Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

Hinweise zum sicheren Umgang mit Passwörtern

Des Landesbeauftragten für den Datenschutz

und die Informationsfreiheit Baden-Württemberg

Tipps und Informationen für Bürgerinnen und Bürger für die Auswahl von Passwörtern

Informationen für verantwortliche Unternehmen und Software-Entwickler

Version 1.0.1 vom 12. 2. 2019

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit Baden-Württemberg

Königstraße 10a
70173 Stuttgart

Telefon: (07 11) 61 55 41-0
Telefax: (07 11) 61 55 41-15

E-Mail: poststelle@lfdi.bwl.de
Homepage: https://www.baden-wuerttemberg.datenschutz.de/

Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.
PGP-Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven lediglich das bestimmende Geschlecht genannt. Selbstverständlich richtet sich dieser Bericht an die Angehörigen aller Geschlechter.

Inhalt

A. Rechtliche Grundlage 4
B. Hinweise zur Auswahl von Passwörtern 4
1) Starke Passwörter wählen 5
Die erster-Buchstabe-Methode 5
Ganzer-Satz-Methode 5
Zufällige Passwörter generieren lassen 5
Passwort-Karten und -Schablonen 6
2) Passwörter niemals doppelt verwenden 6
3) Passwort-Safe verwenden 6
4) Keine Wörter aus Wörterbüchern verwenden 6
5) Passwörter nicht weitergeben 7
6) Nur bei Kompromittierung ändern 7
7) Sichere Passwörter auch auf Smartphones 7
8) Standard-Passwörter immer ändern 7
9) Lügen bei Sicherheitsfragen 7
10) Zwei-Faktor-Authentifizierung aktivieren 8
C. Hinweise für Administratoren und Entwickler 8
1) Passwort-Richtlinie 8
2) Keine regelmäßige Änderung erzwingen 8
3) Sperrung nach fehlerhafter Anmeldung 8
4) Passwörter keinesfalls im Klartext speichern 8
5) Sichere Speicherung von Passwort-Datenbanken 9
6) Zwei-Faktor-Authentifizierung implementieren 9
7) Änderung voreingestellter Passwörter erzwingen 9
8) Fehlgeschlagene Anmeldeversuche protokollieren 10
9) Keine fremden Passwörter sammeln 10

Passwortsicherheit ist ein zentrales Thema bei technisch-organisatorischen Datenschutz-Maßnahmen. Passwörter sind immer noch ein zentrales Element zur Authentisierung von Nutzern, wie z.B. bei der Anmeldung bei einem Web-Dienst oder Computer. Aus diesem Grund bieten wir sowohl Nutzern eine Hilfestellung bei der Auswahl von sicheren Passwörtern als auch Dienstean-bietern, Entwicklern und Administratoren Hinweise für die Aufstellung von Passwort-Richtlinien und die Speicherung von Passwörtern in Anwendungen.

Die Anmeldung mittels Nutzername und Passwort an Computern, bei Web-Diensten, Internet-of-Things- bzw. Smart-Home-Geräten und vielem anderen stellt das gängigste Verfahren zur Authentifizierung dar. Diese Authentifizierungsmethode ist damit oftmals das wesentliche oder gar einzige Sicherheitselement, das vor dem Zugriff durch Unbefugte schützt.

Es sind aber nicht nur Nutzer in der Pflicht, sichere Passwörter zu wählen. Administratoren und Hersteller müssen sichere Vorgaben machen, Passwörter sicher speichern und sollten moderne Techniken wie Zwei-Faktor-Authentifizierung anbieten.

A. Rechtliche Grundlage

Die Authentifizierung mittels Nutzername und Passwort sowohl bei Geräten als auch Diensten stellt eine technische und organisatorische Maßnahme nach Artikel 32 DS-GVO dar. Eine sichere Authentifizierung der Nutzer ist ein Baustein, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten, Systeme und Dienste auf Dauer sicherzustellen (vgl. Art. 32 DS-GVO). Setzen Verantwortliche unzureichende technische und organisatorische Maßnahmen um, können Bußgelder bis zu 10 Millionen Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist (vgl. Art. 83 Abs. 4 DS-GVO). Verantwortliche sind also angehalten, angemessene technische und organisatorische Maßnahmen durchzuführen.

