SECRISK riskien arviointimenetelmän tarkoitus

SecMeter Riskien Arviointi SECRISK on yleiskäyttöinen yrityksen riskien tunnistamiseen, arviointiin, käsittelyyn ja seurantaan tarkoitettu täytettävä riskienhallintatyökalu.

SECRISK eroaa monista perinteisistä riskienarviointimenetelmistä, joissa lähdetään liikkeelle uhista tai tarkastuslistakysymyksistä. SECRISKissä lähtökohtana on yrityksen oma tavoitetila, ja arviointikysymys johdetaan siitä.

Menetelmän avulla voidaan:

- tunnistaa riskit
- arvioida tavoitetilan ja nykytilan välinen poikkeama
- arvioida riskin todennäköisyys ja vaikuttavuus
- luokitella riskit automaattisesti
- seurata korjaavia toimenpiteitä
- muodostaa automaattinen riskimatriisi
- tunnistaa yrityksen merkittävimmät riskit

Menetelmän rakenne

Menetelmä sisältää:

- Raporttisivun
- Riskimatriisin
- 50 riskikorttia

Lähtötietojen täyttäminen

Täytä seuraavat tiedot:

- Arvioitavan yrityksen nimi
- Arvioinnin kohteena oleva toiminto tai yksikkö.
- Arvioitava kokonaisuus.
- Arvioinnin suorittajan nimi.
- Arvioinnin päivämäärä.

Riskikortin täyttäminen

SECRISK-menetelmä perustuu ajatukseen, että riski ei synny pelkästään uhasta tai tapahtumasta, vaan tavoitetilan ja nykytilan välisestä poikkeamasta. Arvioijan tehtävä ei ole keksiä tavoitetiloja itse, vaan selvittää ne yrityksen omista ohjaavista dokumenteista, päätöksistä ja käytännöistä.

Arvioijan tulee ensisijaisesti määrittää tavoitetila yrityksen strategian, tavoitteiden, politiikkojen, prosessikuvausten, työohjeiden, standardien, viranomaisvaatimusten sekä vastuuhenkilöiden haastattelujen perusteella. Riski muodostuu operatiivisessa toiminnassa havaitusta tavoitetilan poikkeamasta. Jokainen riskikortti käsittelee yhtä riskiä.

Arvioinnin ensimmäinen vaihe on selvittää tavoitetilat

Arvioija selvittää ensin:

- Mitä yritys tavoittelee?
- Mitä yritys pitää hyväksyttävänä toimintatapana?
- Mitä yritys on itse päättänyt tehdä?
- Mitä vaatimuksia toimintaan kohdistuu?

Lähteitä voivat olla:

- strategia
- politiikat
- prosessikuvaukset
- työohjeet
- mittarit
- palvelutasot
- viranomaisvaatimukset
- standardit
- johdon päätökset
- haastattelut

Tässä vaiheessa ei vielä arvioida mitään.

Tavoitetilan määrittely

Esimerkki:

- Kaikissa kriittisissä järjestelmissä käytetään monivaiheista tunnistautumista.

Tämä on tavoitetila.

Tavoitetilasta johdetaan arviointikysymys

Kun arvioinnin kohteena olevat tavoitetilat ovat selvillä ja kirjattu SECRISK riskikorteille, muodostetaan arviointikysymys, esimerkiksi:

- Käytetäänkö kaikissa kriittisissä järjestelmissä monivaiheista tunnistautumista?

Arviointikysymys on siis työkalu tavoitetilan todentamiseen.

Selvitetään nykytila

Esimerkiksi:

- MFA on käytössä vain osassa kriittisiä järjestelmiä.

Määritellään poikkeama

Poikkeama tarkoittaa nykytilan ja yrityksen määrittelemän tavoitetilan välistä eroa. Esimerkissä poikkeama syntyy siitä, että kaikissa kriittisissä järjestelmissä ei käytetä MFA:ta.

