Kommunikation über Sicherheit bei Passwörtern

Handlungsempfehlungen des Beirats Digitaler Verbraucherschutz

Einleitung

Passwörter begleiten Verbraucherinnen und Verbraucher täglich. Ratgeber zu sicheren Passwörtern gibt es viele, auch vom BSI.[1] Was ein Passwort sicher macht, ist für die Verbraucherinnen und Verbraucher aufgrund der großen Anzahl unterschiedlicher Ratgeber nicht immer klar erkenntlich. Insbesondere stellen die Sicherheitsanforderungen hinsichtlich Länge und Komplexität die Verbraucherinnen und Verbraucher vor das Problem, wie sie derartige Passwörter verfügbar halten. Zwar existieren mittlerweile auch andere Methoden der Authentisierung, an der Bedeutung sicherer Passwörter ändert dies jedoch wenig, solange den Verbraucherinnen und Verbrauchern nur die Option des Account-Schutzes mittels Passwort angeboten wird.

Zu einer erhöhten Sicherheit bei der Verwendung von Passwörtern trägt vor allem die Verwendung eines zweiten Faktors bei. Die Zwei-Faktor-Authentisierung (2FA) sollte aber wie jeder andere Sicherheitsmechanismus von organisatorischen Maßnahmen begleitet werden

[1] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen und Verbraucher-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

beispielweise durch Reduktion der maximalen Sitzungsdauer oder des Verbots paralleler Sitzungen. Zu beachten ist, dass die Sicherheit zudem erhöht wird, wenn für den zweiten Faktor auch ein zweites Gerät genutzt wird, also beispielsweise die Bankanwendung auf dem Desktop oder die Push-Tan/SMS-TAN auf dem Mobiltelefon. Auf diese Maßnahmen haben die Verbraucherinnen und Verbraucher kaum Einfluss. Gleichzeitig ist für sie auch nicht ersichtlich, welches die jeweils eingesetzten Maßnahmen sind und wie sie in ihrer Schutzwirkung zu beurteilen sind.

Konkret in Bezug auf Passwörter ist festzustellen, dass zwar einerseits Verbraucherinnen und Verbraucher häufig noch zu schwache Passwörter verwenden,[2] dass andererseits jedoch mitunter leicht zu erratende Passwörter oder feste Login/Passwort Kombinationen auch direkt vom Hersteller die in Verbraucher-IT hinterlegt werden. Trotzdem tragen Verbraucherinnen und Verbraucher das Risiko im Falle eines Angriffes alleine.

[2] https://hpi.de/pressemitteilungen/2021/die-beliebtesten-deutschen-passwoerter-2021.html

Das gilt nicht nur für den Fall, dass ein schwaches Passwort gewählt wird, sondern auch, falls ein Passwort (und andere Daten) aufgrund fehlender Sicherheitsvorkehrungen auf Seiten der Anbieter offengelegt oder gestohlen wird. Dies kann vor allem dann enormes Schadenspotential entfalten, wenn die Verbraucherinnen und Verbraucher sich an strenge Passwortvorgaben gehalten haben und ihr so für sicher gehaltenes Passwort bei mehreren Diensten verwendet hatten.

Vor dem Hintergrund, dass Passwörter aktuell die am häufigsten angebotene Authentisierungsvariante darstellen, haben Empfehlungen zur Passwortsicherheit nach wie vor hohe Relevanz. Deshalb bietet der Beirat Digitaler Verbraucherschutz hier eine Hilfestellung an, wie solche Empfehlungen aussehen und kommuniziert werden sollten. Aufgrund der o.g. Gefahren wie der Offenlegung von Passwörtern ist die Nutzung eines zweiten Faktors – falls möglich – dringend geboten. Ein hilfreiches Mittel zur Verwaltung von Passwörtern stellen

Passwortmanager dar. Verbraucherinnen und Verbraucher stehen ihrer Verwendung jedoch mit Skepsis gegenüber. Hier könnten Informationen über deren Funktionsweise sowie für Verbraucherinnen und Verbraucher erkennbare Merkmale der Sicherheitsqualität ein wirksames Instrument darstellen.

Der „Beirat Digitaler Verbraucherschutz“ des BSI hat für 2021/2022 als Fokusthema die Frage gewählt, wie gute Ratgeber für sichere Passwörter und gute Kommunikation über Passwortsicherheit aussehen können. Damit leistet der Beirat einen Beitrag, die Awareness bei Verbraucherinnen und Verbrauchern zu schaffen, ihre Passwörter sicher(er) zu gestalten und Mythen über die Sicherheit von Passwörtern auszuräumen.

