Harjoitustyö 3, ISMS suunnitelman toteutus

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Kyberturvallisuuden hallinta TTC6020-3007
10.11.2024
Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

Taulukot

1 Johdanto

Tämän harjoitustyön tarkoitus on muodostaa ISO-standardin mukainen tietoturvallisuuden hallintajärjestelmä (ISMS, Information Security Management System) ryhmän käytössä olevaan VLE ympäristöön. ISMS on organisaation strateginen ja operatiivinen väline tietoturvariskien hallitsemiseksi. Tehtävänä ei ole luoda kokonaista kattavaa ISMS-suunnitelmaa vaan muodostaa suunnitelmasta tietty osa, joka on kerrottu tämän labran ohjeessa. Tavoitteena on luoda standardin mukainen suunnitelma, joka kattaa organisaation kyberstrategian, liiketoiminnan, palvelut, rakenteen sekä turvallisuusjohtamisen. Lisäksi tehtävässä käsitellään omaisuuden, uhkien, riskien ja jatkuvuuden hallintaa.

Suunnitelman pohjana käytetään ISO 27000 -standardiperhettä, joka tarjoaa ohjeet turvallisuuden hallintakeinoihin. Suunnitelmassa hyödynnetään ISO-standardin vaatimuksia sekä aikaisempien tehtävien toteutuksia.

Organisaation kuvaus

ISMS suunnitelma toteutetaan DefendByVirtual yritykseen, jonka tavoite on kehittää puolustusmekanismeja ja tarjota koulutuspalveluita yrityksille. Liiketoimintavisio on tietoturvakonsultointipalvelut sekä tietoturvakoulutukset. Yritys tarjoaa tietoturva-asiantuntijoita konsultoimaan erityisesti tietoturvakontrollien arviointiin, suunnittelun ja rakentamiseen. Kouluttamisessa yritys keskittyy ISO-standardin mukaiseen tietoturvallisuuden hallintajärjestelmän (ISMS) koulutuksiin. Kohteena on erityisesti ISO-sertifiointia tavoittelevat yritykset.

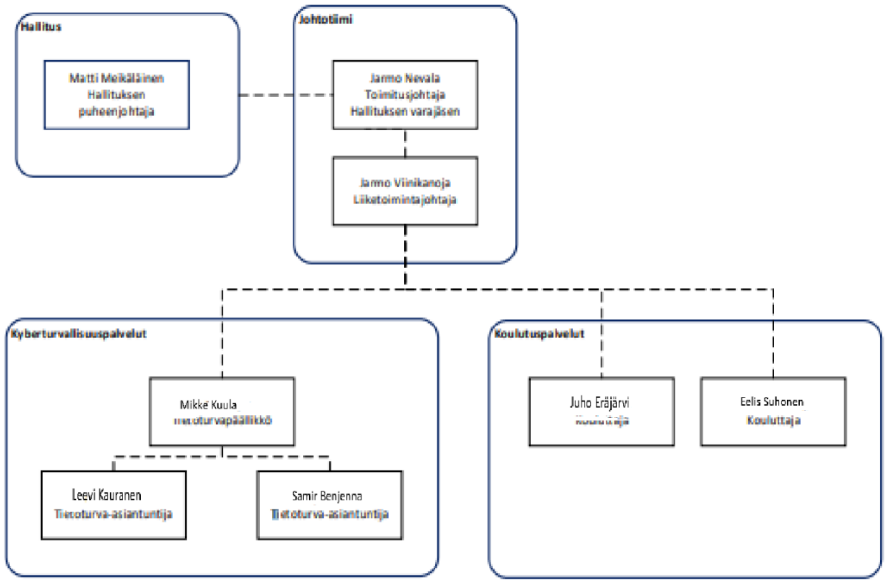
Organisaation rakenne

DefendByVirtualin organisaatio rakenne koostuu kyberturvallisuuspalveluista, koulutuspalveluista ja johdosta. Hallitus huolehtii hallinnon ja toiminnan asianmukaisesta järjestämisestä. Hallituksen jäsenenä ja puheenjohtaja toimii Matti Meikäläinen.

Toimitusjohtajana toimii Jarmo Nevala, joka muodostaa yhdessä teknologiajohtaja Jarmo Viinikanojan kanssa yrityksen johtotiimin. Johtotiimin vastuuna on huolehtia yrityksen operatiivisesta toiminnasta, henkilöhallinnosta, myynnistä sekä markkinoinnista.

Teknologiajohtaja vastaa kyberturvallisuus- sekä koulutuspalveluiden toiminnasta.

Sisäisestä IT:stä ja käyttäjien hallinnasta vastaa tietoturvapäällikkö Mikke Kuula. Tietosuojavastaavina toimivat Leevi Kauranen sekä Samir Benjenna. Alapuolella vielä kuva organisaatio rakenteesta. (Kuvio 1)