Poikkeaman kuvaus

Poikkeamat kuvataan poikkeaman kuvaus kentässä. SECRISK menetelmässä suositellaan käytettäväksi seuraavia yhdenmukaisia poikkeamakuvauksia.

Tavoitepoikkeama

Yrityksen asettamaa tavoitetta ei saavuteta. Esimerkki:

Tavoite: toimitusvarmuus 98 %

Toteuma: 91 %

Poikkeama:

toimitusvarmuustavoite ei täyty

Prosessipoikkeama

Toimintaprosessi ei toteudu sovitulla tavalla.

Esimerkki:

hyväksymiskierros jää tekemättä

asiakaspalautteita ei käsitellä määräajassa

Menettelytapapoikkeama

Työohjetta, politiikkaa tai sääntöä ei noudateta.

Esimerkki:

käyttöoikeuksien poistoprosessi jätetään tekemättä

tarkastuslista täytetään puutteellisesti

Tekninen poikkeama

Järjestelmä, laite tai tekninen ratkaisu ei toimi tavoitetilan mukaisesti.

Esimerkki:

varmuuskopiointi epäonnistuu

MFA ei ole käytössä vaaditussa järjestelmässä

Resurssipoikkeama

Tarvittavat resurssit eivät vastaa tavoitetilaa.

Esimerkki:

henkilöstöä liian vähän

osaaminen puutteellista

budjetti ei riitä

Osaamispoikkeama

Henkilöstön osaaminen ei vastaa tavoitetilaa.

Esimerkki:

koulutus suorittamatta

vaadittua pätevyyttä ei ole

Vastuupoikkeama

Vastuut ovat epäselvät tai niitä ei toteuteta.

Esimerkki:

riskin omistajaa ei ole nimetty

seuranta jää tekemättä

Tiedonhallintapoikkeama

Tieto on puutteellista, virheellistä tai ei kulje.

Esimerkki:

dokumentti vanhentunut

muutoksesta ei tiedoteta

Mittaripoikkeama

Suorituskykymittari poikkeaa tavoitetasosta.

Esimerkki:

reklamaatiotavoite ylittyy

käyttöaste jää tavoitteesta

Vaatimuspoikkeama

Lainsäädännön, standardin, asiakkaan tai yrityksen vaatimuksen täyttyminen ei toteudu.

Esimerkki:

ISO-vaatimus täyttymättä

NIS2-vaatimus puuttuu

sopimusvaatimus ei toteudu

Nykytilan arviointi

Koska SECRISK perustuu tavoitetilan arviointiin, Nykytilan arvio ei saisi perustua arvioijan mielipiteeseen vaan siihen, kuinka hyvin nykytila vastaa tavoitetilaa. Arviointiohjeena suositellaan seuraavia kriteerejä.

Erinomainen 100 %

Tavoitetila toteutuu täysin.

- vaatimus täyttyy kokonaan
- toiminta on vakiintunutta
- näyttöä toteutumisesta on saatavilla
- poikkeamia ei havaita

Esimerkki:

Tavoitetila:

Kaikissa kriittisissä järjestelmissä käytetään MFA:ta.

Nykytila:

MFA käytössä kaikissa kriittisissä järjestelmissä.

Valinta:

Erinomainen

Hyvä 75–99 %

Tavoitetila toteutuu pääosin.

- pieniä puutteita
- poikkeamat eivät merkittävästi heikennä tavoitetilan toteutumista

Esimerkki:

MFA käytössä 95 %:ssa kriittisistä järjestelmistä.

Valinta:

Hyvä

Tyydyttävä 50–74 %

Tavoitetila toteutuu osittain.

- merkittäviä puutteita
- tavoitetila ei toteudu kaikilta osin
- riski on hallittavissa

Esimerkki:

MFA käytössä noin puolessa kriittisistä järjestelmistä.

Valinta:

Tyydyttävä

Heikko alle 50 %

Tavoitetila toteutuu vain vähäisessä määrin.

