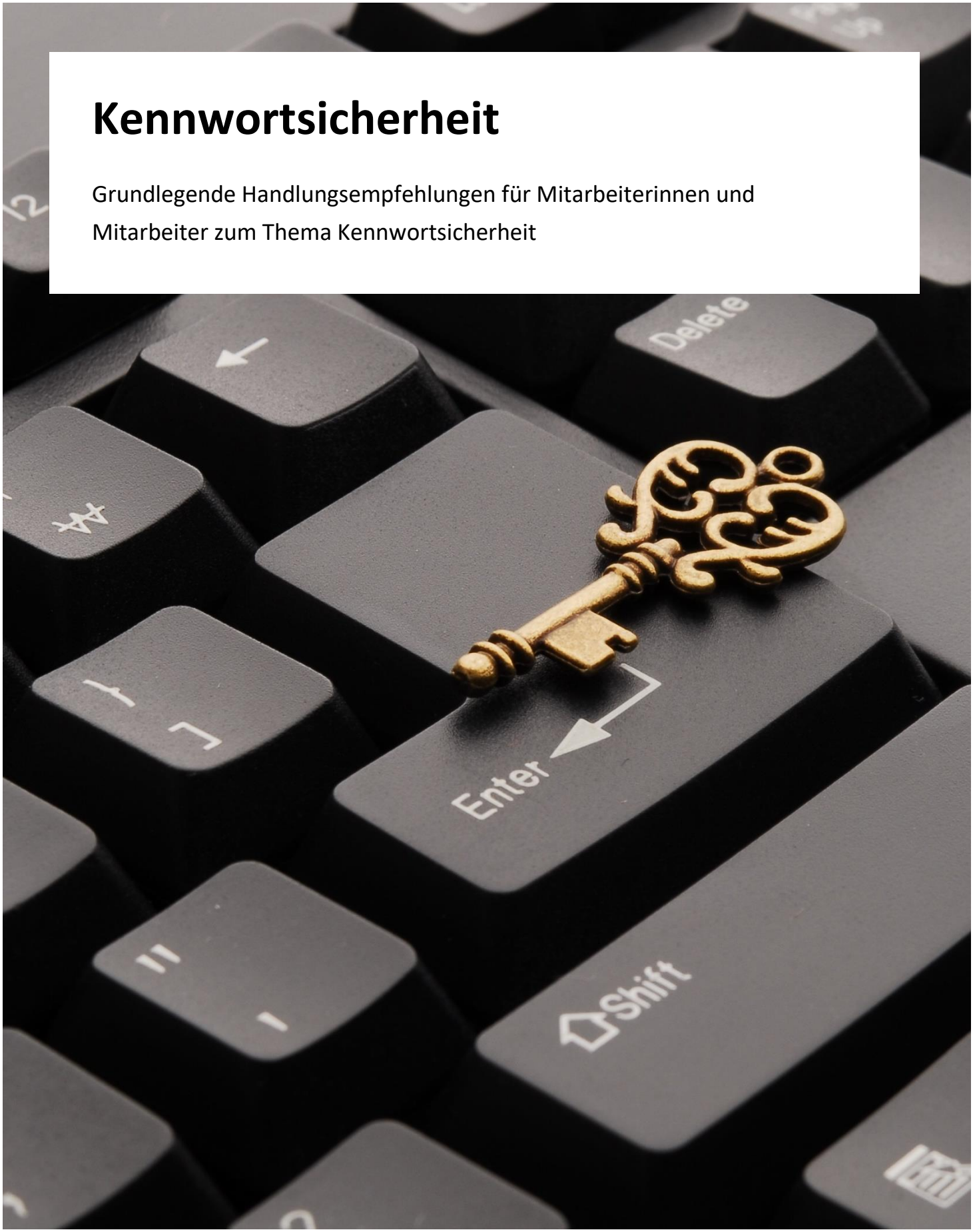
Bundesministerium
Inneres

# Kennwortsicherheit

Grundlegende Handlungsempfehlungen für Mitarbeiterinnen und Mitarbeiter zum Thema Kennwortsicherheit



**Impressum**

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
bmi.gv.at
Autoren: Abteilung IV/10 – Netz- und Informationssystemsicherheit
Direktion Staatsschutz und Nachrichtendienst
Druck: Digitalprintcenter des BMI

**Neuauflage**
**Wien, Februar 2022**



Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an praevention@nis.gv.at | csc@dsn.gv.at

## Einleitung

Die Eingabe von Benutzername und Kennwort ist auch heute noch die bei weitem häufigste Methode, sich gegenüber einem Computersystem zu authentifizieren. Gleichzeitig zeigen jedoch zahlreiche Untersuchungen, dass im Zusammenhang mit Kennwörtern, und hier besonders bei der Kennwortwahl, vielerorts ein erhebliches Potential zur Verbesserung der Sicherheit besteht.

Die vorliegende Ausgabe dieser Schriftenreihe widmet sich daher dem Thema Kennwortsicherheit und versucht, dieses Thema von möglichst allen Seiten zu beleuchten. Ziel ist es, den Mitarbeiterinnen und Mitarbeitern in Ihrem Unternehmen grundlegende Informationen über das Thema zu vermitteln, aber gleichzeitig auch konkrete Handlungsempfehlungen zu einer sicheren Handhabung dieser Authentifizierungsmethode auszusprechen. Dabei bestehen durchaus Bereiche, die auch innerhalb der Branche kontroversiell diskutiert werden. In solchen Fällen haben wir uns bemüht, die unterschiedlichen Sichtweisen neutral zu dokumentieren und konkrete Vor- bzw. Nachteile herauszuarbeiten.

Unser Ziel war es, die Inhalte der vorliegenden Broschüre für alle Mitarbeiterinnen und Mitarbeiter zugänglich zu gestalten und kein spezielles Vorwissen vorauszusetzen. Nichtsdestotrotz finden sich in manchen Bereichen auch vertiefende Ausführungen, die das Thema für Interessierte auf einer höheren Detailebene behandeln.

Wie auch in anderen Bereichen, kann in der Informationstechnik niemals eine hundertprozentige Sicherheit gewährleistet werden. Aus unserer Sicht stellt aber gerade die Kennwortsicherheit eine Möglichkeit dar, bei der mit vergleichsweise geringem Aufwand eine signifikante Erhöhung der Gesamtsicherheit erreicht werden kann. Sie stellt daher einen effektiven und effizienten Hebel dar, die Sicherheit und Resilienz in Ihrem Unternehmen nachhaltig zu erhöhen.

## Inhalt

# 1 Gefahren für die Kennwortsicherheit

> Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months. (Clifford Stoll)

Bevor man sich mit der Frage auseinandersetzt, wie die Kennwortsicherheit erhöht werden kann, erscheint es sinnvoll, mögliche Gefahrenquellen im Zusammenhang mit der Nutzung von Kennwörtern zu identifizieren. Das oben angeführte Zitat von Clifford Stoll skizziert zwei dieser Gefahrenquellen auf ironische Art und Weise.

Die folgende Zusammenstellung soll einen einleitenden Überblick über mögliche Gefahrenquellen geben, auf einzelne Punkte davon wird später im Detail eingegangen.

**Sie geben Ihr Kennwort an Dritte weiter.**

Grundvoraussetzung für Kennwortsicherheit ist es, dass das Kennwort, gleich wie es aufgebaut ist, keinem und keiner Dritten bekannt wird. Um dieses Ziel zu erreichen, ist es entscheidend, dass Sie Ihr Kennwort an niemanden wissentlich weitergeben! Ihre persönlichen Zugangsdaten sollen ausschließlich Ihnen selbst bekannt sein. Es gibt keinen nachvollziehbaren Grund, der eine bewusste Weitergabe Ihres Kennworts an Dritte rechtfertigt.