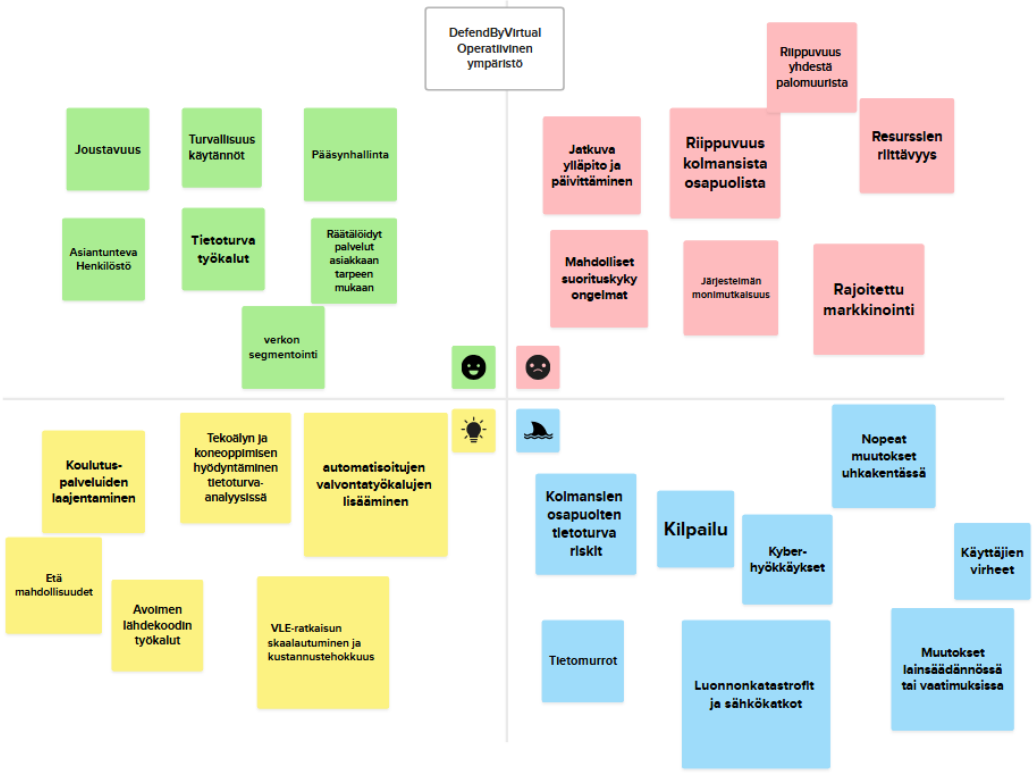


Kuvio 1. Organisaation rakenne

2 Kyberstrategia

Olemme käyttäneet kuviossa 2. SWOT analyysiä kartoittaaksemme operatiivisen ympäristön vahvuuksia, heikkouksia, uhkia sekä mahdollisuuksia. Tämän analyysin avulla saamme kokonaiskuvan siitä, missä ympäristömme on vahvimmillaan ja, missä on mahdollisia kehityskohteita. SWOT-analyysi (kuvio 2) auttaa tunnistamaan alueet, joilla turvallisuutta ja resilienssiä voidaan parantaa, sekä mahdollisuudet, joilla voimme lisätä ympäristön kykyä vastata nopeasti uhkiin ja hyödyntää uusia teknologioita.

SWOT analyysi



Kuvio 2. Swot analyysi

Tietoturvapolitiikka (julkinen)

Yrityksen tietoturvapolitiikka on keskeisessä osassa tietoturvan hallinnointia. Se määrittelee tietojen turvaamisen tavoitteet, vastuut, toteutuksen ja seurannan. Tietoturvapolitiikka on kaikkien työntekijöiden, jäsenten ja yhteistyökumppanien käytössä ja sen noudattamista edellytetään.

2.1.1 Tietoturvan merkitys organisaatiolle

Tietoturva on keskeinen osa organisaation liiketoimintastrategiaa, koska sen avulla varmistetaan liiketoiminnan jatkuvuus ja ylläpidetään asiakkaiden sekä sidosryhmien luottamusta. Digitaalisessa toimintaympäristössä organisaation tiedot, järjestelmät ja palvelut ovat jatkuvasti alttiina uhkille, kuten tietomurroille, haittaohjelmille ja palvelunestohyökkäyksille. Näiden uhkien toteutuessa voi syntyä merkittävää taloudellista vahinkoa, mainehaittaa tai toiminnan keskeytymisiä.

Tämän vuoksi on tärkeää, että tietoturvaan panostetaan aktiivisesti ja johdonmukaisesti. Tietoturvan avulla luodaan myös kilpailuetua, sillä asiakkaat ja kumppanit arvostavat organisaatioita, jotka huolehtivat tietojen turvallisesta käsittelystä ja osoittavat sitoutumista korkeatasoiseen tietosuojan toteuttamiseen.

Organisaation johto on sitoutunut panostamaan tietoturvaan, ja toimimaan lainsäädännön mukaisesti.

Työntekijät osallistuvat aktiivisesti tietoturvakäytäntöjen noudattamiseen ja kehittämään osaamistaan tietoturvan varmistamisessa.

Varmistetaan, että tiedot ovat suojattuja, tarkkoja ja saatavilla asianmukaisille henkilöille. Näin varmistetaan tietojen luottamuksellisuus, eheys ja saatavuus.

Organisaation tietoturvakäytäntöjä tarkastellaan ja päivitetään säännöllisesti.

Yritysturvallisuus

Tapahtumaloki ja seuranta: Tietojärjestelmistä kerätään lokitietoja, joita analysoidaan reaaliajassa tietoturvauhkilta suojautumiseksi. Elastic SIEM on keskeinen työkalu tapahtumalokien seurannassa.

Poikkeamien havainnointi: Järjestelmään on sisällytetty automaattisia hälytyksiä, jotka tunnistavat epäilyttävän toiminnan.

Vaste ja eskalaatio: Jos poikkeama havaitaan, tietoturvatiimi reagoi nopeasti ja tarvittaessa eskaloi tilanteen korkeammalle tasolle. Poikkeamista ollaan myös yhteydessä olennaisille sidosryhmille sellaisen sattuessa.

Jatkuva valvonta: Valvontajärjestelmiä päivitetään säännöllisesti vastaamaan kehittyviin uhkiin. Hyödynnetään myös erilaisia kyberuhkatiedon menetelmiä, jotta pysytään ajan tasalla esiintyvistä uhkista.

