Je website veilig de zomer(vakantie) door

Best veel ellende op het internet...

15-04-2019 12:10	WordPress-sites kwetsbaar door lek in CodeArt-plug-in
27-03-2019 12:18	Lek in Social Warfare-plug-in voor WordPress erger dan gedacht
20-02-2019 14:57	WordPress-sites kwetsbaar door ongepatcht beveiligingslek
16-09-2018 09:39	WordPress-sites aangevallen via lek in Duplicator-plug-in
24-10-2017 11:44	WordPress-sites aangevallen via zeroday-lek in plug-in
10-02-2017 09:42	Ruim 1,5 miljoen WordPress-pagina's aangepast via lek
28-12-2016 09:33	Miljoenen websites kwetsbaar door ernstig PHPMailer-lek

- Nieuwe Mirai-variant infecteert LG SuperSign-televisies
- Gehackte websites verspreiden malafide "browserupdates"
- Softwareontwikkelaar Plone ontkent hack van FBI-cms
- Ernstige kwetsbaarheden in Drupal-cms gedicht
- Cms-maker TYPO3 waarschuwt voor ImageMagick-lek
- Journalist saboteert ex-werkgever via geheim cms-wachtwoord
- CMS-lek kost Amerikaanse stad 760.000 dollar
- Joomla dicht ernstige lekken in CMS-software
- Kritiek lek in CMS-software Drupal gedicht
- TYPO3 waarschuwt voor kritiek lek in CMS

Hoe hou je je website veilig

- Zorg dat je eigen computer virusvrij is (de meeste besmettingen van websites ontstaan via de eigen computer)
- Gebruik alleen extensies en plugins van actieve en goede ontwikkelaars (gebruik geen “verlaten” extensies)
- Hou je extensies en plugins up-to-date
- Vergeet niet om ook je template up-to-date te houden
- Hou je CMS (Joomla!) up-to-date
- Zorg voor een goede hoster die zijn software up-to-date houdt
- Installeer een extra beveiligingslaag zoals Admin Tools of RSFirewall

Je computer virusvrij

- Windows: Gebruik een goede virusscanner zoals Bitdefender of Eset (al schijnt Windows Defender op het moment ook wel goed te zijn)
- Mac en Linux zijn minder vatbaar voor virussen maar ook hier is een virusscanner aan te raden (veilig surfen, blacklist domains)
- Zorg dat je besturingssysteem up-to-date is (maar wacht bij een grote Windows update toch maar even een weekje…). En ook hier geldt: **Backup, backup, backup**!!!!
- Scan je computer regelmatig
- Klik niet op onbekende short-links (zoals bijv. https://go.to/3o4324j33)
- Bezoek geen dubieuze sites
- Reageer niet op SPAM-mailtjes

Hou alle extensies up-to-date

- Gebruik alleen extensies en plugins van actieve en goede ontwikkelaars (bekijk de JED)
- Gebruik extensies en plugins die gebruik maken van de Joomla Updater
- Voordat je updates gaat uitvoeren: **Backup, Backup, Backup**
- Je template is ook een extensie. Hou deze ook up-to-date!

Hou Joomla up-to-date

- Joomla kan eenvoudig, met een druk op de knop, worden geüpdatet
- Voordat je een update van Joomla gaat doen: **Backup, Backup, Backup** (voorkeur Akeeba anders binnen hosting)
- Zorg dat, voor je een update uitvoert, alle extensies / plugins en je template up-to-date zijn
- Na een update-ronde kijken of je temp-map leeg is. Soms kan hier nog wat overblijven als een update niet helemaal goed is gelukt. Dit kan een beveiligingsrisico zijn. (Admin Tools -> Leeg Temp map).

Host je site bij een goede hoster

Een goede hoster

- Is (gratis!) bereikbaar (chat, mail, telefoon)
- Reageert snel
- Heeft de hostingsoftware inclusief de LAMP stack up-to-date
- Biedt DNS-beheer
- Heeft Joomlakennis
- Vraag ervaringen bij andere (Joomla-)gebruikers

Let op: Goedkoop kan duurkoop zijn!!

Extra beveiliging met Akeeba Admin Tools

Als alles up-to-date is kun je nog een extra beveiligingslaag aan je website toevoegen met **Admin Tools** van Akeeba. Admin Tools bevat:

- Web Application Firewall (reageert op verdachte zaken binnen je website)
- .htaccess maker (met dit bestand kun je je site optimaliseren en extra beveiligen)
- Rechten van mappen (755) en bestanden (644) controleren en waar nodig weer goed zetten
- Temp-map opschonen
- Databasetabellen opschonen / repareren
- Generatortag aanpassen
- …

Admin Tools voor beginners

- Installeer Admin Tools
- Voer de Quick Setup Wizard uit
- Administrator secret URL parameter gebruiken
- Disable editing backend users' properties -> Nee
- Forbid frontend Super Administrator login -> Ja
- Enable IP workarounds -> Nee (meestal, behalve als je achter een proxy zit)
- Create a security tightening .htaccess -> Ja
- Opslaan
- Klaar… Nou ja, nog niet helemaal

Admin Tools .htaccess… Toch een beetje gevorderd…

Hoe vind je wat je moet aanpassen?

- Met Firefox en de functie “Element inspecteren”
- Kies dan de tab “Netwerk”
- Alle statussen moeten 200 (Ok) of 304 (Not modified) zijn.
- Status 403 moet opgelost worden in de .htaccess maker

Admin Tools .htaccess… Toch een beetje gevorderd…

In de .htaccess maker

- **Allow direct access to these files**
  - (delen van) bepaalde componenten, bijv. Fabrik
  - Sitemap.xml (als je wilt dat Google deze kan bereiken)
- **Allow direct access, except .php files, to these directories**
  - images/
  - media/
  - cache/plg_jch_optimize
  - media/plg_jchoptimize/cache/css
  - media/plg_jchoptimize/cache/js

Admin Tools .htaccess… Toch een beetje gevorderd…

- **Allow direct access, including .php files, to these directories**
  - templates/yootheme
  - cache/template
  - media/template
  - components/com_fabrik/views/form/tmpl/bootstrap
  - components/com_fabrik/views/list/tmpl/bootstrap

Je site is nu goed beveiligd. Fijne vakantie!

Vragen?