

talous hallinto liitto

Huoltovarmuuskeskus

M1V1: Taloushallintoalan organisaatioon vaikuttava tietosuoja- ja tietoturvalainsäädäntö

Taloushallintoalan johdon tietoturva

Moduuli 1: Tietoturva ja johdon vastuut

2024

Tietosuoja- ja tietoturvalainsäädäntö

- Tietosuoja- ja tietoturvalainsäädäntö vaikuttaa organisaatioihin, jotka käsittelevät henkilötietoja ja digitaalisia tietoja. Nämä lait ja asetukset määrittelevät, miten tietoja tulee suojata ja käsitellä, jotta ne pysyvät turvassa ja yksityisyyden suoja säilyy. Kaikkia organisaatioita koskevien lakien lisäksi on olemassa alakohtaista sääntelyä, erityisesti yhteiskunnalle kriittisille toimijoille.
- Tietosuoja- ja tietoturvalainsäädäntöjen tarkoituksena on varmistaa, että tietoja käsitellään turvallisesti ja vastuullisesti ja että järjestelmät toimivat, jotta yhteiskuntamme pysyy toiminnassa.
- Tietoturva- ja tietosuojalainsäädäntö on kehittynyt viime vuosina heijastamaan digitalisaation mukanaan tuomaa muutosta yhteiskunnan toimintaan.

Tietosuoja ja tietoturva tänään

- Tietoturva- ja tietosuojatoimenpiteet ovat välttämättömiä, sillä niihin liittyvät uhkat koskettavat niin
  - yksittäisiä henkilöitä henkilökohtaisten tietojen menettämisen kautta
  - organisaatioita liiketoimintaan kohdistuvien mahdollisten ongelmien kautta ja
  - koko yhteiskuntaa, sillä olemme täysin riippuvaisia kriittisistä digitaalista palveluistamme.

Tästä syystä eri tahot, esimerkiksi Euroopan Unioni, pyrkivät kehittämään tietoturvaan liittyviä vaatimuksia ja sitä kautta organisaatioiden tietoturvan kypsyystasoa. Tietoturvaan liittyvät tilastotiedot tukevat näkemystä siitä, että tietoturvaan liittyvät haasteet ja ongelmat ovat valitettavan yleisiä:

- Suomessa tietosuojavaltuutetun toimistossa tuli vireille liki 7 000 tietoturvaloukkausilmoitusta vuonna 2023.
- Kyberturvallisuuskeskus käsitteli yli 200 ilmoitusta palvelunestohyökkäyksistä vuonna 2023.
- Suomessa on KTK:n mukaan yli miljoona huijausyritystä kuukausittain (2024)
- Suomalaisilta huijattu pankkien tietojen mukaan 44 miljoonaa euroa (2023)

Tietosuoja ja tietoturva tänään

- Tilastot ovat silti vain jäävuoren huippu, sillä iso osa tietoturvaan liittyvistä ongelmatilanteista ei tule raportoiduksi.
- Paras tapa ehkäistä tietosuojaan ja tietoturvaan liittyviä ongelmia, on johtaa näihin aihepiireihin liittyviä asioita hyvin ja toteuttaa ne huolella.
- Aloitetaan tämä johdon kurssi käymällä läpi aiheeseen liittyvät lainsäädännölliset vaatimukset, eli Suomessa voimassa olevat tietoturva- ja tietosuojalait.

Taloushallintoalan tietoturvan sääntely

Taloushallintoalan sääntely on rajoitettua erityisesti tietoturvan ja jatkuvuudenhallinnan osalta. Vaikka alaa ohjaavat tietyt lait, ne eivät suoraan ota kantaa tietoturvaan tai varautumiseen häiriötilanteissa. Sääntelyn vähäisyyden vuoksi taloushallintoalan yritysten omat toimenpiteet tietoturvan ja jatkuvuuden varmistamiseksi ovat keskeisessä roolissa.

- **Kirjanpitolaki** säätelee kirjanpidon toteutusta ja aineiston säilyttämistä, mutta se ei aseta vaatimuksia tietoturvamenetelmistä tai tietojärjestelmien suojaamisesta. Tämä tarkoittaa, että yritysten on itse huolehdittava siitä, että niiden tietoturvaprosessit suojaavat kirjanpitotiedot asianmukaisesti.
- **Palkkahallintoa** säätelevät Työsopimuslaki ja Työaikalaki, mutta nämä lait käsittelevät ensisijaisesti palkanmaksun ehtoja. Yritysten on siis itse varmistettava, että palkkahallinnon tietojärjestelmät ja prosessit ovat suojattuja.
- Vuonna 2024 voimaan astuva **NIS2-direktiivi** asettaa uusia tietoturvavelvoitteita suurille taloushallintoalan yrityksille. Vaikka direktiivi ei koske pienempiä toimijoita, se tuo esiin tarpeen kehittää vapaaehtoisia tietoturvastandardeja, jotka voisivat parantaa alan kyberturvaa laajemminkin.

Tietosuojalainsäädäntö

- Tietosuojalainsäädäntö määrittelee, miten henkilötietoja tulee kerätä, tallentaa ja käyttää. Se varmistaa, että henkilötiedot käsitellään vain ennalta määriteltyihin tarkoituksiin ja että tietojen käyttö on läpinäkyvää rekisteröidyille. Alueen keskeinen sääntely tulee **EU:n yleisestä tietosuoja-asetuksesta GDPR:sta** sekä **kansallisesta tietosuojalaista**. Lisäksi **laki työelämän yksityisyyden suojasta** asettaa velvoitteita kaikille työnantajille koskien työntekijöiden tietojen suojaamista.
- Tilitoimistot käsittelevät henkilötietoja asiakkaan puolesta, sillä tyypillisesti tilitoimisto hoitaa palkanlaskentaa. Heidän hallinnassaan ovat siis esimerkiksi työntekijöiden osoitteet, henkilöturvatunnukset, ja sairauspoissaoloja koskevat tiedot. Sääntely edellyttää näiden tietojen käsittelyn suojaamista, sillä tietojen päätyminen vääriin käsiin voisi johtaa esimerkiksi identiteettivarkauteen tai muihin riskeihin näille henkilöille.
- Jokaisen yrityksen tulee tuntea henkilötietojen käsittelyn oikeusperusteet. Yleisimmin taloushallintoalan yrityksessä peruste on joko
  - rekisterinpitäjän lakisääteinen velvoite (esimerkiksi työsuhteeseen liittyvä käsittely),
  - sopimus (asiakassuhteeseen liittyvä käsittely), tai
  - rekisteröidyn suostumus (esimerkiksi palveluiden kilpailutukseen liittyvä vapaaehtoinen yhteydenotto).

Yritysten tietosuojavelvoitteet

Yrityksen rooli henkilötietojen käsittelyssä vaikuttaa siihen, mitä vastuita ja velvollisuuksia yrityksellä on.

Rekisterinpitäjän vastuut

Rekisterinpitäjä määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjänä taloushallintoalan yrityksellä on keskeisiä velvollisuuksia:

- Yrityksen on varmistettava, että **henkilötietoja käsitellään oikeusperusteisesti**, kuten suostumuksen perusteella tai lakisääteisten velvoitteiden täyttämiseksi. Henkilötietojen käsittelyssä on noudatettava avoimuutta, ja **rekisteröidyille on annettava selkeää tietoa** siitä, miten heidän tietojaan käytetään.
- Yrityksen vastuulla on varmistaa, että asianmukaiset tekniset ja organisatoriset toimenpiteet ovat käytössä henkilötietojen **suojaamiseksi luvattomalta pääsyltä, tietojen häviämiseltä tai väärinkäytöksiltä**. Tämä koskee myös alihankkijoita ja palveluntarjoajia.
- Yrityksen on varmistettava, että **rekisteröidyt voivat käyttää heille myönnettyjä oikeuksiaan**, kuten oikeutta saada pääsy omiin tietoihinsa. Tällöin heille täytyy toimittaa kopio tai antaa pääsy järjestelmään, josta tiedot on tarkistettavissa. Henkilöillä on myös mm. oikeus oikaista virheellisiä tietoja.
- Yrityksen on pystyttävä osoittamaan, että se noudattaa tietosuoja-asetuksen velvoitteita.

Yritysten tietosuojavelvoitteet

Henkilötietojen käsittelijän vastuut

Taloushallintoalan yritykset toimivat henkilötietojen käsittelijöinä, kun ne käsittelevät henkilötietoja rekisterinpitäjänä toimivan asiakkaan lukuun, esimerkiksi ulkoistetuissa kirjanpito- tai palkkahallintopalveluissa. Henkilötietojen käsittelijällä on seuraavat vastuut:

- Henkilötietojen käsittelijä voi käsitellä tietoja vain **rekisterinpitäjän antamien ohjeiden ja solmitun sopimuksen mukaisesti**. Tämä sopimus, eli tietojenkäsittelysopimus (DPA), määrittelee tarkasti käsittelijän roolin ja vastuut.
- Henkilötietojen käsittelijän on huolehdittava siitä, että käsittelyn yhteydessä henkilötiedot ovat suojattuja. Tämä edellyttää riittäviä teknisiä ja organisatorisia tietoturvatoimia tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi.
- Henkilötietojen käsittelijän on avustettava rekisterinpitäjää velvoitteiden täyttämisessä, kuten **tietoturvaloukkauksien ilmoittamisessa** ja **rekisteröityjen oikeuksien toteuttamisessa**.
- Henkilötietojen käsittelijän on pystyttävä osoittamaan, että se noudattaa tietosuoja-asetuksen vaatimuksia.

11

Tietosuojavaltuutetun rooli

Tietosuojavaltuutettu valvoo tietosuojasääntelyn toteutumista. Yrityksen on hyvä huomioida seuraavat:

- Jos yrityksessä tapahtuu tietoturvaloukkaus (esimerkiksi tietomurto, jossa henkilötietoja vuotaa tai niitä tuhotaan vahingossa), yrityksellä on velvollisuus ilmoittaa asiasta tietosuojavaltuutetulle 72 tunnin kuluessa siitä, kun loukkaus on havaittu.
- Yrityksillä on velvollisuus tehdä yhteistyötä tietosuojavaltuutetun kanssa tämän suorittaessa tehtäviään. Tämä tarkoittaa, että yrityksen on annettava viranomaiselle pyydetyt tiedot henkilötietojen käsittelystä, kuten käsittelytoimien rekisterit, tietosuojan arvioinnit ja muut asiaan liittyvät asiakirjat.
- Tietosuojavaltuutetulla on oikeus tehdä tarkastuksia ja tutkimuksia varmistaakseen, että yritykset noudattavat tietosuojasääntöjä. Mikäli rikkomuksia havaitaan, tietosuojavaltuutettu voi antaa varoituksia, määräyksiä korjata tietosuojaongelmia ja tarvittaessa määrätä hallinnollisia sakkoja, jotka voivat olla merkittäviä. Vuonna 2023 korkein yksittäiselle organisaatiolle määrätty seuraamusmaksu oli yli 400 000 euroa.
- Rekisteröidyt voivat tehdä valituksen tietosuojavaltuutetulle, jos he katsovat, että heidän tietojaan on käsitelty lainvastaisesti. Yritysten on oltava valmiita vastaamaan tällaisiin tutkimuksiin ja osoittamaan, että tietosuojakäytännöt ovat lainmukaisia.

12

Mahdolliset seuraamukset

Puutteet henkilötietojen käsittelyssä vähentävät asiakkaiden ja kuluttajien luottamusta yritykseen. Vahingonkorvausvelvoitteita voi toteutua asiakassopimusten ehtojen rikkomisesta johtuen sekä tietosuojavaltuutetun määräämien huomautusten ja sakkojen muodossa. Esimerkkejä:

- Brittiläinen tilitoimistokonserni Optionis Group joutui haittaohjelmahyökkäyksen kohteeksi vuonna 2022. Hyökkäyksen seurauksena yrityksen hallussa olleita asiakirjoja ja henkilötietoja vuodettiin internetiin. Tapauksessa Ison-Britannian tietosuojavaltuutettu totesi, ettei yrityksessä oltu toteutettu riittäviä tietoturvatoimia kuten monivaiheista tunnistautumista. Lisäksi henkilötietojen elinkaaren hallinnassa ja tietoturvaloukkauksen ilmoitusprosessissa oli puutteita. Yritys sai vakavat moitteet puutteista johtuen, mutta välttyi sakoilta.
- Suomessa 11 yritystä on saanut vähintään 50 tuhannen euron sakon tietosuojaa koskevista puutteista. Pääosin tapauksissa on kyse tietosuojan järjestelyiden sääntelynmukaisuudesta, eikä toteutuneista tietovuodoista.

Tietoturvalainsäädäntö

- Erityinen tietoturvalainsäädäntö kohdistuu erityisesti yhteiskunnan kannalta kriittisiin toimijoihin.
- EU:n tasolta tietoturvalainsäädäntö on viime vuosina kehittynyt:
  - DORA-asetus sääntelee **finanssialan** toimijoiden digitaalista häiriönsietokykyä. Sääntely ei ole kohdennettu esimerkiksi tilitoimistoille. Silti jos tilitoimiston asiakkaana on finanssialan yhtiö, saattavat tämän yhtiön DORA-asetuksesta aiheutuvia vaatimuksia tulla toimittajavaatimuksena myös tilitoimistolle. Vastuu näiden toimitusketjujen tunnistamisesta ja vaatimusten asettamisesta on sääntelyn kohteena olevilla finanssialan toimijoilla.
  - NIS 2-direktiivi ylläpitää **yhteiskunnan kriittisten** toimijoiden toimintavarmuutta. Tilitoimisto voi kuulua direktiivin soveltamisen piiriin, jos se tarjoaa kriittisiä palveluita kuten taloushallinnon palvelut organisaatiolle jotka toimivat rahoitussektorilla tai terveydenhuollossa TAI jos se toimii digitaalisten palveluiden tarjoajana, jotka ovat olennaisia yhteiskunnan kriittisille toimijoille.
- Esimerkiksi tilitoimistoa nämä regulaatiot eivät normaalisti koske suoraan. Silti jos EU-tasoinen lainsäädäntö vaikuttaa myös meillä Suomessa. Sääntelyn tiukentuminen kriittisillä aloilla tuo kehityspaineita myös muiden toimijoiden tietoturvaan, sillä sekä DORA-asetuksessa että NIS2-direktiivissä keskeistä on, että myös niiden piiriin kuuluvien toimijoiden **palveluntoimittajien** tulee hoitaa tietoturva-asiat hyvin.

talous hallinto liitto

Huoltovarmuuskeskus

M1V2: Tietoturvavastuut organisaatiossa

Taloushallintoalan johdon tietoturva

Moduuli 1: Tietoturva ja johdon vastuut

2024

Johdanto: Tietoturvaan liittyvien vastuiden määrittely

talous hallinto liitto

- Tietoturva on tärkeää jokaisessa yrityksessä, sen koosta riippumatta. Jokaisessa yrityksessä käsitellään tietoja, joten tietoturva-asioista huolehtiminen on oleellista jokaisessa organisaatiossa, sen koosta riippumatta.
- Tietoturva voi vaikuttaa laajalta ja vaikeasti lähestyttävältä kokonaisuudelta. Lähestytään asiaa siis käytännöllisestä näkökulmasta:
  - Ensin on tärkeää miettiä, mitä tietoja yrityksemme käsittelee.
  - Sitten millaisia riskejä näiden tietojen väärinkäytöksiin tai menettämiseen liittyy.
  - Tämän jälkeen voimme miettiä, miten järjestämme tekniikan, prosessit ja henkilöstön osaamisen niin, että pystymme suojaamaan tietoja riittävästi.
- Osana tätä kokonaisuutta on oleellista, että määrittelemme minkälaisia vastuita eri tahoilla on tietojen suojaamisessa. Tätä asiaa käsittelemme tässä videossa.

Käydään läpi muutamia tietoturvaan liittyviä tärkeitä tehtäviä. Ovatko nämä asiat sovittu yrityksessäsi?

- Kuka huolehtii henkilöstön käyttämien tietokoneiden tietoturvaan liittyvistä asetuksista?
- Kuka huolehtii tietokoneiden päivitysten ajantasaisuudesta?
- Kuka varmistaa henkilöstölle suunnatun tietoturvaohjeistuksen laatimisesta ja päivittämisestä?
- Kuka kouluttaa uudet työntekijät käyttämään laitteita ja järjestelmiä tietoturvallisesti?
- Kuka arvioi hankittavien pilvipalveluiden ja muiden sovellusten tietoturvallisuuden ennen käyttöönottoa?
- Jos oikeaa vastuutahoa ei ole sovittu, on iso riski siitä, että nämä asiat jäävät tekemättä.

