# Information des DIN-Verbraucherrates

## DIGITALE SICHERHEIT – PASSWÖRTER UND PASSWORTMANAGER

In diesem Papier soll aufgezeigt werden, welche Aspekte bei der Gestaltung von Passwörtern beachtet werden sollten und inwieweit Passwortmanager Verbrauchern eine wertvolle Hilfe sein können. In der Gremienarbeit ist es besonders wichtig zu bedenken, dass die Nutzung von Passwortsicherung kein Ersatz für die Verpflichtung eines Geräte- oder Dienstleistungsanbieters auf IT-Sicherheit sein darf. Auch muss Passwortsicherung einfach für die Verbraucher anwendbar sein, da besonders im IoT (Internet of Things)-Bereich die Verwaltung und Nutzung von Passwörtern aufwändig werden kann.

### Passwortmanagement und sichere Gestaltung der Anwendungsumgebung – was Hersteller und Anbieter tun müssen

Die sichere Gestaltung der Anwendungsumgebung eines Gerätes oder eines Systems obliegt dem Anbieter. Dem Nutzer können nur in einem begrenzten Maße Anforderungen an die sichere Gestaltung übertragen werden. Dieses Bewusstsein sollen die Verbrauchervertreter in der Normung an die Hersteller, Dienstleister und Anbieter übermitteln.

Der wichtigste Faktor im Passwortmanagement sind die Maßnahmen des Herstellers, Dienstleisters oder Anbieters, d.h. wie Passwörter gespeichert und verschlüsselt und vor Missbrauch und unerlaubtem Zugriff geschützt werden. Eine Übertragung von lokalen Passwörtern (z. B. zur Freischaltung von IoT-Geräten) ins Internet ist nicht nötig. Passwörter dürfen niemals im Klartext gespeichert und übertragen werden. Für die Speicherung oder Übertragung sind sichere, dem Stand der Technik entsprechende Hashfunktionen zu verwenden. Diese sollten durch zusätzliche Techniken (z. B. durch die kryptographische Technik des „Salting“) weiter geschützt werden.

Auch muss bedacht werden, dass nicht jeder Nutzer technologieaffin ist und das nötige Bewusstsein und Wissen um Maßnahmen der IT-Sicherheit hat. Der Anbieter muss es dem Verbraucher leicht machen, sich abzusichern und Anwendungsumgebungen per Passwort zu sichern.

Manche Anforderungen an die Gestaltung von Passwörtern sind veraltet[1] und setzen zu hohe Barrieren für den Verbraucher. Die Gestaltungsregeln für Passwörter sind zu vereinfachen: Passwörter sollten nur dann geändert werden müssen, wenn sie

[1] Aktuelle Anforderungen an Passwörter siehe z.B. https://pages.nist.gov/800-63-3/sp800-63b.html.

kompromittiert wurden[2], die Verwendung von Sonderzeichen sollte nicht gefordert werden, muss aber möglich sein. Wichtigste Bedingung ist, dass das Passwort ausreichend lang ist, d.h. der Anbieter muss die minimale Passwortlänge auf 8 Zeichen festlegen, aber erheblich mehr Zeichen (mindestens 64) erlauben. Es darf nicht in Wörterbüchern (auch fremdsprachlichen) und Listen bekannter Passwörter stehen.

Sehr hohe Anforderungen, die dann nachweislich nicht eingehalten werden, weil die Nutzer sich diese Passwörter nicht merken können, sind auch eine Gefahr für die Sicherheit des Systems. In diesem Fall tendieren manche Nutzer dazu, die Passwörter auf einem leicht einsehbaren Zettel aufzuschreiben. Auch wird mit den sehr hohen Anforderungen hauptsächlich gegen Offline-Attacken vorgegangen; sehr viele Angriffe auf Passwörter sind jedoch keine Offline-Attacken, sondern basieren zum Beispiel auf Virus-Infektionen der Geräte, oder auf dem Ausprobieren bereits gehackter Passwörter. Es hilft eine Beschränkung der Anzahl der Fehlversuche für Online-Angriffe.