Die folgenden Abschnitte stellen die Empfehlungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg für den Umgang mit Passwörtern dar.

B. Hinweise zur Auswahl von Passwörtern

Ein großes Risiko ist, dass Passwörter von Dritten auf die eine oder andere Art erraten oder ermittelt werden können. Daher sind einerseits die Nutzer selbst in der Pflicht, starke Passwörter auszuwählen, andererseits müssen aber auch Hersteller und Administratoren sichere Vorgaben machen. Dafür haben sich eine Reihe von Regeln etabliert:

1) Starke Passwörter wählen

Es sollten immer starke Passwörter verwendet werden, die aus zwölf oder mehr Zeichen bestehen. Je wichtiger das Passwort ist, desto länger sollte es sein. Sie sollten sowohl Klein- als auch Großbuchstaben, Ziffern und Satzzeichen enthalten. Auf kompliziert einzugebende Sonderzeichen und Umlaute sollte – je nach Kontext – verzichtet werden, da diese u. U. auf verschiedenen Tastaturen unterschiedlich eingegeben werden müssen.

Es kommt häufig vor, dass Angreifer an die Passwort-Datenbanken von Online-Diensten gelangen. Die verantwortlichen Diensteanbieter sollten zwar keine Passwörter im Klartext speichern, aber auch zu so genannten Passwort-Hashes (quasi eine Art Prüfsumme oder Fingerabdruck) lassen sich die passenden Passwörter durch Ausprobieren finden. Je nachdem welches Verfahren der Verantwortliche gewählt hat, können Angreifer mehrere Milliarden Passwörter pro Sekunde ausprobieren. Daher ist es essentiell, starke Passwörter zu verwenden.

Da solche Passwörter schwer zu merken sind, haben sich einige Verfahren etabliert, damit sich Nutzer leichter an starke Passwörter erinnern können:

Die erster-Buchstabe-Methode

Denken Sie sich einen Satz aus, den Sie sich gut merken können und nehmen von jedem Wort den ersten oder einen markanten Buchstaben:

Ich **m**uss **m**ir **s**elbst **1** **t**ollen **S**atz **a**usdenken**, d**as **h**ier **1**st **n**ur **e**ines **v**on **42** **B**eispielen**.**

Das resultierende Passwort: `Imms1tSa,dh1nev42B.`

Nehmen Sie aber keinen Satz, den jemand anderes erraten kann, der irgendetwas mit Ihnen oder Ihrem Umfeld zu tun hat. Wenn Sie als Satz einen bekannten Spruch, eine Liedzeile oder ein Gedicht nehmen, verfälschen Sie den Inhalt etwas.

Ganzer-Satz-Methode

Wenn Sie schnell tippen können, ist auch ein ganzer ausgeschriebener Satz möglich. Der sollte möglichst aus sinnlosen Phantasiewörtern bzw. zufällig aneinandergereihten Wörtern bestehen:

```
Die-13-lilablassroten-Beispielpasswoerter-nehme-ICH-nieniemals!
```

Zufällige Passwörter generieren lassen

Einige Browser bieten die Option, zufällige Passwörter zu generieren und von einem Passwort-Safe speichern zu lassen, ohne dass Sie diese sehen. Dies ist oftmals die komfortabelste und einfachste Methode – und auch sicher, solange der Passwort-Safe die Daten gut verschlüsselt ablegt und kein Dritter Zugang dazu erhält.

Passwort-Karten und -Schablonen

Es gibt zahlreiche Anbieter von Passwort-Karten und -Schablonen. Seien Sie vorsichtig: diese sind nur sicher, wenn jeder Nutzer unterschiedliche Zeichen bzw. unterschiedliche Schablonen verwendet! Dies ist oftmals nicht gegeben.

2) Passwörter niemals doppelt verwenden

Angreifer haben in den letzten Jahren eine große Menge an echten Passwörtern gesammelt, oftmals indem sie die Passwortdatenbanken großer (auch seriöser) Internet-Portale aufgrund von Sicherheitslücken kopieren konnten. Mehrere Milliarden Passwörter aller Art sind daher öffentlich bekannt. Angreifer nutzen diese, um sich unrechtmäßig bei anderen Diensten anzumelden oder weitere ähnliche Passwörter (die nur minimal geändert wurden) zu knacken. Ob Ihre E-Mail-Adresse betroffen ist, können Sie beispielsweise beim *Identity Leak Checker*[1] des Hasso-Plattner-Instituts nachprüfen. Auf der Webseite *have i been pwned?*[2] können Sie zusätzlich prüfen, ob bestimmte Passwörter bereits öffentlich bekannt wurden.

Um das Risiko doppelt genutzter Passwörter zu vermeiden, müssen Nutzer daher für alle Accounts bzw. Dienste eigene Passwörter nutzen.

3) Passwort-Safe verwenden

Niemand kann sich hunderte Passwörter merken. Daher ist es sinnvoll, Passwörter in einem Passwort-Safe zu speichern. Entsprechende Programme wie KeePass[3] gibt es als Freie- und Open-Source-Software kostenlos, bei einigen Betriebssystemen werden auch bereits welche mitgeliefert (z. B. der Schlüsselbund unter MacOS). Viele Web-Browser unterstützen die Speicherung von Passwörtern – diese sollten aber mit einem Master-Passwort abgesichert werden.

4) Keine Wörter aus Wörterbüchern verwenden

Angreifer können heutzutage – insbesondere wenn sie Zugriff auf Datenbanken mit gehashten Passwörtern haben – in kurzer Zeit automatisiert sehr viele Kombinationen durchprobieren. Gute Passwörter sollten daher weder Begriffe oder Begriffskombinationen aus Wörterbüchern enthalten („Sommer2018“) noch solche wiederverwenden. Die einzige Ausnahme sind wirklich sehr lange Passwörter, die aus einer Reihe zufälliger und nicht zusammenhängender Wörter bestehen.

[1] https://sec.hpi.de/ilc/
[2] https://haveibeenpwned.com/
[3] https://keepass.info/

5) Passwörter nicht weitergeben

Passwörter sollen grundsätzlich nicht weitergegeben werden. Ebenso sollen sie nicht per unverschlüsselter E-Mail versendet oder in unverschlüsselten Dokumenten gespeichert werden. Nutzer sollten beim bzw. nach dem ersten Anmelden ein eigenes, sichereres Passwort vergeben.

6) Nur bei Kompromittierung ändern

Früher wurde empfohlen, Passwörter in regelmäßigen Abständen zu ändern. Diese Empfehlung gilt heutzutage als überholt, da sie nicht zu mehr Sicherheit führt – sondern nur dazu, dass Nutzer sich diese im Klartext notieren, einfache Passwörter wählen, eine Zahl hoch zählen oder ähnliches. Daher sollten Administratoren die Nutzer nicht mehr zwingen, Passwörter in regelmäßigen Abständen zu ändern. Nur wenn es Anzeichen dafür gibt, dass Passwörter oder Passwort-Hashes in fremde Hände gelangt sind, sollten Nutzer diese ändern bzw. zu einer Änderung aufgefordert werden.

7) Sichere Passwörter auch auf Smartphones

Auch wenn Passwörter auf Smartphones oder Tablets schwieriger einzugeben sind, sollten hier sichere und lange Passwörter gewählt werden. Vierstellige PINs oder Wischgesten sind in der Regel nicht ausreichend. Aufgrund der meist vorhandenen biometrischen Authentifizierung sind Passwörter nur relativ selten einzugeben und daher auch zumutbar. Zu beachten ist dabei aber, dass nicht alle Hersteller ein hohes Sicherheitsniveau bei biometrischer Authentifizierung bieten.

8) Standard-Passwörter immer ändern

Standard-Passwörter, die z. B. von Internet-of-Things-Geräten, Fernwartungseinheiten, Software-Paketen und ähnlichem vergeben werden, sind oftmals nicht zufällig sondern bei allen Geräten gleich. Daher müssen diese bei Inbetriebnahme sofort geändert werden.