Tietoturvavastuiden jakautuminen

- **Toimitusjohtaja ja muu johto.** Toimitusjohtajalla ja muulla johdolla on viime kädessä vastuu yrityksen tietoturvasta. Heidän tehtävänään on olla tietoisia yritykseen kohdistuvista tietototurvavaatimuksista – kuten sääntelystä ja sopimuksista – ja yrityksen tietoturvatavoitteista, sekä asettaa alueelle riittävät resurssit. Johdon tulee myös määritellä yrityksen muun henkilöstön vastuut ja kertoa näille niistä.
  - Jos yritys on pieni, johdon vastuulla voi olla myös tietoturvaohjeistuksen laatiminen, henkilöstön kouluttaminen ja tietoturva-asioista palveluntarjoajien kanssa sopiminen. Isommissa yrityksissä näihin asioihin voi olla nimetyt henkilöt.
- **Henkilöstö.** Jokainen yrityksen lukuun työskentelevä henkilö on vastuussa tietoturvan toteuttamisesta omassa työssään annettujen ohjeiden mukaisesti. Henkilöstön vastuulla on myös ilmoittaa havaitsemistaan tietoturvaan ja tietosuojaan liittyvistä havainnoista ja poikkeamista.
- **IT-yksikkö tai -tiimi.** Tyypillisesti IT-yksikkö vastaa käytössä olevista tietoteknisistä laitteista ja palveluista. IT varmistaa, että tekniset suojaustoimenpiteet ovat ajan tasalla ja valvovat, että ne toimivat tehokkaasti. Erityisesti kun IT on ulkoistettu, IT:n vastuulle kuuluvista asioista on sovittava kirjallisesti. Tätä käymme tarkemmin läpi myöhemmin tällä kurssilla.
- Suuremmissa yrityksissä tietoturvaan liittyvät tehtävät voidaan jakaa hyvin granulaarisesti eri rooleille. Tietoturvaan liittyvien henkilöiden lukumäärästä riippumatta on tärkeää aina varmistaa, että kaikki oleelliset tehtävät on vastuutettu ja niiden toteutumiselle on olemassa riittävä seuranta. Näin varmistetaan, että kaikki tehtävät tulevat tehdyksi.

Miten vastuita voi jakaa?

- **Kuka huolehtii henkilöstön käyttämien tietokoneiden tietoturvaan liittyvistä asetuksista?**
- **Kuka huolehtii tietokoneiden päivitysten ajantasaisuudesta?**

Asetukset hoitaa yleensä IT. Jos työntekijän on itse muutettava asetuksia, tähän on oltava olemassa selkeä ohjeistus.

Tietokoneiden päivitys voidaan hoitaa keskitetysti, mutta pienissä yrityksissä on tyypillistä, että työntekijät asentavat itse päivitykset. Tällöin asiaan päivitysten asentamiseen tulee olla riittävä tuki ja seuranta.

- **Kuka varmistaa henkilöstölle suunnatun tietoturvaohjeistuksen laatimisesta ja päivittämisestä?**
- **Kuka kouluttaa uudet työntekijät käyttämään laitteita ja järjestelmiä tietoturvallisesti?**

Ohjeistusta voi laatia kuka tahansa yrityksestä, jolla on siihen riittävä osaaminen. Johdon tehtävänä on tyypillisesti hyväksyä erityisesti koko yrityksessä voimassa olevat, tietoturvaan liittyvät linjaukset.

Työntekijöiden tietoturvakoulutus on pienissä yrityksissä tyypillisesti esihenkilön vastuulla oleva tehtävä.

- **Kuka arvioi hankittavien pilvipalveluiden ja muiden sovellusten tietoturvallisuuden ennen käyttöönottoa?**

Yritys voi arvioida pilvipalveluiden tai sovellusten tietoturvallisuutta itse, tai pyytää ulkopuolista tahoa, esimerkiksi ulkoista IT-palveluntarjoajaansa, arvioimaan niitä.

Tavoitteena yhdessä koettu vastuu

- Työnantaja on lähtökohtaisesti vastuussa työntekijöidensä aiheuttamista vahingoista, jotka työntekijät virheellään tai laiminlyönillään työssä aiheuttavat. Tämän vuoksi on jokaisen yrityksen intressessä varmistaa, että työntekijöillä on riittävät välineet, ohjeet ja osaaminen työnsä tekemiseen tietoturvallisesti.

- Henkilöstön osallistaminen ja hyvä yleinen tietoturvakulttuuri varmistavat sitä, että vahinkoja ei tapahtuisi.

M1V3: Henkilöstön perehdyttäminen ja tietoturvakulttuurin luominen

Taloushallintoalan johdon tietoturva

Moduuli 1: Tietoturva ja johdon vastuut

2024

Johdanto

- Henkilöstöllä on todella merkittävä rooli yrityksesi tietoturvan kannalta.
- Usein, kun yrityksen tietoturva pettää, ihmisillä on tilanteessa ratkaiseva rooli. Tietoturvapoikkeamaan voi johtaa esimerkiksi tilanne, jossa työntekijä on klikannut kalasteluviestissä olevaa linkkiä, luovuttanut tunnuksensa väärälle taholle, tai unohtanut asentaa laitteisiinsa päivitykset.
- Ihminen on kuitenkin usein tietoturvassa myös vahva linkki: joka päivä huolelliset työntekijät tunnistavat kalasteluviestit kalasteluviesteiksi, ovat tarkkoina tunnustensa kanssa – ja niin edelleen.
- Henkilöstön vahva tietoturvaosaaminen on selkeä puolustusmuuri, jonka avulla yrityksen tietoturva vahvistuu entisestään. Tässä videossa käymme läpi, miten voit omassa yrityksessäsi edistää henkilöstön tietoturvaosaamista ja yrityksen tietoturvakulttuuria.

Työntekijöiden tietoturvaosaamisen varmistaminen

- Vanhan suomalaisen sanonnan mukaan kukaan ei ole seppä syntyessään. Sama pätee tietoturvaan: kukaan ei ole kyberosaaja syntyessään.
- Tämä on hyvä muistaa, eli emme voi olettaa henkilöstön osaavan toimia oikein ja tietoturvallisesti, jos heille ei ole koskaan kerrottu oikeita ja tietoturvallisia toimintatapoja.
- Työnantajan vastuulla on antaa työntekijöilleet riittävät ohjeet ja osaaminen työvälineiden käytöstä ja tietoturvallisista toimintatavoista. Tämä on myös yrityksen oma etu, sillä he vastaavat työntekijöidensä tekemisistä asiakkaiden suuntaan.

Työntekijöiden tietoturvaosaamisen varmistaminen

- Taloushallintoliiton ja Huoltovarmuuskeskuksen tuottama Taloushallintoalan työntekijän tietoturvakoulutus on hyvä peruskoulutus kaikille työntekijöille. Se sisältää perustiedot tietoturvasta ja taloushallintoalan työtehtävissä tarvittavista hyvistä tietoturvakäytännöistä.
- Sen lisäksi on kuitenkin järjestettävä työntekijöille koulutusta, jossa käsitellään juuri **teidän työpaikallanne** käytössä olevat käytännöt: esimerkiksi missä järjestelmässä mitäkin tietoja säilytetään, miten tietoturvaloukkauksista ja **tietoturvapoikkeamista tulee ilmoittaa** ja minkälaiset tietosuojaan liittyvät käytännöt teillä on.

Järjestäkää tietoturvakoulutusta säännöllisesti

- Hyvä tietoturvan koulutusohjelma koostuu tehtävään perehdyttämisen yhteydessä tapahtuvasta koulutuksesta, sekä vuosittain toistuvasta täydentävästä koulutuksesta.
- Useimmiten henkilöstölle soveltuu samansisältöinen vuosikoulutus. Erityisissä rooleissa, kuten taloushallinto- ja IT-tehtävissä voi olla perusteltua järjestää tehtävään liittyvää erityistä koulutusta useammin tai kohdennetulla sisällöllä.
- Tietoturva-alueen uhkat kehittyvät jatkuvasti. Siksi olisi hyvä, että organisaatiossa seurataan ja jaetaan soveltuvalla tavalla tietoa niistä. Esimerkiksi Kyberturvallisuuskeskuksen suurelle yleisölle suunnatut varoitukset ja uutiset ovat hyvä lähde: https://www.kyberturvallisuuskeskus.fi/fi.

Tuumasta toimeen

Tässä koulutuksessa kerrotaan sinulle käytännön konkreettisia neuvoja, joilla pääset kehittämään tietoturvaa omassa organisaatiossasi.

Käytännön vinkit on koottu Tuumasta toimeen –nimiseen osioon. Vinkit jaetaan kolmeen eri tasoon: Aloita tästä, Kehitä ja Paranna.

- **Aloita tästä – osiossa** on perustason asioita, jotka jokaisessa yrityksessä pitäisi vähintään laittaa kuntoon. Voi olla, että nämä asiat ovat jo yrityksessäsi hyvällä mallilla. Jos tilanne näiden osalta vaatii kuitenkin kehittämistä, ota käyttöön Aloita tästä –osion toimenpiteet.
- **Kehitä –osioon** on koottu asioita, jotka voi toteuttaa sitten, kun Aloita tästä –tason asiat ovat kunnossa. Näillä vinkeillä viet tietoturvan hyvälle tasolle.
- **Paranna –osio** sisältää vinkkejä, jotka osoittavat erittäin hyvää tietoturvan tasoa. Paranna –tason toimilla yritykseen luodaan mekanismeja, joilla tietoturva kehittyy jatkuvasti eli niin sanotun jatkuvan kehittämisen mallin. Jatkuvan kehittämisen mallin avulla tietoturvaa tarkastellaan säännöllisesti ja varmistetaan, että se ei jää uhkien kehittymisestä jälkeen.

Tuumasta toimeen

1. Aloita tästä

Kun aloitat henkilöstön tietoturvaosaamisen ja organisaation tietoturvakulttuurin kehittämisen, lähde liikkeelle seuraavasti:

- ☑ **Laadi menettelyt ja käytännöt, joita seuraamalla henkilöstö toimii tietoturvallisesti.**
- ☑ **Panosta perehdytykseen.**
- ☑ **Muista esimerkin voima.**

Puhe:
Henkilöstön tietoturvallinen toiminta toteutuu parhaiten, kun organisaatiossa on selkeästi ohjeistettu, mitkä ovat oikeat, tietoturvalliset toimintatavat. Varmista siis ensin, että organisaatiossasi on olemassa menettelyt ja käytännöt, joita seuraamalla henkilöstö toimii oikein ja tietoturvallisesti.

Henkilöstön koulutus on tärkeää aina, ja erityisesti siinä vaiheessa, kun yritykseen tulee uusi työntekijä. Eri yrityksissä on eri tapoja toimia, ja on tärkeää, että uudelle työntekijälle kerrotaan alusta alkaen toimintatavat, joilla teidän yrityksessänne toimitaan tietoturvallisesti, esimerkiksi missä tietoja säilytetään, miten tietoja siirretään ja miten henkilötietoja suojataan.

Muista myös kaikessa toiminnassa esimerkin voima: johdolla on erinomainen tilaisuus näyttää, miten tietoturva huomioidaan työssä ja miten siihen suhtaudutaan.

Tuumasta toimeen

2. Kehitä

Kun pohjatyö on tehty, voit lähteä kehittämään prosesseja seuraavasti:

- ☑ **Dokumentoi menettelyt ja käytännöt kirjallisiksi ohjeiksi.**
- ☑ **Säännöllinen tietoisuuden ylläpito ja koulutus.**

Puhe:
Dokumentoi yrityksessä noudatettavat tietoturvallisuu liittyvät menettelyt ja käytännöt kirjallisesti. Näin varm asioiden oikea suorittamistapa ei ole työntekijän muis varassa.

Oikean suorittamistavan muistaminen on helmpomp kun asioita kerrataan säännöllisesti. Tietoturva-asioic pitäminen säännöllisesti mielessä varmistaa, että tiet toimintamallit eivät pääse unohtumaan. Voit esimerki järjestää yrityksessäsi säännöllisesti tietoturvakoulut tietoturvan teemapäiviä tai nostaa esiin vuosittain lok vietettävää kyberturvallisuuskuukautta.

Tuumasta toimeen

3. Paranna

Tietoturvakulttuuria voit kehittää entisestään:

- ☑ **Säännöllinen viestintä.**
- ☑ **Kehitä ja ota henkilöstö mukaan innovoimaan.**

Puhe:
Edellä mainittujen asioiden lisäksi voit kehittää yrityksen tietoturvakulttuuria entisestään viestimällä tietoturvasta säännöllisesti. Tietoturva voi olla esillä esimerkiksi säännöllisissä palavereissa. Voitte esimerkiksi keskustella työhön liittyvistä tietoturva-asioista, tai käydä läpi, minkälaisia tietoturvauhkia ja-huijauksia Suomessa juuri nyt esiintyy. Hyviä lähdemateriaaleja löytyy esimerkiksi Kyberturvallisuuskeskukselta.

Kun tietoturva on osa yrityskulttuurianne, voit kehittää toimintaa edelleen ja tuoda tietoturva-asioita esiin eri näkökulmista. Henkilöstö kannattaa ottaa mukaan innovoimaan, niin keksitte hyviä ideoita tuoda tietoturvaa säännöllisesti esiin juuri teidän yrityksellenne sopivalla tavalla.

Tuumasta toimeen

- Koulutuksen lisämateriaaleista löydät tehtävän, jonka avulla voit lähteä kehittämään oman organisaatiosi tietoturvaohjeistusta. Selkeillä ohjeilla, jotka ovat henkilöstön saatavilla, varmistat, että tietoturva-asioista on yhteinen näkemys läpi organisaation.

Moduuli 2: Tietoturvan johtaminen taloushallintoalan yrityksissä

talous hallinto liitto

Huoltovarmuuskeskus

M2V1: Organisaation tietoturvakäytäntöjen, riskienhallinnan ja jatkuvuuden hallinnan suunnittelu

Taloushallintoalan johdon tietoturva

Moduuli 2: Tietoturvan johtaminen taloushallintoalan yrityksissä

2024

Johdanto organisaation tietoturvakäytäntöjen, riskienhallinnan ja jatkuvuuden hallinnan suunnitteluun

- Tämän videon aiheena on organisaation tietoturvakäytäntöjen, riskienhallinnan ja jatkuvuuden hallinnan suunnittelu, joka on keskeinen osa liiketoiminnan suojaamista ja sen jatkuvuuden varmistamista.
- Näiden toimien avulla voit suojata yrityksesi tietoja ja järjestelmiä, vähentää riskejä ja varmistaa, että toiminta jatkuu häiriöttömästi myös poikkeustilanteissa.
- Videossa kerrotaan, miten yrityksen johto toimii suunnannäyttäjänä näiden asioiden suunnittelussa. Kokonaisuudessaan tämä aihepiiri on hyvin laaja, ja siihen liittyvää osaamista laajennetaan myös seuraavissa videoissa ja moduuleissa.

Käsitteet haltuun

Tietoturvan hallinta

Tietoturvan hallinnalla tarkoitetaan menettelyitä, joilla huolehditaan tietoturvatoiminnan ja käytäntöjen järjestämisestä. Tietoturvakäytännöillä tarkoitetaan niitä ohjeita ja sääntöjä, jotka määrittelevät, miten yrityksen tietoja ja tietojärjestelmiä suojataan. Ne kattavat muun muassa laitteiden ja tietojen hallinnan ja fyysisen turvallisuuden.

Riskienhallinta

Riskienhallinta on prosessi, jossa tunnistetaan, arvioidaan ja hallitaan muun muassa tietoturvaan liittyviä riskejä. Tämä sisältää riskien tunnistamisen, arvioinnin, hallintatoimenpiteiden suunnittelun ja toteutuksen, sekä riskien jatkuvan seurannan ja arvioinnin. Riskienhallinnan avulla yritys voi tunnistaa heikkoutensa, priorisoida riskit ja kohdentaa resurssit tehokkaasti niiden hallintaan.

Jatkuvuuden hallinta

Jatkuvuuden hallinta tarkoittaa prosessia, joilla varmistetaan, että organisaation toiminnan jatkuvuus erilaisissa poikkeamatilanteissa on ennakoitavaa. Tämä hallintaprosessi sisältää varautumissuunnitelmat, varajärjestelmät, tietojen varmuuskopioinnin ja palautusprosessit. Jatkuvuuden hallinnalla pyritään minimoimaan häiriöiden vaikutukset ja palauttamaan toiminta hallitusti normaaliin tilaan.

Standardisoidut hallintajärjestelmät

Sekä tietoturvan, riskienhallinnan, ja jatkuvuuden hallinnan alueilla on kansainväliset hallintajärjestelmästandardit. Niiden soveltamisesta on erityistä hyötyä silloin, kun yritys kasvaa ja monimutkaistuu.

Standardisoitujen hallintajärjestelmien ajatus on sama kuin vaikkapa ISO 9001-laatujärjestelmässä; saada koko organisaatio toimimaan yhteisten tavoitteiden eteen systemaattisesti.

Tässä mainittuja standardeja saattaa esiintyä taloushallinta-alan kilpailutuksissa tai IT-palvelutoimittajien kuvauksissa.

Tietoturvan hallintajärjestelmän kuvaa standardi ISO 27001. Standardi on melko yleinen, ja Suomessakin on kymmeniä tämän standardin mukaan sertifioituja yrityksiä.

Riskienhallinnan hallintajärjestelmän kuvaa standardi ISO 31000. Tämä on yleinen tietoturvasta riippumaton riskienhallintajärjestelmä, ja sen periaatteita noudatetaan hyvin laajasti etenkin suurten yritysten riskienhallinnassa.

