Informationsblatt

Onlineprüfung: Patch Management bei WordPress / WP Plugins

Stand: 16.11.2018

Rechtliche Grundlage zur Onlineprüfung

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) überwacht als Datenschutzaufsichtsbehörde nach Art. 58 der Datenschutz-Grundverordnung (DS-GVO) die Einhaltung des Datenschutzrechts im nichtöffentlichen Bereich im Bundesland Bayern, d. h. in privaten Wirtschaftsunternehmen, bei freiberuflich Tätigen, in Vereinen und Verbänden. Aufgrund der enorm gestiegenen Gefährdungslage im Internet stärkt das BayLDA seinen Fokus auf präventive Maßnahmen zur Cybersicherheit für bayerische Verantwortliche, damit personenbezogene Daten von diesen angemessen und wirksam vor den täglichen Gefahren im digitalen Zeitalter geschützt werden. Das BayLDA führt für diesen Zweck flächendeckende automatisierte Prüfungen durch, um Sicherheitslücken aufzuzeigen und insbesondere die Betreiber von Webseiten in Bayern zu sensibilisieren. Auch wenn der vorbeugende Charakter der Onlineprüfungen des BayLDA hervorgehoben wird, besteht durch die DS-GVO neben der bereits existierenden gesetzlichen Verpflichtung, für ein ausreichendes Sicherheitsniveau im Umgang mit personenbezogenen Daten zu sorgen, auch grundsätzlich die Möglichkeit, bei schwerwiegenden Verstößen gegen die „Sicherheit der Verarbeitung" Bußgelder gegen den verantwortlichen Websitebetreiber zu verhängen.

Patch Management

Ein zentrales Grundelement der IT-Sicherheit und des Datenschutzes ist das Patch Management. Diese Disziplin beschäftigt sich insbesondere mit der Beschaffung, dem Testen und dem Einspielen wichtiger Updates für Anwendungen. Patches sind als bedarfsorientierte Korrekturen zu betrachten, um gezielt Fehler und bekannte Schwachstellen zu beheben, die den sicheren Betrieb einer Anwendung gefährden. Patch Management ist aus datenschutzrechtlicher Sicht eine gesetzliche Anforderung, um personenbezogene Daten, die durch eine Anwendung verarbeitet werden, angemessen zu schützen. Verantwortliche, d. h. auch Webseitenbetreiber, müssen Verfahren etablieren, um regelmäßig überprüfen, bewerten und evaluieren zu können, ob die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung auch tatsächlich wirksam sind. Im Umfeld von Webseiten ist es daher wichtig, die bereitgestellten Sicherheitspatches zeitnah einzuspielen.

Gefährdungslage bei Content-Management-Systemen (CMS)

Bei CMS-Installationen ist zu prüfen, ob die eingesetzten Versionen dem aktuellen Stand entsprechen. Auf Grund der hohen Verbreitung von CMS im Web besteht eine **sehr große Gefahr**, dass bei nicht rechtzeitig eingespielten Patches Angreifer Schwachstellen flächendeckend ausnutzen und nicht unerheblichen Schaden verursachen. Dem BayLDA sind viele Vorfälle hierzu bekannt. Cyberkriminelle können die Lücken im System selbst oder in Erweiterungen (Extensions) als Einfallstor nutzen, um Daten zu manipulieren, vertrauliche Daten auf dem Webserver abzuschöpfen oder auch gefährlichen Schadcode (Malware) zu platzieren, um die Besucher der Webseite zu infizieren. Somit sind sowohl die betroffenen Kunden geschädigt (ungewollte Weitergabe bzw. Offenbarung von persönlichen Informationen) als auch der verantwortliche Websitebetreiber (u. a. Kosten für Wiederherstellung der Systeme, Reputationsverlust).