Auch zwei oftmals ins Treffen geführte Situationen des dienstlichen Alltags bedürfen bei näherer Betrachtung keiner Weitergabe Ihres Kennwortes:

- Ihre IKT-Betriebsunterstützung wird Sie niemals nach Ihrem Kennwort fragen. Die Kolleginnen und Kollegen der IKT-Fachabteilung benötigen Ihre Zugangsdaten nicht, um Sie bei Problemen zu unterstützen.
- Ihre Urlaubsvertretung benötigt Ihre Zugangsdaten nicht, um Sie während Ihrer Abwesenheit vertreten zu können. Praktisch alle aktuellen Softwareprodukte bieten geeignete Werkzeuge für Vertretungsregelungen an.

Eine weitere Gefahr in diesem Zusammenhang ist die nicht wissentliche Weitergabe Ihres Kennwortes. Dabei versuchen Angreifer, Ihnen Ihre Zugangsdaten mit Hilfe teils perfider Tricks zu entlocken. Diesen Gefahrenbereich nennt man allgemein Social Engineering. Umfassende Ausführungen zu diesem Thema sind in Kapitel 5 enthalten.

**Sie verwenden ein schwaches Kennwort.**

Wenn Sie ein schwaches Kennwort verwenden, ist es für einen Angreifer ungleich leichter, Ihr Kennwort zu kompromittieren. Es gibt eine Reihe von Gründen, warum ein Kennwort als schwach einzustufen ist. Dazu zählen unter anderem:

- Ihr Kennwort weist eine unzureichende Länge und/oder –komplexität auf.
- Sie verwenden Wörter aus Wortlisten oder Wörterbüchern als Kennwort.
- Ihr Kennwort verwendet Tastaturmuster oder besteht aus gängigen Phrasen.
- Mehrere Ihrer Kennwörter verwenden dasselbe sprechende Schema.
- Ihr Kennwort besteht aus Teilen Ihrer persönlichen Daten.

Umfassende Ausführungen zu diesen Gefahrenquellen sind in Kapiel 2.2 enthalten.

**Sie können sich Ihr Kennwort nicht merken.**

Weisen Kennwörter eine so große Länge und/oder Komplexität auf, dass Benutzerinnen und Benutzer nicht mehr in der Lage sind, sich diese zu merken, werden Zugangsdaten zumeist aufgeschrieben. Dies kann eine neue Gefahr hervorrufen.

Grundsätzlich stellt das Aufschreiben von Kennwörtern kein Problem dar. Entscheidend ist, wie Sie die aufgeschriebenen Daten verwahren. Oft ist zu beobachten, dass Menschen aus Bequemlichkeit oder Gleichgültigkeit eine entsprechende Notiz an einer ungeeigneten Stelle verwahren. Im schlimmsten Fall wird das aufgeschriebene Kennwort an einer gut lesbaren Stelle deponiert, wo es von jedem und jeder leicht eingesehen werden kann (z.B. Post-It am Monitor oder auf der Tastatur).

Eine Anzahl solch problematischer Stellen hat es auch in die Medien geschafft, wodurch die jeweiligen Zugangsdaten unbeabsichtigt öffentlich wurden. Beispielhaft seien hier folgende Fälle angeführt:

- Für einen Bericht des französischen Fernsehsenders France2 im April 2015, besuchte ein Kamerateam die Redaktionsräume von TV5 Monde, um ein Interview mit einem Mitarbeiter aufzunehmen. An der Pinnwand hinter dem Redakteur befanden sich auf Notizzetteln die Kennwörter einiger Social-Media-Kanäle des Senders[1].
- Auch das österreichische Bundesheer hatte im Juli 2013 mit einer vergleichbaren Panne zu kämpfen. Ein Pressefoto, das im Rahmen der internationalen Übung Hotblade 2013 aufgenommen wurde, zeigt Pilotinnen und Piloten bei einer Einsatzbesprechung. Auf einer Flipchart im Hintergrund sind Adresse und Zugangsdaten für einen diesbezüglichen E-Mail-Zugang erkennbar[2].

Kennwörter sind nur dann stark, wenn Benutzerinnen und Benutzer sich diese auch merken können. Verschiedenen Ansätze, um sich auch starke Kennwörter leicht merken zu können, sind in Kapitel 3.1 enthalten.

Werden Kennwörter aufgeschrieben, so ist es entscheidend, dass diese sicher verwahrt werden. Eine komfortable Möglichkeit, Kennwörter sicher zu verwahren, ist die Verwendung von Programmen zur Kennwortverwaltung (sogenannte Passwortsafes). Eine beispielhafte Vorstellung eines solches Programmes ist in Kapitel 3.2 enthalten.

**Das Kennwort wird für unterschiedliche Dienste verwendet.**

Die Verwendung von Benutzernamen und Kennwörtern ist auch heute noch die bei weitem häufigste Methode, sich gegenüber einem Computersystem oder Diensten im Internet zu authentifizieren. Aus diesem Grund verfügen die meisten Menschen über eine vergleichsweise große Anzahl an unterschiedlichen Benutzerkonten. Statt sich eine Vielzahl von verschiedenen Kennwörtern merken zu müssen, wählen viele den Weg, ein- und dieselben Zugangsdaten für mehrere Benutzerkonten zu verwenden. Diese Vorgangsweise schafft allerdings erhebliche Risiken.

Werden ein- und dieselben Zugangsdaten für mehr als ein Benutzerkonto genutzt, besteht die Gefahr, dass im Fall der Kompromittierung eines Benutzerkontos gleichzeitig auch alle anderen Benutzerkonten kompromittiert sind.

---

[1] Quelle (Beispiel): https://www.spiegel.de/netzwelt/web/tv5-monde-sender-enthuellt-youtube-passwort-a-1027906.html

[2] Quelle (Beispiel): https://futurezone.at/digital-life/bundesheer-verraet-webmail-zugangsdaten/24.600.214

Insbesondere in folgenden Situationen kann dies zu erheblichen Problemen führen:

- Sie verwenden dieselben Zugangsdaten für dienstliche und private Zugänge. Eine Kompromittierung eines privaten Kennworts bedeutet in diesem Fall auch die Kompromittierung Ihres dienstlichen Zugangs.
- Sie verwenden im privaten Bereich dieselben Zugangsdaten für unkritische (und möglicherweise weniger gut geschützte) Dienste im Internet, aber gleichzeitig auch für sensible Dienste wie Online-Banking, Online-Shopping oder medizinische Zugänge.

Obwohl es aus dem Blickwinkel der Sicherheit vorteilhaft wäre, für jeden Dienst individuelle Zugangsdaten bzw. Kennwörter zu verwenden, erscheint vielen Menschen der Aufwand dafür zu hoch. Es wird allerdings dringend empfohlen, zumindest eine Clusterung in dienstliche Zugänge, sensible private Zugänge und eher unkritische private Dienste durchzuführen und keinesfalls dieselben Zugangsdaten bei Diensten aus unterschiedlichen Clustern zu verwenden.

**Das Kennwort wird nie geändert.**

Werden Kennwörter nicht geändert, kann ein Angreifer, sobald er Kenntnis über Ihr Kennwort erlangt hat, dieses auch weiterhin unbemerkt missbrauchen. Ob und wie oft Kennwörter anlasslos geändert werden sollten, ist ein in der Branche intensiv diskutiertes Thema, für das es folglich keine einheitliche Empfehlung gibt. Eine Übersicht über gängige Empfehlungen ist in Kapitel 2.4 im Abschnitt Kennwortänderung enthalten.

# 2 Kennwörter

> Someone figured out my password. Now I have to rename my dog.
> (Unbekannter Autor)

Eine der zentralsten Anforderungen zur Erhöhung der Kennwortsicherheit ist die Wahl eines geeigneten Kennwortes für die benötigten Anwendungen. Dabei ist es entscheidend, zu verstehen, was im konkreten Anlassfall als geeignet angesehen werden kann.

## 2.1 Starke Kennwörter

Grundsätzlich sollte stets darauf geachtet werden, dass ausschließlich starke Kennwörter zur Anwendung kommen. Die Stärke eines Kennworts hängt dabei im Wesentlichen von zwei Faktoren ab:

### Länge des Kennworts

Unter der Länge eines Kennworts versteht man die **Anzahl der Zeichen**, aus denen das Kennwort gebildet wird. Jedes Zeichen erhöht die Kennwortlänge um genau eine Stelle. Es ist für die Kennwortlänge vollkommen unerheblich, aus welchen Zeichen sich das Kennwort zusammensetzt.