Jatkuvuuden hallinnan hallintajärjestelmän kuvaa standardi ISO 22301. Tätä standardia sovelletaan yleisimmin yhteiskunnan kriittisillä toimialoilla, joissa keskeytysvaikutukset ovat hyvin merkittäviä, ja nopea toipuminen välttämätöntä.

Tietoturvallisuuden osa-alueet

- Tietoturva on laaja kokonaisuus, ja sen suunnittelua helpottaa, kun laajan kokonaisuuden jakaa pienempiin osa-alueisiin. Tällä kurssilla käymme läpi tietoturvan keskeisiä osa-alueita.

Kurssilla käsiteltäviä tietoturvan osa-alueita

Osa-alue	Moduulit	Osa-alueen tavoite	Toimenpide-esimerkkejä
Tietoturvan johtaminen	1, 2	Varmistaa, että tietoturva on osa organisaation strategiaa ja toimintaa.	Tietoturvapolitiikat ja -ohjeet, tietoturvan hallinta, resurssien kohdentaminen, tavoitteiden asettaminen ja strateginen suunnittelu.
Tietojen turvallisuus	2	Suojata tiedot luvattomalta pääsyltä, muutoksilta ja tuhoutumiselta.	Salaus, varmuuskopiointi, käyttöoikeuksien hallinta.
Fyysinen turvallisuus	2	Suojata fyysiset tilat ja laitteet luvattomalta pääsyltä, vahingoittumiselta ja tuhoutumiselta.	Kulunvalvonta, valvontakamerat, ympäristön turvatoimet.
Tekninen tietoturva	2	Suojata tietojärjestelmät, ympäristöt ja verkot teknisiltä uhilta.	Palomuurit, virustorjuntaohjelmat ja tunkeutumisen havaitsemisjärjestelmät.
Toimittajahallinta	3	Hallita ja valvoa tietoturvariskejä, jotka liittyvät ulkopuolisiin toimittajiin ja kumppaneihin.	Sopimukset, auditoinnit, säännölliset arvioinnit.
Tietoturva-poikkeamien hallinta	4	Havaita, tunnistaa ja ratkaista tietoturvapoikkeamat tehokkaasti.	Poikkeamahallintaprosessit, reagointi- ja palautumissuunnitelmat.
Jatkuvuudenhallinta	2, 4	Varmistaa organisaation toiminnan jatkuminen häiriötilanteissa.	Varautumissuunnitelmat, varmuuskopiointi, palautusprosessit.
Riskienhallinta	2, 5	Tunnistaa, arvioida ja hallita tietoturvariskejä.	Riskien arviointi, hallintatoimenpiteiden suunnittelu ja toteutus, jatkuva seuranta.

Tuumasta toimeen

1. Aloita tästä

Varmista, että ainakin seuraavien osa-alueiden prosessit ovat toiminnan riskeihin nähden riittävällä tasolla. Tietoja näiden alueiden riskeistä ja ideoita kehittämiseen saat tältä kurssilta.

- ☑ **Tietoturvan johtaminen –** *Vastuut ja tekemisen prosessi*
- ☑ **Tietojen turvallisuus –** *Mitä tietoja suojaamme ja miksi*
- ☑ **Tekninen tietoturva –** *Tietotekniikan turvalliset määritykset*
- ☑ **Fyysinen turvallisuus –** *Toimitilojen suojaaminen tietoturvanäkökulmasta*

Tuumasta toimeen
2. Kehitä

Varmista, että myös seuraavat prosessit ovat toiminnan riskeihin nähden riittävällä tasolla:

- ☑ **Riskienhallinta** – *Säännöllinen prosessi varmistaa toimenpiteiden kattavuutta*
- ☑ **Tietoturvapoikkeamien hallinta** – *Miten poikkeamiin reagoidaan systemaattisesti*
- ☑ **Toimittajahallinta** – *Tietoturvan vastuiden jakautuminen ja sopimukset*

Tuumasta toimeen
3. Paranna

Ota organisaatiossasi käyttöön systemaattinen tietoturvan hallinnan prosessi, esimerkiksi standardin ISO 27001 mukaisesti:

- ☑ **Toteuta tietoturvan hallinnan prosessit valitsemasi viitekehyksen mukaisesti.**
- ☑ **Seuraa prosessien tehokkuutta säännöllisesti.**
- ☑ **Opi seurannasta ja paranna toimintaa jatkuvasti.**

Riskienhallinnan rooli tietoturvan johtamisessa

talous hallinto liitto

Huoltovarmuuskeskus

- Riskienhallinta on keskeinen osa tietoturvan johtamista. Ilman hyvää käsitystä tietoturvariskeistä on tietoruvaan liittyvien toimenpiteiden kohdentamista ja laajuutta vaikea perustella.
- Tietoturvariskien suhteen on tärkeä oivaltaa, että osa riskeistä on yleisiä ilmiöitä ja toiset kohdennettuja ja yksilöllisiä.
  - Yleisiä riskejä ovat esimerkiksi huijausviestit, yleiset haittaohjelmat, ja automatisoidut tietomurrot web-palveluihin – näihin tulee kaikkien yritysten varautua.
  - Kohdennettuja riskejä ovat esimerkiksi toimialakohtaiset riskit, kuten taloushallintoalan kohdalla valelaskut ja sisäpiirin tekemät taloudelliset väärinkäytökset. Riskien todennäköisyyteen voi myös vaikuttaa yrityksen kiinnostavuus rikollisten silmissä - esimerkiksi yritykset, joissa käsitellään paljon henkilötietoja tuotetaan yhteiskunnalle kriittisiä palveluita, ovat lähtökohtaisesti rikollisia kiinnostavia kohteita.
- Käydään seuraavaksi läpi, minkälaisia tyypilliset tietoturvaan liittyvät riskit ovat.

Tietoturvariskejä

Uhka	Luottamuksellisuus	Eheys	Saatavuus
Liian laajat käyttövaltuusmääritykset	Luvaton henkilö katselee tietoja		
Työntekijän salasana päätyy rikolliselle esim. kalasteluhyökkäyksessä	Rikollinen varastaa tietoja	Rikollinen muuttaa tietoja	
Palvelunestohyökkäys estää järjestelmän käytön		Muuttuneiden tietojen päivittäminen viivästyy	Tietojärjestelmä ja sen tiedot eivät ole saatavilla
Haavoittuvuus taloushallinto-ohjelmistossa	Rikollinen tunkeutuu järjestelmään ja pääsee käsiksi tietoihin	Rikollinen saattaa muuttaa tietoja	Rikollinen tuhoaa tiedot tai kiristää niiden palauttamisella
Valelasku		Perusteeton maksu	
Vika IT-järjestelmässä		Tiedot saattavat korruptoitua	Järjestelmähäiriö estää tietojen käytön

Riskienhallinnan suunnittelu

- Tunnistit varmasti esimerkeistä, että monet niistä voisivat tapahtua sinunkin yrityksessäsi.
- Riskienhallintaprosessilla varmistat, että teillä on yritykseenne liittyvistä riskeistä ja uhkaympäristöstä yrityksen sisällä yhteinen käsitys, ja tarvittavista toimenpiteistä päätetään tiedon pohjalta. Tällöin tietoturvatoimenpiteet ovat toimivia ja kustannustehokkaita.
- Käymme riskienhallintaa tarkemmin läpi tämän kurssin Moduulissa 5.

Jatkuvuuden hallinta

talous hallinto liitto

Huoltovarmuuskeskus

- Jatkuvuuden hallinta on prosessi, jolla varmistetaan organisaation kyky jatkaa toimintaa ennakoitavalla tavalla häiriötilanteessa. Jatkuvuuden hallinta ei siis eliminoi kaikkia jatkuvuuden riskejä, vaan antaa vastauksen siihen, miten häiriötilanteessa aiheutuvat vahingot minimoidaan.
- Jatkuvuuden hallinta käsittää suunnitelmat ja toimenpiteet, jotka auttavat minimoimaan häiriöiden vaikutukset ja palauttamaan normaalin toiminnan mahdollisimman nopeasti.
- Nyrkkisääntö on, että mitä nopeampia toimenpiteitä häiriötilanteessa tulisi tehdä, sitä yksityiskohtaisimpia suunnitelmien tulisi olla. Esimerkiksi henkilöstön influenssaepidemiaa varten suunnitelma voi olla ylimalkaisempi kuin nopeasti tapahtuvaan kriittisen tietojärjestelmän korjaukseen.
- Esimerkki: Taloushallintotiimi hyödyntää pilvipalvelua, johon liittyy riski, että palvelu ei ole käytettävissä häiriön vuoksi. Koska palvelu on ulkoistettu, tiimi ei voi omilla toimillaan poistaa riskiä täysin. Sen sijaan se voi pohtia ja suunnitella ennalta, miten toimittaisiin tilanteessa, jossa palvelussa on pitkittyvä häiriö, joka estää sen normaalin käytön.

Mieti ainakin näitä skenaarioita

Jatkuvuuden hallintaa suunnitellaan yleensä erilaisten skenaarioiden kautta. Pohdi, onko omassa taloushallintotiimissäsi vastaukset esimerkiksi seuraaviin kysymyksiin:

- Millaisia päivittäisen toiminnan jatkuvuutta vaarantavia tietoturvariskejä teillä voi olla? Voisiko niihin kuulua esimerkiksi työasemille kohdistunut haittaohjelma, yrityksen pääkäyttäjätilien kaappaus, tai vaikka pilvipalvelun häiriö? Onko teillä suunnitelmia, miten näissä tilanteissa toimittaisiin?
- Mitä käyttämienne pilvipalveluiden sopimukset sanovat mahdollisten häiriöiden kestosta? Onko toimittaja sitoutunut joihinkin jatkuvuutta tukeviin järjestelyihin ja vasteaikoihin korjauksissa?
- Kun pilvipalvelussa on häiriö, keneen voitte olla yhteydessä asian ratkaisemiseksi? Kenen tulisi asiaa hoitaa tiimissänne?
- Jos pilvipalvelussa tapahtuu häiriö tai kyberhyökkäys, jonka seurauksena sen tiedot tuhoutuvat, onko teillä varmuuskopioita omissa järjestelmissä tai muissa palveluissa?
  - Esimerkki: Talvella 2024 tapahtui Ruotsissa Tietoevryn konesaliin kohdistunut kyberhyökkäys, jossa hyökkääjät tuhosivat useita merkittäviä verkkopalveluita sekä Tietoevryn hallussa olleita varmuuskopioita.

Tuumasta toimeen

1. Aloita tästä

Jatkuvuuden hallinnan osalta lähde liikkeelle seuraavasti:

- ☑ **Tunnista mitä laitteita ja palveluita tiiminne päivittäisessä toiminnassa tarvitaan.**
- ☑ **Pohdi kunkin osalta sitä, mitä vaikutuksia laitteen vikaantumisella tai palvelun katkolla olisi.**
- ☑ **Mieti, olisiko näihin tilanteisiin hyvä olla suunnitelmia, vakuutuksia, tai varajärjestelyjä.**
- ☑ **Toteuta varautumisjärjstelyt havaintojesi mukaan.**

Tuumasta toimeen
2. Kehitä

Kun pohjatyö on tehty, voit lähteä kehittämään jatkuvuudenhallintaa seuraavasti:

- ☑ **Ylläpidä suunnitelmia tärkeimpiin jatkuvuutta vaarantaviin skenaarioihin. Dokumentoi varajärjestelyt tai muut toimet, joilla näitä tilanteita hallitaan.**
- ☑ **Perehdytä tarvittavat muut työntekijät ja yhteistyökumppanit tarpeen mukaan.**

Tuumasta toimeen
3. Paranna

Jatkuvuudenhallintaa voit parantaa entisestään seuraavasti:

- ☑ **Järjestä jatkuvuusharjoituksia.**
- ☑ **Perusta jatkuvuuden hallinnan prosessi, esimerkiksi standardia ISO 22301 mukaillen.**

M2V2: Päätelaitteiden turvallisen käytön suunnittelu

Taloushallintoalan johdon tietoturva

Moduuli 2: Tietoturvan johtaminen taloushallintoalan yrityksissä

2024

Johdanto päätelaitteiden turvalliseen käyttöön

- Taloushallinnon työntekijät käyttävät päivittäiseen työhönsä päätelaitteita, useimmiten tietokoneita ja älypuhelimia. Päätelaitteilta on pääsy kriittisiin taloushallinnon palveluihin ja tietoihin, ja päätelaitteessa itsessään on kopioita tiedoista. Siksi päätelaitteiden turvallisuuden laiminlyönti voi johtaa tietomurtoihin, tietojen menetykseen ja organisaation maineen vahingoittumiseen.
- Tässä videossa käymme läpi, miten voit kehittää yrityksesi käytössä olevien päätelaitteiden turvallista hallintaa.

Päätelaitteisiin liittyvät riskit

- Päätelaitteisiin kohdistuu monenlaisia tietoturvariskejä, kuten esimerkiksi:
  - Haittaohjelmat pyrkivät varastamaan tai tuhoamaan laitteen tietoja.
  - Verkkorikolliset voivat yrittää kaapata päätelaitteen päästäkseen käsiksi taloushallinnon järjestelmiin.
  - Varastettu päätelaite voi joutua esimerkiksi identiteettivarkauden välineeksi.
- Riskien minimoimiseksi päätelaitteiden turvallisuuteen liittyvät vastuut ja prosessit on suunniteltava huolellisesti.

Päätelaitteiden varmuuskopiointi

- Päätelaitteiden osalta on tärkeä varmistaa, että niillä käsiteltäviä tärkeitä tietoja ei säilytetä ainoastaan kyseisellä laitteella, vaan sijainnissa, josta tiedot ovat saatavilla vaikka itse päätelaite katoaisi tai menisi äkillisesti rikki.
- Päätelaitteiden varmuuskopiointia ei yleensä tarvita, jos kaikki olennaiset operatiiviset tiedot, tiedostot ja viestintä sijaitsevat pilvipalveluissa.
  - Esimerkiksi jos yrityksenne käytössä on Microsoft 365-palvelut, on suositeltavaa tallentaa työtiedostot omaan OneDrive-kansioon tai yhteisiin Teams-ryhmiin. Tällöin ne ovat tallessa pilvessä eikä tietokoneen vikaantuminen vaaranna niitä.
  - Googlella on vastaavasti Drive-tiedostopalvelu.
- Päätelaitteiden varmuuskopiointi tuo toki hyötyjä. Esimerkiksi jos käytössänne on iPhone-puhelimia, on suositeltavaa varmistaa, että sen automaattiset varmuuskopiot ovat tallessa Applen iCloud-palvelussa. Tällöin uutta iPhone-puhelinta ei tarvitse asentaa kokonaan alusta ja käyttöönotto on nopeampaa. Muilla valmistajilla on vastaavia palveluita, kuten Samsung Cloud.

Tuumasta toimeen

1. Aloita tästä

Tue päätelaitteiden turvallisuutta varmistamalla, että vähintään seuraavat turvallisuuskontrollit ovat käytössä organisaatiosssi:

- ☑ **Pääsykoodi tai salasana**
- ☑ **Haittaohjelmatorjunta**
- ☑ **Käyttöjärjestelmän automaattiset tietoturvapäivitykset**
- ☑ **Käyttäjien ohjeistaminen**

Puhe:

Ensimmäinen askel on määritellä selkeät tietoturvakäytännöt, jotka varmistavat, että

- kaikki laitteet on suojattu pääsykoodilla tai salasanalla,
- vähintään kaikissa Windows-päätelaitteissa on käytössä Microsof Defender tai muu suojausohjelma, ja
- laitteissa on automaattiset tietoturvapäivitykset käytössä käyttöjärjestelmissä (esim. Windows).

Käyttäjät ovat ensimmäinen puolustuslinja tietoturvauhkia vastaan, ja heidän toiminnallaan on valtava merkitys tietoturvan tasoon. On siis tod tärkeää, että käyttäjille on koulutettu organisaation tietoturvakäytännöt, esimerkiksi, että

- työlaitteet tulee lukita tai sammuttaa aina kun niitä ei käytetä,
- työlaitteisiin ei tule asentaa työhön liittymättömiä sovelluksia kuter pelejä tai harrastesovelluksia, ja
- työlaitteita ei tule lainata perheenjäsenille tai muille.

Tuumasta toimeen
2. Kehitä

Varmista, että myös seuraavat kontrollit ovat käytössä:

- ☑ **Laitteen sisällön suojaaminen salaamalla.**
- ☑ **Sovellusten automaattiset tietoturvapäivitykset.**
- ☑ **Sovellusten asentaminen vain IT-ylläpitäjän oikeuksilla.**
- ☑ **Laitteiden turvallinen hävittäminen.**

Puhe:

Kun lähdet kehittämään yrityksen päätelaitteiden turvallisuutta edelleen, ota käyttöön seuraavat kontrollit:

  - Varmista, että kaikkien laitteiden sisältö on suojattu salaamalla (esim. Windowsin BitLocker-salaus),
  - kaikki sovellukset kuten selaimet (Chrome, Firefox) asentavat tietoturvapäivityksiä automaattisesti, ja
  - ohjelmistojen asentaminen tapahtuu IT-ylläpitäjän oikeuksilla. Muilla työntekijöille ei ole oikeuksia asentaa sovelluksia.

