Verkkosivujesi pimeä puoli

Ohjeita sisällönhallintajärjestelmien kyberuhkien torjumiseksi

2/2016

Viestintävirasto
Kyberturvallisuuskeskus

Sisällysluettelo

Verkkosivujesi pimeä puoli

Verkkosivujen julkaisujärjestelmä (englanniksi content management system, CMS), kuten WordPress, Drupal tai Joomla, kannattaa pitää päivitettynä viimeisimpään versioonsa. Päivittämätön järjestelmä on altis hyökkäyksille ja voi käydä sivuston omistajalle kalliiksi. Menetetyn tiedon palauttaminen, julkisuuskuvan korjaaminen ja verkkonäkyvyyden saaminen takaisin voivat aiheuttaa merkittäviä ylimääräisiä kustannuksia asianmukaiseen ylläpitämiseen verrattuna.

Suosittuihin julkaisujärjestelmiin julkaistaan säännöllisesti uusia päivityksiä. Päivitysten tarkoitus on sekä tuoda järjestelmään uusia ominaisuuksia että korjata puutteita, virheitä ja haavoittuvuuksia. Vaikka järjestelmän ylläpitäjä katsoisikin pärjäävänsä hyvin ilman uusia ominaisuuksia, turvallisuutta parantavat päivitykset on kriittisen tärkeää asentaa.

1 Miksi päivittäisin? Mitä voisi sattua?

Julkaisujärjestelmistä löytyy joka kuukausi niin vakavia haavoittuvuuksia, että hyökkääjä voi ottaa haltuunsa koko järjestelmän. Pahimmillaan hyökkääjä voi varastaa sivuston kaikki käyttäjätiedot, maksuliikennetiedot ja yrityksen sisäiset tuotetiedot. Lisäksi hyökkääjä voi ujuttaa sivustolle haittaohjelmia ja takaportteja[1].

Murretulle sivustolle voidaan asettaa uudelleenohjaus niin, että myös sivuston käyttäjät joutuvat hyökkääjän uhriksi.[2] Sivuston sisältö voidaan vaihtaa johonkin täysin asiattomaan.[3] Pahimmillaan järjestelmän tietokone voidaan ottaa kokonaan haltuun ja orjuuttaa osaksi bottiverkkoa[4], jota pahantekijä voi käyttää omiin tarkoituksiinsa.

Murretun sivuston ja saastutetun järjestelmän korjaaminen ja palauttaminen ennalleen vaatii paljon työtä. Ensin pitää selvittää, mitä ja milloin on rikottu. Se onkin usein eniten aikaa vievä ja taitoa vaativa osuus; hyökkääjän tekemiä muutoksia voi olla missä vain. Jos niitä kaikkia ei korjaa, uusi murtautuminen on liki varmaa.

2 Sivustoja murretaan paljon

Tietomurtoja ei satu vain silloin tällöin vaan niitä tehtaillaan kuin liukuhihnalta. Googlen Selaussuoja-toiminto (Safe Browsing)[5] kirjaa joka viikko yli kymmenen tuhatta uutta murrettua sivustoa, jotka on muokattu ohjaamaan haittaohjelmia jakaville sivustoille. Googlen näkymä murrettuihin sivustoihin ei ole täydellinen, mutta silti ehkä paras saatavilla oleva. Lisäksi Googlen tilastoissa

[1] Takaoven avulla palvelintasi käyttää joku muu <https://www.viestintavirasto.fi/2015/11/ttn201511121608>. Tietoturva nyt! 13.11.2015

[2] Ylläpitäjä: Vanhentunut WordPress vaarantaa sivuston ja sen käyttäjien turvallisuuden <https://www.viestintavirasto.fi/2015/06/ttn201506301518>. Tietoturva nyt! 30.6.2015

[3] Suomalaisia verkkosivustoja murrettu propagandan levittämiseksi <https://www.viestintavirasto.fi/2015/04/ttn201504291532>. Tietoturva nyt! 29.4.2015

[4] Laajan tietomurtosarjan oppi: Ajantasaiset ohjelmistot ennaltaehkäisevät tietomurtoja <https://www.viestintavirasto.fi/2014/02/ttn201402051410>. Tietoturva nyt! 5.2.2014

[5] Google Transparency Report: Making the web safer <https://www.google.com/transparencyreport/safebrowsing/?hl=en> [viitattu 17.2.2016]

eivät näy ne verkkosivut, jotka on murrettu muista syistä.