- vakavia puutteita
- toiminta ei vastaa yrityksen tavoitteita

Esimerkki:

MFA käytössä vain yksittäisissä järjestelmissä.

Valinta:

Heikko

Arvioimatta

Valitaan jos näyttöä ei ole saatavilla, esimerkiksi

- arviointia ei ole vielä tehty
- tietoa ei ole riittävästi

Kehityssuunnan arviointi

SECRISK-ajattelussa kehityssuunnan arvio ei kuvaa nykytilaa, vaan sitä, mihin suuntaan nykytila on kehittymässä suhteessa tavoitetilaan. Esimerkiksi kaksi yksikköä voivat olla tänään täsmälleen samalla tasolla, mutta niiden kehityssuunta voi olla täysin erilainen.

Kehityssuuntaa arvioidaan tavoitetilan saavuttamisen näkökulmasta, onko yritys menossa kohti tavoitetilaa vai poispäin siitä?

Havaittu trendi

Viimeisen 6–24 kuukauden aikana:

- parantunut
- pysynyt ennallaan
- heikentynyt
- Korjaavat toimenpiteet

Onko poikkeaman poistamiseksi:

- tehty toimenpiteitä
- käynnistetty kehityshankkeita
- osoitettu resursseja

Mittarit

Mitä mittarit osoittavat?

Esimerkiksi:

- reklamaatiot
- poikkeamat
- käyttöaste
- toimitusvarmuus
- auditointitulokset
- tietoturvapoikkeamat

Kehityssuunnan arviointiasteikko

Paranee

Valitaan kun:

- poikkeama pienenee
- mittarit kehittyvät oikeaan suuntaan
- korjaavat toimenpiteet ovat käynnissä
- tavoitetilaa lähestytään

Esimerkki:

MFA-käyttöönotto:

viime vuonna 40 %

nyt 75 %

tavoite 100 %

Valinta:

Paranee

Ennallaan

Valitaan kun:

- merkittävää muutosta ei havaita
- tilanne pysyy samalla tasolla
- mittarit eivät muutu olennaisesti

Esimerkki:

Toimitusvarmuus:

95 %

95 %

94 %

Valinta:

Ennallaan

Heikkenee

Valitaan kun:

- poikkeama kasvaa
- tavoitetilasta etäännytään
- mittarit huononevat
- ongelmat lisääntyvät

Esimerkki:

Tietoturvakoulutukset:

viime vuonna 92 %

nyt 71 %

Valinta:

Heikkenee

Arvioimatta

Valitaan kun:

- vertailutietoa ei ole
- trendiä ei voida todentaa
- arviointi tehdään ensimmäistä kertaa

Poikkeaman suuruuden arviointi

SECRISK-menetelmässä poikkeaman suuruus ei tarkoita riskin vakavuutta eikä nykytilan laatua. Se tarkoittaa, kuinka suuri ero on yrityksen määrittelemän tavoitetilan ja havaitun nykytilan välillä.

Kriittinen

Nykytila poikkeaa erittäin merkittävästi tavoitetilasta. Tavoitetila ei käytännössä toteudu.

Esimerkki

Tavoitetila:

Kaikissa kriittisissä järjestelmissä käytetään MFA:ta.

Nykytila:

MFA ei ole käytössä missään kriittisessä järjestelmässä.

Valinta:

Kriittinen

Merkittävä

Tavoitetila toteutuu vain osittain. Suuria puutteita havaitaan.

Esimerkki

Tavoitetila:

Kaikki käyttäjät suorittavat tietoturvakoulutuksen vuosittain.

Nykytila:

Vain 45 % käyttäjistä on suorittanut koulutuksen.

Valinta:

Merkittävä

Keskisuuri

Tavoitetila toteutuu osittain. Puutteet ovat selviä mutta hallittavia.

Esimerkki

Tavoitetila:

Asiakaspalautteet käsitellään 48 tunnissa.

Nykytila:

Keskimääräinen käsittelyaika on 72 tuntia.