- Varmista, että hävitätte käytöstä poistettavat päätelaitteet turvallisesti, jotta laitteille mahdollisesti jääneet tiedot eivät joudu vääriin käsiin.

Tuumasta toimeen
3. Paranna

Kun edellä mainitut asiat ovat kunnossa, voit parantaa päätelaitteiden turvallisuutta vielä näin:

- ☑ **Laitteiden etähallinta.**
- ☑ **Tietoturvatason hallinta keskitetysti.**
- ☑ **Tietoturvahälytysten hallita keskitetysti.**

Puhe:

Varmista, että kaikki laitteet on kytketty etähallintaan, jolloin niiden suojauksen tilaa voidaan valvoa ja ohjata etänä, ja etähallinnan avulla laite voidaan tarvittaessa lukita tai tyhjentää.

- Pienelle yritykselle on suositeltavaa hankkia päätelaitteiden etähallintaan ja valvontaan liittyvät palvelut niihin erikoistuneilta IT-palvelutoimittajilta. Näin saat käyttöösi tarvittavaa osaamista ilman tarvetta palkata ja kouluttaa IT-asiantuntijoita.
  - Palvelutoimittajan kanssa on yhdessä sovittava käytännöt toimet tilanteissa, joissa havaitaan tietoturvapoikkeama. Jos alueen vastuut ja toimintatavat ovat epäselvät, voivat tarvittavat toimenpiteet uhkan torjumiseksi viivästyä.

M2V3: Pääsynhallintaratkaisujen suunnittelu

Taloushallintoalan johdon tietoturva

Moduuli 2: Tietoturvan johtaminen taloushallintoalan yrityksissä

2024

Johdanto: Pääsynhallintaratkaisut

- Pääsynhallinta on tietoturvan peruspilari, joka huolehtii siitä, että vain valtuutetut käyttäjät pääsevät käsiksi luottamuksellisiin tietoihin ja järjestelmiin.
- Tärkeimpien järjestelmien ja tietojen käytöstä pitäisi muodostua automaattisia käyttölokeja, joiden avulla voidaan havaita ja tutkia epäiltyjä väärinkäytöksiä ja tietoturvaloukkauksia. Mikäli lokien muodostumista ei ole huomioitu ennalta tulee niiden puuttuminen ikävänä yllätyksenä vastaan myöhemmin.

Identiteetinhallinnan ja pääsynhallinnan ero

Identiteetinhallinta

Identiteetinhallinnalla tarkoitetaan sitä, että tietojenkäsittely-ympäristön käyttäjillä on yksilöity tunniste, jolla he käyttävät palveluita. Tämä tunniste on käyttäjätunnus, joka yhä yleisimmin etenkin pilviympäristössä on sama kuin sähköpostiosoite.

Identiteetinhallinta käsittelee kysymystä, kenellä pitäisi ylipäänsä olla tunnus meidän palveluihimme, kuka tunnukset luo, ja missä tilanteissa ja miten ne aikanaan suljetaan.

Pääsynhallinta

Pääsynhallinnalla tarkoitetaan sitä, että luvallisilla henkilöillä on kulloinkin tehtäviensä kannalta oikeat pääsyoikeudet tietojenkäsittely-ympäristöön. Oikeudet kytketään identiteettiin.

Pääsynhallinta käsittelee kysymystä, kenellä pitäisi olla pääsy mihinkin palveluihin ja tietoihin, kuka päättää näistä pääsyistä, ja miten oikeuksia lisätään ja poistetaan käytännössä.

Pääsynhallintaratkaisujen tavoitteet ja keskeiset periaatteet

Keskeisiä periaatteita pääsynhallinnassa ovat **vähimpien oikeuksien periaate** ja **kiistämättömyys**.

Vähimpien oikeuksien periaate

Vähimpien oikeuksien periaate tarkoittaa, että käyttäjille annetaan vain ne käyttöoikeudet, jotka ovat **välttämättömiä** heidän työtehtäviensä suorittamiseksi. Esimerkiksi työntekijä, joka tarvitsee pääsyn vain tiettyyn osaan tietokannasta, ei saa laajempia oikeuksia, jotka voisivat vaarantaa järjestelmän turvallisuuden. Tällä vähennetään laajojen käyttöoikeuksien väärinkäytön ja tietovuotojen riskiä.

Käytännössä oikeuksien rajaaminen voi olla vaikeaa pienessä taloushallintoalan yrityksessä, jossa ”kaikki tekevät kaikkea”. Siksi tarvitaan vielä kiistämättömyyden periaatetta.

Kiistämättömyys

Kiistämättömyys tarkoittaa, että kaikki tehdyt toimenpiteet ovat todistettavasti jäljitettävissä tiettyyn käyttäjään. Tämä saavutetaan varmistamalla, että käytetyt sovellukset keräävät lokitietoja käyttötapahtumista, ja että käyttäjillä ei ole käytössä yhteiskäyttöisiä tunnuksia. Näiden seikkojen varmistaminen on keskeistä, jotta esimerkiksi tietoturvaloukkauksia tai kavalluksia voidaan tutkia teknisesti.

Käyttöoikeuksien säännöllinen seuranta ja tarkastus

- Vähimpien oikeuksien periaatetta toteutetaan käytännössä niin, että uuden työntekijän tullessa taloon hänelle myönnetään käyttöoikeudet vain niihin järjestelmiin, sovelluksiin ja tietosisältöihin, joita hän työssään tarvitsee.
- Käytännössä: mitä laajemmat käyttöoikeudet henkilöllä on, sitä pahempi on tilanne, jos henkilö vahingossa luovuttaa tunnuksensa verkkorikolliselle, ja myös väärinkäytösten riski kasvaa. Siksi ylimääräisiä käyttöoikeuksia ei tule myöntää henkilöille “varmuuden vuoksi”.
- Kaikkien työntekijöiden käyttöoikeuksia on myös seurattava säännöllisesti: erityisesti silloin kun työntekijän työtehtävät muuttuvat tai hänelle tulee pitkä poissaolo, on käyttöoikeuksien tarpeellisuutta arvioitava.
- Kun taas työntekijä lopettaa yrityksessä työskentelyn, on tärkeää poistaa hänen käyttöoikeutensa niin yrityksen omiin kuin asiakasyritysten tietoihin.

Salasanat ja tunnistautuminen

talous hallinto liitto

Huoltovarmuuskeskus

Salasanat

Yleisin tunnistusmenetelmä tietojärjestelmissä ja -palveluissa on salasana. Sen etuihin kuuluu käytön helppous, mutta salasanat altistuvat helposti väärinkäytöksille. Tämä johtuu siitä, että käyttäjät valitsevat heikkoja salasanoja, käyttävät samoja salasanoja useissa eri palveluissa, kirjoittavat niitä ylös sivullisten saataville ja jopa jakavat niitä keskenään. Salasanatunnistuksen puutteista johtuen sitä pidetään nykyään heikkona keinona tunnistautua.

Monivaiheinen tunnistautuminen

Salasanojen heikkouden vuoksi kaikissa sovelluksissa on ehdottoman suositeltavaa käyttää monivaiheista tunnistusta. Pilvipalvelut ja muut sovellukset tulee määrittää siten, että käyttäjä ei voi valita pelkkään salasanaan perustuvaa tunnistusta, vaan kaikille ohjataan turvallinen, eli monivaiheinen tapa tunnistautua. Joissakin sovelluksissa monivaiheisen tunnistautumisen käyttö kuitenkin vaatii, että käyttäjä itse valitsee sen käyttöönsä asetuksista.

Salasanojen hallintaohjelmistot

Huomioi myös, että monivaiheisesta tunnistautumisesta huolimatta työntekijöidesi käytössä on todennäköisesti lukuisia salasanoja. Turvallinen tapa näiden hallintaan on ottaa yrityksessä käyttöön salasanojen hallintaohjelmisto.

Vahva tunnistautuminen

Työntekijäsi käyttävät työssään myös vahvaa tunnistautumista esimerkiksi asioidessaan viranomaisten palveluissa. Vahvaan tunnistautumiseen on olemassa useita eri tapoja. Työntekijöiden kanssa kannattaa käydä keskustelua näistä tavoista ja miettiä, mikä vahvan tunnistaumisen tavoista toimii työpaikallanne parhaiten.

Vaaralliset työyhdistelmät

talous hallinto liitto

Huoltovarmuuskeskus

- Vaarallinen työyhdistelmä tarkoittaa sellaista työtehtävien yhdistelmää, joka mahdollistaa väärinkäytöksen – esimerkiksi niin että sama henkilö voi ensin tarkastaa laskun ja sitten hyväksyä sen maksuun.
- Jos vaarallisia työyhdistelmiä ei voida täysin välttää (esimerkiksi yrityksen pienen henkilöstömäärän vuoksi), tulee yrityksen käyttää muita sisäisen valvonnan keinoja väärinkäytösten estämiseen ja havaitsemiseen. Näitä keinoja ovat esimerkiksi auditoinnit, tarkastukset ja muu sisäinen valvonta.
- Käydään seuraavaksi läpi esimerkkejä vaarallisista työyhdistelmistä, jotka liittyvät maksujen käsittelyyn, ja sitten käydään läpi tapoja hallita niitä.

Esimerkkejä vaarallisista työyhdistelmistä

Vaarallinen työyhdistelmä tarkoittaa sellaista käyttöoikeuksien yhdistelmää, jolla voi toteuttaa väärinkäytöksiä.

Laskun tarkastaminen ja hyväksyminen

Jos yksi henkilö vastaa sekä laskun tarkastuksesta että hyväksymisestä, hänellä on mahdollisuus siirtää varoja ilman ulkopuolista valvontaa. Tämä voi johtaa petoksiin, väärinkäytöksiin ja organisaation varojen väärinkäyttöön.

Toimittajien lisäys ja maksujen hyväksyminen

Henkilö, joka voi lisätä toimittajia järjestelmään, ei saisi myös hyväksyä maksuja näille toimittajille. Tämä voi johtaa tekaistujen toimittajien lisäämiseen ja maksuvarojen ohjaamiseen vääriin kohteisiin.

Vaarallisten työyhdistelmien hallintakeinot

Toimenpide	Kuvaus	Esimerkki
Roolien erottelu	Varmista, että kriittiset tehtävät, esimerkiksi maksuliikenteeseen liittyen, ovat määritelty siten, että väärinkäytösten ja inhimillisten virheiden mahdollisuus on hallittu.	Määritä ostolaskujen käsittelyn prosessi siten, että laskun tarkastaja ja maksuun hyväksyjä eivät voi olla sama henkilö.
Valtuutus ja hyväksyntä-prosessit	Ota käyttöön selkeät valtuutus- ja hyväksyntäprosessit, joissa useampi henkilö tarkistaa ja hyväksyy kriittiset toimenpiteet.	Kaikki maksut yli tietyn summan tulee hyväksyä kahden henkilön toimesta ennen suorittamista.
Säännölliset tarkastukset ja auditoinnit	Suorita säännöllisiä sisäisiä tarkastuksia ja auditointeja, joilla varmistetaan, että käyttöoikeuksia ja vaarallisia työyhdistelmiä hallitaan asianmukaisesti.	Käytä ulkopuolista tilintarkastajaa tarkastamaan talousprosessit ja varmistamaan, että valvontamekanismit toimivat.
Järjestelmien käyttöoikeudet	Rajoita järjestelmäkäyttöoikeudet siten, että käyttäjillä on pääsy vain niihin toimintoihin, joita he tarvitsevat työtehtäviensä suorittamiseen.	Kirjanpitäjällä on pääsy kirjanpitojärjestelmään, mutta ei palkanlaskennassa tarvittaviin arkaluontoisiin tietoihin tai maksujärjestelmän hallintaan.

Tuumasta toimeen

1. Aloita tästä

talous hallinto liitto

Huoltovarmuuskeskus

Tue pääsynhallinnan turvallisuutta varmistamalla, että vähintään seuraavat turvallisuuskontrollit ovat käytössä organisaatiossasi:

- ☑ **Käy säännöllisesti läpi tärkeiden liiketoimintasovellusten voimassa olevat käyttöoikeudet ja poista ylimääräiset.**
- ☑ **Ota kaksivaiheinen tunnistaminen käyttöön sitä tukevissa tileissä ja sovelluksissa, esim. Microsoftin ja Googlen tilit.**
- ☑ **Ohjeista käyttäjiä käyttöoikeuksien hallintaan ja kaksivaiheiseen tunnistautumiseen liittyen.**
- ☑ **Ota käyttöön salasanojen hallintasovellus.**

Tuumasta toimeen

2. Kehitä

talous hallinto liitto

Huoltovarmuuskeskus

Varmista, että myös seuraavat kontrollit ovat käytössä:

- ☑ **Arvioi vaarallisten työyhdistelmien mahdollisuudet ja pyri järjestämään oikeudet siten, että vaarallisia työyhdistelmiä ei ole.**
- ☑ **Selvitä muodostuuko tärkeiden liiketoimintasovellusten käytöstä käyttölokia, joista voidaan tarvittaessa jälkikäteen selvittää käyttäjien toimia.**

Tuumasta toimeen

3. Paranna

Varmista, että myös seuraavat kontrollit ovat käytössä:

- ☑ **Määrittele hallintaprosessi ja vuosikellon pääsynhallinnan toteuttamiseen.**

©Taloushallintoliitto

M2V4: Tietojen turvallisen hallinnan ja siirtämisen suunnittelu

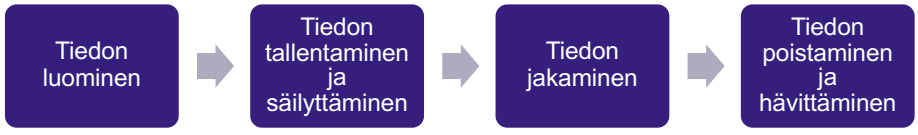
Taloushallintoalan johdon tietoturva

Moduuli 2: Tietoturvan johtaminen taloushallintoalan yrityksissä

2024

Tietojen turvallinen hallinta ja siirtäminen

- Tietojen turvallinen hallinta ja siirtäminen tarkoittavat käytäntöjä ja teknologioita, jotka suojaavat tietoja niiden koko elinkaaren ajan. Tietojen turvallisten hallinta- ja siirtotapojen määrittely on välttämätöntä kaikissa yrityksissä. Näiden käytäntöjen toteuttaminen varmistaa, että organisaation tiedot pysyvät turvassa koko niiden elinkaaren ajan, aina tiedon luomisesta sen turvalliseen poistamiseen saakka.



Tietojen luokittelu

- Eri tiedoilla on lainsäädännöstä, asiakassuhteista, ja liiketoiminnan muista syistä erilaisia suojaustarpeita. Tämän vuoksi pienissäkin yrityksissä on hyvä pohtia tapoja miten tietoja voidaan ryhmitellä ja siten luokitella niiden piirteiden perusteella.
- Aloita ensin tunnistamalla eri tietotyypit ja mihin ryhmiin ne liittyvät, esimerkiksi:
  - Asiakassuhde
  - Lainsäädännön tunnistamat tietotyypit, esim. henkilötieto, kirjanpitoaineisto, tilinpäätösaineisto
  - Säilytysaikavaatimukset
  - Tiedon muoto; data vs. dokumentti
- Kun tiedot on tunnistettu, voit pohtia millaisia luokituksia niille voisi määritellä. Pienelle yritykselle voisi soveltua esimerkiksi seuraava luokitusmalli:
  - Julkinen tieto: Nettisivuilla olevat tiedot, julkiset tilinpäätöstiedot, ja muut avoimet tiedot.
  - Sisäinen tieto: Yrityksen kaikille työntekijöille suunnatut sisäiset ohjeet ja muu sisäinen yleisviestintä.
  - Asiakastieto: Asiakassuhteisiin liittyvät sopimukset, asiakkaan kirjanpitoaineisto, asiakkaan palkanlaskennan aineisto, asiakkaiden henkilötiedot joissa yritys on käsittelijä, ja niin edelleen.
  - Luottamuksellinen: Liiketoimintasalaisuudet, hinnastot, henkilötiedot joissa yritys on itse työnantaja ja siten rekisterinpitäjä.

Luokittelun vaikutus tietojen käsittelyyn

- Edellä kuvatun luokittelun tarkoitus on, että luokkiin voidaan soveltaa selkeästi viestittäviä sisäisiä sääntöjä, jotka ohjaavat tietojen käsittelyä ja suojaustoimia. Näitä sääntöjä voisivat olla esimerkiksi:
  - Missä palveluissa tietoja saa käsitellä?
    - Esimerkki: Asiakastietoja ei saa tallentaa samalle julkaisualustalle, jossa ovat sisäiset tiedot.
  - Miten käyttöoikeuksia tietoihin hallitaan?
    - Esimerkki; Asiakastietoihin ja luottamuksellisiin tietoihin pääsy annetaan vain heille, joilla kulloinkin on työhön perustuva tarve, ei koskaan “varmuuden vuoksi”.
  - Miten tietoja saa lähettää?
    - Esimerkki: Luottamuksellisia tietoja saa lähettää vain suojatulla sähköpostilla.
  - Mikä on tietojen elinkaari?
    - Esimerkki: Asiakastiedot tuhotaan aina heti kun sopimus- ja lakivelvoitteet päättyvät.