Handlungsempfehlungen des BSI-Beirats zur Kommunikation über Passwörter

Basierend auf den Diskussionen kommt der Beirat zu folgenden Handlungsempfehlungen:

Kommunikation

1. Die Kommunikation über Passwörter sollte kurz und leicht verständlich sein.
2. In der Kommunikation sollte nicht das Wort „einfach“ im Zusammenhang mit sicheren Passwort-Praktiken verwendet werden. Der Schutz von Zugangsdaten ist keine triviale Aufgabe, und in vielen Handlungssituationen haben Verbraucherinnen und Verbraucher mit Aufmerksamkeits- und Zeitknappheit zu kämpfen. Diese Herausforderungen anzuerkennen ist wichtig, sonst werden Schwierigkeiten in der Umsetzung als eigene Unfähigkeit interpretiert und führen zum Aufgeben bzw. Abbrechen der Handlung.
3. Die Kommunikation über Passwörter darf Nutzerinnen und Nutzer nicht überfordern. Die Kommunikation sollte zur Umsetzung erster Schritte ermutigen und auf weitergehende Schritte verweisen, die unternommen werden können.
4. Das Aufschreiben von Passwörtern sollte nicht als per se negativ dargestellt werden. Verbraucherinnen und Verbrauchern sollten Hinweise gegeben werden, wie sie Passwörter sicher auf Papier verwahren können.
5. Weitergehende Informationen zu Passwörtern und zur Authentifizierung sollten bereitgestellt werden, damit Verbraucherinnen und Verbraucher selbst einschätzen können, wann Abstufungen hinsichtlich der Komplexität bei einem Passwort möglich sind (z.B. Verwendung eines zweiten Faktors, den potentiellen Risiken und Vorteilen von Passwortmanagern)

Passwort-Praktiken

1. Das „erste Gebot“ für Passwortsicherheit sollte die Einzigartigkeit von Passwörtern sein, d.h. diese nur für ein Konto zu verwenden.
2. Überkomplexe Passwörter [3] und beständige Passwort-Erneuerung sind wenig zielführend.
3. Es ist besser, längere Passwörter oder Passwörter bestehend aus mehreren Worten zu verwenden, die dafür weniger komplex und besser merkbar sind [4].
4. Dienste sollten sofern verfügbar über eine zusätzliche 2-Faktor Authentisierung abgesichert werden.

[3] Gemeint ist eine Folge von zufälligen Zeichen, deren Länge das derzeit nach den anerkannten Regeln notwendige Maß überschreitet.

[4] Vgl.: Das et al. 2014 The tangled Web of Password Reuse; Walia et al. 2020 An empirical analysis on the security and usability of passwords; Golla 2020 on the usability and security of password-based authentication

Sicherheit von Passwörtern allgemein – Diskussionen im Beirat

Der Beirat diskutierte neben den oben genannten Handlungsempfehlungen auch über die Passwortsicherheit allgemein. Dabei wurden verschiedentlich auch die Punkte aufgegriffen, die das BSI und das Bundeskanzleramt in einer gemeinsamen Studie zum Account-Schutz[5] herausgearbeitet haben. In der Diskussion ging der Beirat immer wieder auch auf folgende Probleme von Verbraucherinnen und Verbraucher ein:

- Grenzen der Merkfähigkeit verschiedener Passwörter,
- Zweifel an Wirksamkeit eines sicheren Passwortes,
- Unsicherheit, ab wann ein Passwort sicher genug ist,
- Paradoxes Verhältnis zwischen Passwortanforderungen und Passwortverwendungspraxis.

Laut der Studie umgehen Verbraucherinnen und Verbraucher diese Probleme zum Teil damit, sich Passwörter aufzuschreiben, sie wieder zurücksetzen zu lassen oder leicht abgewandelte

[5] https://www.bundesregierung.de/resource/blob/975272/1732446/4c4377ce98f697a94011955fdc9a1f62/de-passwort-download-zwischenbericht-data.pdf?download=1

Passwörter für die jeweiligen Accounts zu nutzen. Ebenfalls benutzen Verbraucherinnen und Verbraucher zum Teil individuelle Algorithmen zur Passwortbildung oder unterscheiden zwischen wichtigen und unwichtigen Accounts mit entsprechend sicheren Passwörtern. Auf eine technische Unterstützung wie einen Passwortmanager zurückzugreifen, scheint jedoch für viele Menschen nur bedingt eine Lösung zu sein.

Sie können bei einem Passwortmanager häufig nicht nachvollziehen, wie die dort abgespeicherten Passwörter geschützt sind. Entsprechend fehlt es an Vertrauen, vor allem auch darauf, dass der Zugriff auf die Passwörter jederzeit möglich ist und nur durch autorisierte Nutzerinnen und Nutzer erfolgt. Die Verwendung von Passwort-Managern hat Restrisiken, allerdings sollten diese mit den größeren Risiken wie Passwort-Wiederverwendung abgewogen werden. Außerdem wissen viele Verbraucherinnen und Verbraucher nicht, dass Passwort-Manager auch vor der Eingabe von Passwörtern auf gefälschten Webseiten

schützen können.

