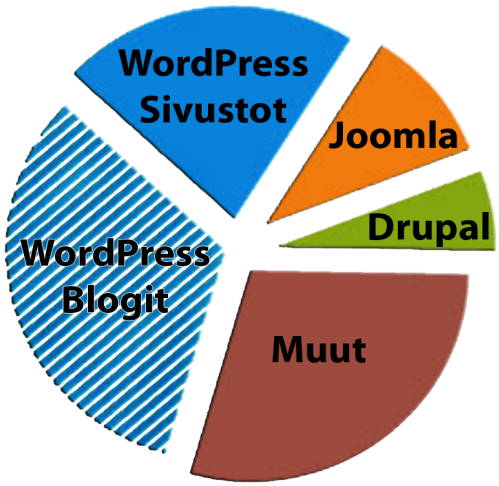
WordPressin tietoturvaopas

Miksi pelkkä julkaisujärjestelmän päivittäminen ei enää riitä?

Tämän oppaan on tarkoitettu kaikille, jotka ovat kohdanneet ongelmia WordPressin tietoturvan kanssa ja haluavat oppia suojaamaan WordPress-sivustonsa nykyaikaisin menetelmin. Oppaasta on sinulle hyötyä riippumatta siitä, onko sinulla teknistä osaamista vai ei.



Kuva: W3techs.com

Kun WordPress-pohjainen sivusto on ollut toiminnassa jonkin aikaa, sen tietoturvaa on varmasti kokeiltu ja sivustoon hyökätty moneen kertaan. Voit suhtautua tähän ikävänä asiaan, merkkinä että sivustosi on saavuttanut jonkinlaisen aseman. Mutta jos sivustosi olisi huomaamaton, kukaan ei olisi kiinnostunut sen hakkeroinnista.

Ongelma

Digitaalinen rikollisuus on ollut ongelmana siitä lähtien kun aloimme käyttää internetiä. Internetin pimeällä puolella varastetut luottokortti- ja henkilökohtaiset tiedot sekä salasanat ovat myytävänä ostajalle sopivaan hintaan.

Verkkorikollisuuden lisäksi myös eräs toinen asia aiheuttaa huolta. Innokkaiden nörttien kunnian hetki on muuttaa pieni aukko tietoturvassa kammottavaksi railoksi. Ja kun on tarpeeksi aikaa ja osaamista, lähes mikä tahansa verkkosivuston tietoturva on murrettavissa.

Nykyään hakkerointi tehdään usein automaattisten ohjelmistojen, eli bottien, avulla. Tämä on nopeuttanut hakkerien työtä, kun he voivat kokeilla niin nopeasti kuin mahdollista tuhansia eri salasanoja ja lomakkeita.

Samalla julkaisujärjestelmien teemojen ja lisäosien tietoturva-aukoista otetaan kaikki mahdollinen hyöty irti, ja muista että hakkeroinnin taustalla on harvoin henkilökohtaista kaunaa sinua kohtaan.

Tietoturvan haavoittuvuudet

Verkkohotelli

Useimmiten tietoturvariskit löytyvät verkkohotellista. Jos nettisivusi sijaitsee jaettulla palvelimella, jota ei päivitetä tarpeeksi usein tai jonka tarkkailu on vajavaista, hakkerit hyödyntävät heikon palvelimen tietoturvaa päästäksesi sivustosi kimppuun.

> **Ratkaisu:** Valitse aina käyttämäsi webhotelli huolella. Suosi palvelua, jolla on paljon kokemusta sivujen hallinnoimisesta. Testaa myös webhotellin asiakastukea tietääksesi, että he vastaavat nopeasti ja ovat halukkaita auttamaan sinua. Itse suosin Dedikoitu palvelin jossa DDOS suojaukset, ssl-sertifikaatit sekä palomuuri- ja virustorjuntamekanismit ajan tasalla.

Teemat

Jotkut teemat käyttävät kirjasto-tyypistä koodinpätkää, joka on luotu tiettyä tehtävää varten. Monet teemat voivat käyttää samaa kirjasto, kuvien koon muuttamiseen. Heti kun haavoittuvuus löydetään niistä, kaikki sitä käyttävät teemat ovat vaarassa tulla hakkeroiduksi.

> **Ratkaisu**: Suosi säännöllisesti päivitettäviä teemoja ja pidä päivitykset ajan tasalla.

Lisäosat

Lisäosat kärsivät samasta ongelmasta kuin teemat. Kehittäjät käyttävät tiettyjä kirjasto-tyyppisiä koodinpätkiä, joita yritetään hyötyä mahdollisimman laajasti. Jos lisäosa on tarpeeksi suosittu ja hakkereiden kannalta kiinnostava, kuten esimerkiksi verkkokaupan lisäosat, iso joukko hakkereita keskittyy saamaan kaiken irti lisäosan heikkouksista.