Luotettavat ja turvalliset tiedonsiirtomenetelmät

Koko henkilöstölle tulee olla selkeät ohjeet siitä, millä välineillä tietoja saa siirtää yrityksen sisällä ja asiakkaille. Työvälineiden määrittelyssä olisi huomioitava seuraavat seikat:

- Oman tiimin kesken on suositeltavaa käyttää palveluita, jotka:
  - takaavat, että tiedot säilyvät talletettuina EU:n alueella,
  - mahdollistavat helposti ylläpidettäviä sekä yleisiä että suljettuja kanavia tai keskusteluryhmiä, ja
  - muodostavat käyttölokeja, joiden kautta voidaan havaita ja reagoida mahdollisiin väärinkäytöksiin.
- Henkilötietojen käsittelyssä ja siirroissa tulisi aina varmistaa, että se tapahtuu salaamalla suojattuna sekä siirron aikana että ollessa tallennettuna laitteille ja palveluissa. Henkilötietoja ei saa siirtää tekemällä kopioita EU/ETA:n ulkopuolelle.
  - Etätyön osalta Euroopan tietosuojaneuvosto on linjannut, että yrityksen oman työntekijän matkustamisen aikana tapahtuva etäkäyttö EU:n ulkopuolelta on sallittua, kunhan kyse on etäkäytöstä eikä edellä mainittua kopiointia muualla sijaitsevaan järjestelmään ei tapahdu.
- Yritysasiakastietojen suojausta koskevista vaatimuksista vastaa asiakas itse, on hyvä sopia heidän kanssaan mitä menetelmiä he edellyttävät tietojen suojaamiseen siirron aikana.

Tietojen turvallinen säilyttäminen

Yrityksen eri tiedoille tulee määritellä hyväksytyt säilytyspaikat. Esimerkiksi, missä järjestelmissä ja sijainneissa säilytetään asiakastietoa, ja missä säilytetään sisäistä tietoa. Tietojen säilytyspaikkojen osalta tulee varmistaa, että tietoja suojataan niissä luvattomalta pääsyltä, niistä muodostuu riittävässä määrin varmuuskopioita ja tiedot säilyvät kyseisessä paikassa koko niiden säilytysajan ajan.

Tietojen oikeat säilytyspaikat tulee ohjeistaa työntekijöille. Muutoin voi käydä niin, että tietoa tallennetaan väärään paikkaan – mistä puolestaan seuraa riski siitä, että tietoihin on liian laaja pääsy, tai että ne eivät säily.

Hyväksyttyjen säilytyspaikkojen lisäksi työntekijöille tulee selkeästi ohjeistaa, missä tietoa EI saa säilyttää. Esimerkiksi, henkilötiedoista ei saa säilyttää kopioita “varmuuden vuoksi” omalla työasemalla tai sähköpostissa.

Tietojen turvallinen poistaminen

- Kun jonkin tiedon osalta sille ei ole enää säilytystarvetta, sen poistaminen tulee ajankohtaiseksi.
- Tämä on erityisen tärkeä huomioida henkilötietojen osalta, sillä tietosuoja-asetuksen mukaan henkilötietoja saa säilyttää vain niin kauan, kuin ne ovat tarpeen henkilötietojen käyttötarkoituksen kannalta.
- Tietojen poistaminen muistinvaraisesti säilytysajan päätyttyä on haastavaa, joten yrityksessä kannattaa hyödyntää järjestelmissä tarjolla olevia tietojen säilytysajan määrittelymahdollisuuksia, jonka jälkeen tiedot poistuvat automaattisesti.

M2V5: Fyysisen tietoturvallisuuden suunnittelu

Taloushallintoalan johdon tietoturva

Moduuli 2: Tietoturvan johtaminen taloushallintoalan yrityksissä

2024

Fyysisen tietoturvallisuuden merkitys tietoturvalle

- Fyysinen tietoturvallisuus on osa tietoturvaa, jossa näkökulmana on esimerkiksi fyysisten asiakirjojen ja tietotekniikan, sekä tietojenkäsittelytilojen turvallisuus.
- Tietojenkäsittelytiloissa, eli esimerkiksi toimistoissa, käsitellään tietoja ja niissä voi olla laitteita, joilla on pääsy tietoihin. Siksi näiden tilojen suojaaminen on oleellista tietoturvan kannalta.
- Tässä videossa käsitellään fyysisen turvallisuuden toimenpiteitä, joilla varmistetaan, että fyysiset tilat, laitteet ja sitä kautta yrityksen suojattavat tiedot ovat turvassa ja käytettävissä vain valtuutetuille henkilöille.

Fyysiseen tietoturvallisuuteen liittyvät tyypilliset riskit

Riski	Kuvaus
Varkaus	Laitteiden, kuten tietokoneiden, palvelinten ja mobiililaitteiden varastaminen voi johtaa tietojen menetykseen ja tietoturvaloukkauksiin. Varkaan todennäköinen motiivi on laitteen jälleenmyynnin mahdollisuus. Jos laitetta ei ole salattu, samalla suojaamattomat tiedot voivat päätyä rikollisten käyttöön.
Tulipalo tai vesivahinko	Kiinteistön tulipalo, vesivahinko tai muu vastaava tapahtuma voi tuhota paperiaineistoja ja laitteita. Tästä aiheutuu yrityksen toiminnan jatkuvuuden ongelmia. Mikäli tapahtuma aiheuttaa henkilötietojen tuhoutumista, se voi myös täyttää henkilötietoja koskevan tietoturvaloukkauksen tunnusmerkit.
Painostus tai kiristys	Henkilöt, joilla on oikeus tehdä tilisiirtoja yritysten tileiltä voivat joutua painostuksen tai kiristyksen alaiseksi. Tällöin fyysistä uhkaa luomalla yritetään saada henkilö maksamaan huomattavia summia rikollisille.

Fyysiset turvajärjestelmät organisaation tiloissa

Kaikissa yritysten toimitiloissa tulisi arvioida riskiperusteisesti tarve fyysisen turvallisuuden teknisille ratkaisuille. Näitä ovat tyypillisesti seuraavat.

Turvaratkaisu	Kuvaus
Lukitus- ja kulunvalvonta	Lukituksen ja kulunvalvonnan ratkaisuilla huolehditaan siitä, että toimitiloissa voi liikkua vain luvallisia henkilöitä.
Hälytysjärjestelmä	Hälytysjärjestelmän avulla huolehditaan siitä, että luvaton liikkuminen toimitiloissa tunnistetaan mahdollisimman nopeasti, jotta siihen voidaan reagoida. Mieti järjestelmän toteutuksessa sitä, että sen järjestelmän operointi on käytännössä helppoa. Toinen tärkeä pohdittava seikka koskee sitä, onko hälytykset paras ohjata joillekin työntekijöille vai esimerkiksi vartiointiliikkeelle.
Kameravalvonta	Tallentavan kameravalvonnan avulla voidaan selvittää myöhemmin toimitilojen tapahtumia. Kameravalvonnan toteutuksessa ja kameroiden sijoituksessa tulee yrityksen erityisesti huomioida yksityisyyden suoja työpaikalla.
Paloilmoitin ja -sammutin-järjestelmät	Rakennusmääräykset ja rakentamisen lupamenettelyt ohjaavat sitä, millaisia paloturvallisuuden järjestelmiä kiinteistöissä pitää olla. Mikäli toimistossanne ei ole kiinteistön paloilmoitinjärjestelmää, voitte hankkia laitteen itse.

Turvallisuutta tukevat toimet organisaation tiloissa

Henkilöstön toimintatavoilla on oma vaikutus fyysisen toimintaympäristön riskien hallinnassa.

Toimet	Kuvaus
Puhtaan pöydän periaate	Puhtaan pöydän periaatteella tarkoitetaan sitä, että toimitiloihin ei jätetä papereita tai muita suojaamattomia aineistoja. Toimistolla säilytettävät aineistot ovat kassakaapissa tai muutoin suojattuna.
Työaseman lukitseminen	Yrityksen periaatteisiin tulisi kuulua se, että työntekijät lukitsevat työvälineensä aina kun ne eivät ole käytössä, myös yrityksen toimitiloissa ollessaan.
Vieraskäytännöt	Mikäli toimitiloissanne käy vieraita, heidän vastaanottoon ja vierailutapahtuman valvontaan tulisi olla yhteiset selvät ohjeet. Vieraita ei tulisi jättää valvomatta yrityksen tiloihin. Lisäksi joskus asiakassopimukset saattavat edellyttää vieraita koskevaa kirjanpitoa. Mieti tällöin tasapaino tietosuojanäkökulmasta; on hyvä käytäntö tuhota vieraskirjanpito heti, kun sille ei ole sopimus- tai turvallisuusperustetta.

Turvallisuutta tukevat toimet etätyössä

Henkilöstön toimintatavoilla on oma vaikutus etätyön riskien hallinnassa.

Toimet	Kuvaus
Työaseman lukitseminen	Yrityksen periaatteisiin tulisi kuulua se, että työntekijät lukitsevat työvälineensä aina kun ne eivät ole käytössä, myös kotona. Mikäli työvälineet jäävät kotiin ilman valvontaa pidemmäksi aikaa, vaikkapa viikonlopun ajaksi, ne on hyvä sammuttaa kokonaan.
Turvallinen työympäristö	Henkilöstöä tulisi ohjeistaa valppauteen työympäristön valinnassa. Yrityksen ja asiakkaiden asioita ei ole hyvä käsitellä vaikkapa lähijunassa tai kahvilassa, jossa on uteliaita korvia ja silmiä lähellä.

M2V6: Tietoturvan itsearviointi ja kehittämissuunnitelman laatiminen

Taloushallintoalan johdon tietoturva

Moduuli 2: Tietoturvan johtaminen taloushallintoalan yrityksissä

2024

14.3.2025

Tietoturvan kypsyystaso ja sen kehittäminen

- Tietoturvan tasoa voi arvioida itsearvioinnilla, käyttämällä tietoturvan kypsyystasoon mittaukseen tarkoitettuja menetelmiä.
- Tietoturvan kypsyystasolla kuvataan organisaation tietoturvakäytäntöjen, -prosessien ja -valmiuksien kehittyneisyyttä ja tehokkuutta – eli kypsyyttä.
- Tietoturvan kypsyystasomittauksilla yritys saa selkeän tiedon siitä, missä tietoturvan parhaiden käytäntöjen osalta mennään – mitkä asiat ovat jo hyvin ja missä on kehitettävää. Tämä tuo konkreettista hyötyä, sillä ilman mittausta tai muuta arviointitapaa voi olla haastavaa saada käsitystä siitä, mikä oman yrityksen tietoturvataso on ja mitä kaikkea käytännössä pitäisi vielä tehdä, jotta tietoturva olisi hyvällä tasolla.

Tietoturvan kypsyystason mittaustavat

- Kypsyystason mittaamiseen on eri menetelmiä. Kaikissa menetelmissä kypsyystasot jaotellaan eri tasoihin, esimerkiksi numeroilla yhdestä neljään, joissa kukin taso edustaa kasvavaa tietoturvakäytäntöjen ja -prosessien kypsyysastetta.
- Monet näistä mittauksista on mahdollista suorittaa itse-arviointina, mutta arvioinnin suorittamiseen voi myös halutessaan hankkia ulkopuolisen arvioijan, jolloin arviointiin tulee objektiivisuutta. Ulkopuolinen arvioija pystyy myös taustoittamaan mittarin kysymyksiä ja raportointivaiheessa suosittelemaan kehittämiskohteita.
- Meillä Suomessa on olemassa esimerkiksi Kybermittari-työkalu, jota julkaisee ja ylläpitää Kyberturvallisuuskeskus.
- Taloushallintoalalla on myös oma arviointimallinsa, Tietoturvan ja tietosuojan arviointityökalu, joka on Taloushallintoliiton jäsenyritysten käytössä.

Tuumasta toimeen

1. Aloita tästä

Lähde tietoturvan itsearvioinnissa liikkeelle seuraavasti:

- ☑ **Varmista tuki ja sitoutuminen.**
- ☑ **Mittaustavan valitseminen.**

Puhe:

Tietoturvan kypsyystason systemaattisen kehitykseen tarvitaan aina yrityksen johdon tuki ja sitoutuminen. Kun johto tukee hanketta, sille on riittävät resurssit ja samalla pystytään sitoutumaan kehittämään toimintaa itsearvioinnin tulosten perusteella. Varmista siis ensin, että yrityksessäsi on riittävä tuki itsearvioinnille ja sen jälkeisille kehittämistoimille.

Päätä sitten mittaustapa, eli valitse jokin valmiina olevista arviointimenetelmistä. Päätä, toteutatko mittauksen itse, vai palveluntarjoajan avulla.

Tuumasta toimeen
2. Kehitä

Toteuta sitten arviointi:

- [x] **Suunnittele aikataulut ja tarvittavat henkilöt.**
- [x] **Arvioinnin toteuttaminen.**
- [x] **Analysoi tulokset.**

Puhe:

Kun menetelmä on valittu, voit lähteä suunnittelemaan ja toteuttamaan itsearviointia. Mittausmenetelmät sisältävät tyypillisesti kysymyksiä tietoturvan eri osa-alueista, mikä auttaa hahmottamaan, missä osa-alueilla yritys on vahvoilla ja mikä kaipaa eniten kehittämistä. Yrityksen koko ja rakenne vaikuttaa siihen, kuinka monta vastaajaa itsearviointiin tarvitaan.

Kun tarvittavat henkilöt ovat tiedossa, aikatauluta ja toteuta arviointi.

Kun arviointi on tehty, analysoi arvioinnin tulokset, niin että saat selkeän käsityksen siitä, mikä yrityksenne tilanne on.

Tuumasta toimeen
3. Paranna

Arvioinnin jälkeen on aika lähteä kehittämään tilannetta:

- [x] **Laadi kehittämissuunnitelmat.**
- [x] **Toteuta kehityssuunnitelmat.**

Puhe:

Kehittämissuunnitelmaa laadittaessa tutustu arvioinnin tuloksiin ja katso sekä arvioinnin kokonaiskuvaa että eri osa-alueiden tuloksia.

- Mitkä osa-alueet tai asiat eivät vielä ole tavoitetasollanne?
- Mitkä kehityskohteet ovat kaikkein merkityksellisimpiä tietoturvan kokonaisuuden kannalta?
- Sisältävätkö kehityskohteet sekä nopeita korjauksia, että asioita, jotka on toteutettava pidemmällä aikavälillä?

Luo kehityssuunnitelma, joka tehokkaimmin kehittää tietoturvaa ja huomioi sekä lyhyen että pitkän aikavälin.

Toteuta parannukset kehityssuunnitelman mukaisesti. Määrittele kehityskohteille tavoiteaikataulut ja vastuuhenkilöt. Seuraa edistymistä säännöllisesti ja varmista, että kaikki uudet tai parannetut tietoturvakäytännöt toimivat aiotulla tavalla. Viesti kehityksestä sisäisesti ja dokumentoi tehdyt muutokset.

talous hallinto liitto

Huoltovarmuuskeskus

Moduuli 3: Tietoturva ja toimittajayhteistyö (10 min)

M3V1: Tietoturvan huomiointi toimittajavalinnoissa

Taloushallintoalan johdon tietoturva

Moduuli 3: Tietoturva ja toimittajayhteistyö

2024

Johdanto: Tietoturvan huomiointi toimittajavalinnoissa

- Yrityksesi tietoturva muodostuu monista tekijöistä. Yksi tärkeimmistä on käyttämiesi IT-toimittajien ja IT-järjestelmien tietoturvan taso. Jos käytössä on tietoturvattomia järjestelmiä tai tietoturvasta piittaamattomia toimittajia, tietoturva-asioihin liittyvä riski kasvaa hyvin korkeaksi.
- Tilitoimistot käyttävät usein taloushallinto-ohjelmaa, joka toimitetaan asennettavana sovelluksena tai sovelluspalveluna. Varmistaaksesi liiketoimintasi tietoturvan, sinun on varmistettava käyttämiesi palveluiden ja palveluntoimittajien tietoturvallisuus. Tässä videossa käymme läpi, miten tietoturvaa voidaan huomioida toimittajavalinnoissa.