9) Lügen bei Sicherheitsfragen

Viele Dienste fragen Sie für Sicherheitsfragen nach persönlichen Informationen, wie dem Name Ihres ersten Haustieres, dem Geburtsdatum der Mutter oder ähnlichem. Die korrekten Antworten auf solche Fragen sind für Angreifer aus Ihrem Umfeld oder insbesondere bei Personen des öffentlichen Lebens oftmals leicht herauszufinden. Zwingt Sie ein Dienst, solche Sicherheitsfragen zu verwenden: Lügen Sie! Es bietet sich an, wie bei Passwörtern zufällige Angaben zu machen und diese im Passwort-Safe zu speichern.

10) Zwei-Faktor-Authentifizierung aktivieren

Viele Web-Dienste bieten eine so genannte Zwei-Faktor-Authentifizierung (2FA) an. Ist diese aktiviert, müssen Sie bei der Nutzung mit einem neuen Gerät noch einen zweiten Faktor eingeben, so wie das beim Homebanking üblich ist. Dieser zweite Faktor wird auf einem anderen Kommunikationsweg übertragen, daher reicht die Kenntnis des Passworts alleine für einen erfolgreichen Angriff nicht aus.

C. Hinweise für Administratoren und Entwickler

1) Passwort-Richtlinie

In einer Passwortrichtlinie für Ihr Unternehmen sollten die obigen Hinweise eingebunden und die Nutzer angewiesen werden diese zu beachten. So weit möglich und sinnvoll, sollten die Hinweise erzwungen werden.

2) Keine regelmäßige Änderung erzwingen

Eine erzwungene regelmäßige Änderung von Passwörtern ist überholt[4]. Administratoren sollten daher ihre Nutzer nicht regelmäßig auffordern oder zwingen die Passwörter zu ändern. Stattdessen sollten die Nutzer für sichere Passwörter sensibilisiert werden.

3) Sperrung nach fehlerhafter Anmeldung

Je nach Umgebung kann eine Account-Sperrung nach mehreren fehlgeschlagenen Anmeldeversuchen, die eine manuelle Freischaltung des Accounts verlangt, sinnvoll sein. Dabei ist aber zu beachten, dass dies auch für Angriffe verwendet werden kann: ein Angreifer kann so lange versuchen sich mit einem ungültigen Passwort anzumelden, bis der betroffene Nutzer gesperrt ist und sich selbst nicht mehr anmelden kann. Oftmals ist es sinnvoller, nach etwa fünf fehlgeschlagenen Anmeldeversuchen eine stetig steigende Verzögerung zu implementieren.

4) Passwörter keinesfalls im Klartext speichern

Entwickler von Anwendungen, Web-Portalen, Apps oder ähnlichem müssen zum Vergleich beim Login die Zugangsdaten der Nutzer speichern. Dabei dürfen sie die Passwörter auf keinen Fall im Klartext speichern, sondern müssen stattdessen moderne Verfahren wie Argon2[5] nutzen, für das fertige Libraries für alle gängigen Programmiersprachen zur Verfügung stehen.[6] Üblicherweise sollten dafür

[4] vgl. z.B. die folgende Meldung des britischen *National Cyber Security Centre* https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry oder Kapitel 5.1.1.2 *Memorized Secret Verifiers* der *Digital Identity Guidelines* des National Institute of Standards and Technology des U.S. Department of Commerce unter https://pages.nist.gov/800-63-3/sp800-63b.html

[5] siehe https://de.wikipedia.org/wiki/Argon2

[6] siehe die Argon2-Referenzimplementierung unter https://github.com/P-H-C/phc-winner-argon2

existierende Software-Bibliotheken und etablierte Verfahren zur Speicherung verwendet werden. Dabei ist auch auf ausreichende Entropie durch „Salt“ und „Pepper“[7] zu achten.

Ungenügend sicher gespeicherte Passwörter sind ein Verstoß gegen Artikel 32 DS-GVO und können auch mit Bußgeldern geahndet[8] werden.

5) Sichere Speicherung von Passwort-Datenbanken

Passwort-Datenbanken müssen besonders gesichert gespeichert werden. Nur ausgewählte Mitarbeiter dürfen einen möglichst eingeschränkten Zugriff auf die Passwort-Datenbank haben. Es ist zu verhindern, dass jemand die Daten kopieren kann.

6) Zwei-Faktor-Authentifizierung implementieren

Entwickler und Administratoren sollten soweit möglich immer eine Zwei-Faktor-Authentifizierung implementieren bzw. konfigurieren. Verantwortliche sollten dies aber nicht dazu nutzen, die Kunden zur Herausgabe einer Mobilfunknummer zu nötigen. Zur Zwei-Faktor-Authentifizierung sollten etablierte Standards wie RFC 6238, *Time-based One-time Password Algorithmus* (TOTP)[9] , genutzt werden.

7) Änderung voreingestellter Passwörter erzwingen

Bei Inbetriebnahme eines Gerätes oder Dienstes müssen eventuell voreingestellte Passwörter geändert werden. Nutzer müssen ihre Passwörter selbst vergeben, Passwort-Änderungen sind von den Nutzern selbst durchzuführen. Entwickler sollten dies so weit möglich erzwingen. Sind Default-Passwörter nötig, sollten sie eine klare Aufforderung zur Änderung enthalten.

Werden Anwendungen z.B. mit Datenbank-Passwörtern von Entwicklungs- über Test- zu Produktivsystemen transferiert, sollten die Passwörter außerhalb der Produktion nicht einfach den Name der Anwendung tragen (Anwendung *„Erdbeere“*, Passwort *„Erdbeere“*), sondern auch hier eine klare Aufforderung, in Produktion ein sicheres Passwort anzulegen (z.B. *„Setze-sicheres-Passwort-in-Produktion“*). Denn ein Datenbank-Administrator, der auf einem produktiven Server ein solches Passwort einrichten soll, hat damit auch eine klare Anweisung.

[7] siehe https://de.wikipedia.org/wiki/Salt_(Kryptologie)
[8] vgl. https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/11/LfDI-Baden-W%C3%BCrttemberg-verh%C3%A4ngt-sein-erstes-Bu%C3%9Fgeld-in-Deutschland-nach-der-DS-GVO.pdf
[9] https://de.wikipedia.org/wiki/Time-based_One-time_Password_Algorithmus

8) Fehlgeschlagene Anmeldeversuche protokollieren

Erfolglose Anmeldeversuche können auf einen Eindringversuch hinweisen. Fehlgeschlagene Anmeldeversuche sollten daher protokolliert und regelmäßig analysiert werden. Entwickler von Online-Plattformen sollten die Nutzer auf fehlgeschlagene Anmeldeversuche hinweisen.

9) Keine fremden Passwörter sammeln

Anbieter von Online-Diensten und ähnlichem dürfen grundsätzlich keine fremden Passwörter verarbeiten.[10] Für die Anmeldung bei verschiedenen Diensten mit den gleichen Zugangsdaten sind etablierte Verfahren wie OAuth2[11] bzw. SAML2[12] zu nutzen.

Geräte, die sich z.B. in lokalen WLAN-Netzen anmelden, dürfen die Zugangsdaten zu diesen auf keinen Fall an den Hersteller oder Dritte übertragen, weder im Klartext noch in sonstiger Form.

[10] Sollte dies dennoch für einen genau bestimmten Zweck unabdingbar sein, ist dieser Zweck zu dokumentieren, eine eventuelle Speicherung hat ausschließlich besonders gesichert zu erfolgen, die Passwörter dürfen für keine anderen Zwecke verwendet werden und der Nutzer muss über den Zweck informiert werden.

[11] siehe https://de.wikipedia.org/wiki/OAuth und https://oauth.net/

[12] siehe https://de.wikipedia.org/wiki/Security_Assertion_Markup_Language und http://www.oasis-open.org/committees/security/