### Komplexität des Kennworts

Unter der Komplexität eines Kennworts versteht man hingegen die **Anzahl von unterschiedlichen Kategorien** von Zeichen, aus denen sich ein Kennwort tatsächlich zusammensetzt (Zeichenvorrat). Dabei können grob folgende Kategorien abgegrenzt werden:

- Ziffern
- Kleinbuchstaben
- Großbuchstaben
- Sonderzeichen

Grundsätzlich könnte man annehmen, dass die Sicherheit eines Kennworts mit steigender Länge und Komplexität immer weiter zunimmt. Wie zuvor dargestellt, ist diese Annahme allerdings nur dann zutreffend, wenn die Benutzerinnen und Benutzer auch in der Lage sind, sich das jeweilige Kennwort auch zu merken oder/und es sicher zu verwahren.

## 2.2 Schwache Kennwörter

Der richtige Umgang mit Kennwörtern stellt weltweit einen großen Problembereich dar. Schwache Kennwörter sind nach wie vor weit verbreitet. Dies ist auch empirisch belegbar. Die amerikanische Firma SplashData, Inc. veröffentlicht jährlich eine Aufstellung der am häufigsten genutzten Kennwörter weltweit. Zu diesem Zweck werden von dem Unternehmen geleakte Kennwortdatenbanken (vergleiche Kapitel 6.3) anonymisiert und ausgewertet. Eine Übersicht über die letzten Jahre zeigt erschreckende Ergebnisse.

Tabelle 1 Weltweit häufigste Kennwörter gemäß SplashData, Inc.

| Rang | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|
| **1** | **123456** | **123456** | **123456** | **123456** | **123456** | **123456** |
| **2** | password | password | password | password | password | 123456789 |
| **3** | 12345 | 12345678 | 12345 | 12345678 | 123456789 | qwerty |
| **4** | 12345678 | qwerty | 12345678 | qwerty | 12345678 | password |
| **5** | qwerty | 12345 | football | 12345 | 12345 | 1234567 |
| **6** | 123456789 | 123456789 | qwerty | 123456789 | 111111 | 12345678 |
| **7** | 1234 | football | 1234567890 | letmein | 1234567 | 12345 |
| **8** | baseball | 1234 | 1234567 | 1234567 | sunshine | iloveyou |
| **9** | dragon | 1234567 | princess | football | qwerty | 111111 |
| **10** | football | baseball | 1234 | iloveyou | iloveyou | 123123 |

Es gibt eine Reihe von Gründen, weswegen ein Kennwort als schwach bzw. unsicher zu betrachten ist. Die folgende Aufstellung gibt einen Überblick über die wichtigsten Gründe.

**Geringe Kennwortlänge und/oder –komplexität**

Kennwörter, die eine zu geringe Stellenanzahl und/oder Komplexität aufweisen, können von Angreifern durch das automatisierte Durchprobieren aller möglichen Zeichenkombinationen gehackt werden. Entsprechende Angriffe werden Brute Force-Angriffe genannt (siehe Kapitel 6.2).

**Wörter aus Wortlisten oder Wörterbüchern**

Oft geht einem Brute Force-Angriff ein sogenannter Wortlisten-Angriff (Dictionary Attack) voraus. Dabei werden vor dem aufwändigen Durchprobieren aller möglichen Zeichenkombinationen, zuerst alle Wörter aus gängigen Wörterbüchern durchprobiert.

Bei Wörterbüchern in diesem Sinne muss es sich allerdings nicht ausschließlich um natürlichsprachige Wörterbücher handeln. Vielmehr sind hier beliebige Listen potentieller Kennwörter mit zu betrachten. Im Internet kursieren viele derartige Listen, die Millionen von potentiellen Kennwörtern enthalten. Ein Beispiel für eine solche Liste ist die jährlich erscheinende SplashData-Kennwortliste (siehe Tabelle 1).

Verwendet man Kennwörter, die in solchen Listen enthalten sind, reduziert man den Aufwand eines Angreifers zum Hacken des jeweiligen Benutzerkontos erheblich und erhöht damit die Gefahr für die Kennwortsicherheit.

**Muster und Phrasen**

Gleiches gilt sinngemäß auch für Kennwörter, die aus typischen Tastaturmustern, aus Teilen bekannter Lieder oder anderen Texten (z.B. Zitate, Sprichwörter) abgeleitet sind. Beispielhaft könnte man in diesem Zusammenhang anführen:

- `qwertz` bzw. `qwerty` auf englischen Tastaturen (Tastaturmuster)
- `borninamerica` (Liedertext)
- `venividivici` (Zitat)

Die oben angeführten, zahlreich im Internet kursierenden Wortlisten mit Millionen von potentiellen Kennwörtern, enthalten auch solche typischen Muster und Phrasen, die in der Folge bei einem Wortlisten-Angriff ebenfalls durchprobiert werden.

**Sprechende Schemata**

Eine weit verbreitete, aber gleichzeitig sehr gefährliche Möglichkeit, für jeden Zugang ein individuelles Kennwort zu verwenden und gleichzeitig den Aufwand zum Merken der Kennwörter zu minimieren, ist die Verwendung sogenannter sprechender Schemata.

Dabei wird in der Regel ein für alle Zugänge einheitliches, meist kurzes Kennwort verwendet, dem je nach entsprechendem Benutzerkonto eine individuelle Endung nachgestellt wird. So könnten beispielsweise Variationen des Kennworts `maxi` für verschiedene Benutzerkonten verwendet werden:

- `maxi-amazon` (für Online-Shopping mit einem Amazon-Benutzerkonto)
- `maxi-twitter` (für Social Media-Nutzung mit einem Twitter-Benutzerkonto)
- `maxi-bankaustria` (für Online Banking mit einem Bank Austria-Benutzerkonto)

Diese Vorgangsweise sollte unbedingt vermieden werden, da im Falle der Kompromittierung eines der Kennwörter, gleichzeitig auch alle anderen Kennwörter als nicht mehr sicher betrachtet werden müssen.

**Persönliche Daten**

Die Verwendung persönlicher Daten als Bestandteil von Kennwörtern wird insbesondere dann zum Problem, wenn sich ein Angriff gezielt gegen eine bestimmte Person richtet und der Angreifer im Vorfeld Recherchen über diese Person anstellt.

Es sollte unter allen Umständen vermieden werden, Daten, die ein Angreifer durch Recherchen (z.B. in Sozialen Medien) ermitteln kann, als Teil von Kennwörtern zu verwenden. Einige Beispiele für solche Kennwörter könnten sein:

- Name des Partners
- Namen von Kindern
- Namen von Haustieren
- Kosenamen
- Geburtsdaten
- Autonummern

Richtet sich ein Angriff konkret gegen eine bestimmte Person, so recherchieren Angreifer oft mit großem Aufwand private und dienstliche Details aus dem Leben des Opfers und stellen aus allem und jedem, was sie dabei finden können, eine individuelle Wortliste her, die genauso wie die oben beschriebenen Listen für einen Wortlisten-Angriff verwendet werden.

## 2.3 Kennwortwahl

Die vorgegebenen Rahmenbedingungen für die Wahl eines Kennwortes sind Gegenstand intensiver Diskussionen innerhalb der Branche. Insbesondere das Verhältnis zwischen Länge und Komplexität wird kontroversiell diskutiert. Vereinfacht dargestellt, haben sich zwei Ansätze herauskristallisiert.

### Klassischer Ansatz

Der klassische Ansatz stammt in seinem Kern aus der Special Publication 800-63 (Appendix A) der amerikanischen Standardisierungsbehörde NIST (National Institute of Standards and Technology) aus dem Jahr 2003. In diesem Dokument hat die NIST seinerzeit die Anforderungen für sichere Kennwörter festgelegt.

Zwei der wesentlichsten Grundsätze des klassischen Ansatzes lassen sich wie folgt zusammenfassen:

- Das Kennwort soll eine maximale Komplexität aufweisen (d.h. aus Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen bestehen).
- Dass Kennwort soll (anlasslos) regelmäßig geändert werden.

