Bayerisches Landesamt für
Datenschutzaufsicht

Bayer. Landesamt für Datenschutzaufsicht | Postfach 606 | 91511 Ansbach

Unternehmen ABC
Geschäftsführung
Musterstraße XYZ
12345 Musterstadt

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 | 91522 Ansbach
Telefon: 0981 53 1300
Fax: 0981 53 98 1300
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Ihr Ansprechpartner
[...]
[...]@lda.bayern.de
Telefon: 0981 53 [...]
Fax: 0981 53 [...]

MUSTER

Ihr Zeichen	**Unser Aktenzeichen**	
-	[...]	Ansbach, -.2018

Aufsicht nach § 58 Datenschutz-Grundverordnung (DS-GVO);

Datenschutzprüfung hinsichtlich des Einsatzes sicherer Online-Shop-Systeme in Bayern;
hier: Kontrolle der Magento-Installation auf Ihrer Website [...]

Anlagen: Informationsblatt, Ergebnisblatt, Antwortbogen

Sehr geehrte Damen und Herren,

wir, das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), überwachen die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich in Bayern, das heißt primär in den privaten bayerischen Wirtschaftsunternehmen, bei den freiberuflich Tätigen, in Vereinen sowie in Verbänden. Im Rahmen unserer Cybersicherheitsinitiative prüfen wir die Sicherheit der Verarbeitung personenbezogener Daten, die über das Internet versendet oder erreicht werden können. Dafür untersuchen wir die in unserer Zuständigkeit befindlichen bayerischen Webseiten gezielt dahingehend, ob diese über ein angemessenes Sicherheitsniveau verfügen und die personenbezogenen Daten (u. a. die der Webseitenbesucher und der Kunden) gemäß den gesetzlichen Datenschutzanforderungen nach dem Stand der Technik verarbeiten.

Nachdem wir zuletzt Untersuchungen hinsichtlich HTTPS, WordPress und Ransomware in Bayern durchgeführt haben, ist Prüfungsgegenstand dieser Kontrolle der sichere Einsatz von Online-Shop-Systemen. Konkret prüfen wir derzeit stichprobenartig **Magento**-Shops dahingehend, ob bei den betroffenen Systemen alle verfügbaren kritischen Sicherheitspatches eingespielt und bekannte Schwachstellen behoben wurden. Des Weiteren wird überprüft, ob die verantwortlichen Websitebetreiber über einen geregelten Prozess zum Patch Management verfügen sowie die datenschutzrechtlichen Verpflichtungen im Umgang mit Sicherheitsverletzungen im Bedarfsfall umsetzen können (Incident Response).

Hintergrund dieser Datenschutzprüfung sind öffentlich diskutierte, kritische Sicherheitsvorkommnisse beim Einsatz von Magento-Shops. Bereits 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer Pressemitteilung darüber berichtet, dass über 1.000 deutsche Online-Shops von Online-Skimming betroffen sind. Ursache war der Einsatz veralteter Shop-Software, wodurch Kriminelle schädlichen Programmcode in die jeweilige Website einschleusen konnten. Im September 2018 wurde erneut über einen großangelegten Angriff auf Magento-Shops in IT-Fachmagazinen berichtet, bei dem Administratorenkonten geknackt und anschließend Malware zur Protokollierung der Nutzereingaben platziert wurde. Auch wir als Aufsichtsbehörde haben im Rahmen von Meldungen nach Art. 33 DS-GVO zuletzt direkt von konkreten Hacking-Vorfällen bei Magento-Installationen erfahren. Diese Vorkommnisse zeigen uns, dass nicht bei jedem Websitebetreiber die Anforderungen für einen sicheren und datenschutzkonformen Betrieb bekannt sind oder, falls doch, vernachlässigt werden.

Für Websitebetreiber ist es notwendig, durch gezieltes Patch Management vorhandene Lücken zu schließen und die vom Hersteller bereitgestellten neuesten Versionen zeitnah einzuspielen, um so den vielfältigen Angriffsmöglichkeiten von Cyberkriminellen präventiv entgegenzutreten. Patch Management ist dabei nicht nur als wichtige Disziplin aus dem IT-Sicherheitsbereich anzusehen, sondern eben gerade auch im Datenschutzumfeld als gesetzlich verpflichtende Vorgabe verankert. Ohne das Einspielen von kritischen Sicherheitspatches und Updates kann der Schutz personenbezogener Daten auf der jeweiligen Website nicht gewährleistet und nachgewiesen werden kann. Ein Verstoß gegen Vorgaben zur Sicherheit der Verarbeitung nach Art. 32 DS-GVO kann dabei mit einem Bußgeld bis zu 10 Millionen EUR oder 2% des weltweit erzielten jährlichen Umsatzes geahndet werden.

Im Rahmen dieser Onlineprüfung wurde Ihre Webseite zufällig ausgesucht und gemeinsam mit einigen anderen Websites hinsichtlich bestimmter Prüfkriterien kontrolliert. Hauptfokus lag dabei darauf, ob kritische Sicherheitspatches des Herstellers eingespielt wurden und Ihr Online-Shop vor typischen Angriffen geschützt ist. Die Hintergründe zu dieser Prüfung können Sie dem beigefügten Informationsblatt entnehmen.

Die Prüfkriterien und das detaillierte Ergebnis unser Datenschutzprüfung Ihrer Magento-Installation haben wir auf einem separaten Ergebnisblatt zusammengefasst. Wir bitten Sie, die dort aufgelisteten Punkte zur Kenntnis zu nehmen und zu prüfen, ob Sie die adressierten Ergebnisse bestätigen können. Sollten Defizite von uns festgestellt worden sein, sind Abhilfemaßnahmen durchzuführen. Wir bitten Sie danach, den beiliegenden Antwortbogen zu nutzen, um uns Ihre Stellungnahme hierfür zukommen zu lassen und zu bestätigen, dass Sie die erforderlichen Abhilfemaßnahmen (bei Bedarf) getroffen haben. Von individuellen Antwortschreiben und telefonischen Nachfragen ist auf Grund des Charakters der Prüfung abzusehen, da es sich um eine Großprüfung mit mehreren angeschriebenen Verantwortlichen handelt. Sollten Sie Fragen zur Prüfung haben, bitten wir stattdessen die dafür eingerichtete E-Mail-Adresse [...] zu nutzen.

Für die Zusendung Ihres Antwortbogens haben wir uns den [...].2018 vorgemerkt.

Wir weisen vorsorglich darauf hin, dass wir es uns grundsätzlich vorbehalten, im Nachgang zu Onlineprüfungen einzelne Unternehmen auch vor Ort zu kontrollieren, um uns von der erfolgreichen Umsetzung der angegebenen Maßnahmen persönlich zu überzeugen.