VERKKOPALVELUN TIETOTURVAN VARMENTAMINEN

Tietoturvaopas

1

Johdanto

Olemme vuodesta 2005 lähtien toteuttaneet yli 1000 verkkopalvelun haavoittuvuustestausta ja auditointia sekä tietoturvan varmentamiseen liittyvää projektia. Näistä syntyneeseen kokemukseen pohjautuen olemme koonneet tähän oppaaseen, miten tietoturva on hyvä varmentaa verkkopalvelujen kehityksessä, käyttöönotossa ja elinkaaren aikana. Tietoturvaan liittyvät toimenpiteet on kuvattu modulaarisesti, jotta kukin voi soveltaa eri vaiheita joko täysimääräisesti tai osittain oman tarpeensa ja riskikykynsä mukaan.

Toivotamme haavoittuvuusvapaita verkkopalveluita!

- 2NS Haavoittuvuustutkimustiimi

Sisällysluettelo

1. Tiivistelmä

Verkkopalvelun tietoturva on hyvä varmentaa vaiheittain jo kehityksen alusta asti, vaikkakin jo käytössä olevasta palvelustakin pystytään vielä haavoittuvuudet tunnistamaan ja sitä kautta poistamaan. Verkkopalvelun tietoturvan varmentamisen vaiheet elinkaaren aikana ovat:

1. Kehittäjien koulutus
2. Uhkamallinnus
3. Koodikatselmointi
4. Tietoturva-auditointi/haavoittuvuustestaus
5. Säännöllinen skannaus ja tarkastukset
6. Tietoturvatilanteen reaaliaikainen valvonta käytön aikana

2. Tietoturvan varmentamisen vaiheet

2.1. Kehittäjien koulutus

Sovelluskehittäjien koulutuksessa annetaan kehittäjille ja projektipäälliköille kattavasti tietoa miten järjestelmän tietoturva tulee huomioida kehitysvaiheen aikana. Koulutuksissa tehdään usein myös käytännön harjoituksia esim. hakkeroimalla omaa järjestelmää tai koulutuksen järjestäjän demojärjestelmää.

Hyviä aiheita koulutukselle ovat esimerkiksi:

• Miten tietoturva tulee huomioida sovelluskehityksen eri vaiheissa (tietoturvavaatimusten luominen, uhkamallinnus, hyökkäyspinta-alan minimointi, turvalliset kehitysmenetelmät jne.)

• Yleisimmät haavoittuvuudet (OWASP TOP 10)

• Tietoturvan periaatteet ja oikein mitoitettu panostaminen

• Harjoitustehtävät (haavoittuvuustestauksessa käytettävien työkaluihin tutustuminen, hyökkääminen sovelluksia ja järjestelmiä vastaan jne.)

2.2. Uhkamallinnus

Uhkamallinnuksessa (esim. workshop) kerätään järjestelmään kohdistuvat riskit sekä priorisoidaan ne. Tämän perusteella muodostetaan tietoturvavaatimuslista sekä suunnitelma tietoturvakontrollien teknisestä toteuttamisesta, joiden pohjalta on mahdollista toteuttaa turvallinen järjestelmä.

2.3. Koodikatselmoinnit

Tietoturvan kannalta keskeisimmille osa-aluillle (esim. tiedon validointi funktiot / luokat jne.) on hyvä tehdä koodikatselmointi. Koodikatselmoinnin lopputuloksena saadaan korjausehdotukset mahdollisista puutteista, jotta ne kyetään korjaamaan kustannus-tehokkaasti jo kehityksen aikana.

2.4. Tietoturva-auditointi / haavoittuvuustestaus

Varsinaisella tietoturva-auditoinnilla / haavoittuvuustestauksella varmistetaan palvelun tietoturva. Auditoinnissa tunnistetaan palvelussa olevat haavoittuvuudet, havainnollistetaan niiden hyväksikäyttötapaukset sekä annetaan niiden korjaussuositukset. Tietoturva-auditoinnilla on hyvä kattaa sekä sovellus että palvelinympäristö. Auditoinnissa keskitytään muun muassa alla esitettyihin haavoittuvuuksiin, mutta myös muut mahdolliset haavoittuvuudet tunnistetaan:

Injektiot
Autentikointi ja istunnonhallintahaavoittuvuudet
Cross Site Scripting
Turvattomat suorat objektiviittaukset
Turvattomat konfiguraatiot
Arkaluonteisen tiedon paljastuminen
Puuttuva funktiotason pääsynhallinta
Pyyntöväärennös (CSRF)
Haavoittuvien komponenttien käyttö
Validoimattomat edelleenohjaukset

(OWASP TOP 10 haavoittuvuudet, lähde OWASP)

2.5. Korjausten verifiointi

Auditoinnissa havaitut haavoittuvuudet korjataan, jonka jälkeen verifioidaan, että korjaukset on tehty asianmukaisesti.

