Keeping a Web Site Safe and Available With or Without a CDN

By *Roy Schestowitz*
Created *23/10/2019 - 7:47pm*
Submitted by Roy Schestowitz on Wednesday 23rd of October 2019 07:47:35 PM Filed under Site News [1]

THE site *Tux Machines* is and has been online for over 15 years. It has not suffered security-related incidents. The same is true for *Techrights*, which soon turns 13. *Tux Machines* uses Gallery and Drupal, whereas *Techrights* uses MediaWiki, WordPress and Drupal. WordPress is its most important component as it contains over 26,000 posts. *Tux Machines* has about 130,000 nodes in Drupal. We don't use a CDN as we have a reasonably powerful server that can cope with the load on its own. For security we use best practices and keep critical issues plugged. I was recently asked for advice on these matters and explained things as follows.

There are mainly two types of attacks (maybe three if one includes social engineering, e.g. tricking a citizen journalist/blogger/administrator into a trap):

1) capacity-based, e.g. DDOS attack

2) exploiting vulnerabilities to degrade/compromise site's quality of service (similar to (1) above but not the same), access site data (confidential), spy on people (writers/staff/visitors) without them being aware.

WordPress runs lots of stuff and powers a lot of the Web, maybe 20% (or more) of today's Web sites. It's regularly checked for security issues and bugs are regularly fixed. Updates can be set to automatic, which means they happen in the background without user intervention. I check the site for updates several times per day, e.g. this one from yesterday [2].

I've used WordPress for 15 years as an early adopter and developer.

What's known as the "core" of WordPress is generally secure if kept up to date, manually or automatically (for large sites it might make sense to apply patches manually to reduce risk of unnoticed incidents and enable quality control, patch assessment etc). It's also important to keep the underlying operating system and pertinent packages like PHP (programming language), mysql/psql (WordPress and Drupal typically use MariaDB or MySQL as the database, but PostgreSQL should be possible too) and Apache (there are simpler alternatives e.g. NGINX for Web server) up to date.

If we get to keep everything up to date, and moreover we don't install WordPress extensions that cannot be trusted or are no longer maintained (or scarcely maintained), we should be OK. The social engineering part involves stuff such as phishing, e.g. someone sending out an E-mail in an attempt to obtain passwords of privileged users.

If you use a CDN for content distribution, e.g. CloudFlare, then availability will be mostly down to the CDN company. WordPress generates pages on the fly (dynamic), but it has caching mechanisms that can be further improved with extensions. The CDN likely obviates the need for those. So, if the site is receiving 'too many' requests, the CDN can probably scale to deal with that (maybe a more expensive protection plan).

I peronsally would never use CloudFlare (for a lot of reasons), but to many people it's the only CDN that 'counts' or exists. Brand recognition perhaps. ?

Site News

Links:
[1] http://www.tuxmachines.org/taxonomy/term/122
[2] https://wordpress.org/news/2019/10/wordpress-5-3-rc2