3 Suojattavan omaisuuden hallinta

Omaisuudenhallinta DefendByVirtual yrityksessä on määritelty aiemmin luomassamme raportissa (Asset Management) ja Excel-taulukossa, joka pitää sisällään omaisuuserät ja niiden luokittelun. Mainittua materiaalia (Omaisuuksienhallinta raportti ja taulukko) käytetään tässä pohjana. Alla omaisuudenhallinnan eri vaiheet, jotka perustuvat ISO 27001 ja ISO 27002- standardeihin.

Omaisuuksien hallinta on tärkeä osa tietoturvallisuuden hallintajärjestelmää (ISMS), koska siinä oleviin omaisuuserien tunnistamiseen ja luokitteluun, hallintajärjestelmän muut kohdat perustuvat, kun tiedetään turvattavat asiat. Omaisuuksien hallinta siis kertoo organisaation laajuuden ja laittaa sen omaisuuserät, kuten tieto, henkilöstö ja laitteet, tärkeysjärjestykseen.

Omaisuudenhallinnan tavoitteena on varmistaa kaikkien omaisuuserien listaaminen ja kategorointi niiden tärkeyden ja ominaisuuksien mukaan. Näin saadaan tietoon tärkeimmät omaisuuserät,

jotta organisaatio voi suojata kriittisiä tietojaan. Omaisuudenhallinta on tärkeässä osassa myös, jos tavoitellaan ISO 27001 -sertifiointia. (Max Edwards. 2023)

Omaisuudenhallinta yrityksessä

Omaisuusluettelo: Organisaation kaikki tieto-omaisuus ja niihin liittyvät fyysiset tai digitaaliset omaisuuserät (esim. palvelimet, tietokannat, tallennusvälineet) yksilöidään ja dokumentoidaan. Omaisuusluettelo on jatkuvasti ylläpidettävä ja ajantasainen. Se sisältää omaisuuserien nimet, sijainnin, tiedon luokituksen, omistajat ja prosessit, joihin omaisuuserä liittyy.

Tietojen luokittelu ja omistajuus: Tieto-omaisuus luokitellaan arkaluonteisuuden ja käytön perusteella (esim. salainen tai julkinen tieto), ja jokaiselle omaisuuserälle määritetään vastuullinen omistaja. Omistajan vastuulla on varmistaa, että tietojen käsittely ja suojaus noudattavat organisaation tietoturvavaatimuksia.

Omaisuuserien käytön hallinta: Dokumentoidaan ja viestitään hyväksyttävän käytön säännöt tietojen ja niihin liittyvien omaisuuserien käsittelylle. Tämä sisältää muun muassa pääsyoikeudet, tietojen suojauksen ja niiden oikean käytön. Henkilöillä, joilla on pääsy tietoihin, on oltava asianmukainen koulutus ja tietoturvakäytäntöjen tuntemus.

Omaisuuden palauttaminen: Työsuhteen tai sopimuksen päättyessä varmistetaan, että kaikki organisaation omaisuus, mukaan lukien fyysiset laitteet ja digitaaliset tiedot, palautetaan asianmukaisesti. Tämän prosessin osana varmistetaan, että organisaation tiedot poistetaan turvallisesti työntekijän hallusta ja ettei mitään ole jäänyt työntekijän käyttöön.

Tietojen siirto ja hävitys: Organisaatio määrittää menettelyt turvalliselle tietojen siirrolle ja hävittämiselle. Tämä kattaa sekä sähköisen siirron että fyysisten tallennusvälineiden käsittelyn, ja menettelyissä otetaan huomioon tietojen luokittelu ja arkaluonteisuus. Tallennusvälineet ja tiedot hävitetään turvallisesti, jotta estetään tietojen väärinkäyttö tai päätyminen ulkopuolisille.

Suojattavan omaisuuden luokittelu ISMS

Taulukkoon (Taulukko 1) valitut omaisuuserät ovat PaloAlto, ElasticSIEM, Kali-WS, Palvelimet, Verkkoyhteydet, Asiakastiedot ja Henkilöstö. Organisaation omaisuuksien luokittelu on tehty kolmella tavalla liittyen omaisuuserien ominaisuuksiin ja niiden kriittisyyteen liiketoiminnan kannalta. Taulukossa Kali-WS eli Linux-käyttöjärjestelmällä operoiva työasema on luokiteltu vähemmän kriittiseksi, luokkaan 3, kun asiakastiedot on merkitty 5 eli kriittisimpään luokkaan. Luokittelun perustana on tietyn omaisuuserän vaikutus organisaation toimintaan/liiketoimintaan. Kali-WS on tarpeellinen organisaatiolle penetraatiotestauksen ja muuten, sisäverkon konfiguroinnin kannalta, mutta se ei ole suoraan yhteydessä esimerkiksi yrityksen nettisivuston kaatumiseen. Asiakastietojen vuotaminen taas olisi organisaation maineen kannalta kriittinen isku, jolla olisi suora vaikutus liiketoimintaan.

3.1.1 Omaisuuden merkitysluokittelu

- **Ensisijaiset omaisuudet (Primary Assets)**: Omaisuuserät, jotka vaikuttavat suoraan ja kriittisesti organisaation liiketoimintaan.
  → Esimerkkejä: Kriittiset tiedot ja liiketoimintaan suoraan liittyvät resurssit.

- **Tukiomaisuudet (Supporting Assets)**: Omaisuudet, jotka ovat keskeisiä ja tukevat toimintaa, mutta eivät vaikuta siihen täysin suoraan.
  → Esimerkkejä: Laitteistot, ohjelmistot ja henkilöstö.