In der Folge fanden diese Anforderungen Eingang in die Literatur der Sicherheitsbranche, in entsprechende Empfehlungen vieler europäischer Institute und Gremien und damit auch in die Kennwortrichtlinien zahlreicher Unternehmen und Behörden.

### Aktueller Ansatz

Die aktuelle Version der Kennwortrichtlinie des NIST bricht radikal mit einigen der bisherigen Grundsätze. Der Grund ist einfach. Untersuchungen haben gezeigt, dass zu hohe Kom-

plexitätsanforderungen und häufige Änderungsverpflichtungen dazu führen, dass Endnutzerinnen und Endnutzer versuchen, im Rahmen der Vorgaben möglichst einfache Lösungen zu finden (z.B. Nutzung von Tastaturmustern oder die rollierende Nutzung der immer gleichen Kennwörter). Dies wirkt sich am Ende des Tages insgesamt negativ auf die Kennwortsicherheit aus.

Die wesentlichsten Aussagen des überarbeiteten Ansatzes lauten daher:

- Eine hohe Komplexität von Kennwörtern soll hinkünftig nicht mehr zwingend erforderlich (wohl aber möglich) sein.
- Stattdessen sollen Kennwörter generell länger werden. Empfohlen wird die Verwendung von Passphrasen (z.B. Eingabe ganzer Sätze) statt Kennwörtern.
- Anlasslose, regelmäßige Kenntwortänderungen sollen nicht mehr zwingend erforderlich sein. Änderungen sollen nur mehr dann durchgeführt werden, wenn ein konkreter Verdacht auf eine Kompromittierung des Kennworts vorliegt.

Darüber hinaus werden durch das NIST auch Empfehlungen für die serverseitigen Rahmenbedingungen festgelegt:

- Die Verwendung ungeeigneter oder geleakter Kennwörter (z.B. 1234567890) soll durch den Einsatz von Blacklists unterbunden werden.
- Es soll nicht mehr möglich sein, das Kennwort durch die Beantwortung trivialer Sicherheitsfragen (z.B. Mädchenname der Mutter) zurückzusetzen.
- Die Hinterlegung von selbst erstellten Kennworthinweisen durch Benutzerinnen und Benutzer soll nicht mehr möglich sein.

## 2.4 Handlungsempfehlungen

Die folgenden Ausführungen stellen unverbindliche Handlungsempfehlungen des Bundesministeriums für Inneres da. Die vorgeschlagenen Maßnahmen richten sich dabei gleichermaßen an Mitarbeiterinnen und Mitarbeiter, wie auch an die jeweiligen Unternehmen. Während Unternehmen die Handlungsempfehlungen in Form von technischen Vorgaben umsetzen können, wird Mitarbeiterinnen und Mitarbeitern empfohlen, diese Maßnahmen auch bei all jenen dienstlichen und privaten Zugängen anzuwenden, bei denen keine technisch erzwungene Umsetzung erfolgt.

## Bedrohungsanalyse

Eine Authentifizierung mittels Benutzername und Kennwort findet bei ganz unterschiedlichen Diensten mit ganz unterschiedlichen Sicherheitsanforderungen statt. Am Anfang jeglicher Überlegung zur Wahl eines Kennwortes sollte daher eine Art Bedrohungsanalyse stehen. Folgende Schritte sollten für jeden Zugang durchgeführt werden:

1. Analyse der Konsequenzen bei einer Kompromittierung des bereffenden Zugangs
2. Analyse weiterer begleitender Sicherheitsmaßnahmen beim betreffenden Zugang
3. Auswahl eines angemessenen Sicherheitsniveaus der Kennwortsicherheit

Nicht jeder Zugang benötigt zwingend dasselbe Sicherheitsniveau. Diese Vorgangsweise stellt sicher, dass für jeden Zugang ein angemessenes Niveau im Zusammenhang mit Kennwortsicherheit hergestellt werden kann.

> Wir empfehlen, die vorgegebenen Rahmenbedingungen für die Wahl eines Kennworts dem jeweils erforderlichen Sicherheitsniveau anzupassen. Die immer gleichen (hohen) Anforderungen für alle verwendeten Kennwörter, unabhängig vom Bedrohungspotential, belasten Ihre Mitarbeiterinnen und Mitarbeiter unnötig und führen dazu, dass versucht wird, im Rahmen der verpflichtenden Vorgaben die einfachsten Möglichkeiten für alle Kennwörter auszuloten. Das wiederum reduziert das Sicherheitsniveau auch der sensiblen Zugänge.

## Kennwortwahl

Ein Kennwort ist nur dann wirklich sicher, wenn die betreffende Person in der Lage ist, sich dieses Kennwort auch zu merken. Unrealistische (verpflichtende) Anforderungen hinsichtlich der Länge und/oder Komplexität führen unweigerlich dazu, dass Kennwörter aufgeschrieben werden.

Das Aufschreiben von Kennwörtern an sich ist zwar per se kein Problem, zum Risiko wird diese Vorgangsweise allerdings dann, wenn das aufgeschriebene Kennwort nicht sicher verwahrt wird (zumindest in versperrten Möbelstücken). Allzu oft ist es gelebte Praxis, das Kennwort auf eine Post-It Notiz zu schreiben und auf den Montitor oder unter die Tastatur zu kleben. Dies muss in jedem Fall vermieden werden.

Wir empfehlen einen Verzicht auf verpflichtende Komplexitätsanforderungen nur dann, wenn stattdessen bei Zugängen mit einem hohen Bedrohungspotential adäquate Rahmenbedingungen sichergestellt sind. Dazu zählt einerseits eine minimale Kennwortlänge von mehr als 14 Stellen, sowie ein serverseitiger Abgleich der gewählten Kennwörter gegen Blacklists von häufigen oder ungeeigneten Kennwörtern.

## Kennwortrücksetzung

Bei vielen Zugängen und Diensten besteht für Benutzerinnen und Benutzer die Möglichkeit, das eigene Kennwort durch die Beantwortung teils trivialer Sicherheitsfragen zurückzusetzen bzw. zurücksetzen zu lassen. Dies ist sowohl elektronisch, als oft auch telefonisch möglich.

Dabei ist zu berücksichtigen, dass die besten Rahmenbedingungen für die Sicherheit von Kennwörtern ausgehebelt werden, wenn ein Angreifer das Kennwort durch Nennung beispielsweise des Mädchennamens der Mutter rücksetzen (lassen) kann.

Wir empfehlen, eine Rücksetzung von Kennwörtern durch Benutzerinnen und Benutzer nur unter sicheren Rahmenbedingungen zuzulassen. Auf die Möglichkeit einer Rücksetzung durch Beantwortung trivialer Sicherheitsfragen sollte vollständig verzichtet werden.

## Kennwortänderung

Insbesondere mögliche Verpflichtungen zur anlasslosen Änderung von Kennwörtern sind Gegenstand intensiver Diskussionen innerhalb der Branche. Die allgemeine Tendenz geht dabei eindeutig in die Richtung, auf eine verpflichtende anlasslose Änderung von Kennwörtern zu verzichten.

Demzufolge gäbe es nur mehr eine Handvoll Gründe, ein Kennwort zu ändern:

- Es besteht ein konkreter Verdacht, dass das eigene Kennwort unberechtigten Dritten bekannt wurde, z. B. wenn man festgestellt hat, dass man bei der Kennworteingabe von einem Dritten beobachtet wurde (Shoulder Surfing).
- Es liegen Anhaltspunkte vor, dass das eigene Kennwort kompromittiert wurde, z. B. wenn der Verdacht besteht, dass mit dem durch das Kennwort geschützen Zugang Transaktionen durch Dritte durchgeführt wurden.
- Es wird festgestellt, dass die eigenen Zugangsdaten Bestandteil eines bekannt gewordenen Datenleaks geworden sind.

