INFORMATIONSBLATT

Onlineprüfung: Patch Management

Stand: 08.02.2018

Rechtliche Grundlage zur Onlineprüfung

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) überwacht als Datenschutzaufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes (BDSG) die Einhaltung des Datenschutzrechts im nicht-öffentlichen 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 gezielt aufzuzeigen und die Betreiber der betroffenen Plattformen in Bayern zu sensibilisieren. Auch wenn der vorbeugende Charakter der Onlineprüfungen des BayLDA hervorgehoben wird, besteht künftig 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 nach der EU-Datenschutz-Grundverordnung (DS-GVO) Bußgelder gegen den Verantwortlichen 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 insbesondere 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 ein 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 regelmäßig 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. Cyberkriminelle können die Lücken als Einfallstor nutzen, um Daten zu manipulieren (z. B. verfassungswidrige Inhalte veröffentlichen), vertrauliche Daten auf dem Webserver abzuschöpfen oder auch gefährlichen Schadcode (Malware) zu platzieren, um die Besucher der Webseite zu infizieren. Im politischen Umfeld ereignen sich auch sog. „Defacement"-Attacken, bei dem Hacker durch die Schwachstellen auf die Startseite des Webauftritts ihre eigenen politischen Botschaften platzieren und den eigentlichen Betreiber bloßstellen.

WordPress Versionen

WordPress ist eine der meistgenutzten CMS-Applikationen und daher besonders im Fokus von Angreifern. Es ist stets zu prüfen, ob für die eigene Webseite neue Sicherheitsupdates verfügbar sind und eingespielt werden können. Zeitnahes Handeln ist hierbei 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 eingesetzte Plugins und Themes für das CMS. Folglich ist es notwendig, bei den Plugins und anderen Komponenten ein ebenso konsequentes Patch Management zu betreiben. Zum Zeitpunkt der Prüfung war die aktuelle WordPress-Version 4.9.2, durch welche die eine Lücke zum Cross-Site-Scripting geschlossen wurde (CVE-2018-5776). Allerdings wurde kurz nach der Prüfung, noch vor dem Versenden der Schreiben an die verantwortlichen Webseitenbetreiber in Bayern, auch in der Version 4.9.2 eine Schwachstelle gefunden (CVE-2018-6389). Mittlerweile sind die Versionen 4.9.3 und 4.9.4 veröffentlicht worden.

Tipps zum sicheren Einsatz eines CMS

- ✓ Regelmäßige Backups
- ✓ Absicherung des Konfigurations- und Admin-Bereichs (z. B. Verzeichnis wp-admin)
- ✓ Sicherheitspatches einspielen
- ✓ Benutzerrechte einschränken
- ✓ Verschlüsselten Login nutzen (und ggf. Zwei-Faktor-Authentifizierung)

Bedeutung von HTTPS, insb. bei CMS

HTTPS ist eine Ergänzung des Internetprotokolls HTTP, durch das Daten auf dem Transportweg verschlüsselt werden. Ohne diese Verschlüsselung sind Daten, die über das Internet übertragen werden, von den an der Kommunikation beteiligten im Klartext lesbar. Dadurch wird die gesetzliche Anforderung unterlaufen, nach der zu gewährleisten ist, dass personenbezogene Daten bei der elektronischen Übertragung nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können. Bestandteil der Onlineprüfungen des BayLDA ist daher stets, ob Webseiten über eine ausreichende HTTPS-Verschlüsselung verfügen, um den Datentransfer zwischen dem Browser des Nutzers und dem Webserver des Verantwortlichen abzusichern. Dies gilt besonders für Webseiten, bei denen Kontakt- oder Zahlungsdaten eingegeben werden können, aber auch bei CMS-Webseiten, die u. a. über Login-Möglichkeiten verfügen. Setzt ein Verantwortlicher bspw. WordPress als CMS ein, so ist meist über den Standardlink *wp-login.php* die Eingabe von Benutzername/E-Mail-Adresse und Passwort möglich. In den Fällen, in denen diese Seite nicht mit HTTPS verschlüsselt ist, können die eingegebenen Daten des Nutzers u. U. in falsche Hände geraten. Die Anmeldung muss daher zwingend per HTTPS abgesichert werden.

Anforderungen für eine HTTPS-Verschlüsselung

- ✓ Kein Einsatz veralteter Verschlüsselungsprotokolle (SSL2, SSL3)
- ✓ TLS 1.2 als Standardprotokoll
- ✓ Priore Verwendung von Perfect Forward Secrecy (PFS)
- ✓ Geeignete Schlüssellänge des SSL-Zertifikats
- ✓ Keine SSL-Zertifikate mit SHA-1
- ✓ Keine unsicheren Kryptoalgorithmen (z. B. RC4, Export-Chiffren,…)
- ✓ Verwendung aktueller Softwareversionen (z. B. Webserver, Firewall,…)
- ✓ Verwendung von HTTP Strict Transport Security (HSTS)
- ✓ Geeignete SSL-Zertifikate
- ✓ Einsatz von HTTP Public Key Pinning (nicht zwingend, aber empfohlen)