Toimittajanhallinnan peruselementit

Toimittajahallinnan johtaminen

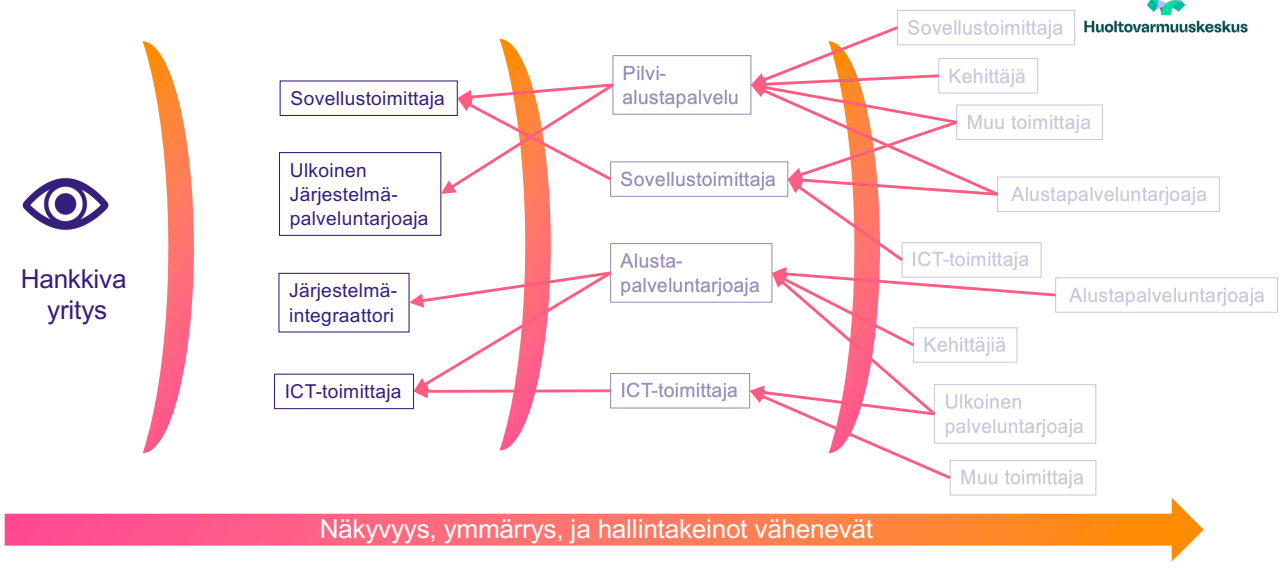
- Toimittajahallinnan linjaukset
- Toimittajahallinnan menettelyt ja hallinta
- Toiminnan reunaehdot: Vastuullisuus, laatu, teknologiat, jatkuvuus, tietosuoja, tietoturva
- Toimittajariskien tunnistaminen ja arviointi
- Valvonta ja viranomaisraportointi

Yksittäisen hankinnan elinkaari: Suunnittelu ja sopimus → Voimassaolo → Päättäminen

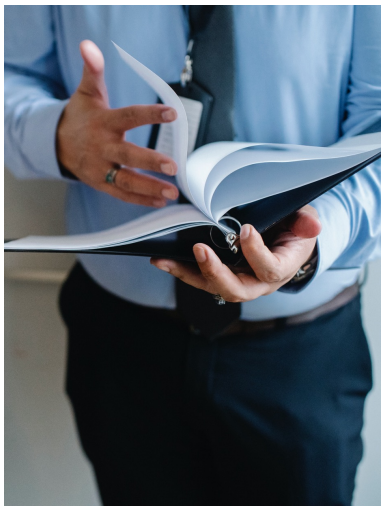
Yksittäisen hankinnan toteutus ja seuranta

- Hankintaa koskevat hallintamenettelyt
- Kehittäminen ja koulutus
- Poikkeamien seuranta ja hallinta

Yrityksen näkyvyys, ymmärrys ja toimitusketjun hallinta



Tietoturvan huomioiminen toimittajasuhteissa



Suunnitteluvaiheessa

Itsearvioinnit	Ulkoiset auditoinnit

Sopimusvaiheessa

Sopimukset	Politiikat	Prosessit ja menettelytavat	Vaatimukset ja kontrollit

Voimassaolon aikana

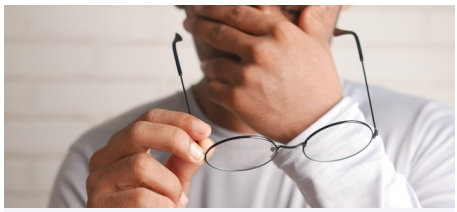
Seuranta	Itsearvioinnit	Auditoinnit	Raportointi

Organisaation tarpeet IT kumppanille

- Tietoturvatavoitteet ja -vaatimukset
- Tietoturvan tekniset kontrollit

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

Periaatteet kyberturvallisuuden toimitusketjun hallintaan

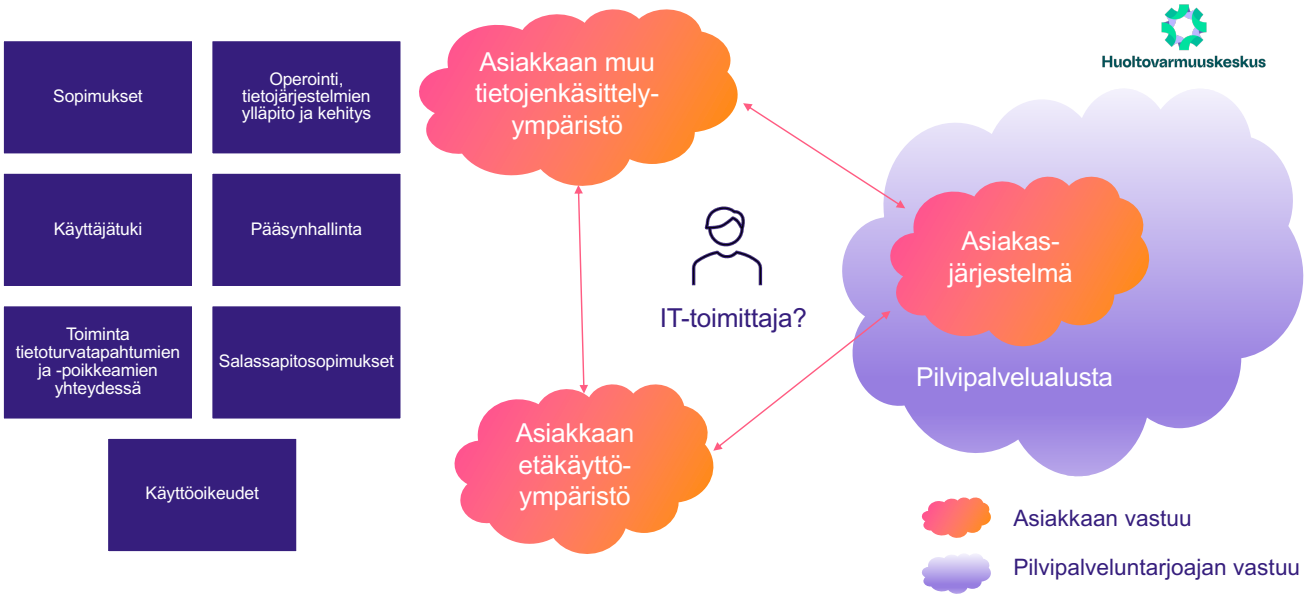


Kehitä monikerroksista puolustusta sen periaatteen pohjalta, että järjestelmäsi murretaan väistämättä.

Kyberturvallisuus ei ole pelkästään teknologinen ongelma.

Turvallisuus on turvallisuutta. Fyysisten ja tietoteknisten hallintatoimien tulisi olla keskenään tasapainossa.

Tietoturvan vastuunjako



https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_pilvipalvelujen_turvallisuudesta_123-2019.pdf

Toimittaja- ja toimitusketjuriskit

- IT-toimittajat voivat olla vastuussa yrityksesi tietoturvan ylläpidosta ja kehittämisestä ja heillä voi olla pääsy organisaatiosi järjestelmiin. Tästä syystä ICT-toimittajiin ja toimitusketjuihin liittyvät riskit on keskeistä huomioida ja luoda menetelmät, jolla tätä riskiä hallitaan.
- Käytännössä riski konkretisoituu niin, että tietomurrot ja tietovuodot voivat tapahtua toimittajien järjestelmien tai toiminnan kautta. Esimerkiksi:
  - Puutteet toimittajien kanssa tehdyissä sopimuksissa voivat aiheuttaa tilanteita, joissa tietoturvaan liittyvistä tehtävistä ja vastuista ei ole sovittu selkeästi. Tämä voi johtaa siihen, että jotakin tietoturvan kannalta tärkeää jää kokonaan tekemättä.
  - Toimittajilla voi olla käytössä alihankkijoita, ja useista toimittajista muodostuva toimitusketjussa voi jossakin kohtaa toimitusketjua olla tietoturvaheikkouksia, jota on vaikea havaita, koska kyseinen toimittaja ei ole suorassa toimittajasuhteessa yritykseen.
  - ICT-toimittajien järjestelmät voivat olla alttiita tietomurroille ja tietovuodoille. Jos toimittajan tietoturva ei ole riittävällä tasolla, hyökkääjät voivat päästä käsiksi organisaation arkaluontoisiin tietoihin toimittajan kautta.
  - Toimittajan palvelujen häiriöt, kuten käyttökatkokset tai suorituskykyongelmat, voivat vaikuttaa suoraan organisaation toimintaan ja liiketoiminnan jatkuvuuteen.

IT-toimittajan tietoturvakyvykkyyksien arviointi

- Kun olet valitsemassa uutta toimittajaa, tarkista, millaiset tietoturvakyvykkyydet toimijalla on. Käydään seuraavaksi läpi keskeisiä asioita, joista on hyvä saada selvyys.
- Arvioinnissa kannattaa huomioida, millaista tukea olet IT-toimittajalta hankkimassa. Jos IT-toimittaja tulee kokonaan vastaamaan yrityksesi IT:n ylläpidosta tai toiminnalle kriittisestä palvelusta, kiinnitä erityistä huomiota toimittajan tietoturvan tasoon.
  - Esimerkiksi kirjanpito-ohjelmisto on taloushallinnossa kriittinen järjestelmä, ja sen toimitusketjun luotettavuudesta ja toimittajan tietoturvakäytännöistä on hyvä varmistua riittävästi.

IT-toimittajan tietoturvakyvykkyyksien arviointi

Osa-alue	Tarkistuslista	Perustelut
Tietoturvan johtaminen	• Pyydä toimittajalta listaus heidän tärkeimmistä tietoturvapolitiikoistaan ja siitä, milloin ne on viimeksi päivitetty. Pyydä kirjallinen kuvaus siitä, miten he huomioivat toiminnassaan tietosuoja-asetuksen. • Kysy toimittajalta, millä tavoin he hallitsevat tietoturvaan liittyviä riskejä ja onko riskienhallintaprosessista olemassa kirjallista kuvausta. • Kysy, miten toimittaja kouluttaa henkilöstöään tietoturva-asioista.	Se miten tietoturvaa johdetaan organisaatiossa, luo pohjan tietoturvalliselle toiminnalle. Kirjalliset ohjeet luovat tietoturva-asioihin varman pohjan, kun toiminta on johdettua ja kaikki toimivat samalla tavalla. Tietoturvaan liittyvät riskit kehittyvät ja siksi riskejä tulee arvioida säännöllisesti. Myös henkilöstön osaamisen ajan tasalla pitäminen vaatii organisaatiolta aktiivisia toimia.
Tietoturvan taso	• Tarkista, onko toimittajalla jokin tietoturvasertifikaatti, kuten ISO 27001. • Selvitä, suorittaako toimittaja säännöllisiä tietoturva-auditointeja, kuinka usein ne tehdään ja mikä niiden laajuus on.	Tietoturvan tasoa voi mitata erilaisilla tavoilla. Tietoturvaan liittyvä sertifikaatti tarkoittaa, että riippumaton osapuoli on arvioinut tietoturvan tasoa. Varmista kuitenkin aina, mitkä toiminnot sertifikaatti kattaa. Säännölliset auditoinnit kertovat siitä, että tietoturvaan ja sen ylläpitoon panostetaan.
Pääsynhallinta	• Arvioi, miten toimittaja hallitsee käyttöoikeuksia ja valvoo pääsyä kriittisiin tietoihin. • Varmista, että toimittaja käyttää monivaiheista tunnistautumista suojatakseen pääsyn kriittisiin järjestelmiin.	Pääsynhallinta on kriittistä, sillä IT-toimittajilla voi olla laajoja pääsyjä asiakkaidensa järjestelmiin.
Tekninen tietoturva	• Kysy, mitä tietoturvateknologioita toimittaja käyttää. Varmista, että toimittaja käyttää ajantasaisia virustorjunta- ja haittaohjelmien torjuntaratkaisuja. • Tarkista, että toimittaja suorittaa säännöllisesti kaikkien järjestelmien ja ohjelmistojen tietoturvapäivitykset.	IT-toimittajaa valitessa on syytä varmistaa, että heidän oma tekninen tietoturvansa, samoin kuin heidän tarjoamiensa palveluiden tekninen tietoturva on hyvin hoidettua.
Tietoturvan valvonta ja poikkeamatilanteiden hallinta	• Selvitä, miten toimittaja hallinnoi ja valvoo järjestelmiä ja palveluita epäilyttävän toiminnan havaitsemiseksi. • Pyydä tietoa toimittajan tietoturvapoikkeamien hallintaprosesseista. Miten he havaitsevat, ilmoittavat ja käsittelevät tietoturvapoikkeamia? • Varmista, että toimittaja suorittaa säännöllisiä varmuuskopiointeja ja että palautusprosessit on testattu.	Tietoturvaan liittyviä poikkeamia ja tilanteita voi sattua. Mitä nopeammin nämä huomataan ja mitä tehokkaammat reagointiprosessit niihin on, poikkeamasta voidaan saada ote varhaisessa vaiheessa ja mahdollisesti välttyä lisävahingoilta.

M3V2: Vastuunjako ICT-kumppanin kanssa ja toimittajayhteistyön hallinta

Taloushallintoalan johdon tietoturva

Moduuli 3: Tietoturva ja toimittajayhteistyö

2024

Johdanto: Vastuunjako ICT-kumppanin kanssa ja toimittajayhteistyön hallinta

- Tämän videon aiheena on vastuunjako ICT-kumppanin kanssa ja toimittajayhteistyön hallinta.
- Vastuunjaon selkeä määrittely yrityksesi ja sen käyttämien ICT-toimittajien välillä varmistaa, että molemmat osapuolet ymmärtävät omat velvollisuutensa tietoturvan ylläpidossa ja kehittämisessä.
- Käymme läpi, kuinka vastuunjaosta sovitaan ICT-kumppanin kanssa ja millä tavoin toimittajayhteistyötä hallitaan tavalla, joka auttaa hoitamaan tietoturva-asioita hyvin.

Toimittajahallinnan tärkeät elementit

Vastuunjako

Vastuunjaon selkeä määrittely yrityksen ja ICT-toimittajien välillä auttaa estämään väärinkäsityksiä ja olettamuksia, jotka pahimmillaan voivat johtaa siihen, että jotakin tietoturvan kannalta tärkeää asiaa ei hoida kukaan.

Riskien tunnistaminen

Asiakkaan tulee tuntea toimittajansa ja pystyä arvioimaan niihin liittyviä riskejä.

Sopimukset

Palvelutasoa-, tietoturvaa-, ja tietosuojaa koskevat sopimukset muodostavat häiriöttömän yhteistyön perustan.

Vastuunjako asiakkaan ja ICT-toimittajien välillä

- Jos vastuut eivät ole selkeästi määriteltyjä, voi olla vaikeaa pitää osapuolet vastuullisina tietoturva-asioiden hoitamisesta ja esimerkiksi ongelmatilanteiden nopeasta ja hallitusta selvittämisestä.
- Epäselvä vastuunjako voi myös johtaa tietoturvakäytäntöjen laiminlyöntiin, mikä lisää tietomurtojen ja tietovuotojen riskiä.
- Asiakkaana sinun täytyy ottaa selvää perusasioista, kuten
  - kuka vastaa tietojen varmuuskopioinnista ja miten tuhottuja tietoja voidaan palauttaa,
  - kuka vastaa tietoturvan ylläpitämisestä vai jakautuuko vastuu asiakkaan ja toimittajan kesken joiltakin osin,
  - kuka vastaa tietoturvatapahtumien valvonnasta ja mitä asioita valvonta kattaa,
  - miten yhteistyö tietoturvapoikkeamissa tapahtuu?
- Vastuunjako on huomioitava myös valmisohjelmistoja käytettäessä. Niissä tietoturvaan liittyvät vastuut tyypillisesti jakautuvat ohjelmiston toimittajalle ja sen käyttäjälle ja on tärkeää olla selvillä siitä, mitkä ovat omat vastuusi tietoturvan osalta. Esimerkiksi pilvipalveluissa asiakkaalle tyypillisesti kuuluvat käyttövaltuushallintaan liittyvät vastuut ja ohjelmiston oletusasetusten muuttaminen yrityksen tarpeisiin paremmin soveltuviksi.