Der Grund für diese Tendenz liegt darin, dass eine häufige Verpflichtung zur anlasslosen Kennwortänderung Mitarbeiterinnen und Mitarbeiter dahingehend motiviert, mögliche Wege zu suchen, den Merkaufwand trotzdem zu minimieren. Dies führt unter anderem zur rollierenden Nutzung der immer selben Kennwörter oder dem „Durchnummerieren“ eines immer gleichen Grund-Kennwortes.

Wir empfehlen, trotz der allgemeinen Tendenz zum vollständigen Verzicht auf anlasslose Änderungspflichten, folgende verpflichtende Kennwortänderungen vorzusehen:

- **im Anlassfall**: bei einem der oben angeführten Gründe
- **ohne Anlassfall**: zumindest alle 6 bis 12 Monate

# 3 Aufbewahrung von Kennwörtern

> "One of the keys to happiness is a bad memory." (Rita Mae Brown)

Im Zusammenhang mit der Kennwortsicherheit kommt der geeigneten Aufbewahrung von Kennwörtern eine große Bedeutung zu. Zum einen erfordert die tägliche Praxis, dass man sich zumindest eine erhebliche Anzahl an Kennwörtern auswendig merkt. Zum anderen ist es in der Regel von Vorteil, wenn Kennwörter für den Bedarfsfall (z.B. Vergessen eines Kennwortes) verschriftlicht vorliegen. Im Folgenden werden zwei Möglichkeiten für die sichere Aufbewahrung von Kennwörtern aufgezeigt.

## 3.1 Mnemotechnik

Untersuchungen haben gezeigt, dass sich das menschliche Gehirn ganze Sätze wesentlich leichter merken kann, als abstrakte Zeichenfolgen. Zum Merken starker Kennwörter bietet sich daher die Nutzung von Sätzen an, und zwar unabhängig davon, ob der klassische oder der aktuelle Ansatz zur Anwendung kommt.

- **Klassischer Ansatz**

Um sich komplexe Kennwörter leichter merken zu können, erscheint die Verwendung von Schlüsselsätzen empfehlenswert. So ist der folgende Satz relativ leicht merkbar:

> Als ich sechs Jahre alt war, besuchte ich die erste Klasse der Volksschule.

Um daraus nun ein komplexes Kennwort zu machen, müssen bei der Kennworteingabe lediglich die Anfangsbuchstaben der einzelnen Worte in korrekter Groß- bzw. Kleinschreibung und die vorhandene Interpunktion aneinandergereiht werden. Zahlenwörter werden durch die entsprechende Ziffer ausgedrückt.

> Als ich sechs Jahre alt war, besuchte ich die erste Klasse der Volksschule.

Dadurch wird aus einem einfachen Schlüsselsatz ein starkes Kennwort:

```
Ai6Jaw,bid1KdV.
```

Verwendet man für unterschiedliche Benutzerkonten unterschiedliche Zugangsdaten, kann die Verwendung von Schlüsselsätzen mit Situationsbezug bzw. Raumbezug angedacht werden. Dabei bezieht sich der jeweilige Schlüsselsatz in geeigneter Form auf den verwendeten Computer oder Dienst (z.B. „An der Wand hinter meinem Computer hängt ein großes Bild von einem Leuchtturm.“ ( `AdWhmCh1gBv1L.` ).

- **Aktueller Ansatz**

Auch in diesem Fall können Sätze als Grundlage für starke Kennwörter herangezogen werden. Statt wie im obigen Beispiel aus einem Schlüsselsatz ein Kennwört abzuleiten, kann man bei diesem Ansatz den Satz gleich in seiner urspünglichen Form als Kennwort verwenden.

Im konkreten Beispiel wäre somit der Satz „Als ich sechs Jahre alt war, besuchte ich die erste Klasse der Volksschule.“ bereits selbst das Kennwort. Dabei muss allerdings berücksichtigt werden, dass nicht jede Kennworteingabe die Nutzung von Leerzeichen zulässt. Diese müssten gegebenenfalls weggelassen werden.

> Wir empfehlen zum leichteren Merken von starken Kennwörtern generell die Verwendung ganzer Sätze. Aus diesen kann bei der Kennworteingabe entweder ein komplexes Kennwort abgeleitet werden (klassischer Ansatz) oder man verwendet den Satz in seiner ursprünglichen Form als Passphrase (aktueller Ansatz).

## 3.2 Programme zur Kennwortverwaltung

Für viele Menschen ist es trotz der Verwendung von Merktechniken wie Schlüsselsätzen sehr schwierig, sich für unterschiedliche Benutzerkonten mehrere individuelle Kennwörter zu merken. Eine Möglichkeit, diesem Problem entgegen zu wirken, kann die Verwendung von Programmen zur Kennwortverwaltung (sogenannten Password Safes) sein. Gleichzeitig sind solche Programme auch sehr nützlich, um ein vergessenes Kennwort nachschlagen zu können.

Programme zur Kennwortverwaltung verwalten alle Zugangsdaten (Benutzernamen und Kennwörter) eines Benutzers oder einer Beutzerin in einer stark verschlüsselten Datenbank, die nur mit einem sicheren Master-Kennwort geöffnet und ausgelesen werden kann. Dieses Master-Kennwort ist fortan das einzige Kennwort, dass sich die betreffende Person merken muss. Die Nutzung eines Password Safes kann wie folgt zusammengefasst werden:

- Der Benutzer oder die Benutzerin legt die Zugangsdaten (Usernamen und Kennwörter) aller eigenen Benutzerkonten im Password Safe ab.
- Der Safe wird mit einem Master-Kennwort verschlüsselt. Dieses muss zwingend ein starkes Kennwort sein.
- Benötigt der Benutzer oder die Benutzerin Zugangsdaten aus dem Safe (z.B. zur Anmeldung an einem Online-Dienst), so wird das Programm zur Kennwortverwaltung aufgerufen und das Master-Kennwort eingegeben.
- Dann können der Username und das Kennwort über die normale Zwischenablage aus dem Safe herauskopiert und in die Anmeldemaske eingetragen werden. Einige Sekunden nach dem Kopiervorgang wird die Zwischenablage durch das Programm automatisch geleert.
- Mit dem Schließen des Password Safes werden alle etwaigen temporären Datenartefakte zu diesem Vorgang am Rechner vollständig gelöscht.

Üblicherweise bieten gängige Password Safes auch die Möglichkeit, sichere Kennwörter für Benutzerkonten automatisch zu generieren. Ein Beispiel für einen frei erhältlichen und quelloffenen Password Safe ist das Programm KeePass 2 (https://keepass.info)[3].

Die Datenbankdatei wird stark verschlüsselt auf der lokalen Festplatte abgespeichert und ist ohne das installierte Programm benutzbar. Um den Password Safe ortsunabhängig nutzen zu können, kann die Datenbankdatei auch in einer Cloud abgespeichert werden oder beispielsweise auf einem USB-Schlüsselanhänger permanent mitgeführt werden. Unter der Voraussetzung eines starken Master-Kennworts erscheint die Verschlüsselung ausreichend, um eine ausreichende Sicherheit auch in diesen Anwendungsfällen gewährleisten zu können.

[3] In diesem Dokument namentlich genannte Produkte und Dienste sind lediglich als Beispiele zu verstehen und stellen keine Empfehlung durch das Bundesministerium für Inneres (BMI) dar. Das BMI hat keinerlei direkte oder indirekte Verbindung zu den jeweiligen Herstellern bzw. Betreibern und kann daher keine Garantie für die Funktion und die Sicherheit des jeweiligen Produkts bzw. Dienstes übernehmen.

# 4 Mehrfaktor-Authentifizierung

> „If you spend more on coffee than on IT security, you will be hacked,
> What's more, you deserve to be hacked." (Richard Clarke)

Eine Mehrfaktor-Authentifizierung ist eine hochwirksame Möglichkeit, die Sicherheit des Anmeldevorganges an einem System oder an einem Online-Dienst stark zu erhöhen. Für die Benutzerinnen und Benutzer entsteht dabei beim Anmeldevorgang ein gewisser Mehraufwand, dieser sollte jedoch im Hinblick auf den erzielbaren Gewinn an Sicherheit vernachlässigbar sein.