WordPress Versionen

WordPress ist eine sehr weit verbreitete CMS-Applikation und daher besonders im Fokus von Angreifern. Es ist stets zu prüfen, ob für die eigene Webseite bzw. eigene WordPress-Installation neue Sicherheitsupdates verfügbar sind und eingespielt werden können. **Zeitnahes Handeln ist hierbei besonders wichtig**, da das Zeitfenster vom Bekanntwerden einer Lücke bis zum Ausnutzen der selbigen nur wenige Stunden betragen kann. Zu beachten ist, dass nicht nur ein CMS wie WordPress selbst Angriffsfläche bieten kann, sondern auch die eingesetzten Plugins (Extensions) und Templates (Themes). Folglich ist es notwendig, bei den Plugins und den anderen Komponenten ein ebenso konsequentes Patch Management zu betreiben.

Schwachstelle in WordPress-Erweiterung „WP GDPR Compliance“

Anfang November 2018 wurde bekannt, dass in der WordPress-Erweiterung WP GDPR Compliance eine **schwerwiegende Sicherheitslücke** besteht. Setzt ein Websitebetreiber diese Erweiterung auf seiner eigenen WordPress-Website ein, können Cyberkriminelle ohne nennenswerten Aufwand die vollständige Kontrolle über die WordPress-Installation und ggf. sogar den Webserver übernehmen. Bis einschließlich Version 1.4.2 ist das Plugin verwundbar und als äußerst kritisch einzustufen. Dem BayLDA sind bereits einige Fälle bekannt, bei denen die Websites von Unbefugten „übernommen“ wurden und der Schutz der Daten somit nicht mehr gewährleistet werden konnte. Sollten Sie bislang keine Informationen zu dieser Lücke haben, empfehlen wir Ihnen in Ihrem eigenen Interesse im Web kurz zu recherchieren und die Meldungen von IT-Fachmagazinen dazu zu verfolgen.

Was ist zu tun, wenn das Plugin in der Version 1.4.2 (oder kleiner) zum Einsatz kommt?

Die Versionen 1.4.2 oder kleiner dieser Erweiterung sind als **verwundbar** einzustufen. Entsprechend muss das Plugin entweder deinstalliert oder auf die derzeit abgesicherte Version 1.4.3 aktualisiert werden. Auf Grund des Einsatzes des unsicheren Plugins besteht die reale Gefahr, dass sich ein Angreifer bereits Zugang zum betroffenen WordPress-System verschafft hat. Folglich muss zeitnah, wenngleich aber auch sorgsam geprüft werden, ob Veränderungen am System durchgeführt wurden. Die Wahrscheinlichkeit, dass es bereits „fremde“ Nutzer mit Admin-Rechten in den betroffenen Systemen gibt, schätzen wir für **sehr hoch**. Zwingend untersucht muss die Nutzerverwaltung dahingehend, ob „neue“ Administratoren-Nutzer wie z. B. „t2trollherten“ angelegt wurden – dies ist ein Hinweis dafür, dass sich ein Angreifer durch die Sicherheitslücke Zugang zum System verschaffen konnte. Unbekannte Nutzer sind zu löschen. Eine Auswertung der vorhandenen Log-Files ist zielführend (Access Logs). Durch einen Sicherheitsscan kann meist schnell festgestellt werden, ob Dateien oder die Datenbank verändert wurden. Im Zweifel muss nicht nur das eigene Administratorenpasswort geändert, sondern auch ein sicheres Backup der WordPress-Installation eingespielt werden, um die infizierte Version zu bereinigen.

Was ist zu tun, wenn das Plugin bereits in der „abgesicherten“ Version 1.4.3 eingesetzt wird?

Durch eine kurzfristig zur Verfügung gestellten Version 1.4.3 ist die Sicherheitslücke behoben worden. Websitebetreiber, die die Version 1.4.3 der WP GDPR Compliance Erweiterung einsetzen, sind somit nicht mehr akut über diese Sicherheitslücke angreifbar. Das bedeutet jedoch nicht, dass dadurch ausgeschlossen werden, dass die Lücke in dem „offenen Zeitraum“ ausgenutzt wurde. Entsprechend müssen die betroffenen Websitebetreiber auch hier prüfen, ob im Zeitraum bis zur Aktualisierung der Erweiterung (Update auf 1.4.3) ein Angriff stattgefunden hat. Hierzu muss insbesondere begutachtet werden, ob sich ein Unbefugter Zugang zum System verschaffen konnte – die oben aufgeführten Prüfmaßnahmen sind daher auch hier durchzuführen.