Informationsblatt

Onlineprüfung: Patch Management bei Magento-Shops

Stand: 29.10.2018

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 Online-Shops

Bei Shop-Installationen ist zu prüfen, ob die eingesetzten Versionen dem aktuellen Stand entsprechen. Auf Grund der hohen Verbreitung von Shop-Systemen im Web besteht eine sehr große Gefahr, dass bei nicht rechtzeitig eingespielten Sicherheitspatches Angreifer Schwachstellen nicht nur einzeln, sondern auch flächendeckend ausnutzen und erheblichen Schaden verursachen. Dem BayLDA sind viele aktuelle Vorfälle hierzu bekannt. Cyberkriminelle können die Lücken als Einfallstor nutzen, um vertrauliche Daten der Kunden auf dem Webserver abzuschöpfen oder auch gefährlichen Schadcode (Malware) zu platzieren, um die Besucher der Website zu infizieren. Somit sind sowohl die betroffenen Kunden geschädigt (ungewollte Weitergabe bzw. Offenbarung von persönlichen Informationen wie z. B. Zahlungsdaten) als auch der verantwortliche Websitebetreiber (u. a. Kosten für Wiederherstellung der Systeme, Reputationsverlust).

Magento-Versionen

Magento ist ein in Deutschland weit verbreitetes Shop-System und daher besonders im Fokus von Angreifern. Es ist von Verantwortlichen stets zu kontrollieren, ob für die eigene Webseite neue Sicherheitsupdates des Herstellers verfügbar sind und eingespielt werden können (siehe https://magento.com/security). Zeitnahes Handeln ist hierbei äußerst 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 Shop-System wie Magento selbst Angriffsfläche bieten kann, sondern auch die eingesetzten Erweiterungen (Extensions) und individuellen Anpassungen (Customizing). Folglich ist es notwendig, bei allen auf dem Webserver eingesetzten Komponenten ein konsequentes Patch Management zu betreiben. Zum Zeitpunkt unserer Prüfung war die aktuelle verfügbare Magento Commerce und Open Source Version 2.2.6, durch welche kritische Sicherheitslücken, u. a. zum Cross-Site-Scripting, in Vorversionen geschlossen wurden. Im Ergebnisblatt zur Prüfung werden die Prüfkriterien benannt und das auf Ihrer Website vorgefundene dazugehörige Ergebnis dargestellt.

Datenschutz-Tipps zum sicheren Einsatz von Magento-Shops

- ✓ Regelmäßige Backups durchführen und sicher aufbewahren
- ✓ Updates grundsätzlich zeitnah einspielen (Fokus auf Security Patches)
- ✓ Magento Security Scan nutzen, um serverseitige Schwachstellen zu entlarven
- ✓ Magento Best Practices des Herstellers berücksichtigen (magento.com/security/best-practices)
- ✓ Falls Dienstleister eingesetzt werden: Beim Abschluss eines Auftragsverarbeitungsvertrags klar definieren, wer für was zuständig ist (insb. für das Einspielen von Patches)
- ✓ Absicherung des Konfigurations- und Administrationsbereichs des Shops (z. B. nur von vorgegebenen IP-Adressen aufrufbar konfigurieren, .htaccess als zusätzlichen Schutz einrichten)
- ✓ Verstecken sensibler Ressourcen und Pfade wie /admin/
- ✓ Anzahl erlaubter Anfragen zum Zurücksetzen eines Passworts ebenso wie die Anzahl der möglichen Login-Versuche einschränken (z. B. auf den Wert „3“ setzen)
- ✓ Beim Erreichen der Höchstzahl an Fehlversuchen eine Sperrung vornehmen
- ✓ Zeit zum Ablaufen des Passwortlinks bei Zurücksetzen-Anfragen möglichst gering halten (z. B. eine Stunde)
- ✓ Falls möglich: CAPTCHA-Abfragen für den Administratorenbereich nutzen
- ✓ Am besten: Zwei-Faktor-Authentifizierung für den Administratorenbereich implementieren (z. B. auch durch eine Extension möglich)
- ✓ Voreingestellte Nutzer und Standardkennungen wie „admin“ ändern oder löschen
- ✓ Benutzerrechte einschränken und stets sichere Passwörter erzwingen (Länge, Komplexität)
- ✓ Ausschließlich verschlüsselten Login nutzen (siehe HTTPS unten)
- ✓ Kundendaten nur verschlüsselt speichern (sicheren Kryptoalgorithmus verwenden)
- ✓ Durchgängig HTTPS bei der gesamten Website verwenden:
    - Kein Einsatz veralteter Verschlüsselungsprotokolle (SSL2, SSL3)
    - TLS 1.2 als Standardprotokoll (auch TLS 1.3 im Blick behalten)
    - Vorrangige Verwendung von Perfect Forward Secrecy (PFS)
    - Geeignete Schlüssellänge des SSL-Zertifikats
    - Keine SSL-Zertifikate mit SHA-1 und unsichere Kryptoalgorithmen (z. B. RC4)
    - HTTP Strict Transport Security (HSTS) nutzen
    - Geeignete SSL-Zertifikate (nicht selbstsigniert, passende CA)
    - Einsatz von HTTP Public Key Pinning empfohlen
- ✓ Sichere und aktuelle Komponenten verwenden (u. a. Themes, Extensions)
- ✓ Über den Einsatz einer Web-Application-Firewall nachdenken (insb. Schutz vor SQL-Injections und XSS)
- ✓ Monitoring-Tools für den Online-Shop bzw. die Website nutzen
- ✓ Top 10 des Open Web Application Security Projects (OWASP) im Auge behalten