Es wäre hilfreich, z.B. in einer DIN-Norm, allgemeingültige Regeln an die Gestaltung von Passwörtern festzulegen, die es dem Nutzer ermöglichen, sein Wissen über Passwörter zu übertragen. Möglich wäre es Passwortregeln für verschiedene Sicherheitsniveaus unterschiedlich zu gestalten, für weniger sicherheitsrelevante Umgebungen könnten dann einfachere Passwörter verwendet werden.

Auch andere einfach nutzbare und passwortlose Authentifizierungsverfahren sind möglich, z.B. die Nutzung eines NFC (near field connection)–Token in Smartphone/Smartwatch oder von Apps (wie Microsoft Authentificator) auf dem Smartphone.

Eine Möglichkeit der weiteren Absicherung ist die Nutzung von Zwei-Faktor-Authentifikation (z. B. ein Passwort und ein sogenannter Token (z. B. eine Identifikationskarte oder ein USB-Stick) oder ein Passwort und eine Transaktionsnummer (TAN)). Biometrische Merkmale wie Fingerabdrücke, Gesichtsbilder oder Sprache/Stimme können als Authentifikationsfaktor oder als zweiter Faktor einer Zwei-Faktor-Authentifikation dienen. Sie haben im Vergleich zum Token oder Passwort den Vorteil, dass man sie nicht vergessen oder verlieren kann; allerdings können sie nicht ersetzt werden.

[2] Unter https://haveibeenpwned.com findet man beispielsweise über 8 Milllionen Passwörter aus ca. 400 Hackerangriffen der letzten Jahre.

**Passwortgestaltung und Passwortmanager – was Verbraucher tun können**

Verbraucher haben oftmals nur wenige Optionen der Passwortgestaltung, da sie den Regeln und Anforderungen von Herstellern und Anbietern genügen müssen. Eine wichtige Regel ist aber: Passwörter unter Verschluss halten, z. B. durch Nutzung eines Passwortmanagers

Passwortmanager sind eine gute Möglichkeit, sich im Passwortdschungel zurecht zu finden. Allerdings muss man dem Programm vertrauen können, denn Schwachstellen bei der Sicherheit eines Passwortmanagers können katastrophale Folgen für den Verbraucher haben. Besonders wichtig ist also, dass das gewählte Masterpasswort höchsten Sicherheitsanforderungen genügt. Manche Passwortmanager erhöhen den Schutz durch Nutzung einer Zwei-Faktor-Authentifikation. Hinzu kommt die Notwendigkeit der einfachen Nutzung eines Passwortmanagers. Ohne diese ist dem Verbraucher nicht geholfen. Passwortmanager werden regelmäßig von der Stiftung Warentest auf Gebrauchstauglichkeit und Sicherheit getestet (z. B. test 10/2017).

Viele Browser bieten die Möglichkeit der Passwortsicherung. Dies scheint einfach zu sein, weist jedoch erhebliche Sicherheitslücken auf, wie Tests der Stiftung Warentest feststellen. Auch werden im Gegensatz zum Passwortmanager hier keine Passwörter generiert, d.h. die schwierige Aufgabe ein sicheres Passwort zu wählen verbleibt weiterhin beim Nutzer.

Die Möglichkeit der Nutzung von Single-Sign-On-Diensten, bei denen eine Authentifikation z. B. bei Facebook oder Google zum Zugang auf weitere Anwendungen genutzt wird, wird Verbrauchern häufig angeboten und bietet Vorteile hinsichtlich der leichten Nutzbarkeit. Sie sind aber nicht uneingeschränkt empfehlenswert, da, wenn ein Passwort kompromittiert wird, gleichzeitig der Zugang zu anderen Anbietern kompromittiert wird.

DIN-Verbraucherrat, Dezember 2019

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages