Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden
des Bundes und der Länder

Arbeitskreis Technische und organisatorische Datenschutzfragen

Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung

Stand 29. März 2019

1 Vorbemerkung

Anbieter von Online-Diensten, die personenbezogene Daten von Nutzerinnen und Nutzern verarbeiten, fallen unter die Regelungen der DS-GVO. Sie haben insbesondere die Vorschriften zur Sicherheit der Verarbeitung (Art. 32) zu beachten. Hierzu gehören auch Maßnahmen zur Sicherung des Zugangs zu den Diensten.

Die vorliegende Orientierungshilfe beschreibt Maßnahmen, die nach Ansicht der Datenschutzaufsichtsbehörden dem Stand der Technik entsprechen und einen effektiven Schutz gewährleisten können. Die Auswahl und Implementation obliegt den Anbietern der Online-Dienste in eigener Verantwortung (Art. 24 DS-GVO).

Anbieter von Online-Diensten sollten sich zudem an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik im IT-Grundschutz-Kompendium zum Identitäts- und Berechtigungsmanagement orientieren (u. a. Basisanforderung ORP.4.A8 „Regelung des Passwortgebrauchs“ oder ORP.4.A11 „Zurücksetzen von Passwörtern“).

2 Maßnahmen zur Zugangssicherung

2.1 Passwortstärke messen und anzeigen

Die Stärke der von den Nutzerinnen und Nutzern gewählten Passwörter muss gemessen und angezeigt werden, um eine sichere Passwortvergabe zu unterstützen. Hierbei sind insbesondere die Länge, der Einsatz von Ziffern-/Sonderzeichen, Zeichenketten aus Wörterbüchern, landesspezifische Tastaturhäufungen (z.B. qwertz), unsichere Trivialpasswörter (z.B. 1234567890) sowie unsichere triviale Ersetzungen von Zeichen (wie o durch 0 oder I durch 1) zu berücksichtigen. In Abhängigkeit der kryptographischen Speicherverfahren sind dabei in der Regel Passwortlängen von mindestens 10 Zeichen erforderlich, um von einem angemessenen Passwort mittlerer Güte zu sprechen. Zudem sollte sichergestellt sein, dass bereits kompromittierte Passwörter nicht erneut genutzt werden dürfen.

2.2 Passwortwechsel nur in Sonderfällen erzwingen

Sofern starke Passwörter (nach 2.1) verwendet werden, ist ein regelmäßiger Passwortwechsel nicht zwingend erforderlich. Der Wechsel von Passwörtern soll insbesondere dann erzwungen werden, wenn der Dienstanbieter ein Initialpasswort in einer Weise zugeteilt hat, dass eine Kenntnisnahme durch Dritte nicht ausgeschlossen werden kann (z. B. durch postalischen Versand), oder wenn Hinweise auf eine Kompromittierung des Kontos oder sicherheitsrelevante Schwachstellen eingesetzter Softwarekomponenten vorliegen.

2.3 Umgang mit fehlgeschlagenen Anmeldeversuchen

Das Fehlschlagen von Anmeldeversuchen ist zu registrieren und der bzw. dem Berechtigten beim nächsten erfolgreichen Login anzuzeigen. Nach einer anwendungsabhängig festzulegenden Anzahl von Fehlversuchen sollte die Anmeldung zeitweise oder dauerhaft gesperrt werden. Dabei sollen sowohl Angriffsversuche auf ein konkretes Konto mit sich ändernden Passwörtern als auch auf viele verschiedene Konten mit sich nicht/kaum ändernden Passwörtern wirksam berücksichtigt werden.

2.4 Umgang mit kompromittierten Diensten

Sollte ein Anbieter Kenntnis erlangt haben, dass sein angebotener Dienst kompromittiert worden ist, so muss er entsprechend Artikel 33 DS-GVO die zuständige Aufsichtsbehörde und seine Nutzer ohne zeitliche Verzögerung darüber informieren. Zudem sind geeignete Maßnahmen zu ergreifen, die dafür sorgen, dass Unbefugte mit diesen kompromittierten Informationen keinen Zugriff auf die Konten erhalten.

2.5 Sinnvolle Benachrichtigungen

Anbieter sollten ihre Nutzer über wichtige Ereignisse informieren, etwa darüber, dass gerade eine Telefonnummer oder eine E-Mail-Adresse geändert wurde, über die der Zugang zu einem Konto ermöglicht wird. Hierzu zählen auch erfolgreiche Logins aus anderen Ländern.

2.6 Sicheres Passwort-Reset

Es sind Passwort-Reset-Verfahren anzubieten, die gegen unbefugte Zugriffsversuche und Social Engineering resistent sind. Verfahren, die ein neues Passwort per E-Mail versenden sind ungeeignet. Stand der Technik sind Passwort-Reset-Links, bei denen der Link nur ein einziges Mal funktioniert und nur eine kurze Gültigkeitsdauer (max. 1 Stunde) besitzt. Insbesondere für das Recovery von E-Mail-Konten muss ein zweiter Kanal verwendet werden.

Zusätzliche Sicherheitsfragen beim Anstoßen eines Passwort-Reset-Verfahrens bieten eine größere Sicherheit als ein Versand eines Passwort-Reset-Links ohne weitere Authentisierung, können aber einen zweiten sicheren Kanal nicht ersetzten. Wenn Sicherheitsfragen zum Einsatz kommen, sollten mehrere Fragen eingesetzt werden und neben vorgegebene Fragen auch nutzergenerierte Fragen möglich sein. Fehleingaben bei Sicherheitsfragen müssen wie Fehleingaben von Passwörtern zumindest zu temporären Sperrungen führen.

2.7 Passwörter verschlüsselt übertragen

Passwörter sind vom Nutzer bei der Registrierung und Nutzung über einen nach Stand der Technik kryptographisch abgesicherten Transportkanal an den Endpunkt des Diensteanbieters zu übertragen. Dort muss sichergestellt werden, dass diese in der Server-Anwendung unmittelbar in ein geeignetes Hashverfahren (siehe 2.8) überführt werden.

2.8 Passwörter verschlüsselt speichern

Anbieter dürfen Passwörter nur nach Verarbeitung mittels kryptographischer Einwegverfahren (insbesondere (Salted-)Hashverfahren) nach Stand der Technik speichern. Eine Speicherung mittels symmetrischer Verschlüsselungsalgorithmen (z. B. AES) ist in der Regel nicht notwendig und führt zu einem erhöhten Risiko, sollte der Verschlüsselungsschlüssel neben den verschlüsselten Daten entwendet werden.

2.9 Passwort-Datenbanken vor unbefugtem Zugriff sichern

Anbieter müssen die Datenbanken, in denen sie Nutzerpasswörter speichern, vor unbefugtem Zugriff durch eigenes Personal und Dritte sichern. Dazu sollen regelmäßig unabhängige Penetrations- und Schwachstellentests durchzuführen.

2.10 Schulung der Beschäftigten von Anbietern

Anbieter müssen ihre Beschäftigten regelmäßig zu Fragen des Datenschutzes und der Informationssicherheit schulen. Dies betrifft insbesondere Schulungen, um die Beschäftigten für Social Engineering Angriffe zu sensibilisieren.

2.11 Zwei-Faktor-Authentisierung anbieten

Zusätzlich zum Passwortschutz soll eine Zwei-Faktor-Authentisierung angeboten werden. Der zweite Faktor muss auf einem anderen Gerät, einem anderen Kommunikationskanal oder einer anderen ausreichenden Trennung zwischen Passwort und Verwaltung des zweiten Faktors basieren. Einmal aktiviert, darf die Zwei-Faktor-Authentisierung nur unter Verwendung angemessen sicherer Verfahren deaktiviert werden können. Eine Zwei-Faktor-Authentisierung ist bei Verarbeitungen mit hohem Risiko keine reine Empfehlung, sondern

zum Erreichen eines angemessenen Schutzniveaus notwendig. Dabei sollen bevorzugt offene Verfahren wie Time-based One-time Password Algorithmus (TOTP) angeboten werden, welche nicht mit einer Offenbarung zusätzlicher personenbezogener Daten (Mobilfunknummern) verbunden sind. Werden durch den Anbieter der Zwei-Faktor-Authentisierung dennoch personenbezogene Daten wie Mobilfunknummern verarbeitet, sind geeignete Garantien anzubieten, welche eine Zweckbindung der Daten ausschließlich für die Zwei-Faktor-Authentisierung dauerhaft sicherstellen. Weiterhin sollten standardisierte Verfahren wie bspw. WebAuthn unterstützt werden.

2.12 Trennung von Authentifikations- und Nutzdaten

Um die Folgen einer möglichen Kompromittierung von Daten zu beschränken, sollen die zur Authentifikation verwendeten Daten, insbesondere Passwörter, logisch getrennt in unterschiedlichen Datenbank-Instanzen von den Inhaltsdaten gespeichert werden. Dies kann auch durch eine gesonderte Verschlüsselung der Inhaltsdaten bewirkt werden.

2.13 Über Passwort-Manager informieren

Nutzerinnen und Nutzern sollen über geeignete Passwort-Manager-Lösungen und deren Gebrauch informiert werden.

2.14 Sicherheit als integrierte Aufgabe

Zur Erreichung eines angemessenen Schutzniveaus muss die Sicherheit einer Anwendung als Ganzes betrachtet werden. Der Umgang mit Passwörtern und der Einsatz eines wirksamen Authentisierungsverfahrens stellen dabei einen wichtigen Baustein dar. Das Sicherheitskonzept einer Anwendung muss gemäß Art. 32 DS-GVO regelmäßig auditiert, evaluiert und verbessert werden. Auch die Grundsätze des Data-Protection-by-Design und Data-Protection-by-Default (Art. 25 DS-GVO) sind zu beachten.