Anforderungen an das Login bei Shops, Internet-Foren etc.

Sehr geehrte Datenschutz-Kunden,

mit meiner heutigen Rundmail wende ich mich an eine relativ kleine Gruppe innerhalb meiner Mandate. Nichtsdestotrotz habe ich mich zu diesem Thema entschlossen, weil die Anforderungen seitens der Datenschutz-Aufsichtsbehörden auch mich teilweise überraschen und - weil auch dieser Kundeninformation wieder ein Fall zugrunde liegt, bei dem ein nicht unerhebliches Bußgeld verhängt wurde[1)]: Es geht um die Login-Anforderungen beim Betrieb von Foren, Internet-Portalen, Online-Shops etc.

In der Regel dient die Benutzeranmeldung dazu, Einzelpersonen Informationen zur Verfügung zu stellen oder von diesen abzufragen, die im Bereich schützenswerter personenbezogener Daten angesiedelt sind. Dies können Kommunikationsdaten, Warenkörbe, sog. Beobachtungs- oder Favoritenlisten, Zahlungsverkehrsinformationen, Login-Statistiken, Korrespondenzdaten im Sinne von Geschäftsbriefen und vieles mehr sein. Unbestritten ist, dass diese Daten vom Verantwortlichen durch geeignete technisch-organisatorische Maßnahmen vor unbefugtem Zugriff zu schützen sind.

Selbstverständlich, werden Sie sagen, ist das so. Daher speichern wir von Passwörtern nur deren Hashwert, haben eine 2-Factor-Authentication bei der Registrierung vorgesehen, verarbeiten das Ganze ausschließlich auf Servern in der EU und haben mit den beteiligten Dienstleistern vollständige Verträge zur Auftragsverarbeitung abgeschlossen. Was will man mehr?

Im genannten Bußgeldbescheid werden (für mich das erste Mal, dass mir eine solche Anforderung begegnet) konkrete Mindestanforderungen an die Länge und Komplexität von Passwörtern gestellt. Ist es dem aufgeklärten Benutzer also nicht selbst überlassen, für welches Maß an Passwort-Sicherheit er sich entscheidet? Offenbar nicht. Das betroffene Unternehmen hatte für sein Shop-System bisher lediglich Passwörter gefordert, die mindestens sechs Zeichen umfasst haben. Haben Angreifer 19 Fehlversuche getätigt, so wurde die anfragende IP-Adresse für eine Minute gesperrt, was einen automatisierten Brut-Force-Angriff erschweren sollte.

Alles viel zu lasch, bewertet die französische Aufsichtsbehörde den Sachverhalt und benennt die nach ihrer Ansicht erforderlichen Mindestanforderungen:

"...Einführung einer verbindlichen Passwort-Management-Politik für Kundenkonten nach einer der folgenden Modalitäten:
- Die Passwörter bestehen aus mindestens zwölf Zeichen, die mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten
- Die Passwörter bestehen aus mindestens acht Zeichen, die drei der vier Zeichenkategorien (Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen) enthalten und mit einer zusätzli-

Volker Baron (Dipl.-Geograph / IT-Systemelektroniker) – **Tel.:** +49 89 18923500 – **Fax:** +49 89 18923501
Büro: Haydnstraße 2, 80336 München – **E-Mail:** volker.baron@baron-consult.de – **Internet:** www.baron-consult.de
Finanzamt München I, USt-ID: DE 216791626
Bankverbindung: Münchner Bank eG, IBAN: DE84 7019 0000 0000 3389 15, BIC: GENODEF1M01

chen Messung wie dem Aufschub des Kontozugangs nach mehreren Fehlschlägen (zeitweilige Sperrung des Zugriffs, deren Dauer sich im Laufe der Versuche verlängert) einhergehen, Einrichtung eines Mechanismus zur Absicherung gegen automatisierte und intensive Einreichungen von Versuchen (z. B. captcha) und/oder Sperrung des Kontos nach mehreren erfolglosen Authentifizierungsversuchen (höchstens zehn)."[2)]

So präzise, so gut. Klar können wir jetzt damit argumentieren, dass die französische Aufsichtsbehörde, insbesondere in Bezug auf den Onlinehandel, strengere Maßstäbe anlegt als dies aus Deutschland bekannt ist. Allerdings schätze ich die Situation so ein, dass sich die Maßstäbe der nationalen Aufsichtsbehörden innerhalb der EU mit der Zeit eher angleichen werden, zumindest der mitteleuropäischen Staaten wie Frankreich und Deutschland. Denn mit welchem Grund sollte die Verhältnismäßigkeit technisch-organisatorisches Maßnahmen im europäischen Raum unterschiedlich bewertet werden? Und falls Sie Waren oder Dienstleistungen über ein Unternehmen oder eine Niederlassung in Frankreich an Verbraucher in Frankreich vertreiben, kommen Sie an der Beachtung der Anforderungen ohnehin nicht vorbei.

Daher empfehle ich, die Login-Prozeduren für Ihre Internet-Angebote entsprechend den o. g. Anforderungen zu überprüfen.

München, 2020-08-11

Volker Baron

[1)] Ich beziehe mich hier auf den Bußgeldbescheid gegen die société SPARTOO SAS mit Sitz in Grenoble / Frankreich in Höhe von 250.000 EUR, ausgestellt am 2020-08-05 von der französischen Aufsichtsbehörde CNIL unter Bezugnahme auf die EU-DSGVO. SPARTOO SAS betreibt ein Online-Schuhgeschäft mit mehreren Internetpräsenzen, das sich an Konsumenten in 13 EU-Staaten richtet. Das Bußgeld wurde für eine Reihe von Datenschutz-Verstößen verhängt, der geschilderte Sachverhalt bezieht sich nur auf einen von diesen.

[2)] Originaltext aus dem Bußgeldbescheid:
"... mettre en œuvre une politique de gestion des mots de passe contraignante, s'agissant des comptes clients selon l'une des modalités suivantes;
- les mots de passe sont composés d'au minimum douze caractères, contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial;
- les mots de passe sont composés d'au moins huit caractères, contenant trois des quatre catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) et s'accompagnent d'une mesure complémentaire comme la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : captcha) et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses (au maximum dix). ..."