3.1.2 Omaisuuden kriittisyyden luokittelu (asteikolla 1–5)

- **Arvo 5**: Todella kriittinen omaisuus – erittäin tärkeä organisaation toiminnan jatkuvuudelle.
- **Arvo 3**: Melko kriittinen omaisuus – tärkeä, mutta ei täysin välttämätön organisaatiolle.
- **Arvo 1**: Vähemmän tärkeä omaisuus – ei merkittävää vaikutusta toiminnan kannalta.

3.1.3 ISO-standardiin perustuva omaisuusluokittelu

a. Laitteisto

→ Fyysiset laitteet, kuten palvelimet ja työasemat.

b. Ohjelmistot

→ Tietojärjestelmät ja ohjelmistot, esimerkiksi ElasticSIEM.

c. Infrastruktuuri

→ Verkkoyhteydet ja palvelimet, jotka mahdollistavat tietojärjestelmien toiminnan.

d. Tiedot

→ Organisaatiossa liikkuvat ja käytettävät tiedot, kuten asiakastiedot, jotka ovat olennaisia liiketoiminnalle.

e. Ihmiset

→ Organisaation henkilöstö sekä siihen liittyvät sidosryhmät.
(ISO_27002FIN. Sivu 10. 2022)

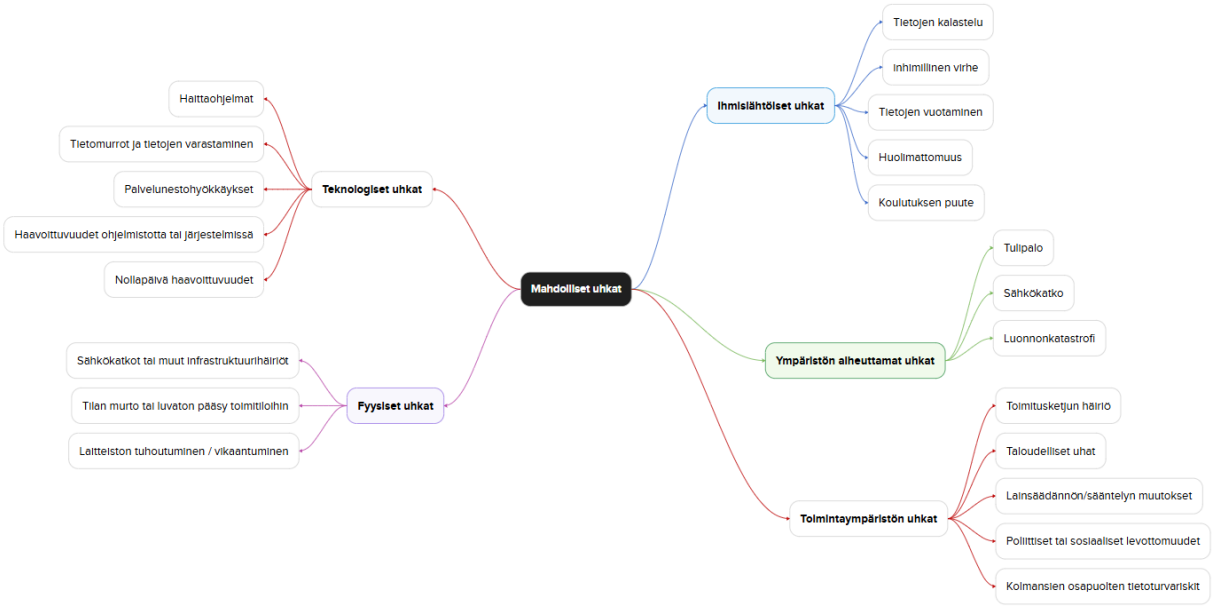
Resurssi	Kuvaus	Luokittelu	Kriittisyys	ISO Omaisuusluokittelu	Perustelut
PaloAlto (Palomuuri)	Virtuaalinen palomuuri	Ensisijainen omaisuus	5	Laitteisto, Ohjelmisto	Tärkein puolustuslinja VLE-ympäristön ja ulkoisen verkon välillä.
ElasticSIEM	Tietoturvatapahtumien hallinta- ja seurantatyökalu	Ensisijainen omaisuus	5	Ohjelmisto	Keskitetty tapa seurata tietoturvatapahtumia eri järjestelmistä.
Kali-WS	Työasema penetraatiotestaukseen	Tukiomaisuus	3	Ohjelmisto, Laitteisto	Tarpeellinen haavoittuvuuksien testaamisessa ja järjestelmän konfiguroinnissa.
Palvelimet (GNA)	Palvelimet ja tietojärjestelmät	Ensisijainen omaisuus	5	Laitteisto, Ohjelmisto, Infrastruktuuri	Palvelevat kriittisiä tietoja ja toimintoja järjestelmässä.
Verkkoyhteydet (GNA)	Tietoliikenteen mahdollistaja	Tukiomaisuus	4	Infrastruktuuri, Palvelut	Verkkoyhteys välttämätön tietoliikenteelle ja järjestelmän toiminnalle.
Asiakastiedot	Asiakasrekisterit ja -tiedot	Ensisijainen omaisuus	5	Tieto, Ihmiset	Ensisijaisen tärkeät tiedot liiketoiminnalle.
Henkilöstö	Työntekijät ja asiantuntijat	Tukiomaisuus	5	Ihmiset	Osaava henkilökunta on organisaation toiminnalle kriittistä.

