

Uhkamallinnus ohjelmiston elinkaaren aikana

Miksi uhkamallinnusta päivitetään?

Uhkamallinnus ei ole kertaluontoinen tehtävä, vaan jatkuva osa ohjelmiston kehittämistä ja ylläpitoa.

Ohjelmisto muuttuu koko elinkaarensa ajan: siihen lisätään uusia ominaisuuksia, integraatioita ja käyttötilanteita, ja sen arkkitehtuuri kehittyy. Jokainen muutos voi tuoda mukanaan uusia tietoturvaohjelmistojen tai muuttaa jo tunnistettujen riskien todennäköisyyttä ja vaikutusta.

Samalla myös toimintaympäristö muuttuu. Uusia haavoittuvuuksia löydetään, hyökkäystavat kehittyvät ja uhkatoimijoiden kyvykkyudet kasvavat. Ratkaisu, joka oli riittävän turvallinen eilen, ei välttämättä ole sitä enää tänään.

Tämän vuoksi uhkamallinnusta on päivitettävä säännöllisesti. Päivittäminen varmistaa, että riskienhallinta pysyy ajan tasalla ja vastaa todellista tilannetta, uudet ja muuttuneet uhat tunnistetaan ajoissa ja olemassa olevien riskien merkitys arvioidaan uudelleen.

Uhkamallinnusta kannattaa hyödyntää myös ennen merkittäviä muutoksia jo suunnitteluvaiheessa, jotta eri vaihtoehtoihin liittyvät riskit tunnistetaan ajoissa ja päätöksenteko perustuu parempaan tietoon. Ajantasainen uhkamalli toimii päätöksenteon tukena: se auttaa kohdistamaan toimenpiteet olennaisiin asioihin, välttämään turhaa työtä ja ylisuorittamista sekä parantamaan riskienhallinnan kustannus-hyötysuhdetta. Samalla voidaan ehkäistä kalliita korjauksia myöhemmissä vaiheissa.

Säännöllisesti päivitettävä uhkamallinnus auttaa varmistamaan, että tietoturva kehittyy ohjelmiston ja sen toimintaympäristön mukana.

Milloin uhkamallinnus pitää päivittää?

Päivitä uhkamallinnus vähintään kaksi kertaa vuodessa tai aina, kun:

- Lisätään uusi merkittävä ominaisuus
- Tehdään arkkitehtuurimuutos
- Lisätään uusi integraatio tai rajapinta
- Vaihdetaan teknologiaa tai alustaa
- Muutetaan tunnistautumista tai käyttöoikeuksia
- Siirretään palvelu uuteen ympäristöön
- Tapahtuu tietoturvaepäily
- Otetaan käyttöön uusi toimittaja tai ulkoinen palvelu
- Tehdään merkittäviä muutoksia toimittajasopimukseen tai vastuunjakoon
- Käynnistetään uuden ratkaisun tai muutoksen suunnittelu (ennen toteutuspäätöksiä)
- Käsiteltävän datan luonne muuttuu (esim. henkilötiedot, luottamuksellisuus kasvaa)
- Palvelun käyttötapa tai käyttäjämäärä muuttuu merkittävästi
- Tunnistetaan uusia uhkia organisaatiossa tai toimialalla

Uhkamallinnusta päivittäessä on hyvä huomioi-da, että muutokset voivat liittyä ohjelmiston eri elinkaaren vaiheisiin. Ohjelmiston elinkaaren vaiheiden huomioiminen auttaa varmistamaan, että uhkamallinnus kattaa muutosten vaikutukset riittävän kattavasti.

- Suunnitteluvaiheessa muutokset koskevat usein arkkitehtuuria, tietovirtoja tai uusia toimittajia.
- Toteutuksessa voi syntyä ratkaisuja, jotka poikkeavat alkuperäisestä suunnitelmasta.
- Testaus voi paljastavat uusia haavoittuvuuksia.

- Tuotantoon siirryttäessä käyttöympäristö, pääsynhallinta ja valvonta voivat tuoda uusia riskejä.
- Tuotantovaiheessa käyttötilanteet, käyttäjämäärät tai uhakuva voivat muuttua.
- Myös käytöstä poistoon liittyy tietoturvariskejä, kuten datan turvallinen käsittely ja rajapintojen sulkeminen.

Mitä päivittäminen tarkoittaa käytännössä?

Päivittäminen ei tarkoita koko uhkamallinnuksen tekemistä alusta. Päivitä vain ne kohdat, joihin muutokset vaikuttavat. Käytä kolmen kysymyksen mallia:

1. Mitä on muuttunut?

Tunnista kaikki muutokset edellisen uhkamallinnuksen jälkeen. Pohdi erityisesti:

- Onko tullut uusia komponentteja, integraatioita tai rajapintoja?
- Onko tietovirtoihin tullut muutoksia?
- Onko käyttöympäristö tai teknologia vaihtunut?
- Onko käyttäjissä tai käyttötavoissa tapahtunut muutoksia?
- Onko käsiteltävä data muuttunut (esim. arkaluonteisemmaksi)?

2. Mitä uusia uhkia syntyy?

Mieti, miten muutokset vaikuttavat uhakuvaan ja mitä uusia hyökkäysmahdollisuuksia tai heikkouksia ne voivat synnyttää. Voit käyttää apuna esimerkiksi:

- Voiko joku päästä käsiksi uuteen rajapintaan?
- Voiko tietoa nyt vuotaa uudessa kohdassa?
- Voiko joku muuttaa tietoa uudella tavalla?
- Voiko palvelua kuormittaa tai häiritä helpommin?
- Tuleeko mukaan uusia luottamussuhteita (esim. toimittaja)?

3. Muuttuuko jokin olemassa oleva riski?

Arvioi aiemmin tunnistetut riskit uudelleen. Pohdi esimerkiksi:

- Onko riskin todennäköisyys kasvanut tai pienentynyt?
- Onko riskin vaikutus muuttunut (esim. enemmän käyttäjiä, kriittisempi data)?
- Onko riskiä jo pienennetty tehdyillä toimenpiteillä?
- Onko jokin riski poistunut kokonaan?

Mitä päivitetään?

Päivityksessä käydään läpi:

- Järjestelmän kuvaus (arkkitehtuuri, tietovirrat, integraatiot)
- Uhat (uudet ja muuttuneet)
- Riskit (vaikutus ja todennäköisyys)
- Toimenpiteet (toteutus ja riittävyys)

Dokumentointi

Uhkamallinnus ja riskitaulukko ovat eläviä dokumentteja, joita päivitetään jatkuvasti ohjelmiston elinkaaren aikana. Niitä ei käsitellä kertaluonteisena tuotoksena, vaan työkaluna ohjelmistoturvallisuuden ja riskienhallinnan tukena.

Päivityksissä:

- päivitetään olemassa olevaa dokumenttia, ei luoda uutta versiota erilliseksi tiedostoksi
- kirjataan tehdyt muutokset dokumentin versiohistoriaan
- merkitään, milloin uhka tai riski on viimeksi käsitelty
- päivitetään riskien nykytila (avoin, käsittelyssä, valmis, hyväksytty)

Uusien riskien osalta:

- lisätään riski riskirekisteriin
- määritetään vastuuhenkilö ja tarvittavat toimenpiteet

Tärkeää:

- dokumentin tulee kuvata aina ajantasainen tilanne
- historia säilytetään versionhallinnan tai muutostenmerkintöjen kautta, ei erillisinä kopioina