

Uhkamallinnus lyhyesti: mitä, milloin ja miksi?

Mitä on ohjelmiston uhkamallinnus?

Ohjelmiston uhkamallinnus on menetelmä, jolla tunnistetaan yksittäiseen järjestelmään, ohjelmiin tai palveluun kohdistuvia tietoturva-uhkia ja arvioidaan niihin liittyviä riskejä.

Käytännössä uhkamallinnus tarkoittaa sitä, että tarkastellaan ohjelmistoa ja sen toimintaa ja kysytään:

- mitä tässä järjestelmässä voisi mennä pieleen
- missä kohdassa tietoturva voi pettää

Uhkamallinnus kohdistuu ohjelmiston:

- toiminnallisiin
- käsiteltävään tietoon
- rajapintoihin ja integraatioihin
- käyttäjiin ja käyttötilanteisiin

Uhkamallinnus on yhteinen ajatteluharjoitus, jossa hyödynnetään eri roolien osaamista. Parhaat havainnot syntyvät, kun ohjelmistoa tarkastellaan useasta näkökulmasta yhdessä.

Uhkamallinnuksen avulla muodostetaan yhteinen ymmärrys siitä, missä kohtaa ohjelmistoa voi olla tietoturvan kannalta heikkoja kohtia.

Miksi uhkamallinnusta tehdään?

Ohjelmiston uhkamallinnuksen tarkoituksena on tunnistaa tietoturvaan liittyvät riskit riittävän ajoissa, jotta ne voidaan huomioida suunnittelussa ja toteutuksessa.

Ilman uhkamallinnusta monet riskit havaitaan

vasta myöhemmin, esimerkiksi testauksessa tai tuotannossa, jolloin niiden korjaaminen on työläämpää ja kalliimpaa.

Uhkamallinnuksen avulla:

- tehdään parempia suunnittelu- ja toteutus päätöksiä
- kohdistetaan toimenpiteet olennaisimpiin riskeihin
- lisätään yhteistä ymmärrystä ohjelmiston tietoturvasta
- tunnistetaan ohjelmiston heikot kohdat ennen kuin niitä hyödynnetään

Uhkamallinnus tukee ohjelmiston kehitystä koko sen elinkaaren ajan ja auttaa varmistamaan, että tietoturva huomioidaan osana normaalia kehitystyötä – ei vasta jälkikäteen.

Milloin uhkamallinnus tehdään?

Ohjelmiston uhkamallinnus tulisi tehdä ensimmäisen kerran jo ohjelmiston suunnitteluvaiheessa. Tällöin tietoturvaan liittyvät riskit voidaan huomioida ennen toteutusta, jolloin niiden hallinta on helpointa ja kustannustehokkainta.

Uhkamallinnus tehdään myös aina, kun ohjelmistoon tulee muutoksia, jotka voivat vaikuttaa tietoturvaan.

Tyypillisiä tilanteita ovat:

- uuden ohjelmiston tai palvelun suunnittelu
- merkittävän uuden ominaisuuden toteutus
- uusi integraatio tai rajapinta
- arkkitehtuurimuutos tai teknologian vaihto
- ennen tuotantoon vientiä

Uhkamallinnus ei ole kertaluonteinen tehtävä, vaan sitä tulee päivittää ohjelmiston elinkaaren aikana.

Uhkamallinnus kannattaa päivittää myös, kun:

- ohjelmiston käyttö muuttuu merkittävästi
- havaitaan tietoturvapoikkeama tai läheltä piti -tilanne
- edellisestä mallinnuksesta on kulunut aikaa (esimerkiksi puolivuositain)

Tavoitteena on varmistaa, että ohjelmiston tietoturvariskit tunnistetaan aina sen nykytilannetta vastaavasti.

Ketkä osallistuvat

Ohjelmiston uhkamallinnus tehdään yhteistyössä. Mukaan tarvitaan henkilöt, jotka tuntevat ohjelmiston toiminnan, rakenteen ja käyttötarkoituksen.