Valinta:

Keskisuuri

Vähäinen

Tavoitetila toteutuu lähes kokonaan. Poikkeama on pieni.

Esimerkki

Tavoitetila:

Toimitusvarmuus 98 %.

Nykytila:

Toimitusvarmuus 96,8 %.

Valinta:

Vähäinen

Arvioimatta

Valitaan kun:

tavoitetilaa ei ole määritelty riittävän tarkasti. nykytilaa ei tunneta ti näyttöä ei ole saatavilla.

Todennäköisyyden arviointi

SECRISK-menetelmässä todennäköisyys ei kuvaa sitä, kuinka todennäköisesti jokin uhka tapahtuu, vaan sitä, kuinka todennäköisesti havaittu poikkeama johtaa ei-toivottuun seuraukseen, jos poikkeama jää korjaamatta. Tämä on merkittävä ero perinteiseen riskienarviointiin.

Jos poikkeama jätetään korjaamatta, kuinka todennäköisesti siitä seuraa haitallinen tapahtuma tai tavoitetilan toteutumisen estyminen? Tämä sitoo todennäköisyyden suoraan havaittuun poikkeamaan eikä yleiseen uhkakuvakeskusteluun.

Perinteinen kysymys on:

"Kuinka todennäköisesti hyökkäys tapahtuu?"

SECRISKin kysymys on:

"Kuinka todennäköisesti nykyinen poikkeama aiheuttaa haitallisen seurauksen?"

Todennäköisyyden arviointiperusteet

Arvioinnissa huomioidaan:

Poikkeaman esiintyvyys

Kuinka usein poikkeama esiintyy?

Esimerkiksi:

- yksittäinen havainto
- satunnainen ilmiö
- toistuva ilmiö
- jatkuva tila

Altistuminen

Kuinka usein toiminta altistuu poikkeamalle?

Esimerkiksi:

- kerran vuodessa
- kuukausittain
- viikoittain
- päivittäin
- jatkuvasti

Historiatiedot

Onko vastaavia tapahtumia ollut aiemmin?

Esimerkiksi:

- ei koskaan
- yksittäisiä tapauksia
- toistuvasti

Hallintakeinot

Kuinka hyvin poikkeamaa hallitaan?

Esimerkiksi:

- useita tehokkaita hallintakeinoja
- osittaiset hallintakeinot
- ei hallintakeinoja

SECRISK-todennäköisyysasteikko

1 – Epätodennäköinen

Poikkeama johtaa haitalliseen seuraukseen vain poikkeuksellisissa olosuhteissa.

Tyypillisesti:

- erittäin harvinainen
- vahvat hallintakeinot
- ei aiempia tapahtumia

Esimerkki:

Varmuuskopioiden palautustesti viivästynyt kerran.

2 – Harvinainen

Poikkeama voi johtaa seuraukseen, mutta vain satunnaisesti.

Tyypillisesti:

- yksittäisiä tapauksia
- useita suojaavia tekijöitä

3 – Mahdollinen

Poikkeama voi kohtuullisen realistisesti johtaa seuraukseen.

Tyypillisesti:

- tunnettu ongelma
- puutteelliset hallintakeinot
- tapahtuma mahdollinen normaalitoiminnassa

4 – Todennäköinen

Poikkeama johtaa seuraukseen melko suurella todennäköisyydellä.

Tyypillisesti:

- ongelma esiintyy säännöllisesti
- hallintakeinot eivät riitä
- useita varoitusmerkkejä

5 – Lähes varma

Poikkeama johtaa seuraukseen käytännössä varmasti, ellei sitä korjata.

Tyypillisesti:

- poikkeama on jatkuva
- suojaavat tekijät puuttuvat
- seurauksia on jo havaittu

SECRISK-menetelmän esimerkki

Tavoitetila

- Kaikissa kriittisissä järjestelmissä käytetään MFA:ta.

Nykytila

- MFA puuttuu kolmesta kriittisestä järjestelmästä.