Taulukko 1. Omaisuuksien luokittelu

4 Uhkien hallinta

Uhkien hallinta toteutetaan ensin kartoittamalla mahdolliset uhat, joita saattaa kohdistua organisaatioon, sekä mahdollinen seuraus uhan toteutuessa. Tämän jälkeen listataan resurssit ja niihin vaikuttavat uhat. Tunnistetaan haavoittuvuudet, joita organisaatiosta löytyy ja, joita uhka saattaa hyödyntää. Seuraavaksi arvioidaan uhkan vaikutus omaisuutta kohtaan, johon se kohdistuu. Kun aiemmat vaiheet on suoritettu, laaditaan toimenpiteitä uhkien torjumiseksi ja vaikutuksen minimoimiseksi, kuten uhkien ehkäisyyn, havaitsemiseen ja reagointiin liittyvät toimet.

Kuviossa 3 on mindmap-tyylisesti lueteltuna yrityksen mahdolliset uhkat.



Kuvio 3. Yrityksen mahdolliset uhkat

Kuviossa 4 on määritelty resursseja, niihin mahdollisesti kohdistuvia uhkia ja niiden tyyppejä.

Resurssi	Mahdollinen uhka	Vaikutuksen tyyppi	Uhkan mahdollisesti hyödynnettävä haavoittuvuus	Seuraus
PaloAlto	Haittaohjelmat, Palvelunestohyökkäykset, Haavoittuvuudet ohjelmistossa tai järjestelmässä	Suora	Konfigurointivirheet,päivittämät tömät tietoturvapäivitykset	Estää verkkoliikenteen suodatuksen ja aiheuttaa verkon suojausongelmia
ElasticSiem	Nollapäivähaavoittuvuudet, tietomurrot, Haavoittuvuudet ohjelmistossa	Epäsuora	Päivittämätön ohjelmisto, puutteellinen lokitietojen valvonta	Voi menettää näkyvyyden tietoturvatapahtumiin
Kali-WS	Luvaton pääsy, ohjelmistovirheet	Suora	Heikko käyttöoikeuksien hallinta	Haavoittuvuuksien testaamisen keskeytyminen, järjestelmän väärinkäyttö
Palvelimet(GNA)	Sähkökatkot, tietomurrot, haittaohjelmat, luvaton pääsy	Suora	Varajärjestelmän puute, puutteellinen virustorjunta	Palvelun keskeytyminen ja tietojen menetys
Verkkoyhteydet(GNA)	Infrastruktuurihäiriöt, palvelunestohyökkäykset	Epäsuora	Rajalliset verkkovalvontajärjestelmät	Yhteyksien katkeaminen, liiketoiminnan keskeytyminen
Asiakastiedot	Tietojen kalastelu, tietojen vuotaminen	Suora	Heikko salaus, henkilöstön tietoturvatietoisuuden puute	Asiakasluottamuksen menetys ja tietovuotoriski
Henkilöstö	Inhimilliset virheet, koulutuksen puute	Epäsuora	Väärin asennettu ohjelmisto, tietojen tahaton vuotaminen	Tietojen vuotaminen, hyökkääjän pääsy järjestelmiin

Kuvio 4. Resurssien uhkat

5 Riskienhallinta

Riskienhallinta organisaatiossa kattaa uhkien tunnistamisen, riskien arvioinnin ja riskitasojen hallinnan tasolle, joka ei vaaranna organisaation liiketoimintaa. Riskienhallintaprosessi on sitoutettu organisaation turvallisuustavoitteisiin ja prosesseihin sekä lainsäädännön ja säädösten noudattamiseen. Hyödynnämme tässä ISO 31000-standardissa kuvattua riskienhallintaprosessia, johon kuuluu seuraavat vaiheet.

- **Toimintaympäristön kuvaus:** Toimintaympäristön määrittelyvaiheessa tehdään riskien arvioinnin rajaukset, kuten mitä sisällytetään arviointiin. Määritellään riskikriteerit

- **Riskien arviointi:** Riskien arviointiin kuuluu riskien tunnistaminen, riskianalyysi sekä riskin merkityksen arviointi
    - **Riskien tunnistaminen:** Havaitaan kaikki merkittävät riskit ja niiden lähteet, vaikutusalueet, tapahtumat ja syyt sekä mahdolliset seuraukset
    - **Riskianalyysi:** Muodostetaan käsitys tunnetuista riskeistä. Tarkastellaan riskin syitä ja lähteitä, arvioidaan riskin seurauksia sekä riskin toteutumisen todennäköisyyttä ja vaikutusta hyödyntämällä ISO 31000-standardin mukaista riskimatriisia
    - **Riskien merkityksen arviointi:** Tavoite on helpottaa päätösten tekoa siitä mitä riskejä on tarpeen käsitellä ja missä järjestyksessä.

- **Riskien käsittely:** Määritellään hallintakeinoja riskien vähentämiseksi hyväksyttävälle tasolle.

- **Seuranta:** Toimintaympäristön sisäisten ja ulkoisten muutosten sekä riskien muutosten havaitseminen. Voidaan määrittää määräväli, jolloin katselmointi- ja seurantatoimia suoritetaan.

- **Viestintä ja tiedonvaihto:** Viestitään toimintaympäristöön ja riskeihin liittyvien eri osapuolten välillä. Varmistetaan, että tieto riskeistä tavoittaa ne osapuolet, joille tämä tieto on oleellista.

ISO 31010-standardin mukaisessa riskienhallintataulukossa (Kuvio 5) on arvioitu uhkien riskitasot ja hallintakeinot sekä riskijäännös.

