Bitte senden Sie den Antwortbogen bis **spätestens [...]** ausgefüllt und unterschrieben an:

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 (Schloss)
91522 Ansbach

Kreuzen Sie bitte alle zutreffenden Angaben an. Sollten längere Begründungen erforderlich sein, bitten wir diese als Anhang beizufügen und in das jeweilige Antwortfeld dann ein Referenzzeichen (z. B. siehe a) auf Anhang) einzutragen.

Antwortbogen

Onlineprüfung: Patch Management bei WordPress / WP Plugins

Aktenzeichen: [...]
Webseite: [...]

MUSTER

Auf Grund der flächendeckenden Onlineprüfung des BayLDA wurde der oben genannte Webauftritt hinsichtlich des Einsatzes des WordPress-Plugins „WP GDPR Compliance" mit kritischer Sicherheitslücke untersucht. Hiermit wird bestätigt, dass die übermittelten Prüfergebnisse zur Kenntnis genommen und eine Prüfung möglicher Angriffe durchgeführt wurde sowie bei Bedarf auch geeignete Abhilfemaßnahmen getroffen worden sind.

1. Einsatz der Erweiterung „WordPress GDPR Compliance Plugin"

☐ Das Plugin kommt nicht mehr zum Einsatz.
☐ Das Plugin kommt in der abgesicherten Version 1.4.3 zum Einsatz.
☐ Das Plugin kommt in der unsicheren Version 1.4.2 (oder kleiner) zum Einsatz, weil

_____

(Begründung angeben)

2. Sicherheitsprüfung

☐ Die eingesetzte WordPress-Version ist aktuell und wird regelmäßig hinsichtlich Updates untersucht.
☐ Die eingesetzte WordPress-Version ist derzeit nicht die neueste verfügbare Version, weil

_____

(Begründung angeben)

☐ Alle relevanten Sicherheitspatches des Herstellers wurden installiert.
☐ Alle relevanten Sicherheitspatches des Herstellers sind noch nicht installiert, weil

_____

(Begründung angeben)

☐ Veränderungen in der Datenbank wurden erkannt.
☐ Veränderungen in Dateien in der WordPress-Installation wurden erkannt.
☐ Unbekannte Admin-Nutzer wurden erkannt.
☐ Automatische Updates sind aktiviert.
☐ Es wurde ein sicheres Backup eingespielt, weil Veränderungen festgestellt wurden.

3. Kenntnis über Schwachstellen

☐ Veröffentlichungen zur Sicherheit von WordPress und Plugins werden regelmäßig gelesen.

☐ Veröffentlichungen zur Sicherheit von WordPress und Plugins können nicht oder nicht regelmäßig gelesen werden, weil

_____

(Begründung angeben)

☐ Die OWASP Top 10 sind bekannt und werden bei dem Webauftritt berücksichtigt.

☐ Die OWASP Top 10 werden bei dem Webauftritt nicht berücksichtigt, weil

_____

(Begründung angeben)

☐ Die Schwachstelle im WordPress-Plugin „WP GDPR Compliance" war mir bislang nicht bekannt.

☐ Die Schwachstelle im WordPress-Plugin „WP GDPR Compliance" ist mir bekannt und folglich wurden schon entsprechende Sicherheitsmaßnahmen ergriffen.

☐ Die Schwachstelle im WordPress-Plugin „WP GDPR Compliance" ist mit bekannt, aber es wurden keine Sicherheitsmaßnahmen ergriffen, weil

_____

(Begründung angeben)

6. Patch Management

☐ Ein geregelter Prozess zum Patch Management liegt vor und wird in der Praxis ausreichend umgesetzt.

☐ Ein geregelter Prozess zum Patch Management liegt nicht vor und/oder wird in der Praxis zumindest nicht konsequent umgesetzt, weil

_____

(Begründung angeben)

7. Umgang mit Sicherheitsvorfällen

☐ Sicherheitstools werden eingesetzt, um Schwachstellen auf der eigenen Website aufzuspüren.

☐ Die Meldepflicht bei Datenschutzverletzungen nach Art. 33 DS-GVO ist geläufig.

☐ Bei Datenschutzverletzungen ist bekannt, wo und wie was zu melden ist.

☐ Es ist mir bewusst, dass Verstöße gegen Art. 32 bis 34 DS-GVO bußgeldbewehrt sind.

☐ Die Bestimmung des Datenschutzrisikos bei Sicherheitsvorkommnissen ist problemlos möglich.

☐ Für die Sicherheit und Betreuung der geprüften Website nutze ich Dienstleistungen folgenden Anbieters:

_____

(Anschrift des beauftragten Unternehmens angeben)

_____ _____

Unterschrift des Verantwortlichen Datum