Poikkeama

- Kaikissa kriittisissä järjestelmissä ei käytetä MFA:ta.

Todennäköisyyttä ei arvioida kysymällä:

- "Kuinka todennäköisesti hakkeri hyökkää?"

vaan:

- "Kuinka todennäköisesti tämä MFA-poikkeama johtaa tunnusten väärinkäyttöön tai muuhun tietoturvaloukkauksen?"

Jos järjestelmät ovat internetiin avoimia ja käyttäjätunnuksia käytetään päivittäin, arvio voisi olla:

- Todennäköinen (4)

Vaikuttavuuden arviointi

SECRISK-menetelmässä vaikuttavuus ei kuvaa poikkeaman kokoa, koska sitä arvioidaan jo kohdassa poikkeaman suuruus. Vaikuttavuus kuvaa:

> Kuinka vakavat seuraukset yritykselle aiheutuvat, jos poikkeama johtaa haitalliseen tapahtumaan.

Toisin sanoen:

- Poikkeaman suuruus = kuinka kaukana nykytila on tavoitetilasta.
- Todennäköisyys = kuinka todennäköisesti poikkeama aiheuttaa haitallisen tapahtuman.
- Vaikuttavuus = kuinka vakava haitallinen tapahtuma olisi yritykselle.

Jos poikkeama toteutuu haitallisena tapahtumana, kuinka vakavat seuraukset siitä aiheutuvat yrityksen tavoitteille, liiketoiminnalle tai toimintakyvylle?

Tämä pitää vaikuttavuuden arvioinnin erillään sekä poikkeaman suuruudesta että todennäköisyydestä ja tekee riskin laskennasta johdonmukaisen.

Vaikuttavuuden arviointiperusteet

Arvioinnissa tarkastellaan vaikutuksia esimerkiksi:

- liiketoimintaan
- talouteen
- asiakkaisiin
- henkilöstöön
- tuotantoon
- tietoturvaan
- lainsäädännön noudattamiseen
- maineeseen

SECRISK-vaikuttavuusasteikko

1 – Merkityksetön

Seurauksella ei ole käytännössä vaikutusta yrityksen toimintaan.

> Esimerkkejä:
>
> - vähäinen viive
> - yksittäinen korjattava virhe
> - ei taloudellista vaikutusta

2 – Vähäinen

Vaikutus on rajallinen ja helposti hallittava.

Esimerkkejä:

- yksittäinen reklamaatio
- pieni lisätyö
- vähäinen kustannus

3 – Kohtalainen

Vaikutus näkyy toiminnassa ja vaatii toimenpiteitä.

Esimerkkejä:

- useita asiakasreklamaatioita
- tuotannon häiriö
- merkittävä lisätyö
- sisäinen poikkeama

4 – Merkittävä

Vaikutus haittaa liiketoimintaa olennaisesti.

Esimerkkejä:

- toimituskatkos
- merkittävä tietoturvapoikkeama
- huomattava taloudellinen menetys
- sopimusvelvoitteen rikkominen

5 – Kriittinen

Vaikutus uhkaa yrityksen toimintakykyä, jatkuvuutta tai olemassaoloa.

Esimerkkejä:

- pitkä tuotannon keskeytys
- vakava tietomurto
- merkittävät viranomaisseuraamukset
- suuri taloudellinen menetys
- vakava mainehaitta

SECRISK-menetelmän esimerkki

Tavoitetila

- Kaikissa kriittisissä järjestelmissä käytetään monivaiheista tunnistautumista.

Nykytila

- MFA puuttuu kolmesta kriittisestä järjestelmästä.

Poikkeama

- Kaikissa kriittisissä järjestelmissä ei käytetä MFA:ta.

Todennäköisyys

- Arvioidaan, kuinka todennäköisesti tämä poikkeama johtaa tietoturvaloukkaukseen?

Valinta:

- Todennäköinen (4)

Vaikuttavuus arvioidaan:

- Jos tietoturvahäiriö toteutuu, kuinka vakavat seuraukset siitä aiheutuvat yritykselle?