Die Authentifizierung gegenüber einem beliebigen System, also der Nachweis der eigenen Identität, kann grundsätzlich auf drei verschiedenen sogenannten Faktoren beruhen:

### Etwas, das ich weiß

Für eine Authentifizierung ist lediglich die Kenntnis der jeweiligen Zugangsdaten erforderlich (z.B. Kennwort, PIN-Code, Mobiltelefon-Wischmuster).

### Etwas, das ich habe

Für eine Authentifizierung ist das Vorhandensein eines physischen Gegenstandes erforderlich (z.B. Token-Generator, Keycard). Auch das beim jeweiligen Geldinstitut registrierte Mobiltelefon beim mTAN-Verfahren (Online-Banking) zählt zu diesem Faktor.

### Etwas, das ich bin

Zur Authentifizierung werden körperliche Merkmale des Benutzers herangezogen (z.B. Fingerabdruck, Venenmuster, IRIS- oder Retinaabbild).

Wenn für einen Authentifizierungsvorgang Daten aus zumindest zwei Faktoren erforderlich sind, spricht man von Mehrfaktor-Authentifizierung. Entscheidend für einen optimalen Sicherheitsgewinn ist dabei, dass die Authentifizierung mit Daten aus unterschiedlichen Faktoren durchgeführt wird. Beispiele für eine Mehrfaktor-Authentifizierung in diesem Sinne sind:

- Fingerabruck und Eingabe eines Kennworts
- Eingabe eines Kennworts und Verwendung einer Keycard

Bei einem mehrstufigen Authentifizierungsvorgang mit Daten aus ein- und demselben Faktor handelt es sich streng genommen nicht um eine Mehrfaktor-Authentifizierung im eigentlichen Sinn. Dazu zählen beispielsweise das Erfordernis der Eingabe von zwei Kennwörtern nacheinander (zwei Mal etwas, das ich weiß) oder die Durchführung eines Fingerabdruck- und eines Netzhautscans (zwei Mal etwas, das ich bin).

Eine weit verbreitete Methode der Mehrfaktor-Authentifizierung ist das, besonders im Online Banking-Bereich genutzte, mTAN-Verfahren. Dabei ist es erforderlich, zuerst Zugangsdaten (Benutzername/Verfügernummer und Kennwort) einzugeben und danach eine Transaktion mit einem TAN-Code zu bestätigen. Dieser TAN-Code wird für jede Transaktion individuell auf ein zuvor registriertes Mobiltelefon übermittelt. Ohne das Vorhandensein des physischen Gegenstandes (Mobiltelefon) wäre also die Durchführung einer Transaktion nicht möglich.

Die Mehrfaktor-Authentifizierung erhöht die Sicherheit eines Anmeldevorgangs erheblich und sollte daher überall dort genutzt werden, wo sie zur Verfügung steht (insbesondere bei der Nutzung von Online-Diensten). Zahlreiche große Online-Dienste bieten eine derartige Möglichkeit an, die jedoch nicht immer an prominenter Stelle angeboten wird. Eine gute Übersicht über Dienste, die Mehrfaktor-Authentifizierung anbieten, bietet die Website „Two Factor Auth“ (https://2fa.directory)[4].

[4] In diesem Dokument namentlich genannte Produkte und Dienste sind lediglich als Beispiele zu verstehen und stellen keine Empfehlung durch das Bundesministerium für Inneres (BMI) dar. Das BMI hat keinerlei direkte oder indirekte Verbindung zu den jeweiligen Herstellern bzw. Betreibern und kann daher keine Garantie für die Funktion und die Sicherheit des jeweiligen Produkts bzw. Dienstes übernehmen.

# 5 Social Engineering

> There is no technology today that cannot be defeated by social engineering. (Frank Abagnale)

Eine besondere Art von Cyberangriffen stellen Attacken auf Basis von Social Engineering-Techniken dar. Social Engineering ist ein zielgerichteter Angriff auf die „Schwachstelle Mensch“. Dabei werden mitunter perfide Tricks angewendet, die menschliche Eigenschaften wie Neugierde, Vertrauen oder mangelndes Sicherheitsbewusstsein konsequent ausnutzen. Solche Cyberangriffe werden daher mitunter auch ironisch „angewandte Sozialwissenschaft“ genannt.

Der Begriff Social Engineering wird unterschiedlich verwendet. Während einige unter dieser Begrifflichkeit ausschließlich Aktivitäten verstehen, bei denen Angreifer unter Verwendung sozialer Interaktion (z.B. vorgebliche Liebesbeziehung) versuchen, eine Zielperson zu bestimmten Handlungen zu bewegen oder dieser vertrauliche Informationen zu entlocken, versteht man darunter allgemein auch alle Aktivitäten, bei denen eine Person oder Organisation durch trickreiche Vorspiegelung falscher Tatsachen angegriffen wird.

Solcial Engineering ist ein weites Feld, das eine nahezu unerschöpfliche Bandbreite von Angriffsszenarien beinhaltet. Im Rahmen dieser Broschüre werden ausschließlich ausgewählte Angriffsszenarien dargestellt, die unmittelbar mit der Kennwortsicherheit in Zusammenhang stehen.

## 5.1 Smalltalking

Es ist überraschend, mit welcher Leichtigkeit es für geschickte Angreifer möglich ist, einer ahnungslosen Zielperson im Verlauf eines scheinbar harmlosen Gesprächs Informationen, einschließlich deren persönliche Zugangsdaten, zu entlocken. In Fällen wie diesen ist es entscheidend, dass sich potentielle Opfer der möglichen Gefahren solcher Situationen bewusst sind und rechtzeitig und gezielt gegensteuern.

Solche Situationen werden auch immer wieder gerne in Unterhaltungssendungen thematisiert, wobei nicht vergessen werden darf, dass die scheinbar humoristische Darbietung einen ernsten Hintergrund hat[5]. Niemand ist grundsätzlich vor solchen Angriffen sicher.

## 5.2 Shouldersurfing

Shouldersurfing bezeichnet eine Situation, in der eine Zielperson von einem Angreifer durch einen „Blick über die Schulter“ bei der Eingabe vertraulicher Daten beobachtet wird. Während sich dieser Begriff grundsätzlich auf alle Arten von Daten beziehen kann, erscheint im Zusammenhang dieser Broschüre insbesondere die Eingabe von Zugangsdaten (Benutzernamen und Kennwörter) von Relevanz.

Während bei der Benutzung von Geldausgabeautomaten mittlerweile ein vergleichsweise hohes Sicherheitsbewusstsein in der Bevölkerung herrscht und Dritten die freie Sicht auf die Codeeingabe in der Regel aktiv verwehrt wird, wird auf solche Vorsichtsmaßnahmen in anderen Bereichen leider allzuoft vollkommen verzichtet. Ein Angreifer, der sich geschickt in den Nahbereich einer Zielperson begibt, kann somit leicht persönliche Zugangsdaten ausspähen. Insbesondere, aber keinesfalls ausschließlich, ist in folgenden Situationen größtmögliche Vorsicht geboten:

- Entsperren des Mobiltelefons in öffentlichen Verkehrsmitteln
- Anmeldung am Notebook in öffentlichen Wartebereichen (z.B. Flughafen)
- Eingabe von Zugangsdaten in videoüberwachten Bereichen
- Unbewusstes Mitsprechen des Kennwortes bei der Eingabe in Gegenwart Dritter (auch am Telefon)

Es ist bei der Eingabe von beliebigen Zugangsdaten unbedingt erforderlich, sich vor der Eingabe bewusst mit der unmittelbaren Umgebung auseinanderzusetzen, um ein Mitlesen Dritter auszuschließen.

[5] Beispiel: https://www.youtube.com/watch?v=opRMrEfAIiI

## 5.3 Telefon-Betrug

Das Telefon ist generell ein sehr verbreitetes Angriffsmittel bei Social Engineering-Angriffen, da sich Angerufene mangels einer face2face-Situation in der Regel leichter von vorgespiegelten Sachverhalten überzeugen lassen. Auch ist es am Telefon vergleichsweise leicht, Benutzerinnen und Benutzer zu verunsichern und auf diese Weise unter Druck zu setzen.