2.6. Tietoturvan ylläpito ja säännöllinen varmentaminen

Saavutettu tietoturvan taso on hyvä ylläpitää. Esimerkiksi uudet ominaisuudet ja muutokset sovelluksessa ja palvelinympäristössä, palvelimen päivitystilanne sekä uusien hyväksikäyttömenetelmien syntyminen saattavat aiheuttaa riskiä. Säännölliseen varmentamiseen yleisiä toimenpiteitä ovat muun muassa:

Ajastettu automaattinen haavoittuvuusskannaus

Kustannustehokas koneellinen tapa havaita uusia haavoittuvuuksia

Verkkopalvelun tietoturvantilanteen reaaliaikainen valvonta

Käynnissä oleviin hyökkäyksiin kyetään reagoimaan heti.

Säännöllinen tietoturvatarkastus / auditointi

Tietoturvakriittisyyden mukaan verkkopalvelun tietoturva on suositeltavaa tarkastaa säännöllisin väliajoin (uudet hyväksikäyttömenetelmät, muutokset ja uudet ominaisuudet sovelluksessa ja palvelimella, palvelimen päivitystilanne jne.)

3. Mitä muuta voi tehdä tietoturvan parantamiseksi

3.1. Tekniset toimet

Suorituskykytestaus / kuormitustestaus

Palvelun saatavuus on usein myös tärkeä ominaisuus esimerkiksi kuormitustilanteissa. Testauksessa selvitetään kuormituksen vaikutus palvelun tasoon ja saatavuuteen. Tämä tehdään simuloimalla suurta määrää yhtäaikaisia käyttäjiä sovituilla käyttötapauksilla, jotta opitaan palvelun käyttäytyminen kuormituksen aikana ja kyetään tekemään mahdolliset korjaukset palvelun suorituskykyyn.

Penetraatiotestaus

Penetraatiotestaus on hyvä tehdä kriittisille palveluille. Tässä otetaan kokonaisvaltaisempi näkökulma, kuin yksittäisten haavoittuvuuksien testaamisessa. Palvelusta löytyneitä teknisiä haavoittuvuuksia yhdistellään ja lisäksi käytetään myös muita hyökkäyskomponentteja kuten sosiaalista manipulointia tai muista tietojärjestelmistä löytyneitä haavoittuvuuksia. Tavoitteena on varmentaa tietojärjestelmän tietoturvan riittävyys tapauksessa, kun järjestelmään vastaan hyökätään järjestelmällisesti.

3.2. Tietoturvan huomiointi verkkopalveluita hankittaessa

Tarjouspyynnön vaihe - Tietoturvavaatimukset

Tarjouskilpailun onnistumisen kannalta on tärkeää, että tietojärjestelmätoimittajat osaavat ottaa tarjousta tehdessään huomioon järjestelmälle asetetut tietoturvavaatimukset. Tämä asettaa tarjoajat samalle lähtöviivalle. Mikäli tietoturvavaatimuksia tuodaan jälkikäteen tarjouksen hyväksymisen jälkeen, on vaarana, että niiden mahdollisesti aiheuttamista kustannuksista tulee erimielisyyksiä.

Tarjousten vertailun vaihe - Tietoturvakuvausten vertaaminen

Toimitettavan järjestelmän tietoturvatoteutus tulisi ilmetä riittävällä tasolla toimittajien tarjouksista. Tarjousten katselmoinnissa tarjouksen sisältöä peilataan tarjouspyynnössä annettuja tietoturvavaatimuksia vasten. Tarjousten katselmoinnin yhteydessä kootaan havainnot löydetyistä puutteista ja listataan tarkentavia kysymyksiä toimittajille. Vaiheen lopputuloksena muodostetaan kuva kunkin toimittajan kyvystä vastata asetettuihin tietoturvavaatimuksiin. Tätä voidaan käyttää päätöksenteon tukena valittaessa tai karsittaessa toimittajia.

4. Yleisimmät aiheeseen liittyvät viitekehykset

Viitekehyksiä joita esimerkiksi ammattilaiset seuraavat ovat:

OWASP (Open Web Application Security Project)

OSSTMM (Open Source Security Testing Methodology Manual)

Second Nature **Security**

2NS on vuodesta 2005 asti toteuttanut yli 1000 tietoturva-auditointia ja haavoittuvuustestausta.

Palvelemme yli 150 koti- ja ulkomaista asiakasta (Suomi, USA, Ruotsi, Hollanti, Viro, Latvia, Norja). Asiakaskuntamme koostuu muun muassa yrityksistä, julkishallinnosta ja finanssialasta.

Palvelemme asiakkaitamme tinkimättömällä ammattitaidolla. Meille on tärkeää, että asiakas saa tulokset ymmärrettävässä muodossa selkeiden korjauskehoitusten kera.

Meillä on kokemusta valtakunnan kriittisimmistä ympäristöistä: Asiakkaamme ovat pienistä ohjelmistoyrityksistä suurempiin toimijoihin, muun muassa Finnair, Neste Oil, Veikkaus, CSC, VRK, Affecto, Innofactor, Tallink Silja, Huhtamäki ja Varma.

Haavoittuvuustutkimustiimimme on julkaissut lukuisia haavoittuvuustiedotteita, muun muassa SAP:n, Oraclen, F-Securen, IBM:n ja HP:n laitteista ja järjestelmistä.

Ota yhteyttä, autamme mielellämme!

www.2ns.fi

Second Nature Security Oy www.2ns.fi | 010 322 9000 | info@2ns.fi