Uhka	Vaikutus (1-3)	Todennäköisyys (1-3)	Riskitaso (vaikutus x todennäköisyys)	Kontrolli	Kontrollin vaikutus	Riskijäännös	Riskin omistaja
Haittaohjelmat	2	2	4	Palomuuri ja muut haittaohjelmien torjuntaohjelmat	1	2	Tietoturvapäällikkö
Tietomurrot	3	2	6	Tunkeutumisen havainnointi ja ehkäisyjärjestelmät	2	2	Tietoturvapäällikkö
Sähkökatkot	2	1	2	Varavoimajärjes-telmä	1	1	Toimitusjohtaja
Inhimillinen virhe	2	2	4	Henkilöstön koulutus ja automaattinen tallennus	1	2	Tietoturvapäällikkö, liiketoimintapäällik-kö
Palvelunesto hyökkäykset	3	3	9	DDoS-suojauspalvelu	1	6	Tietoturvapäällikkö
Luonnonkatastrofi	3	1	3	Varautumissuunnitelma, hajautettu infrastruktuuri	2	1	Toimitusjohtaja
Tietojen kalastelu	3	3	9	Henkilöstön koulutus	1	6	Tietoturvapäällikkö
Toimitusketjun häiriöt	3	2	6	Toimittajien riskinhallinta, varmuustoimittajat	2	2	Liiketoimintapäällik-kö
Laitteiston vikaantuminen	3	2	6	Ennakoiva ylläpito	1	4	Liiketoimintapäällik-kö
Tulipalo	3	2	6	Hälytys- ja sprinklerijärjestel-mät	2	2	Liiketoimintapäällik-kö

Kuvio 5. Riskienhallintataulukko

5.1.1 Riskimatriisi

Riskienhallintaa voidaan myös havainnollistaa riskimatriisin avulla. Matriisissa riskit luokitellaan todennäköisyyden ja vaikutuksen kertoimella (riskitaso). Riskit saavat liikennevalo-värikoodin perustuen niiden riskitasoon. Värit voidaan jakaa riskeille myös vaadittujen toimenpiteiden, ja kyseisten toimenpiteiden kiireellisyyden mukaan.

Esimerkiksi suurempien sähkökatkojen todennäköisyys on pieni

Todennäköisyys (y) \ Vaikutus (x)	1 (Matala)	2 (Keskitaso)	3 (Korkea)
3 (Korkea)	Luonnonkatastrofi 3	Tietomurrot 6	Palvelunesto hyökkäys 9
2 (Keskitaso)	Inhimillinen virhe 2	Haittaohjelmat 4	Toimitusketjun häiriöt 6
1 (Matala)	Sähkökatkot 1	Laitteiston vikaantuminen 2	Tietojen kalastelu 3

6 Jatkuvuuden hallinta

Organisaatioiden omaisuuserien suojaaminen ja liiketoiminnan jatkuvuuden varmistaminen ovat keskeisiä osia nykyaikaisessa riskienhallinnassa. Yksi tärkeä osa-alue on jatkamis- ja palautussuunnitelman kehittäminen omaisuuserille, joilla on tunnistettu merkittävä riskijäännös. Riskijäännös on riskienhallinnan vaihe, jossa kaikki toimenpiteet eivät täysin poista riskiä, vaan jäljelle jäävä riski on edelleen arvioitava ja hallittava.

Tässä luvussa tarkastellaan, kuinka suoritetaan kohteen jatkamis- ja palautussuunnitelma tilanteessa, jossa riskijäännös on todettu liian korkeaksi. Käsittelemme omaisuuserälle tehtävää BIA-analyysiä (Business Impact Analysis), jossa arvioidaan kohteen liiketoiminnallista merkitystä ja sen mahdollisen toimintakatkoksen vaikutuksia. Näiden tietojen perusteella laaditaan konkreettinen jatkamis- ja palautussuunnitelma, joka sisältää toimenpiteet mahdollisten häiriöiden tai keskeytysten varalta.

Lisäksi käsittelemme suunnitelman testausvaihetta, jossa harjoitellaan ja varmistetaan toimintamallien tehokkuus mahdollisen katastrofitilanteen varalta. Testauksen ja harjoittelun avulla voidaan tunnistaa suunnitelman mahdolliset puutteet ja kehittää sitä edelleen, jotta organisaatio on valmis palauttamaan kriittiset toiminnat mahdollisimman nopeasti ja tehokkaasti häiriötilanteessa.

Kuviossa 6 on kuvattu omaisuuteen kohdistuvaa uhkaa ja sen aiheuttamaa riskijäännöstä.

Uhka	Kontrolli	Riskijäännös	Altistuvat omaisuudet
Haittaohjelmat	Palomuuri ja muut haittaohjelmien torjuntaohjelmat	2	PaloAlto, Kali-WS, Palvelimet
Tietomurrot	Tunkeutumisen havainnointi ja ehkäisyjärjestelmät	2	Asiakastiedot, Palvelimet, Henkilötiedot
Sähkökatkot	Varavoimajärjestelmä	1	Palvelimet, Kali-WS, Verkkoyhteydet,
Inhimillinen virhe	Henkilöstön koulutus ja automaattinen tallennus	2	Henkilöstö, Asiakastiedot,
Palvelunesto hyökkäykset	DDoS-suojauspalvelu	6	PaloAlto, Palvelimet, Verkkoyhteydet,
Luonnonkatastrofi	Varautumissuunnitelma, hajautettu infrastruktuuri	1	Verkkoyhteydet, Palvelimet,
Tietojen kalastelu	Henkilöstön koulutus	6	Asiakastiedot, Henkilöstö,
Toimitusketjun häiriöt	Toimittajien riskinhallinta, varmuustoimittajat	2	
Laitteiston vikaantuminen	Ennakoiva ylläpito	4	Palvelimet, Kali-WS, Verkkoyhteydet, PaloAlto, ElasticSiem
Tulipalo	Hälytys- ja sprinklerijärjestelmät	2	Palvelimet, henkilöstö,

Kuvio 6. Omaisuus-riskijäännös taulukko

Riskijäännökset on luokiteltu seuraavasti.