Im Zusammenhang mit Kennwortsicherheit besteht ein verbreitetes Angriffsszenario beispielsweise darin, dass sich ein Angreifer telefonisch bei Benutzerinnen oder Benutzern als IKT-Fachabteilung meldet und der angerufenen Person einen für sie unverständlichen, IT-technischen Sachverhalt schildert, der angeblich unmittelbar mit ihr zusammenhänge. Es wird suggeriert, dass in dieser Situation dringend eine Lösung gefunden werden muss, da sonst großer Schaden entstehen kann. In dieser Stresssituation wird die angerufene Person dann zur Bekanntgabe der eigenen Zugangsdaten aufgefordert, da die normal üblichen Vorgangsweisen in dieser speziellen Situation angeblich zu lange dauern würden.

Als Grundsatz gilt, dass man auch in solchen Situationen niemals persönliche Zugangsdaten an einen Dritten weitergeben darf. Werden Sie darüber hinaus in einem dienstlichen Kontext von einem Unbekannten, der angibt, im Auftrag Ihres Unternehmens zu handeln, aufgefordert, irgendwelche Ihnen nicht nachvollziehbare Aktivitäten zu setzen, empfiehlt es sich, diese Behauptung vor der Befolgung der Anweisungen (z.B. durch Rückruf an die Ihnen bereits zuvor bekannte Rufnummer der IKT-Betriebsunterstützung) gesichert zu verifizieren.

## 5.4 Phishing

Bei einem Phishing-Angriff versucht ein Angreifer, an persönliche Daten (insbesondere an Benutzernamen und Kennwörter) eines Opfers zu gelangen, um diese dann missbräuchlich zu verwenden. Der Begriff selbst ist ein Kunstwort aus „password“ und „fishing“. Ziele eines Phishing-Angriffs sind zumeist Zugangsdaten für Online Banking oder für beliebige andere Onlinedienste, wie beispielsweise Webmail-Anwendungen.

Ein Phishing-Angriff erfolgt in der Regel durch die Zusendung einer vom Angreifer vorbereiteten E-Mail-Nachricht an das potentielle Opfer. In dieser Nachricht wird ein bestimmtes Szenario entworfen, welches die Zielperson dazu bringen soll, möglichst unmittelbar auf einen, in der Nachricht eingebetteten, Hyperlink zu klicken (z.B. müsse man sofort seine

Online Banking-Zugangsdaten bestätigen). Dabei ist unbedingt zu beachten, dass das im fortlaufenden E-Mail-Text angezeigte Ziel eines Hyperlinks technisch nicht mit dem tatsächlichen Ziel übereinstimmen muss. Im Fall von Phishing wird das Opfer in Wirklichkeit auf einen Server des Angreifers umgeleitet, auf dem das eigentlich erwartete Eingabefeld für die jeweiligen Zugangsdaten (z.B. Online Banking-Eingabefeld) täuschend ähnlich nachgebaut ist. Im Glauben, seine Zugangsdaten auf einer legitimen Seite einzugeben, stellt man diese jedoch somit unbewusst dem Angreifer zur Verfügung.

Eine Teilmenge dieser Angriffsart sind sogenannte Spearphishing-Angriffe. Während sich normale Phishing-Angriffe („Fischen mit einem Fischernetz“) stets an eine sehr große Anzahl potentieller, dem Angreifer in der Regel nicht bekannte Opfer richten, handelt es sich bei Spearphishing („Fischen mit einem Speer“) um einen zielgerichteten Angriff auf eine einzelne Zielperson. Spearphishing-Nachrichten sind im Unterschied zu normalen Phishing-Nachrichten immer maßgeschneidert und stark personalisiert. Der Angreifer hat im Vorfeld des Angriffs erhebliche Ressourcen dafür aufgewendet, Details über die Zielperson in Erfahrung zu bringen, um somit die Nachricht möglichst persönlich und vertrauenswürdig gestalten zu können (z.B. plausibler Kontext der Nachricht, Ansprache mit korrektem Namen, Nutzung von konkreten Details aus dem Arbeitsumfeld der Zielperson). Das Ziel des Angriffs, nämlich das Ausspähen des Kennwortes des Opfers, bleibt jedoch dasselbe.

Wie schon im Falle von Social Engineering, wird auch der Phishing-Begriff unterschiedlich verwendet. Ursprünglich geht es einem Phishing-Angreifer ausschließlich darum, an die Zugangsdaten des Opfers zu gelangen. In letzter Zeit werden jedoch (vor allem in Massenmedien) zunehmend auch E-Mail-Nachrichten, die nur dazu dienen, Systeme mit Schadcode zu infizieren, fälschlicherweise ebenfalls als Phishing-E-Mail bezeichnet.

Das Wichtigste im Zusammenhang mit Phishing ist ein diesbezügliches Bewusstsein im Umgang mit fragwürdigen E-Mail-Nachrichten. Mit einem diesbezüglichen Bewusstsein, ein wenig Aufmerksamkeit und gesundem Misstrauen lassen sich die meisten Gefahren nachhaltig neutralisieren.

# 6 Kennworthacking

> "Time is what determines security. With enough time nothing is unhackable." (Aniekee Tochukwu Ezekiel)

Dieser Abschnitt soll die Notwendigkeit der im Bereich der Kennwortsicherheit empfohlenen Maßnahmen unterstreichen, indem skizziert wird, wie das Hacken von Kennwörtern in der Praxis durchgeführt wird und auf welche Weise starke Kennwörter dieses verhindern können.

## 6.1 Hashwerte

In der Regel werden Kennwörter auf Systemen nicht im Klartext, sondern in Form von sogenannten Hashwerten gespeichert, die von den jeweiligen Kennwörtern abgeleitet sind. Um einen Hashwert zu erzeugen, wird das jeweilige Kennwort mit einem (bekannten) mathematischen Einwegalgorithmus umgerechnet. Einweg- bedeutet in diesem Zusammenhang, dass der Algorithmus so aufgebaut ist, dass zu jedem Kennwort genau ein Hashwert errechnet wird. Dieser Hashwert kann allerdings nicht mehr in das ursprüngliche Kennwort zurückgerechnet werden. Hashwerte haben, unabhängig von der Länge des zugrundeliegenden Kennworts, immer eine konstante Länge[6].

Zur Authentifizierung wird folglich nicht das Kennwort, sondern immer nur der abgeleitete Hashwert herangezogen. Auf den Systemen, gegenüber denen sich der Benutzer authentifizieren muss (z.B. Server eines Online-Dienstes), besteht daher auch keine Notwenigkeit, Kennwörter im Klartext abzuspeichern oder solche dorthin zu übermitteln.

[6] In der Praxis können darüber hinaus verschiedene Verfahren angewandt werden, um ein höheres Sicherheitsniveau zu erzielen. Beispielsweise kann an ein Klartextkennwort vor der Erzeugung des Hashwertes eine zufällig gewählte Zeichenfolge angehängt werden, um die Entropie der Eingabe zu erhöhen („Salting").

Von Kennwörtern abgeleitete Hashwerte werden, zusammen mit den zugehörigen Benutzernamen, sowohl auf lokalen Systemen, als auch auf Servern abgespeichert und über dazwischenliegende Netzwerke übertragen. In der Regel ist der erste Schritt zum Diebstahl von Kennwörtern ein Angriff mit dem Ziel, die Hashwerte der verwendeten Kennwörter potentieller Opfer zu erbeuten. Gelingt dies, verfügen Angreifer über eine Liste der hinterlegten Kombinationen aus Benutzernamen (das sind heute zumeist E-Mail-Adressen) und den zugehörigen Hashwerten.

## 6.2 Brute Force-Angriffe

Ein Brute Force-Angriff ist, wie der Name bereits suggeriert, ein Angriff mit roher Gewalt. Das bedeutet in diesem Kontext, dass der Angreifer beabsichtigt, ein Kennwort durch das Durchprobieren aller möglichen Zeichenkombinationen zu hacken. Diese Angriffe finden aber nicht, wie oft vermutet, an der Kennwort-Eingabemaske des Betriebssystems oder des Online-Dienstes statt. Stattdessen geht einem Brute Force-Angriff in der Regel das Erbeuten der Zugangsdaten (Benutzername und Hashwert des Kennwortes) voraus.

