<Hankkeen tunnus ja nimi >

Tietoturvatarkastuksen tulokset

Versio <nro>

<pp.kk.vvvv>

VERSIOHISTORIA

| Päivä | Versio | Kuvaus | Tekijä |
| --- | --- | --- | --- |
| <pvm> | 0.1 | Dokumentin perustaminen | <etumini, sukunimi> |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sisällys

[1 Johdanto 4](#_Toc469655307)

[2 Tarkastuksen kohde ja rajaukset 5](#_Toc469655308)

[3 KäytetYT menetelmäT 6](#_Toc469655309)

[4 Tulokset 7](#_Toc469655310)

[5 JohtopäätökseT 8](#_Toc469655311)

[6 LIITTEEt 9](#_Toc469655312)

1. **Johdanto**

[Lyhyt kappale, jossa kuvataan mikä on tarkastuksen tarkoitus, mikä on kysymys johon tarkastuksella halutaan selvyys. Missä vaiheessa hanke on nyt ja mitä se vaikuttaa tarkastukseen?]

1. **Tarkastuksen kohde ja rajaukset**

[Mihin kokonaisuuteen tarkastus on kohdistunut, mitkä sen rajat ja rajapinnat. Mitä osia on tarkastettu ja mistä näkökulmasta (hallinnollinen/tekninen).

Jos osia on rajattu ulkopuolelle, mitä ja miksi? Oliko sovittu menetelmärajoituksista (esim. ei palvelunestotestejä)? Oliko sovittu aikataulurajoituksia? Oliko sovittu että tarkastus kohdistuu vain tiettyjen roolien toimintaan?]

1. **KäytetYT menetelmäT**

[Mitä menetelmiä oli käytetty tarkastuksessa (esim. tekniset testit, haastattelut, prosessin tapaustutkimus)?

Olennaista on kuvata menetelmä, prosessi ja työkalut niin, että tarvittaessa testit voitaisiin toistaa.

* Mitä teknisiä työkaluja käytettiin ja mitä niiden versioita?
* Mitä tukimateriaalia tarkastajilla oli (esim. prosessikuvaukset, käyttäjätunnukset järjestelmiin, järjestelmän lähdekoodi ja dokumentaatio)?
* Mistä/missä tarkastus oli tehty (esim. yksikkö X, rakennus Z, IP-osoite Y).
* Milloin tarkastus tehtiin?
* Keitä henkilöitä oli läsnä esim. haastatteluissa tai avustamassa teknisissä testeissä.

Mitä kriteeristöä vastaan poikkeamat oli analysoitu (esim. OWASP ASVS, työkalun haavoittuvuustietokanta, prosessikuvaus päivätty X.Y. tai kansainvälinen standardi Y)?

Miten löydösten riskitaso on arvioitu, onko taso saatu suoraan jostakin työkalusta vai onko luotu omat kriteerit.

Ketkä olivat tarkastuksen tekijät ja mikä on heidän pätevyytensä.]

1. **Tulokset**

[Jokaisesta löydöksestä tulee kuvata vähintään seuraavat asiat:

* *Ongelman tunnus* on yksikäsitteinen tunnus, esimerkiksi pelkkä juokseva numero tai kategoriaan liittyvä (vaikka DB-6 tietokantaan liittyvälle haavoittuvuudelle numero 6).
* *Haavoittuvuuden kuvaus* selittää ongelman järjestelmän toiminnan kautta esimerkiksi ”Puutteellisten oikeustarkastusten vuoksi käyttäjä voi nähdä toisen käyttäjän tietoja lisätietonäkymässä” tai ”Prosessissa ei estetä väärän tiedon syöttämistä järjestelmään X”.
* *Riskitaso*, joka kuvaa yhdellä sanalla kuinka vakava ongelma on. Yleensä käytetään kolmi- tai nelitasoista vakavuusasteikkoa (esim. kriittinen, vakava, lievä, huomautus), mutta tärkeintä on se, että käytetty vakavuusasteikko on jollain tavalla kuvattu edellisessä kappaleessa.

Lisäksi voidaan kuvata seuraavia asioita silloin kun se on ongelman kannalta olennaista (esim. teknisistä haavoittuvuuksista):

* *Tekninen selostus* selittää haavoittuvuuden kuvauksen teknisesti, esim. ”/api/additional\_info ei tarkasta että kysyjä saa nähdä parametri uid:ssa identifioidun käyttäjän tietoja”.
* *Toisto-ohjeet* sisältävät ohjeet ongelman toistamiselle, jotta ongelman korjaajat ymmärtävät miten ongelma on saatu esiin.
* *Lisätietoa*, viite tai linkki yleiseen keskusteluun tai kuvaukseen haavoittuvuudesta tai ongelmasta.

Jos halutaan, kuhunkin löydökseen voidaan lisätä myös osio

* *Korjausehdotus*

Olisi hyvä jos löydös voidaan havainnollistaa kuvilla tai ruutukaappauksilla.

]

1. **JohtopäätökseT**

[Tarkastajan kokonaisarvio siitä, mikä on tarkastetun kokonaisuuden tietoturvallisuuden taso, vastaus luvussa 1 esitettyyn kysymykseen.

Jos löytyi ongelmia, yhteenveto siitä kuinka paljon ja kuinka kriittisiä. Tarkastajan suositukset siitä, mitkä ovat korjausprioriteetit.

Mahdollinen vertailu edellisiin samasta järjestelmästä tehtyihin tarkastuksiin, onko tilanne parempi vai huonompi.

Muut tarkastajan mielestä oleelliset huomiot, esimerkiksi onko havaittujen yksittäisten ongelmien takana jotain systemaattista tai prosessiongelmaa, josta hankkeen tulisi olla tietoinen.]

1. **LIITTEEt**

[Mahdolliset työkalujen tuottamat raportit, auditointilokit yms]