Jos järjestelmät sisältävät kriittistä asiakasdataa:

- Kriittinen (5)

Riskitaso:

- 4 × 5 = 20

Riskiluokka:

- Avainriski

Arviointilausunto

SECRISK-menetelmässä arviointilausunto on riskikortin tärkein kenttä, koska siihen tiivistetään arvioijan ammatillinen johtopäätös.

Arviointilausunnon tarkoitus ei ole toistaa tavoitetilaa, nykytilaa tai poikkeamaa, vaan vastata kysymykseen:

Mitä havainto tarkoittaa yrityksen kannalta ja mitä sille pitäisi tehdä?

Arviointilausunnon rakenne

Arviointilausunto laaditaan aina neljästä osasta:

1. Havainto
    - Mitä arvioinnissa havaittiin?
2. Merkitys
    - Miksi havainto on tärkeä?
3. Riski
    - Mihin seurauksiin poikkeama voi johtaa?
4. Suositus
    - Mitä pitäisi tehdä?

Esimerkki 1

Tavoitetila

- Kaikissa kriittisissä järjestelmissä käytetään MFA:ta.

Nykytila

- MFA puuttuu kolmesta kriittisestä järjestelmästä.

Arviointilausunto

Monivaiheinen tunnistautuminen ei ole käytössä kaikissa kriittisissä järjestelmissä. Havaittu poikkeama kasvattaa tunnusten väärinkäytön ja luvattoman pääsyn riskiä.

Nykyiset hallintakeinot eivät täysin vastaa yrityksen tavoitetilaa. Suositellaan MFA:n käyttöönottoa kaikissa kriittisissä järjestelmissä sekä käyttöönoton seurannan lisäämistä.

Esimerkki 2

Tavoitetila

- Kaikki työntekijät suorittavat vuosittaisen tietoturvakoulutuksen.

Nykytila

- 72 % henkilöstöstä on suorittanut koulutuksen.

Arviointilausunto

Tietoturvakoulutuksen kattavuus ei täytä yrityksen tavoitetasoa. Osa henkilöstöstä toimii ilman ajantasaista tietoturvaosaamista, mikä lisää inhimillisten virheiden mahdollisuutta.

Kehityssuunta on kuitenkin positiivinen ja koulutusten kattavuus on parantunut edellisestä arvioinnista. Suositellaan koulutusten suorittamisen seurantaa ja puuttuvien suoritusten täydentämistä määräajassa.

Esimerkki 3

Vähäinen poikkeama

Arviointilausunto

Arvioitu toiminta vastaa pääosin yrityksen tavoitetilaa. Havaitut poikkeamat ovat vähäisiä eivätkä tällä hetkellä merkittävästi heikennä toiminnan tavoitteiden saavuttamista. Nykyiset hallintakeinot ovat riittävät. Tilannetta suositellaan seurattavaksi normaalin toiminnan yhteydessä.

Arviointilausunnon pituus

Tyypillisesti:

- 3–8 virkettä
- noin 50–200 sanaa

Liian lyhyt:

- MFA puuttuu. Riski on olemassa.

Liian pitkä:

- usean sivun analyysi

Arviointilausunnon kirjoituskaava

Arvioija voi käyttää aina samaa rakennetta:

> Arvioinnissa havaittiin, että [havainto]. Tämä poikkeaa yrityksen tavoitetilasta siten, että [poikkeama]. Poikkeama voi johtaa [seuraus]. Nykyiset hallintakeinot ovat [arvio]. Suositellaan [toimenpide].

SECRISK-periaate

Arviointilausunto ei saa olla pelkkä riskikuvaus. Sen tulee vastata kolmeen kysymykseen:

1. Mitä havaittiin?
2. Miksi sillä on merkitystä?
3. Mitä pitäisi tehdä?

Näin arviointilausunnosta tulee johdon kannalta käyttökelpoinen johtopäätös eikä pelkkä havaintomuistiinpano.