- **0–2:** Pieni riski
- **3–5:** Keskisuuri riski
- **6–7**: Suuri riski
- **8–9:** Erittäin suuri riski

Riskijäännösten pohjalta tehdään BIA-analyysi (Business Impact Analysis) omaisuuserälle, jolle riskijäännös jää liian suureksi eli 6–9. Otamme esimerkiksi tähän asiakastiedot, johon kohdistuva riskijäännös on 6.

6.1 Asiakastiedot BIA-analyysi

Kuvaus: Asiakastiedot sisältävät asiakkaiden henkilökohtaisia tietoja, yhteystietoja, sopimuksia ja mahdollisesti arkaluonteisia tietoja. Näiden tietojen eheys, luottamuksellisuus ja saatavuus ovat kriittisiä liiketoiminnan toimivuudelle ja organisaation maineelle.

Kriittisyys: Erittäin kriittinen. Asiakastietojen menetys tai tietovuoto voi johtaa merkittäviin taloudellisiin menetyksiin, oikeudellisiin seuraamuksiin ja maineen menetykseen.

Toimintojen keskeytyksen sietokyky: Pieni. Asiakastiedot on oltava saatavilla jatkuvasti, ja kaikki pitkäkestoiset keskeytykset voivat aiheuttaa suuria vahinkoja.

Vaikutukset:

- **Taloudellinen:** Asiakastietojen menetyksestä voi koitua suoria taloudellisia tappioita tietomurtokustannusten ja mahdollisten sakkojen vuoksi.
- **Lainsäädännöllinen ja säätely:** GDPR ja muiden tietosuojalainsäädäntöjen rikkomukset voivat johtaa suuriin sakkoihin.
- **Toiminnallinen:** Asiakaspalvelu voi keskeytyä, ja asiakassuhteet voivat kärsiä tiedon puutteesta.
- **Maineellinen:** Merkittävä haitta brändille ja asiakastyytyväisyydelle

Jatkuvuus- ja palautus suunnitelma

Tehdään seuraavaksi asiakastiedot omaisuuserälle jatkuvuus- ja palautus suunnitelma, jonka avulla on mahdollista minimoida häiriöstä aiheutuvat vaikutukset ja varmistaa nopea toipuminen, jotta liiketoiminta voi jatkua mahdollisimman pienin keskeytyksin.

Tavoitteet ja laajuus:

- Suojaa asiakastietoja vahingonteolta, menetyksiltä ja luvattomalta käytöltä
- Varmistaa, että asiakastiedot ovat palautettavissa nopeasti häiriötilanteen sattuessa
- Varmistaa liiketoiminnan jatkuvuus ja minimoida asiakkaille aiheutuvat vaikutukset
- Noudattaa lainsäädäntöjä ja tietosuojavaatimuksia, kuten GDPR

Varmuuskopiointi ja palautus:

- **ISO/IEC 27002 –standardin mukaan**: “Tiedoista, ohjelmistoista ja järjestelmistä olisi otettava varmuuskopiot ja ne olisi testattava säännöllisesti varmuuskopiointia koskevien kohdennettujen toimintaperiaatteiden mukaisesti”. (ISO_27002FIN. Sivu 111. 2022).

- **Varmuuskopiointikäytännöt**: Määritellään käytännöt, joiden avulla kriittiset tiedot ja ohjelmat saadaan palautettua häiriöiden, laitteiden vikaantumisen tai tietojen menetyksen jälkeen. Käytäntöjen tulee keskittyä tarvittavien varmuuskopioiden tallentamiseen ja palauttamiseen, ja näiden toteutukseen tulee laatia selkeät suunnitelmat.

- **Testaus ja toimivuus**: Varmuuskopioiden toimivuus ja palauttaminen on testattava säännöllisesti. Tallennusvälineet ja palautustoiminnot tulee testata säännöllisesti, jotta toimivuudesta voidaan olla varmoja.

- **Säilytys ja suojaukset**: Varmuuskopioiden on oltava suojattuina ja eri paikassa, organisaation muista tiedoista ja järjestelmistä. Varmuuskopiot tulee suojata katastrofeilta, kuten tulipalolta tai tulvalta, ja niihin käsiksi pääsyä tulee rajoittaa asianmukaisella salauksella.

Riskianalyysi ja keskeiset riskit:

- **Tietomurrot:** Asiakastiedot voivat altistua tietomurroille, joka johtaisi tietojen vuotamiseen tai vahingoittumiseen
- **Inhimillinen virhe:** Huolimaton käsittely, tahattomat muutokset tai poistot voivat vaarantaa asiakastiedot

- **Fyysiset uhat:** Palot, tulvat ja muut ympäristöstä aiheutuvat uhat voivat vahingoittaa fyysisiä tai tietoverkossa olevia asiakastietoja
- **Tekniset häiriöt:** Laitteistojen tai ohjelmistojen vikaantuminen voi estää pääsyn tietoihin tai johtaa tiedon menetykseen

Toimintasuunnitelma häiriötilanteessa

Tietomurron varalta:

- **Vaihe 1: Havaitseminen ja eristäminen:** Mikäli havaitaan tietomurto, se pysäytetään mahdollisimman pian. Tarvittaessa kytke tietojärjestelmä offline-tilaan.
- **Vaihe 2: Ilmoittaminen:** Ilmoita tietoturvasta vastaaville henkilöille ja tarvittaessa tietosuojavaltuutetulle ja asiakkaille tietovuodosta.
- **Vaihe 3: Korjaavat toimenpiteet:** Analysoi murron syy ja vahvista suojaustoimenpiteet, esimerkiksi paranna palomuuria tai tunnistusjärjestelmiä.
- **Vaihe 4: Tiedon palauttaminen:** Palauta asiakastiedot viimeisimmästä varmuuskopiosta, jos tiedot ovat vaurioituneet tai kadonneet.