Der Angreifer berechnet in der Folge auf einem eigenen, lokalen System (unter Anwendung der öffentlich verfügbaren Algorithmen) für jede mögliche Zeichenkombination den entsprechenden Hashwert. Stimmt das Ergebnis eines solchen Versuches mit dem zuvor erbeuteten Hashwert überein, hat der Angreifer das Kennwort gehackt - die Zugangsdaten sind kompromittiert.

Die folgende Tabelle soll einen Überblick darüber geben, wie viele Möglichkeiten bei einem Brute Force-Angriff vom Angreifer in Abhängigkeit von der Länge und der Komplexität eines Kennworts maximal durchprobiert werden müssen, um zu einem erbeuteten Hashwert nach der oben beschriebenen Methode das Kennwort herauszufinden.

Tabelle 2 Anzahl möglicher Kennwortkombinationen

| Zeichenvorrat | 2 Stellen | 8 Stellen | 12 Stellen |
|---|---|---|---|
| **Nur Ziffern** (10 Zeichen) | 100 | 100 Millionen<br>100000000 | 1 Billion<br>1.000.000.000.000 |
| **Nur Kleinbuchstaben** (26 Zeichen) | 676 | ~ 208 Milliarden<br>208.827.064.576 | ~ 95 Billiarden<br>95.428.956.661.682.200 |
| + Großbuchstaben (52 Zeichen) | 2.704 | ~ 53 Billionen<br>53.459.728.531.456 | ~ 390 Trillionen<br>390.877.006.486.250.000.000 |
| + Ziffern (62 Zeichen) | 3.844 | ~ 218 Billionen<br>218.340.105.584.896 | ~ 3 Trilliarden<br>3.226.266.762.397.900.000.000 |
| + Sonderzeichen (95 Zeichen) | 9.025 | ~ 6,5 Billiarden<br>6.634.204.312.890.620 | ~ 540 Trilliarden<br>540.360.087.662.637.000.000.000 |

Diese Zahlen wirken auf den ersten Blick extrem hoch. Wie allerdings bereits ausgeführt, werden die Berechnungen zur Rückführung eines Hashwertes in ein Kennwort vom Angreifer auf einem eigenen, lokalen System durchgeführt. Je nach Rechnerhardware und verwendetem Algorithmus können dabei zwischen einigen Millionen Kennwörtern pro Sekunde (normaler PC) und zwei Billionen Kennwörtern pro Sekunde (derzeit laut Literatur höchste diesbezüglich bekannte Rechenkapazität) ausprobiert werden[7].

Geht man von einem leistungsfähigen, für Privatpersonen noch leistbaren Einzelsystem aus, kann man etwa drei Milliarden Versuche pro Sekunde ansetzen. Die oben angeführten Angaben zu Kennwortkombinationen könnten somit (grob vereinfacht) wie folgt in Zeitspannen umgerechnet werden. Die angebenen Zeitspannen geben an, wie lange ein Angreifer in der jeweils gegebenen Kombination von Länge und Komplexität eines Kennwortes maximal benötigen würde, um einen erbeuteten Hashwert in ein Kennwort rückzuführen.

[7] Diese Angaben (und die daraus abgeleiteten Zeitspannen) sind als reine Abschätzung zu verstehen, die in Abhängigkeit vom Algorithmus und etwaigen zusätzlichen Maßnahmen auf Seiten der potentiellen Opfer (z.B. Salting) oder Angreifer (z.B. vorangehende Wortlisten-Angriffe oder Verwendung von Rainbox-Tables) gravierend abweichen können.

Tabelle 3 Abschätzung der Rechenzeit zur Rückführung eines Hahswertes in ein Kennwort (Annahme: 3 Milliarden Versuche/Sekunde)

| Zeichenvorrat | 2 Stellen | 8 Stellen | 12 Stellen |
|---|---|---|---|
| **Nur Ziffern** (10 Zeichen) | 0 | 0 | ~ 17 Minuten |
| **Nur Kleinbuchstaben** (26 Zeichen) | 0 | ~ 70 Sekunden | ~ 3 Jahre |
| + Großbuchstaben (52 Zeichen) | 0 | ~ 5 Stunden | ~ 12.000 Jahre |
| + Ziffern (62 Zeichen) | 0 | ~20 Stunden | ~ 102.000 Jahre |
| + Sonderzeichen (95 Zeichen) | 0 | ~ 26 Tage | ~ 17.000.000 Jahre |

Geht man hingegen von der laut Literatur höchsten diesbezüglich bekannten Rechenkapazität aus, kann man etwa zwei Billionen Versuche pro Sekunde ansetzen. Dies reduziert die erforderlichen Zeitspannen massiv.

Tabelle 4 Abschätzung der Rechenzeit zur Rückführung eines Hashwertes in ein Kennwort (Annahme: 2 Billionen Versuche/Sekunde)

| Zeichenvorrat | 2 Stellen | 8 Stellen | 12 Stellen |
|---|---|---|---|
| **Nur Ziffern** (10 Zeichen) | 0 | 0 | ~ 1 Sekunde |
| **Nur Kleinbuchstaben** (26 Zeichen) | 0 | 0 | ~ 13 Stunden |
| + Großbuchstaben (52 Zeichen) | 0 | ~ 27 Sekunden | ~ 6 Jahre |
| + Ziffern (62 Zeichen) | 0 | ~ 2 Minuten | ~ 51 Jahre |
| + Sonderzeichen (95 Zeichen) | 0 | ~ 1 Stunde | ~ 8.600 Jahre |

Diese Überlegungen lassen zwei wesentliche Schlussfolgerungen zu:

- Die Möglichkeit eines Brute Force-Angriffs besteht unabhängig davon, ob ein System (an der Eingabemaske) nach einer bestimmten Anzahl von Fehlversuchen weitere Eingaben unterbindet.
- Die Länge und Komplexität eines Kennworts sind also in jedem Fall von wesentlicher Bedeutung.

## 6.3 Datenleaks

Mit erschreckender Regelmäßigkeit berichten Medien über erfolgreiche Angriffe auf die Kundendaten von großen Unternehmen. In vielen Fällen werden bei solchen Angriffen Millionen von Zugangsdaten (Benutzernamen und Hashwerte der Kennwörter) der Kunden des jeweiligen Unternehmens erbeutet. Es wurden aber auch Datendiebstähle bekannt, bei denen bis zu einer Milliarde Kundendatensätze betroffen waren.

In der Folge werden die erbeuteten Hashwerte unter Aufbietung hoher Rechenleistung mit Wortlisten- bzw. Brute Force-Angriffen auf die Kennwörter rückgeführt. Oftmals landen diese Zugangsdaten (einschließlich der rückgeführten Kennwörter) dann als Datenleak im Internet. Das Missbrauchspotential solcher Kennwortleaks ist enorm.

Die Website „Have I been pwned?“ (https://haveibeenpwned.com)[8] bietet die Möglichkeit an, die eigene E-Mail-Adresse dahingehend zu überprüfen, ob sie in einem bekannten Datenleak (oder einer im Internet kursierenden Liste) enthalten ist oder war. Ist die überprüfte E-Mail-Adresse Teil eines Datenleaks oder einer Liste, wird man entsprechend informiert. In diesem Fall muss das zugehörige Kennwort schnellstmöglich geändert werden.

[8] In diesem Dokument namentlich genannte Produkte und Dienste sind lediglich als Beispiele zu verstehen und stellen keine Empfehlung durch das Bundesministerium für Inneres (BMI) dar. Das BMI hat keinerlei direkte oder indirekte Verbindung zu den jeweiligen Herstellern bzw. Betreibern und kann daher keine Garantie für die Funktion und die Sicherheit des jeweiligen Produkts bzw. Dienstes übernehmen.

**Bundesministerium für Inneres**
Herrengasse 7, 1010 Wien
praevention@nis.gv.at | csc@dsn.gv.at
bmi.gv.at