Tyypillisesti osallistujia ovat:

- kehittäjät
- arkkitehti
- tuoteomistaja tai muu palvelusta vastaava henkilö
- liiketoiminnan edustaja (loppukäyttäjien tarpeet tunteva henkilö)

Tarvittaessa mukaan voidaan ottaa myös:

- tietoturva-asiantuntija
- infra- tai pilviympäristöstä vastaava henkilö

Uhkamallinnuksen kannalta on tärkeää, että mukana on riittävästi eri näkökulmia. Yksittäinen henkilö ei yleensä pysty tunnistamaan kaikkia olennaisia uhkia, mutta yhdessä muodostuu kattavampi ymmärrys ohjelmiston riskeistä

Osallistujamäärä kannattaa pitää rajattuna (suositus 5–7 henkilöä), jotta työskentely pysyy tehokkaana.

Mitä uhkamallinnuksesta syntyy?

Ohjelmiston uhkamallinnuksen tuloksena syntyy yhteinen näkemys ohjelmistoon liittyvistä tietoturvariskeistä ja siitä, miten niitä hallitaan.

Käytännössä uhkamallinnuksesta syntyy:

- lista tunnistetuista uhkista ja heikkouksista
- arvio uhkien vaikutuksesta ja todennäköisyydestä
- priorisoitu näkemys merkittävimmistä riskeistä
- sovitut toimenpiteet riskien pienentämiseksi
- vastuuhenkilöt ja aikataulu toimenpiteille

Uhkamallinnuksen tuloksia hyödynnetään päätöksenteon tukena ohjelmiston kehityksessä. Tunnistetut toimenpiteet viedään osaksi normaalia kehitystyötä, ja niiden avulla voidaan kohdentaa resursseja kohtiin, joissa riskit ovat merkittävimmät.

Tavoitteena ei ole löytää kaikkia mahdollisia ongelmia täydellisesti, vaan tunnistaa keskeisimmät riskit riittävän ajoissa, jotta niihin voidaan reagoida.

Hyödynnettävät menetelmät (esim. STRIDE)

Uhkamallinnuksen tueksi on olemassa valmiita menetelmiä, kuten STRIDE, PASTA sekä Attack Tree. Ne toimivat ajattelun tukena ja auttavat tunnistamaan uhkia systemaattisesti.

Menetelmien tarkoitus on:

- auttaa huomioimaan keskeiset tietoturvanäkökulmat (luottamuksellisuus, eheys, saatavuus)
- tuoda rakennetta uhkien tunnistamiseen
- vähentää riskiä, että olennaisia uhkia jää huomaamatta

Menetelmien käyttö ei ole pakollista, vaan tärkeintä on yhteinen keskustelu ja olennaisten uhkien tunnistaminen. Menetelmät tuovat tekemiseen rakennetta ja tukevat uhkien systemaattista käsittelyä, mutta niiden ei tulisi ohjata ajattelua liian kaavamaisesti. Kevyessä uhkamallinnuksessa riittää, että menetelmiä hyödynnetään tarvittaessa esimerkiksi kysymysten tukena muistilistoina.

Keskeiset käsitteet

Uhkamallinnuksessa käytetään muutamia peruskäsitteitä, jotka on hyvä ymmärtää ennen aloittamista.

Uhka

Uhka tarkoittaa tilannetta tai tapahtumaa, jossa jokin voi mennä pieleen.

Riski

Riski tarkoittaa uhkan toteutumisen vaikutusta ja todennäköisyyttä.

Toisin sanoen: kuinka vakavaa olisi, jos uhka toteutuu, ja kuinka todennäköistä se on.

Riskianalyysi

Riskianalyysissä arvioidaan tunnistetut uhkat: kuinka suuri vaikutus niillä on ja kuinka todennäköisesti ne toteutuvat.

Riskimatriisi

Riskimatriisi on työkalu, jolla riskin suuruus määritetään vaikutuksen ja todennäköisyyden perusteella. Sen avulla riskit voidaan luokitella ja asettaa keskinäiseen tärkeysjärjestykseen.

Riskienhallinta

Riskienhallinta tarkoittaa toimenpiteitä, joilla riskejä pienennetään, poistetaan, siirretään tai hyväksytään.