Erään tutkimuksen mukaan 72 prosenttia maailman miljoonan suosituimman sivuston joukossa olleista WordPressiä käyttävistä sivustoista oli haavoittuvia päivittämättömän WordPress-ohjelmiston vuoksi.[6] Muista yleisistä julkaisujärjestelmistä ei löydy yhtä perusteellisia tutkimuksia, mutta tilanteen voi olettaa vastaavaksi niidenkin suhteen.

Lisäksi jokaisella WordPressiä käyttävällä sivustolla on käytössä keskimäärin 3–4 WordPressin laajennusosaa. Lukuisissa laajennusosissakin on koko verkkosivuston tietoturvan vaarantavia haavoittuvuuksia; erään tutkimuksen mukaan puolet WordPressiä koskevista haavoittuvuuksista johtuu laajennusosista.[7] Monia laajennusosia korjataan harvoin, joten sivusto voi pysyä pitkään haavoittuvana tunnetuille hyväksikäyttötavoille, vaikka sivuston ylläpitäjä päivittäisikin ohjelmistoa ahkerasti.

Haavoittuvat sivustot missä tahansa päin maailmaa ovat suhteellisen helposti löydettävissä sellaiselle, joka osaa etsiä teknisiä tunnisteita www-palvelinten vastauksista. Etsintä ja murtautuminen voidaan automatisoida.

Haittaohjelmia voi tulla myös mainoksiin piilotettuina.[8] Mainosten tarjoajien murretuille sivuille piilotetuista haittaohjelmista koituu ikävyyksiä kaikille haitallisia mainoksia käyttäville sivustoille.

3 Murto tulee kalliiksi

Tietomurron aiheuttamia tappioita ja kustannuksia on arvioitu esimerkiksi B2B Internationalin ja tietoturvayhtiö Kasperskyn kyselytutkimuksessa[9]. Maailmanlaajuinen keskiarvo pienen tai keskisuuren yrityksen kustannuksille ja tappioille, jotka johtuvat tietoverkkoon murtautumisesta tai hakkeroinnista oli noin 65 000 Yhdysvaltain dollaria (vuoden 2014 tieto), josta tekniset korjauskulut muodostivat vajaan kolmasosan. Näin tilastoidut tapaukset sisältävät muihinkin kohteisiin kuin verkkosivuille murtautumisia, mutta kulut lienevät ainakin pienillä yrityksillä samaa luokkaa verkkosivuille tehdyissä murroissa.

4 Älä joudu mustalle listalle

Haitalliset sivustot eristetään nopeasti mustille listoille. Mustia listoja haitallisista sivustoista käytetään esimerkiksi verkkoselaimissa, virustorjuntaohjelmistoissa ja hakukoneiden tulosten muodostamisessa. Pahantahtoinen hyökkääjä voi hyödyntää järjestelmän aukkoja ujuttamalla sivustolle haittakoodia. Kun haittakoodi paljastuu, sivusto voidaan ilmiantaa mustalle listalle, minkä jälkeen asiakkaiden selaimet eivät suostu enää menemään sivulle eivätkä hakukoneet enää indeksoi sivustoa. Mustalta listalta pääseminen takaisin luotettujen kirjoihin on pitkä ja työläs prosessi.

[6] WP WhiteSecurity: Statistics Show Why WordPress is a Popular Hacker Target <http://www.wpwhitesecurity.com/wordpress-security-news-updates/statistics-70-percent-wordpress-installations-vulnerable/> [viitattu 17.2.2016]

[7] VP WhiteSecurity: Statistics Highlight the Biggest Source of WordPress Vulnerabilities <http://www.wpwhitesecurity.com/wordpress-security/statistics-highlight-main-source-wordpress-vulnerabilities/> [viitattu 17.2.2016]

[8] Haittaohjelma tarttuu, vaikka et klikkaisi mitään <https://www.viestintavirasto.fi/2015/09/ttn201509171541>. Tietoturva nyt! 17.9.2015

[9] Kaspersky lab: It Security Risks Survey 2014: A Business Approach To Managing Data Security Threats <http://media.kaspersky.com/en/it_security_risks_survey_2014_global_report.pdf> [viitattu 17.2.2016]

5 Brändiä ei voi varmuuskopioida

Haittaohjelmatartunta tuhoaa hetkessä suositunkin sivuston maineen. Vuosien työllä rakennettu nettibrändi on kultaakin arvokkaampi. Huolimattomasti ylläpidetyn sivuston murtaminen, käyttäjätietojen joutuminen vääriin käsiin ja käyttäjien altistaminen haittaohjelmille karkottaa asiakkaat nopeasti. Tiedot voi palauttaa varmuuskopiolta, mutta luotettavan palvelun mainetta ei.

6 Miten suojaudun ongelmilta?

Hyökkäyksien kohteiksi valikoituu yleensä vanhentuneita ja päivittämättömiä julkaisujärjestelmiä. Pelkkä asianmukainen päivityssyklien seuraaminen pelastaa jo useimmilta harmeilta, joita huolimattomasta ylläpidosta voi seurata. Kytke julkaisuohjelmiston automaattiset päivitykset käyttöön.

Käytä vain tunnettuja ja aktiivisesti ylläpidettyjä julkaisuohjelmistojen laajennusosia. Poista tarpeettomat laajennusosat pois käytöstä. Varmista, että myös laajennusosien käyttämät laajennusosat saavat korjauksia ja päivitetään. Riippuvuusketju voi olla hämmästyttävän pitkä. Päivitykset kannattaa asentaa siitäkin syystä, että ne yleensä parantavat järjestelmän eri osien yhteentoimivuutta.

Sisällönhallintajärjestelmän salasanojen on oltava laadukkaita ja ainutkertaisia. Tarpeettomat tunnukset kannattaa poistaa. Esimerkiksi asennusvaiheessa automaattisesti luotavaa "admin"-nimistä tunnusta ei sisällönhallintajärjestelmissä yleensä tarvitse: täydet ylläpito-oikeudet voi antaa itse luomalleen tunnukselle. Näin tietomurtoja tehtailevien rikollisten täytyy arvata salasanan lisäksi myös ylläpitäjän käyttäjätunnus.

Etukäteen varautumalla voi helpottaa elämäänsä siinäkin tapauksessa, että sivustolle kaikesta huolimatta murtauduttaisiin. Säännölliset täydelliset varmuuskopiot sivuston sisällöstä helpottavat murron ajankohdan määrittämistä ja murtoa edeltäneen sisällön palauttamista. Varmuuskopioista on apua myös, jos jokin päivitys rikkookin sivuston toimivuuden.

7 Lisää aiheesta

- Tuore haavoittuvuus ja exploit kit -hyökkäysohjelmistot ovat vaarallinen yhdistelmä <https://www.viestintavirasto.fi/2015/07/ttn201507091330> (Tietoturva nyt! 9.7.2015)
- Haittaohjelma tarttuu, vaikka et klikkaisi mitään - osa 2 <https://www.viestintavirasto.fi/2015/09/ttn201509280841> (Tietoturva nyt! 28.9.2015)
- Ohje 1/2011 Verkkopalvelun ohjelmistoalustan valinta ja palvelun turvallinen ylläpito <https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje12011verkkopalvelunohjelmistoalustanvalintajapalvelunturvallinenyllapito.html>
- Incapsula: Why CMS Platforms Are Common Hacking Targets (and what to do about it) <https://www.incapsula.com/blog/cms-security-tips.html> [viitattu 17.2.2016]
- Sucuri: The Impacts of a Hacked Website <https://blog.sucuri.net/2015/03/the-impacts-of-a-hacked-website.html> [viitattu 17.2.2016]

Yhteystiedot
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi