PHP 5.6 - veraltet (Evtl. interessant für die ein oder andere Schulhomepage)

Beitrag von „Volker_D“ vom 25. Januar 2019 22:24

Danke für das Vertrauen, aber meine PHP-Kenntnisse sind gering.

Bei meinem Webhoster wurde ich über diesen Sachstand vor ein paar Monaten sowohl per Mail als auch per Blog informiert:
https://www.goneo.de/blog/2018/10/1...-november-2018/

Da sich bei mir der Webhoster um die Installation und Wartung von PHP kümmern, brauchte ich nur zwei einfache Punkte druchführen:
- Nachlesen, ob Contentmanager, Blog, ... neuere PHP Versionen unterstützen. Ggf neuere Versionen des Contantmanagers, Blog, ... installieren und/oder testen, ob es mit der neueren Version läuft.
- im Menü auf die neue PHP umstellen
In einfachen Fällen handelt es sich also - je nach Webhoster - um maximal zwei einfache Klicks im Menü des Webhosters.

Falls man seinen Webserver selbst konfiguriert hat, muss man dann doch etwas mehr Arbeit investieren. Aber ich denke, dass die Lehrer, die den Webserver komplett selbst aufgesetzt haben auch von alleine wissen was sie machen müssen. Sollten Sie feststellen, dass ein Lehrer PHP (bzw. die Homepage) damals aufgesetzt hat und es danach (abgesehen vom Inhalt) nie mehr jemand gepflegt hat, dann besteht das Problem streng genommen nicht erst seit dem 31.12, sondern schon viel länger. Denn kritische Sicherheitspatches für PHP gab es in den letzten Monaten immer wieder. Man muss daher regelmäßig neue Versionen einspielen!
Da die meisten Lehrer dafür keine Zeit bzw zu wenig Ahnung haben, kann ich nur dringend empfehlen sich einen Webhoster zu suchen, der dies regelmäßig für seine Kunden macht.

Und dies ist kein theroretisches Problem, sondern sehr erst. So ernst, dass php sogar noch einmal außerplanmäßig ein Update herausgebracht hat:
http://php.net/ChangeLog-5.php
Nur so als Hinweis für Ahnungslose: Immer wenn da soetwas wie "fixed Heap Buffer Overflow" steht, dann war das eine potentielle kritische Sicherheitslücke. Angreifer, die ein bischen Ahnung haben, brauchen da also nicht viel ausprobieren und "hacken"; die lesen im Changelog nach wo die Sicherheitslücke besteht und wissen dann auch recht schnell wie man diese Lücke für Angriffe ausnutzt.