Sicherheit ist Verbraucherinnen und Verbrauchern wichtig, aber die problemlose Handhabung und der Zugang im Alltag ist wichtiger – die Sicherheit eines Online Kontos nützt nichts, wenn der dafür erforderliche Aufwand die primäre Zielverfolgung zu behindert. Usability von Sicherheit sollte demnach bei allen Empfehlungen im Vordergrund stehen. Da Verbraucherinnen und Verbraucher bereit zu sein scheinen, auch hohen Anforderungen an Passwörter nachzukommen, wenn ihnen gleichzeitig eine sichere und einfache Lösung für deren Aufbewahrung angeboten wird, sollte über diesen Aspekt besonders nachgedacht werden: Wann sind Papierlösungen oder Passwortmanager sicher?

2-Faktor-Authentisierung

Gleichzeitig mit der Diskussion des Beirats und der Erarbeitung der Handlungsempfehlungen führte der vzbv mit dem BSI eine Untersuchung dazu durch, wie bekannt und wie verbreitet die 2-Faktor-Authentisierung (2FA) unter Verbraucherinnen und Verbrauchern ist. Die Ergebnisse wurden ebenfalls im Beirat diskutiert.

Dabei zeigte sich, dass der Begriff „Zwei-Faktor-Authentisierung“ ohne weitere Erläuterung nur 43 Prozent aller Internetnutzerinnen und -nutzer ab 16 Jahren bekannt ist. Mit Erläuterung ist das Prinzip der zweistufigen Anmeldung dagegen drei Vierteln (75 Prozent) bekannt. Die bekanntesten und auch die meistgenutzten Verfahren zur Zwei-Faktor-Authentisierung sind SMS-TAN (85 Prozent Bekanntheit unter den „2FA-Kennern“) und Code per E-Mail (76 Prozent). Weniger als die Hälfte der 2FA-Nutzerinnen und Nutzer wüsste, was im Falle eines Verlustes/Defekts des zweiten Faktors zu tun wäre.

2-Faktor-Authentisierung

Als besonders schützenswerte Dienste werden von den 2FA-Kennerinnen und Kennern am häufigsten Online-Banking (90 Prozent) und Bezahldienstleister wie PayPal (84 Prozent) genannt. Diese hohen Werte überraschen nicht, denn mit der Zahlungsdiensterichtlinie PSD2 (Payment Services Directive2) wurde bei solchen Finanzdienstleistungen die 2FA verpflichtend eingeführt.

Das E-Mail-Postfach wird immerhin noch von 61 Prozent als besonders schützenswert angesehen – jedoch nutzen zum Zeitpunkt der Befragung nur 17 Prozent der Kennerinnen und Kenner ein 2FA-Verfahren für die Anmeldung bei ihrem E-Mail-Dienst.

Die Hälfte (50 Prozent) der 2FA-Kennerinnen und Kenner würde es nicht stören, wenn sie sich bei einem Dienst nur noch mittels 2FA anmelden könnten und man sich das genutzte Verfahren jeweils aussuchen könnte.

2-Faktor-Authentisierung

Die Ergebnisse zeigen, dass Verbraucherinnen und Verbraucher sichere Anmeldeverfahren oft noch nicht nutzen. Ein wesentlicher Grund dürfte darin liegen, dass bisher nur wenige Onlinedienste entsprechende Angebote machen. Daher sollten seitens der Onlinedienste die bestmöglichen Voraussetzungen dafür geschaffen werden, dass Verbraucherinnen und Verbraucher ihre Online-Accounts gut schützen können.

Die vorliegende Publikation stellt Arbeitsergebnisse des „Beirates Digitaler Verbraucherschutz“ dar. Der Beirat unterstützt das BSI in beratender Funktion beim Auf- und Ausbau seiner Aufgaben im Bereich des Digitalen Verbraucherschutzes.

Kontakt Dr. Katharina Witterhold
Geschäftsstelle des Beirates Digitaler Verbraucherschutz
Referat WG 31 - Grundsatzfragen des Digitalen Verbraucherschutzes und Kooperationen
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn

beiratdigitalerverbraucherschutz@bsi.bund.de

Weitere Informationen zum „Beirat Digitaler Verbraucherschutz“ des BSI unter

https://bsi.bund.de/dok/beirat-dvs

Gestaltung: FAKTOR 3 AG, Kattunbleiche 35, 22041 Hamburg, www.faktor3.de

Stand: Juli 2022