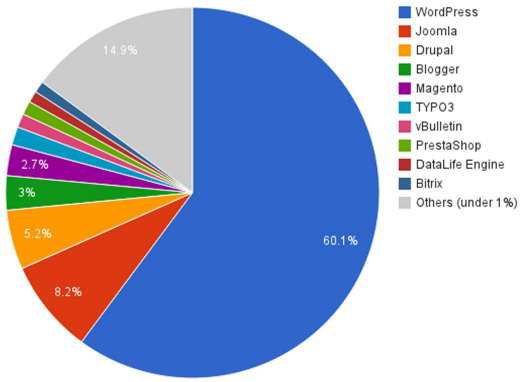
> **Ratkaisu**: Pidä lisäosat päivitettynä. Tämä on erityisen tärkeää silloin, jos käytössäsi on minkäänlainen asiakastietoja keräävä sivusto, verkkokaupat vielä erikseen mainittuna. Jälkimmäisessä tapauksessa suosittelen yhteydenottoa ammattimaiseen sivuston ylläpitäjään.

Salasanat

Jos salasanasi on lyhyt tai käyttää sanakirjasta löydettäviä sanoja, se on vaarassa tulla “arvaatuksi” ***brute force*** -hyökkäyksessä, jossa hakkerit kokeilevat automaattisten bottien avulla suurta määrää käyttäjätunnuksia ja salasanoja. Lopulta salasana murretaan ja hakkerit

pääsevät käsiksi sivustoosi. Suosittelen strongpasswordgenerator.com salasanageneraattori-palvelua jos ei ole saatavana itse julkaisujärjestelmässä sisäänrakennettua salasanageneraattoria.

Ratkaisu: Salasanasi tulisi olla vähintään 10 merkkiä pitkä ja sisältää numeroita, isoja ja pieniä kirjaimia sekä erikoismerkkejä. Jos sinulla on vaikeuksia muistaa salasanoja, käytä LastPass.com tai muuta vastaava palvelua salasanojen varastointiin, eli sellainen palvelu joka luo ja huolehtii kullekin sivustollesi yksilöllisen salasanan.

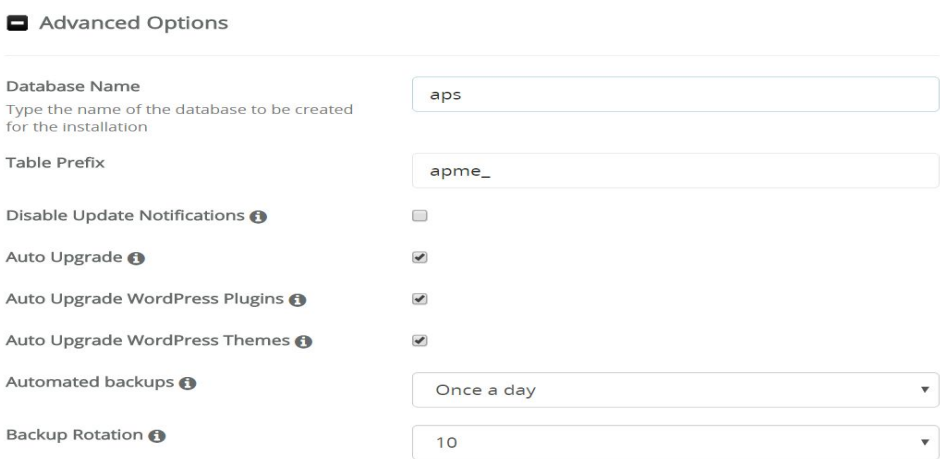


Kuva: W3techs.com 2015

Turvallinen WordPress asennus

Kunnolla asennettu ja konfiguroitu WordPress-pohjainen julkaisujärjestelmä on turvallinen, vaikka välillä ilmaantuu tietoturva-aukkoja. Lisäksi WordPressillä on nykyään automaattinen päivitysmekanismi ja WordPress -pohjaisen julkaisujärjestelmän päivitys on ollut helppoa viimeiset kuusi vuotta.

Ratkaisu: Pidä WordPress päivitettynä. Tarjoamme ammattimaisen ylläpito- ja päivitys palvelun, joten otathan Somea Oy:n yhteyttä, jos tarvitset apua WordPressin tietoturva-asioissa.



Tietokannat

On tiettyjä toimenpiteitä, joilla voit turvata WordPress-tietokannan. Esimerkiksi vaihtamalla asennuksen yhteydessä tietokantataulun etuliitteen (table prefix): Oletuksena annetaan **wp_**, joka on tietenkin kaikkien tiedossa ja täten tietoturvariski. Valitse etuliitteeksi satunnainen merkkijono, ja olet yhden askeleen lähempänä turvallista WordPress-tietokantaa.

> **Ratkaisu**: Tietokannan haavoittuvuuksien korjaus vaatii osaamista. Tietyt lisäosat auttavat tässä asiassa. Katso WordPressin yleisimmät tietoturvan lisäosat.

Oman sivuston turvaaminen

Tarjolla on monia lisäosia, jotka on suunniteltu suojaamaan verkkosivustoja boteilta ja pahantahtoisilta käyttäjiltä. WordPressin tietoturvasta on puhuttu paljon, joten uusia tietoturvalisäosia entistä edistyneemmillä ominaisuuksilla ilmestyy koko ajan. Tietoturvalisäosat joutuvat usein hyökkäysten kohteeksi siitä yksinkertaisesta syystä, että hakkerit kokevat haasteena tietoturva-lisäosan suojauksen murtamisen.

WordPressin yleisimmät tietoturva lisäosat

Ohessa lista tietoturvalisäosista, joita käytän itse omilla ja asiakkaitteni sivustoilla.

All in One WP Security & Firewall

Vahvuudet

- Ohjausnäkymän mittarit antavat helpon näkymän sivustosi turvatasosta.
- Jokainen toiminto on selitetty hyvin, joten saat tietoa ennen toiminnon päälle kytkemistä

Heikkoudet

- Tarjolla on muutama toiminto, jolla voit helposti rikkoa sivustosi.

WordFence Security

Vahvuudet

- WordFence on korkein arvostettu tietoturva lisäosista, josta on saatavana myös Premium versio.
- Voi tarkastaa sekä sivustosi että WordPressin alkuperäiset tiedostot varmistaakseen, että tiedostoissa ei ole tapahtunut muutosta.
- Voi tarkastaa WordPress-hakemiston ulkopuoliset tiedostot, kuten teemat, lisäosat ja ydin-tiedostot.
- Todella edistyksellisiä ominaisuuksia, kuten kirjautumismahdollisuus älypuhelimella.
- Maksullinen versio on aktivoinnin arvoinen.

Heikkoudet

- Oikeiden asetusten tekeminen voi olla hieman hankalaa.

Muut lisäosat

Tarjolla on paljon tietoturvalisäosia, joista paras on yleensä suosituin tai korkeimmalle pisteytetty. Suosioon vaikuttaa se, että kehittäjä on panostanut lisäosan kehitykseen ja päivitettynä pitämiseen.

Tietoturvalisäosien päivitys tulee olla säännöllistä, joten jos huomaat lisäosan päivityksestä kuluneen jo hyvän aikaa, kannattaa tietoturvalisäosa vaihtaa tuoreempaan versioon.

Jos testaat ja havaitset tietoturvalisäosien ilmaisversiot hyviksi, maksulliseen versioon siirtyminen kannattaa: Se auttaa kehittäjiä pysymään ajan tasalla ja antaa taloudellista tukea lisäosan kehittämiseen.

www.somea.org
Jan-Erik Finlander - 2016

Sivustoni on hakkeroitu! Mitä voin tehdä?

WordPress -pohjaisen verkkosivuston voi hakkeroida esimerkiksi yksinkertaisesti kirjoittamalla java-koodin sivun kommenttiosioon.

Vaihe 1

Rauhoitu hetkeksi. Jos olet paniikissa, et saa korjattua sivustosi parhaalla mahdollisella tavalla.

Vaihe 2

Jos hyökkäys näkyy julkisesti sivustosi kävijöille, kytke sivusi väliaikaisesti pois päältä. Tähän on tarjolla useampikin lisäosa: voit joko ilmoittaa kävijälle sivustosi olevan huoltotilassa tai ohjata hänet yksinkertaiselle sivulle ja jatkaa sivustosi huoltoa.

Tykkään itse käyttää WP Security -lisäosan sisäänrakennettua huoltotilaa, kun sivusto on alhaalla päivityksen tai huollon aikana. Toisaalta jos katko on yhtään pidempi (esim. yli tunti), itse käytän Ultimate Coming Soon Page -lisäosaa luodakseni kunnollisen sisääntulosivun.

Esimerkkejä huoltosivun tekstistä:

- Sivustoa huolletaan, joten se on hetken pois päältä. Pahoittelemme aiheuttamaamme hankaluuksista.
- Sivustoa huolletaan parhaillaan. Kokeile myöhemmin uudelleen!
- Sivusto on hetkellisesti poissa käytöstä. Vastaamme kysymyksiin Facebookissa!

Näin varmistat, etteivät mahdolliset asiakkaasi tai kilpailijasi näe sitä, mitä et halua heidän näkevän.

Vaihe 3

Tee koneellesi täysi virustarkastus: Et voi olla liian perusteellinen. Jos koneellesi on asennettu keylogger, se tallentaa kaikki näppäilyt, myös sivustosi salasanat. Seuraavan vaiheen salasanan vaihdossa ei ole järkeä, jos hakkerit saavat sen uudelleen haltuunsa!

Kun olet varma, ettei tietokoneesi itsessään ole tietoturvariski, voit siirtyä seuraavaan vaiheeseen.

Vaihe 4

Muuta WordPress-asennuksesi salasana. Joskus hakkerit ovat päässeet ohjauspaneeliin muuttamaan ylläpitäjän salasanasi, mikä tietysti joskus tuntuu aika pelottavalta. Tässä tapauksessa sinun täytyy palauttaa salasanasi alkutilaan. Helpoin tapa tähän on klikata "Salasana hukassa?" -linkkiä, jonka kautta saat sähköpostiisi ohjeet salasanan vaihtamiseen.

Jos et saa viestiä sähköpostiisi, on mahdollista, että hakkerit ovat poistaneet käyttäjätunnuksesi tai muuttaneet siihen liitetyn sähköpostiosoitteen.

Tästä linkistä löytyy yksityiskohtaiset ohjeet erilaisiin salasanan palautus menetelmiin. Valitse itsellesi paras ja jatka.

Vaihe 5

On aika tehdä WordPress-asennuksesi perusteellinen tarkastus. Tähän on tarjolla useita lisäosia, joissa kaikissa on hyvät ja huonot puolensa.

Itse käytän WordFence-lisäosaa kaikilla sivustoilla tarkistaakseni, onko palvelimen tiedostoihin tehty muutoksia. WordFenceä on kätevä käyttää, mutta ennen tarkastusta muutama asetuksen voimassaolo kannattaa varmistaa, jotta tarkastus olisi paras mahdollinen:

1. Siirry ohjauspaneeliin > WordFence > Options > Scans to include
2. Varmista, että kaikki asetukset (lukuun ottamatta "*Enable HIGH SENSITIVITY scanning. May give false positives.*") ovat päällä, erityisesti:
    - Scan theme files against repository versions for changes
    - Scan plugin files against repository versions for changes
    - Scan files outside your WordPress installation

Näiden muutosten avulla varmistat, että teema ja lisäosat ovat ehjinä, ja näet myös tiedostoissa tapahtuneet muutokset, jolloin osaat varautua tulevaa varten.

Vaihe 6

Varmista, ettei sivustosi ole mustalla listalla. Googlen musta lista on pahin kaikista, koska se voi vaikuttaa sivustosi hakukonenäkyvyyteen sekä maksettuihin mainoksiin, ja vierailu sinun yritys sivustolla voi myös lisätä varoituksen.

Viimeistään nyt sinun kannattaa tehdä Google-tili ja käyttää Google verkkovastaavan työkaluja, ne ilmoittavat, jos sivuillasi on ongelmia. Samassa paikassa voit tehdä sitemap.xml-tiedoston lähetyksen, näet sivuston näkyvyyden hakukonetuloksissa sekä saat neuvoja hakukonenäkyvyyten parantamiseen.

Vaihe 7

Tarkasta hosting-tilisi mahdollisten ongelmien varalta.

1. Muuta hallintapaneelin salasanasi.
2. Tarkasta WordPress-asennuksesi mm. käyttämättömien ali-toimialueiden varalta. Hyökkääjät voivat esim. luoda tarpeettomalle ali-toimialueelle skriptin, joka huonosti tehdyn uudelleenohjauksen myötä vahingoittaa varsinaista sivustoa.
3. Poista WordPressin turhat ja vanhat asennukset sekä testi- ja kokeiluversiot.

Vaihe 8

Joskus sivusto voi olla niin vahingoittunut, että ainoastaan varmuuskopion avulla sivusto palautuu ennalleen. Tarjolla on monia lisäosia varmuuskopiointiin, kuten WP Backup, jonka voi automatisoida ottamaan varmuuskopio WordPressistä: se voi myös lähettää varmuuskopion ulkopuoliselle palvelimelle, kuten Dropboxiin, Google Drivelle tai muuhun pilvitallennustilaan.

Vaihe 9

Päivitä WordPress asennuksen asetukset ja muuta kaikki salasanasi vielä kertaalleen.

Vaihe 10

Ota vielä kaiken varalta varmuuskopio korjatusta sivustasi. Harkitse myös valvonta- ja varmuuskopiointi palvelujen ostamista sivustosi suojaamiseksi jatkossa.

Tarvitsetko apua?

Tarjoamme WP tietoturvapalvelua, joka sisältää WordPressin täyden ylläpito- ja tietoturvapalvelun.

Tietoturva palvelupaketin päätoiminnot ovat:

- WordPressin tietoturvan implementointi ja -valvonta
- Järjestelmän, lisäosien ja teeman päivitykset
- Tiedostojen tarkistus muutosten varalta
- Eheystarkastukset
- Sivuston säännölliset varmuuskopiot
- Varmuuskopion palautus