

von Katharina Putz

Webshop mit veralteter Software: DSGVO-Bußgeld in Höhe von 65.000€

Laut dem Tätigkeitsbericht der Landesbeauftragten für Datenschutz Niedersachsen wurde gegen ein Unternehmen aus Niedersachsen ein DSGVO-Bußgeld in Höhe von 65.000 € verhängt. Grund dafür war die Verwendung einer veralteten Shop-Software. Dadurch waren die Nutzer-Passwörter unzureichend gesichert, was als Verstoß gegen die Pflicht zur Einrichtung hinreichender technischer und organisatorischer Maßnahmen gewertet wurde. Lesen Sie mehr zum Fall und zu den Hintergründen.

Technische und organisatorische Maßnahmen für die Datensicherheit

Bei der Datenverarbeitung haben Verantwortliche die Sicherheit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen (TOMs) zu gewährleisten. Eine entsprechende Pflicht ergeht aus Art. 5 Abs. 1 lit. f und Art 32 DSGVO. Für die Wahl und Umsetzung der geeigneten Maßnahmen steht den Verantwortlichen im Online-Handel dabei ein gewisser Spielraum zu. Ziel ist es der gesetzgeberischen Intention nach, ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Auswahl der entsprechenden Maßnahmen sind vor allem der Stand der Technik und die Implementierungskosten zu berücksichtigen.

Sicherheitslücken durch veraltete Web-Shop-Anwendung

Der Stand der Technik wurde einem Webshop-Betreiber nun jüngst zum Verhängnis. Nach Meldung einer Datenpanne durch den Shop-Betreiber selbst wurde der Online-Shop durch die Landesbeauftragte für Datenschutz auf technische Gesichtspunkte überprüft. Dabei stellte sich heraus, dass eine Web-Shop-Anwendung verwendet wurde, die seit spätestens 2014 veraltet ist. Dementsprechend war diese Anwendung über einen langen Zeitraum hinweg vom Hersteller auch bereits nicht mehr mit Sicherheitsupdates versorgt worden. Der Hersteller warnte sogar davor, die betroffene Version nicht mehr einzusetzen, da daraus **erhebliche Sicherheitslücken** resultieren könnten. Diese Sicherheitslücken ermöglichten unter anderem SQL-Injection-Angriffe.

SQL-Injection-Angriffe

Bei SQL-Injection-Angriffen handelt es sich um Angriffe auf eine Datenbank. Dabei wird die mangelnde Maskierung ausgenutzt. Der Angreifer kann in den Besitz der Zugangsdaten aller in der Anwendung registrierten Personen kommen. Der Angreifer kann eigene Befehle in die Datenbank einschleusen, Daten ausspähen, ändern oder sogar die Kontrolle über die Datenbank erhalten.

Ermittlungen der niedersächsischen Datenschutzbehörde ergaben, dass die in der Datenbank vorhandenen Passwörter zwar mit der kryptographischen Hashfunktion „MD 5“ gesichert waren. Diese sei aber nicht für den Einsatz von Passwörtern geeignet. Außerdem wurde vom Website-Betreiber **kein Salt verwendet**. Ohne diese entsprechenden Sicherheitsvorkehrungen sei eine **schnelle Berechnung der Klartext-Passwörter möglich** gewesen. Ein Angreifer hätte die ermittelten Passwörter bei den ebenfalls in der Datenbank hinterlegten E-Mail-Adressen testen und erhebliche Folgeschäden anrichten können.

Passwortschutz durch Salt

Salt ist eine Methodik aus der Kryptologie zum Passwortschutz. Ein Salt wird für jedes Passwort individuell generiert und verlängert ein Passwort. Damit wird die systematische Berechnung des Passworts erheblich erschwert. Ziel der Verwendung von Salt ist es, dass ein Angreifer für jedes Passwort eine komplette Neuberechnung durchführen muss. Ohne Salt würde hingegen eine gemeinsame Berechnung für eine komplette heruntergeladene Datenbank genügen.

Abgemildertes Bußgeld

In den mangelhaften technischen Datensicherungsmaßnahmen des Webshop-Betreibers sah die niedersächsische Datenschutzbehörde einen Verstoß gegen Art. 32 Abs. 1 DSGVO. Das Bußgeld wurde von der Landesbeauftragten für Datenschutz Niedersachsen auf 65.000 € festgesetzt. Dabei wurde mildernd berücksichtigt, dass das Unternehmen die betroffenen Personen bereits vor dem Bußgeldverfahren darüber informiert hatte, dass ein Passwortwechsel notwendig sei.

Beseitigung der Sicherheitslücken ohne erheblichen Aufwand

Die Beseitigung der erheblichen Sicherheitslücken sei für das Unternehmen nicht mit unverhältnismäßigem Aufwand verbunden. Ausreichend hierfür wäre die Implementierung einer Salt-Funktion und eines aktuellen, auf Passwörter ausgelegten Hash-Algorithmus. Diese Funktionen könnten bereits mit einer neueren Version der Software eingepflegt werden. **Ein Update auf eine aktuelle Software-Version sowie regelmäßige Aktualisierungen derselben würden also genügen, um Sicherheitslücken und Schwachstellen zu schließen.**

Fazit

Webshop-Betreiber sollten dieses DSGVO-Bußgeld der Landesbeauftragten für Datenschutz Niedersachsen zum Anlass nehmen, die verwendete Shop-Software auf Aktualität und vor allem implementierte Passwortschutz-Maßnahmen auf ihre technische Zeitgemäßheit zu überprüfen.

Ist es bereits zu spät, zeigt der vorliegende Fall, dass ein proaktives Vorgehen gegenüber den betroffenen Personen und der Datenschutzbehörde zumindest mildernde Umstände im Zusammenhang mit dem verhängten Bußgeld darstellen kann.

Autor:

Katharina Putz

Wissenschaftliche Mitarbeiterin