Fyysisten uhkien varalta:

- **Tietojen suojaus:** Sijoita asiakastietoja sisältävät palvelimet turvallisiin tiloihin, joissa on palosuojaus, varavoima ja fyysiset turvajärjestelyt. Tässä tapauksessa varmistetaan, että palvelun tarjoaja täyttää nämä vaatimukset.
- **Tietojen varmuuskopiointi:** Varmista, että tiedoista tehdään säännölliset varmuuskopiot ja niitä säilytetään erillisessä sijainnissa tai pilvipalvelussa.
- **Palauttaminen:** Mikäli tiedot vahingoittuvat, käytä varmuuskopioita niiden palauttamiseen.

Inhimillisen virheen varalta:

- **Ennaltaehkäisevät toimet:** Kouluta henkilöstöä laitteiden sekä asiakirjojen oikeaoppiseen käsittelyyn ja huolehtimiseen. Varmista, että järjestelmissä on oikeat käyttöoikeudet- ja rajoitukset sekä, että päivitykset ovat kunnossa.
- **Tiedon palauttaminen:** Versionhallinta ja säännöllisin ajoin tehty varmuuskopiointi, jotta vioittuneet tai poistuneet tiedot saadaan palautettua.

Testaus ja harjoitukset:

- **Toimintasuunnitelman testaus:** Jatkuvuussuunnitelma testataan puolen vuoden välein, jotta varmistutaan suunnitelman toimivuudesta. Myös henkilöstön valmiutta testataan ja esimerkiksi varmuuskopiointiin tarvittavien laitteiden toimivuudesta varmistutaan. Testataan esimerkiksi simulaation avulla, kuinka tietomurto vaikuttaa järjestelmään ja kuinka nopeasti se saadaan palautettua normaaliin tilaan.

- **Harjoitusten arviointi:** Harjoituksen tulokset arvioidaan, kerätään henkilöstön omat arviot siitä, ja parannetaan suunnitelmaa tarpeen vaatiessa. Tavoitteena on tunnistaa mahdolliset puutteet, joiden avulla kehitetään jatkuvuuden hallintaa parempaan suuntaan. Uuden suunnitelman avulla pitäisi saada turvattua liiketoiminnan jatkuvuus mahdollisesti vieläkin nopeammin ja tehokkaammin häiriötilanteen jälkeen.

7 Jatkuva hallinta

Tämä kappale käsittelee ISMS:n jatkuvan hallinnan ja parannusten toteutusta PDCA-mallin mukaisesti. Mallin tavoitteena on varmistaa tietoturvakäytäntöjen ja kontrollien ajantasaisuus sekä riskienhallinnan tehokkuus organisaatiossa. Vuosikellon (Taulukko 2.) avulla jäsennellään säännölliset parannustoimet, ja seurantajärjestelmän avulla varmistetaan läpinäkyvä raportointi ja nopeat reaktiot havaittuihin riskeihin.

Kuukausi	Parannustoimi
Tammikuu	Riskien arviointi ja omaisuuskartoituksen päivitys
Maaliskuu	Tietoturvapolitiikan katselmointi ja päivitys
Toukokuu	Haavoittuvuustestauksen toteutus

Heinäkuu	Henkilöstön tietoisuus- ja koulutustarkistus
Syyskuu	Sisäisten auditointien toteutus ja tulosten analysointi
Marraskuu	Järjestelmän parannusehdotusten valmistelu ja arviointi
Joulukuu	Seuraavan vuoden toimenpiteiden suunnittelu

Taulukko 2. Vuosikello

7.1.1 Seuranta ja raportointi

Seurantaa ja raportointia suoritetaan säännöllisesti.

Seuranta: Säännöllinen katselmus, jossa käydään läpi tietoturvapoikkeamat, toteutetut kontrollit ja niiden toimivuus. Seurantaan käytetään tikettijärjestelmää, jotta jokainen poikkeama ja kehityskohde tulee dokumentoitua ja niiden tilaa seurataan jatkuvasti. Tikettijärjestelmän avulla havaintojen käsittely ja seuranta pysyvät läpinäkyvinä, mikä tukee nopeampaa reagointia ja auttaa kohdistamaan resurssit oikein.

Raportointi: Kuukausittainen raportointi, jossa esitellään toteutetut toimenpiteet, havaitut riskit ja parannusehdotukset riskien minimoimiseksi. Raportoinnissa korostetaan parannustoimien priorisointia, jotta resurssit saadaan kohdennettua kriittisimpiin kehityskohteisiin. Raportit antavat selkeän tilannekuvan siitä, kuinka hyvin toteutetut tietoturvakontrollit vastaavat yrityksen turvallisuustavoitteisiin ja mahdollisiin sääntelyvaatimuksiin

Lähteet

Max Edwards. What is the objective of Annex A.8.1? ISMS online artikkeli. 2023. Viitattu 31.10.2024. https://www.isms.online/iso-27001/annex-a-8-asset-management/

Liitteet

Liite 1. Liitteen otsikko

ISO_27001FIN.pdf