Esimerkkejä vastuunjaosta asiakkaan ja IT-toimittajan välillä

Asia	Kuvaus	Vastuutaho, yleensä
Tietoturvapolitiikan määrittely	Luoda ja ylläpitää tietoturvapolitiikkaa	Asiakas
Riskienhallinta	Tunnistaa ja hallita tietoturvariskejä	Asiakas (organisaation oman toiminnan osalta) IT-toimittaja (toimittamiensa palveluiden ja oman organisaationsa osalta)
Tietoturvakoulutus	Kouluttaa henkilöstö tietoturvakäytännöistä	Asiakas (oma henkilöstö) IT-toimittaja (IT-toimittajan henkilöstö) Huom! Asiakkaan kannattaa kuitenkin joissakin tapauksissa perehdyttää IT-toimittajan henkilöstö omien käytäntöjensä osalta.
Tietosuojasäännösten noudattaminen	Varmistaa tietosuoja-asetuksen ja muiden säädösten noudattaminen	Asiakas & IT-toimittaja (kumpikin oman toimintansa osalta)
Pääsynhallinta	Hallita käyttöoikeuksia ja pääsyoikeuksia	Asiakas (määrittely, henkilöstön koulutus), IT-toimittaja (toteutus)
Tietoturvapoikkeamien hallinta	Havaita, ilmoittaa ja hallita tietoturvapoikkeamia	IT-toimittaja (havainto ja ilmoitus), Asiakas (hallinta)
Tietoturvaraportointi	Raportoida tietoturvan tilasta ja poikkeamista	IT-toimittaja (raportointi) – Asiakas (arviointi)
Tekniset suojausratkaisut	Toteuttaa ja ylläpitää tekniset suojausratkaisut	Asiakas (vaatimukset) – IT-toimittaja (toteutus)
Tietoturvapäivitykset	Tietoturvapäivitysten ajantasainen käyttöönotto	Asiakas (vaatimukset) – IT-toimittaja (toteutus)
Tietojen varmuuskopiointi	Suorittaa säännölliset varmuuskopioinnit	Asiakas (vaatimukset) – IT-toimittaja (toteutus)
Tietojen salaus	Käyttää ja ylläpitää tietojen salaustekniikoita	Asiakas (vaatimukset) – IT-toimittaja (toteutus)
Tietoturvatyökalujen ylläpito	Ylläpitää virustorjunta- ja haittaohjelmistot	Asiakas (vaatimukset) – IT-toimittaja (toteutus)

Keskeiset sopimukset

Palvelutasosopimus (SLA)

Määrittele palvelutaso-vaatimukset, kuten palvelut ja vastuut, vasteajat ja seuraukset palvelutason alittumisesta. SLA:n tulee olla joustava, jotta se voi mukautua liiketoiminnan ja teknologian muutoksiin.

Tietoturvasopimus tai -liite

Sisällytä tietoturvasopimukseen vaatimukset tietoturvakäytännöistä sekä esimerkiksi riskienhallinnasta, varmuuskopioinnista ja poikkeamahallinnasta. Sopimuksen tulee olla riittävän kattava, mutta myös joustava uusia uhkia ja teknologioita

Tietosuojasopimus tai -liite

Määrittele tietosuojasopimuksessa vaatimukset siitä, miten henkilötietoja käsitellään, suojataan ja säilytetään, noudattaen tietosuoja-asetuksen vaatimuksia.

M3V3: Kyberuhkiin varautuminen sopimuksin ja vakuutuksin

Taloushallintoalan johdon tietoturva

Moduuli 3: Tietoturva ja toimittajayhteistyö

2024

Sopimusten merkitys kyberuhkien hallinnassa

- Hyvin laaditut hankintasopimukset ovat keskeisiä kyberuhkien hallinnassa, koska ne määrittävät selkeästi vastuut, velvollisuudet ja odotukset yrityksen, sen palveluntoimittajien ja asiakkaiden välillä.
- Sopimukset auttavat varmistamaan tietoturva- ja tietosuojakäytäntöjen noudattamisen, tehokkaan poikkeamien hallinnan ja raportoinnin sekä oikeudellisen suojan. Sopimukset määrittelevät myös, mitä toimenpiteitä on suoritettava tietoturvauhkiin varautumiseksi ja miten poikkeamat käsitellään. Tämä koskee sekä palveluntoimittajia että asiakkaita.
- Sopimukset **asiakkaiden kanssa** voivat sisältää vaatimuksia henkilötietojen käsittelystä, suojauksesta ja säilytyksestä. Sopimukset voivat myös sisältää vaatimuksia tietoturvakäytännöistä ja -prosesseista, joita on noudatettava. Sopimukset voivat myös määritellä prosessit tietoturvapoikkeamien havaitsemiseksi, ilmoittamiseksi ja käsittelemiseksi.
- **IT-toimittajien kanssa tehdyt sopimukset** voivat sisältää vaatimuksia säännöllisestä tietoturvaraportoinnista, mikä auttaa pysymään ajan tasalla tietoturvan tilasta ja mahdollisista uhista.

Esimerkkejä tietoturva-alueen sopimusehdoista

Tietoturva-alueella sopimusehdot käsittelevät tyypillisesti seuraavia aiheita:

- Toimittajan ja asiakkaan välinen vastuunjako eri tietoturvan osa-alueista: Tämä on tyypillinen sovittava alue esimerkiksi pilvipalveluna toimitettavien sovellusten kohdalla. Kuka vastaa vaikkapa tietojen varmuuskopioinnista tai pääsynhallinnasta asiakkaan tietoihin?
- Tietoturvakäytännöt: Salassapitosopimuksissa yleensä määritellään kattavasti sopimuksen piirissä olevat suojattavat tiedot, mutta miten niitä pitää suojata käytännössä? Toimittajalta voidaan esimerkiksi vaatia, että tiedot tallennetaan suojattuna vahvoilla tunnistusmenetelmillä, järjestelmät ovat jatkuvasti päivitetty tietoturvan osalta, ja että järjestelmien käyttöä valvotaan tunkeutumisten havaitsemiseksi.
- Millaisista tietoturvapoikkeamista täytyy ilmoittaa toiselle sopijaosapuolelle: Esimerkiksi palvelutoimittaja, joka käsittelee asiakkaan luottamuksellisia tietoja, on yleensä velvollinen ilmoittamaan havaitsemistaan tietoturvapoikkeamista, jos kyse on mahdollisesti asiakkaan tietoihin liittyvästä loukkauksesta.
- Henkilötietojen käsittelyn erityisehdoista sovitaan yleensä erillisellä DPA-sopimuksella (Data Processing Agreement).
- Asiakas voi varata tietoturva-alueen auditointioikeuden tai edellyttää, että sovelluspalvelutoimittaja esimerkiksi testauttaa oman teknisen tietoturvan tasoa säännöllisesti.

Yritysten kybervakuutukset

- Kybervakuutukset eli tietoturvavakuutukset tarjoavat yrityksille taloudellista suojaa kyberhyökkäysten ja tietoturvaloukkausten varalta. Yrityksen tulisi arvioida niiden soveltuvuus itselle tutustumalla vakuutusyhtiöiden palveluihin.
- Eri vakuutusyhtiöiden tarjoamat kybervakuutukset voivat erota toisistaan kattavuuden osalta, mutta pääsääntöisesti kybervakuutus auttaa kattamaan tietomurroista ja tietovuodoista aiheutuvia suoria kustannuksia, kuten asiantuntijakuluja, ja tappioita, jotka johtuvat liiketoiminnan keskeytymisestä kyberhyökkäysten vuoksi.
- Tyypillisesti vakuutuksen saaminen edellyttää, että yrityksen kyberriskit arvioidaan ja tietoturvakäytännöt ovat yritykselle soveltuvalla perustasolla. Esimerkiksi, mikäli yrityksen laitteet tai sovellukset ovat vanhentuneita, tai niitä on ylläpidetty tietoturvan kannalta puutteellisesti, voi olla ehtojen mukaan korvausta alentava tilanne.

Tuumasta toimeen

1. Aloita tästä

Lähde liikkeelle toimintaanne kohdistuvista vaatimuksista:

- ☑ **Selvitä millaisia tietoturvaa koskevia sitoumuksia asiakassopimuksissanne on, ja onko teillä selkeää näyttöä niiden toteutumisesta. Toteuta vaaditut asiat.**

Tuumasta toimeen

2. Kehitä

Selvitä seuraavaksi, millaiset ehdot teillä on toimittajienne kanssa, ja vastaavatko ne tiedossa oleviin tietoturvariskeihinne:

- ☑ **Tutustu tärkeimpien toimittajasopimustenne tietoturvaehtoihin ja vastuunjakoon. Vastaako vastuunjako käsitystänne siitä, miten olette varautuneet erilaisiin tietoturvariskeihin?**
- ☑ **Pyri tarvittavin osin parantamaan sopimusehtoja niiltä osin kun ehdot ovat epäselvät tai kannaltanne huonot. Tämä voi tapahtua joko neuvottelemalla nykyisen toimittajan kanssa tai hakemalla markkinoilta uusia vaihtoehtoja.**

Lisää ideoita sopimusehdoista: Huoltovarmuuskeskus – Kyberturva ICT-sopimuksissa

Tuumasta toimeen

3. Paranna

Kun olette päässeet sopimuksenhallinnassa hyvään alkuun, voitte kehittää sitä edelleen seuraavasti:

- ☑ **Kehittäkää sopimustenhallintaan systematiikkaa, joka varmistaa kytkennän tietoturvan riskiprosesseihin, esimerkiksi siten, että tunnettujen riskien rekisterissä mainitaan asiaan liittyvät sopimukset ja ehtolauseet. Riskiprosessia käsitellään myöhemmin tällä kurssilla.**

talous hallinto liitto
Huoltovarmuuskeskus

©Taloushallintoliitto

Moduuli 4: Poikkeamanhallinta (10 min)

talous hallinto liitto

Huoltovarmuuskeskus

M4V1: Toiminta henkilötietojen tietoturvaloukkauksissa

Taloushallintoalan johdon tietoturva

Moduuli 4: Poikkeamanhallinta

2024

14.3.2025 ©Taloushallintoliitto

Henkilötietojen tietoturvaloukkaukset: Mitä ne ovat ja miten ne voivat vaikuttaa yrityksen toimintaan

- Henkilötietojen tietoturvaloukkauksessa yrityksen hallussa olevia henkilötietoja joutuu luvattoman pääsyn, tuhoutumisen, muuttamisen tai vahingossa tapahtuvan paljastumisen kohteeksi.
- Tyypillisiä esimerkkejä taloushallintoalan yrityksissä tapahtuvista tietoturvaloukkauksista:
  - Henkilötietoja lähetetään väärälle vastaanottajalle.
  - Henkilötietoja tuhotaan tai muutetaan vahingossa.
  - Luvaton taho pääsee käsiksi pilvipalveluun ja vie henkilötietoja.
  - Yrityksen työntekijä tarkastelee henkilötietoja ilman työhön liittyvää syytä, esimerkiksi uteliaisuudesta.
  - Henkilötietoja sisältävä tietokone, jonka sisältöä ei ole suojattu salaamalla ja pääsykoodilla, varastetaan.
- On tärkeää huomata, että tietoturvaloukkaus syntyy edellä kuvatuissa tilanteissa riippumatta siitä, onko riski rekisteröityjen oikeuksille korkea vai ei.

Vaikutukset yrityksen toimintaan

- Henkilötietojen tietoturvaloukkaukset voivat johtaa oikeudellisiin seuraamuksiin, erityisesti jos taustalta paljastuu puutteita henkilötietojen suojaamisen käytänteissä. Yritykselle voidaan määrätä hallinnollinen seuraamusmaksu tietosuojarikkomuksesta, joka tietosuoja-asetuksen mukaan voi olla maksimissaan 20 miljoonaa euroa tai 4 % yrityksen maailmanlaajuisesta liikevaihdosta – kumpi tahansa on suurempi. Lisäksi yrityksen avainhenkilöille voi koitua rikosoikeudellisia seurauksia ja yritykselle asiakkaiden vahingonkorvausvaatimuksia.
- Näiden lisäksi yritykselle voi koitua lukuisia epäsuoria vaikutuksia, jotka vaikeuttavat sen liiketoimintaa. Esimerkiksi tietoturvaloukkaus voi heikentää yrityksen mainetta ja johtaa asiakkaiden ja kumppaneiden luottamuksen menettämiseen.
- Tietoturvaloukkauksista aiheutuu tyypillisesti myös operatiivisia kuluja esimerkiksi asiantuntija-avun käyttämisestä asian tutkintaan ja tietojen palauttamiseen.

Johdon rooli tietoturvaloukkauksissa

- Johto vastaa siitä, että henkilötietojen käsittelyyn on asianmukaiset toimintamallit ja ohjeet, että henkilöstö on koulutettu niiden mukaisesta toiminnasta, ja että tietoturvaloukkauksiin varaudutaan asianmukaisesti. Jos organisaatio toimii henkilötietojen käsittelijänä, jolloin rekisterinpitäjä on esimerkiksi asiakasyritys, on varmistettava, että henkilötietojen käsittelyssä noudatetaan rekisterinpitäjältä saatuja ohjeita.
- Johdon rooli on myös kriittinen siinä, miten toteutuneita tietoturvaloukkauksia käsitellään viestinnällisesti sekä organisaation sisällä että ulkoisesti.

Tietoturvaloukkausten käsittely

Tietoturvaloukkauksen sattuessa yrityksessä on toimittava nopeasti ja systemaattisesti. Ennalta määritellyt käsittelyvaiheet varmistavat, että yritys pystyy minimoimaan loukkauksen aiheuttamat vahingot ja palautumaan mahdollisimman tehokkaasti.

Seuraavaksi kuvattu toimintamalli on lähtökohta, jota voit tarpeen mukaan muokata sellaiseksi, että se toimii yrityksessäsi. Tärkeää on, että vaiheet kattavat tilanteen koko elinkaaren aina loukkauksen havaitsemisesta toipumiseen asti.

Henkilötietojen tietoturvaloukkauksen käsittelyn vaiheet

Vaihe	Toimenpide	Kuvaus
1. Havaitseminen ja arviointi	Loukkauksen havaitseminen	Käytä valvontatyökaluja ja järjestelmiä, jotka tunnistavat poikkeavan toiminnan ja ilmoittavat mahdollisesta tietoturvaloukkauksesta välittömästi. Myös henkilöstö tulisi olla koulutettu tunnistamaan tietoturvaloukkaus, esimerkiksi tilanne, jossa henkilötietoja vahingossa päätyy väärälle vastaanottajalle.
	Ensivaiheen arviointi	Arvioi nopeasti loukkauksen laajuus ja vakavuus. Selvitä, mitkä tiedot ovat mahdollisesti vaarantuneet ja kuinka laaja loukkaus on.
2. Ensimmäiset kriittiset toimet	Vaikutusten rajoittaminen	Toteuta toimenpiteitä, jotka rajoittavat loukkauksen aiheuttamia vahinkoja. Esimerkiksi ota käyttöön tilapäisiä suojatoimenpiteitä, kuten käyttöoikeuksien rajoittaminen tai tiettyjen palvelujen keskeyttäminen.
3. Ilmoitusvelvollisuus	Eskaloi sisäisesti	Raportoi loukkaus välittömästi yrityksessäsi tietosuoja-asioista vastaavalle henkilölle ja johdolle. Mikäli loukkaus koskee tietoja, joissa toimitte henkilötietojen käsittelijänä ja rekisterinpitäjä on toinen yritys, ilmoita asiasta heille.
	Ilmoita viranomaisille	Jos tietoturvaloukkaus aiheuttaa luonnollisten henkilöiden oikeuksille ja vapauksille riskin, rekisterinpitäjän tulee informoida asiasta tietosuojaviranomaisia 72 tunnin kuluessa. Ilmoitusvelvollisuus kuuluu rekisterinpitäjälle.
	Ilmoita rekisteröidyille	Jos tietoturvaloukkaus on olennainen ja aiheuttaa todennäköisesti riskin rekisteröidyn oikeuksille, on rekisteröityjä informoitava. Ilmoitusvelvollisuus kuuluu rekisterinpitäjälle.
4. Toipuminen ja palautuminen	Tietojen ja sovellusten palauttaminen	Mikäli tietoja ja sovelluksia on jouduttu rajoittamaan, palauta tiedot ja sovellukset toimintaan vaiheittain, varmistaen, että ne ovat täysin turvallisia ja että kaikki mahdolliset haavoittuvuudet on korjattu ennen palauttamista.
5. Tilanteesta oppiminen	Oppiminen ja parantaminen	Suorita loukkauksen jälkeen analyysi ymmärtääksesi, miten ja miksi loukkaus tapahtui. Käytä näitä tietoja parantaaksesi organisaation tietosuoja- ja tietoturvakäytäntöjä ja –prosesseja tulevien loukkausten estämiseksi.

M4V1: Tietoturvapoikkeamat

Taloushallintoalan johdon tietoturva

Moduuli 4: Poikkeamanhallinta

2024

Tietoturvahäiriöt, -tapahtumat ja -poikkeamat

- Tietoturvaan liittyvät häiriöt, tapahtumat ja poikkeamat ovat tilanteita, joissa tietoturva vaarantuu. Kullakin termillä erilainen merkitys ja vakavuusaste, ja niiden ymmärtäminen auttaa jäsentämään tietoturvaan liittyviä ongelmatilanteita.
- Tietoturvahäiriö (issue) tarkoittaa häiriö- tai ongelmatilannetta, joka liittyy tietoturvaan, mutta siitä ei ole aiheutunut konkreettista ja havaittavaa vahinkoa. Esimerkiksi puuttuva tietoturvapäivitys voi olla häiriö.
- Tietoturvatapahtuma (event) on tilanne, jossa on tapahtunut konkreettinen ja havaittu tietoturvaan kohdistuvaa haitallista toimintaa. Esimerkiksi havaittu epäilyttävä kirjautuminen sovellukseen on tietoturvatapahtuma, joka edellyttää tarkempaa tutkintaa.
- Tietoturvapoikkeama (incident) on tarkoittaa tilannetta, jossa on tapahtunut havaittu väärinkäytös, rikos palvelunestohyökkäys, tai muu vakava tietoturvan loukkaus. Esimerkiksi edellä kuvattu tapahtuma voi osoittautua poikkeamaksi, jos tutkinta tuo ilmi, että epäilyttävään kirjautumiseen liittyy vaikka tietojen luvaton lataaminen sovelluksesta.

Tyypilliset häiriö/poikkeamatilanteet ja niiden vaikutukset

- Olemme tällä kurssilla käsitelleet useita erilaisia tietoturvauhkia- ja riskejä, joiden toteutuminen tarkoittaa yleensä tietoturvapoikkeamaa.
- Tietoturva-alueen poikkeamat ovat niitä tilanteita, jotka toteutuessaan haittaavat tai aiheuttavat vahinkoa tietojenkäsittelylle tai tiedoille. Eli kohteena voivat olla ICT-laitteet, -sovellukset ja -palvelut, ja toisaalta niiden sisältö, kuten asiakirjat ja tietoaineistot.

Vaikutukset yrityksen toimintaan

- Erityisesti tietoturvapoikkeamat voivat aiheuttaa operatiivisia häiriöitä yrityksen toiminnassa ja voivat siten aiheuttaa suoria taloudellisia menetyksiä, kuten tietojen palautuskustannuksia, korjaus- ja jälleenrakennuskuluja sekä mahdollisia sakkoja ja oikeudenkäyntikuluja. Myös tietoturvatapahtumat voivat aiheuttaa kustannuksia, jos ne vaativat laajempia tutkimuksia ja toimenpiteitä riskien hallitsemiseksi.
- Vakava tietoturvaan liittyvä ongelmatilanne voi heikentää yrityksen mainetta asiakkaiden, yhteistyökumppaneiden ja sijoittajien silmissä. Jos yritys ei pysty osoittamaan vahvaa tietoturvaa, asiakkaat voivat menettää luottamuksensa, mikä voi johtaa asiakaskatoon ja vaikeuttaa uusien asiakkaiden hankintaa.
- Aiemmin tällä kurssilla käsitellyt henkilötietojen tietoturvaloukkaukset ovat eräs tietoturvapoikkeamien tyyppi. Näiden loukkausten seurauksia ja käsittelyä kuvataan tarkemmin tuossa kurssin osassa.
- Käydään seuraavaksi läpi prosessi, jota tyypillisesti noudatetaan tietoturvaan liittyvissä poikkeamatilanteissa. Poikkeamatilanteisiin löytyy paljon hyviä ohjeita Kyberturvallisuuskeskukselta. Ohjeisiin kannattaa tutustua rauhassa, kun käynnissä ei ole poikkeamatilannetta, ja poimia sieltä omalle yritykselle hyvät toimintamallit.

Tietoturvapoikkeaman käsittelyn vaiheet

Tähän piirretty prosessikaavio.

Vaihe	Toi	
1. Havaitseminen ja arviointi	Poi hav	llisesta ukkaus.
	Ens arv	sesti vaarantuneet ja
2. Ensimmäiset kriittiset toimet	Vai rajo	joidenkin tunnusten teydestä ja säilyttää
	Esk tah	an selvittämiseen. Mikäli a heille. Heidän
3. Selvitys ja toimenpiteet	Sel kys tarv	ista toimenpiteistä sken. Hyödynnä vitykseen.
	Ilm vira	densa mukaisesti. ilmoituksia kaikista
4. Toipuminen ja palautuminen	Tiet sov pal	allisia ja että kaikki
5. Tilanteesta oppiminen	Opp parantaminen	äitä tietoja parantaaksesi yrityksen tietoturvakäytäntöjä.

M4V3: Johdatus tietoturvallisuuden ja jatkuvuuden hallinnan harjoittelutoimintaan

Taloushallintoalan johdon tietoturva

Moduuli 4: Poikkeamanhallinta

2024

Johdanto:

- Tämän videon aiheena on tietoturvallisuuteen ja jatkuvuuden hallintaan liittyvä harjoittelutoiminta.
- Tietoturvapoikkeamatilanteiden harjoittelu on tärkeää, koska se valmistaa yritystäsi toimimaan nopeasti ja tehokkaasti todellisen tietoturvauhkan sattuessa. Harjoittelu auttaa tunnistamaan mahdolliset heikkoudet tietoturvatoimenpiteissä ja parantamaan valmiuksia poikkeamien käsittelyssä. Lisäksi se varmistaa, että henkilöstö tietää roolinsa ja vastuualueensa kriisitilanteissa, mikä vähentää vahinkoja ja nopeuttaa palautumista.

Tyypillisiä harjoitusmuotoja

Jatkuvuuden ja poikkeamatilanteiden harjoittelu on hyvä tapa varmistaa, että olemassa olevat prosessit ja käytännöt ovat riittäviä erilaisten skenaarioiden hallintaan. Harjoitusmuotoja on erilaisia:

- **Työpöytäharjoitus** sopii hyvin pienen yrityksen tai tiimin harjoitteluun. Siinä järjestetään fasilitoitu työpaja yhden tai useamman kriisiskenaarion käsittelemiseksi. Tavoite on keskustelun kautta tunnistaa onko varautumisen taso riittävää ja millä alueilla sitä voisi edelleen kehittää.
- **Sähköpostiharjoitus** on harjoitustyyppi, jossa viestintä tapahtuu sovitun aikataulun mukaan kiireettömästi sähköpostilla. Tämä tekee sähköpostiharjoituksesta hyvän tilanteissa, joissa osallistuvien tahojen on vaikea löytää yhteistä aikaa harjoituksen järjestelmiseen. Kyberturvallisuuskeskus on julkaissut asiaan liittyvän ohjeen **https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohje-sahkopostiharjoituksen-toteuttamiseen**
- **Kriisisimulaatio** sopii parhaiten yrityksille, jossa laadullinen tavoitetaso kriisien ja jatkuvuuden hallinnassa on korkea. Tämä on toiminnallinen harjoitus, jossa harjoitteleva ryhmä – esimerkiksi yrityksen kriisijohtoryhmä – arvioi tilannetta, johtaa kriisiä, ja tekee päätöksiä mahdollisimman aidosti. Simulaatioharjoitus kestää yleensä puolesta päivästä päivään.

Kaikkia edellä kuvattuja harjoitusmuotoja voi soveltaa itsenäisesti tai ottamalla harjoitukseen mukaan asiakkaita, toimittajia tai muita sidosryhmiä.

Lisäksi viranomaiset järjestävät avointa Taisto-harjoitusta, johon mahdollista myös yritysten osallistua: https://dvv.fi/taisto

Poikkeamatilanteista oppiminen: Jatkuvan parantamisen ja oppimisen merkitys

- Tietoturvatoiminnassa on hyvä pyrkiä aina jatkuvan kehittämisen ajattelumalliin, jossa epämieluisistakin asioista pyritään oppimaan, jotta jatkossa osattaisiin toimia paremmin.
- Poikkeamatilanteet ovat ikäviä tilanteita, joissa opitaan kantapään kautta yrityksen tietoturvakäytäntöjen ja -prosessien tehokkuudesta. Niistä saadut opit ovat kuitenkin arvokkaita, ja ainoa tapa välttää tilanteen toistumista, on oppia tilanteesta ja kehittää toimintaansa.

Poikkeamatilanteista oppiminen: Jatkuvan parantamisen ja oppimisen merkitys

- Poikkeamatilanteiden jälkikäteisanalyysi on keskeinen osa organisaation tietoturvatoimintojen jatkuvaa parantamista.
- Jälkikäteisanalyysin tarkoituksena on ymmärtää poikkeaman syyt ja mitä toimenpiteitä tarvitaan vastaavien tilanteiden estämiseksi tulevaisuudessa.
  - Jos poikkeama paljasti teknisiä heikkouksia, kuten vanhentuneita ohjelmistoja tai riittämättömiä pääsynhallintakäytäntöjä, korjaa ongelmat välittömästi.
  - Jos poikkeama paljasti puutteita prosesseissa tai toimintatavoissa, laadi suunnitelma näiden korjaamiseksi. Tämä voi sisältää uusien prosessien luomista, olemassa olevien päivittämistä tai lisäkoulutusta henkilöstölle.
  - Kun parannustoimenpiteet on otettu käyttöön, seuraa niiden vaikutusta säännöllisesti. Onko uudet prosessit ja käytännöt toimineet odotetusti?
- Organisaation tietoturva kehittyy, kun jatkuvan parantamisen mallista tehdään osa organisaation kulttuuria. Kaikki tietävät, että ongelmatilanteita ei tule lakaista maton alle, vaan niistä tulee kertoa, jotta toimintaa voidaan kehittää niin, että tilanne ei enää toistuisi.

Moduuli 5: Tietoturvariskienhallinta (10 min)

talous hallinto liitto

Huoltovarmuuskeskus

M5V1: Riskienhallinta

Taloushallintoalan johdon tietoturva

Moduuli 5: Tietoturvariskienhallinta

2024

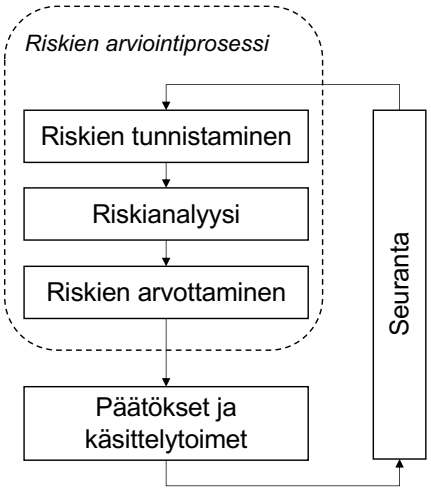
14.3.2025 ©Taloushallintoliitto

Johdatus tietoturvariskienhallintaan

- Tietoturvassa on kyse tiettyjen operatiivisiin riskeihin kuuluvien riskityyppien hallinnasta. Tarkemmin, tarkastelemme tietoturvatoiminnassa niitä riskejä, jotka aiheuttavat poikkeamia tietojenkäsittelyn laitteisiin ja -palveluihin, tietoprosesseihin ja tietoihin.
- Kuten aina, tietoturva-alueen riskien hallinnan tarkoituksena on torjua riskien toteutumista, ja rajoittaa niiden riskien vaikutuksia, joita emme voi poistaa.
- Mikä tekee tietoturva-alueen riskienhallinnasta erityisen kompleksista on, että riskeihin vaikuttava uhkaympäristö elää jatkuvasti; toisaalta rikolliset keksivät yhä uusi tapoja huijata työntekijöitä ja toteuttaa teknisiä hyökkäyksiä, ja samaan aikaan suojattava IT-ympäristömme muuttuu tietotekniikan, sovellusten ja palveluiden jatkuvien muutosten myötä. Tämä jos joku on liikkuva maali ja edellyttää valppautta jokaisessa yrityksessä!

Hyvä riskienhallintaprosessi

- Tiedämme kaikki esimerkkejä, joissa riskienhallinta ei toimi hyvin. On inhimillistä ottaa samoja riskejä, joita aiemminkin on otettu, ja vähätellä riskejä, joita ei tunne hyvin, tai sivuuttaa jokin riskienhallintatoimenpide kiireen vuoksi.
- Kansainvälinen standardi ISO 31000 määrittelee hyvän prosessimallin riskienhallintaan. Sen periaatteet sopivat kaikkiin operatiivisiin riskilajeihin, myös tietoturvariskeihin.
- Ohessa on standardista yksinkertaistettu prosessikuvaus. Prosessin keskeinen periaate on, että se erottelee riskien tunnistamiseen, analyysiin, arvottamiseen ja päätöksiin liittyvät vaiheet toisistaan siten, että prosessi toimisi mahdollisimman luotettavasti ja analyyttisesti.
- Käsitellään näitä vaiheita seuraavaksi.



Tietoturvariskienhallinnan keskeiset vaiheet

Riskien tunnistaminen

- Tunnista yrityksesi kriittiset tiedot ja järjestelmät, joiden suojaaminen tietoturvariskeiltä on ensisijaisen tärkeää. Nämä voivat olla esimerkiksi asiakkaiden taloustiedot tai henkilötiedot, omat liiketoiminnan tiedot ja liiketoiminnan kannalta kriittiset IT-palvelut.
- Tunnista mahdolliset uhat ja haavoittuvuudet, jotka voivat liittyä edellä kuvattuihin resursseihin, ja aiheuttaa riskin. Näihin voi kuulua esimerkiksi kyberhyökkäykset, haittaohjelmat, tietojen kalastelu, inhimilliset virheet tai sähkökatkot.
- Kirjaa resurssit ja riskit riskirekisteriin, joka voi olla tiedosto tai erityinen sovellus.
- Aiemmin tällä kurssilla käsitelty hyvä tietoturvakulttuuri edesauttaa riskien tunnistamista; riskejä ei tällöin vähätellä eikä inhimillisten tekijöiden osuutta tietoturvariskeissä peitellä.

Riskien arviointi

- Analysoi mitkä tekijät vaikuttavat kielteisesti tai myönteisesti riskiin. Esimerkiksi pilvipalveluna hankittu taloushallinnan palvelu on altis luvattomalle käytölle, koska sitä voi käyttää mistä vain internetistä. Toisaalta jos pääsy on suojattu vahvalla tai monivaiheisella tunnistautumisella, se vähentää luvattoman käytön todennäköisyyttä.
- Kun riskit on analysoitu, voit määrittää niiden arvon eli todennäköisyyden ja vaikutuksen.
- Kirjaa kaikki tiedot riskirekisteriin.

Tietoturvariskienhallinnan keskeiset vaiheet

Hallintapäätökset

- Tee tarvittavat päätökset edellä tunnistettujen ja arvotettujen riskien osalta. Arvoltaan vähäisiä riskejä tyypillisesti siedetään ja jäännösriski hyväksytään. Merkittävien riskien osalta tee päätös keinoista joilla riskin voi poistaa tai vähentää:
  - Välttäminen: Poista tai vähennä toimintoja, jotka altistavat riskille.
  - Siirtäminen: Siirrä riski kolmannelle osapuolelle, kuten vakuutusyhtiölle.
  - Vähentäminen: Ota käyttöön teknisiä, organisatorisia ja hallinnollisia toimenpiteitä riskin pienentämiseksi, kuten vahva pääsynhallinta, tietojen salaaminen ja säännölliset tietoturva-auditoinnit.
  - Hyväksyminen: Joissain tapauksissa yritys voi päättää hyväksyä riskin, jos sen hallintakeinot ovat kalliimpia kuin itse riskin mahdolliset vaikutukset.
- Kirjaa tehdyt päätökset ja tarvittavat lisätiedot, kuten aikataulu ja vastuut, riskirekisteriin.

Tietoturvariskienhallinnan keskeiset vaiheet

talous hallinto liitto

Huoltovarmuuskeskus

Seuranta

- Toteuta edellä päätetyt riskienhallintatoimet. Seuraa että aikatauluista pidetään kiinni ja toimenpiteet ovat tehokkaita. Kun toimet edistyvät, muista pitää riskirekisteri ajan tasalla.
- Arvioi miten henkilöstöä tulisi pitää ajan tasalla riskeistä ja heidän roolistaan niiden hallinnassa. Aiemmin tällä kurssilla käsittelimme henkilöstön osaamista ja koulutusta, ja tämä on keskeinen hallintatoimi tietoturva-alueella.
- Sovi koska riskit päivitetään seuraavaksi. Riskirekisteriin tulisi palata vähintään vuosittain, ja arvioida uudelleen edellä kuvattujen vaiheiden kautta tarvittavat muutokset.

Tuumasta toimeen

1. Tee ainakin nämä

talous hallinto liitto

Huoltovarmuuskeskus

Jos yrityksesi vasta aloittelee tietoturvariskienhallintaa, lähde liikkeelle pienin askelin ja pyri tunnistamaan suurimmat riskit:

☑ **Arvioi tärkeimmät tietoturvariskit ja pohdi hallitaanko niitä nyt riittävästi. Tee tarvittavat korjaukset. Eri riskialueita ja mahdollisia hallintatoimia on käsitelty tämän koulutuksen aiemmissa videoissa.**

Tuumasta toimeen
2. Parempi

Kun olette tunnistaneet riskejä, dokumentoi ne, jolloin saat aikaan riskirekisterin:

- ☑ **Ylläpidä tunnistetuista riskeistä riskirekisteriä, jota päivitetään aika-ajoin. Rekisteri luetteloi minimissään riskit, niiden nykyiset hallintatoimet, ja arvion onko nykyinen hallinta riittävää.**
- ☑ **Käytä riskien todennäköisyyksien ja seurausten arviointiin yhtenäistä ohjeistusta ja asteikkoa.**

Tuumasta toimeen
3. Paras

Kun olette päässeet riskienhallinnassa hyvään alkuun, voitte kehittää sitä edelleen seuraavasti:

- ☑ **Määrittele riskienhallintaprosessi ja vuosikello sen toteuttamiseen.**

talous hallinto liitto

Huoltovarmuuskeskus