

Einleitung:

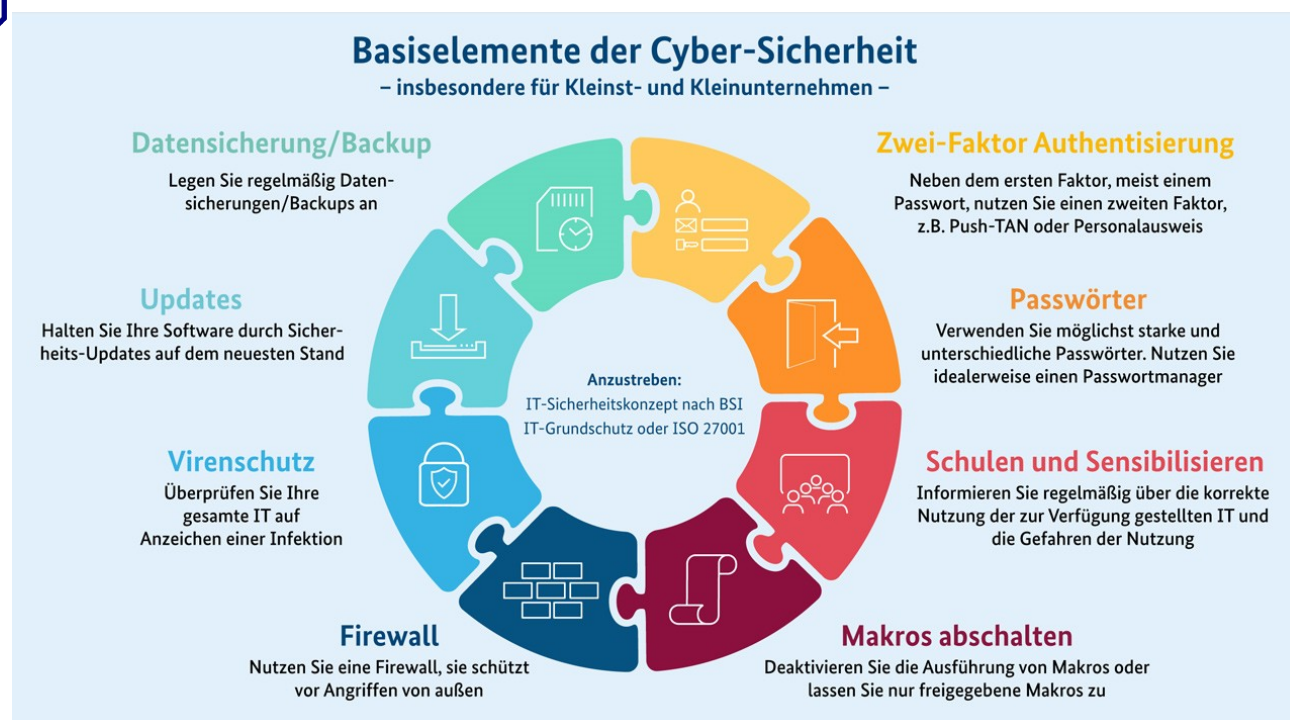
Das Bundesamt für die Sicherheit in der Informationstechnik stellt mit dem „IT-Grundschutz“ umfangreiche Maßnahmen zum Schutz der IT zur Verfügung, aber ... eben umfangreich. Für ein „Management – Summary“ gibt es von mir eine Zusammenfassung für Verantwortliche auf 6 Seiten¹. Als „leichtere Kost“ hier die Zusammenfassung aus den Informationsmails zum Einstieg in die Cybersicherheit vom BSI² für kleine und mittlere Unternehmen.

Inhaltsverzeichnis

| | | | |
|---------------------------------|---|--|---|
| Basiselemente (Infografik)..... | 1 | 4. Firewall..... | 3 |
| 1. Datensicherung/Backup..... | 1 | 5. „Makros“..... | 4 |
| 2. Updates..... | 2 | 6. Schulen & Sensibilisieren..... | 5 |
| 3. Virenschutz..... | 2 | 7. Passwörter & Zwei-Faktor-Authentisierung..... | 6 |



Basiselemente (Infografik)



Quelle: Bundesamt für Sicherheit in der Informationstechnik

1. Datensicherung/Backup

- Wann sind Sicherheitskopien die Rettung?

| | | |
|-----------------|---|--------------------------|
| 1. Bei Defekt | 3. Bei verschiedenen Schadprogrammen | 5. Bei Gerätediebstahl |
| 2. Bei Löschung | 4. Bei Gebäudeschäden / Naturkatastrophen | 6. bei Cloud – Problemen |
- Was soll gesichert werden?
 1. Das Betriebssystem, wenn die individuelle Konfiguration nicht verloren gehen soll
 2. Die Anwendungsprogramme, wenn die individuelle Konfiguration nicht verloren gehen soll
 3. Die Anwendungsdaten auf jeden Fall, denn diese sind sonst verloren, dafür gibt es keine Standard-Wiederherstellungsfunktion.
- Wie soll gesichert werden?

1 LINK: <https://volkerschroer.de/DSGVO/BSI.Basiswissen.IT-Grundschutz.pdf>

2 Quelle: BSI: „Leichter Einstieg“

- ▶ Volldatensicherung *Für jede Sicherung werden sämtliche Daten gesichert
(+) Alles gesichert (-) Könnte viel Platz und Zeit brauchen*
- ▶ Inkrementelle Datensicherung *Nach einer Volldatensicherung werden mit jeder weiteren Sicherung nur die Veränderungen zu vorgehenden Sicherung gespeichert. (+) Spart Kapazitäten und Zeit (-) Rücksicherung nur mit allen Teilsicherungen*
- ▶ Differentielle Datensicherung *Nach einer Volldatensicherung werden bei jeder Sicherung alle Änderung zur Ursprungssicherung gespeichert. (+) Die Wiederherstellung ist unkomplizierter (-) Braucht mehr Kapazitäten und Zeit als die Inkrementelle Sicherung.*
- Durchführung *Mit Windows kann über die Systemsteuerung > Alle Systemsteuerungselemente > Wiederherstellung eine Sicherung konfiguriert werden, oder man nutzt eine Software (Vereinfachung bei Netzwerken mit Client und Servern), mit der eine Wiederherstellung auch notfalls auf einer anderen Hardware vorgenommen werden kann. In jedem Fall auf einem externen Medium oder in der Cloud. Dann allerdings verschlüsselt vor Übertragung (Beispielhaft eine Übersicht im Testvergleich³)*

2. Updates

Updates dienen zwar auch dazu, einer Software neue Funktionen hinzuzufügen, ohne diese neu installieren bzw. aufsetzen zu müssen. Viel wichtiger sind aber die Sicherheitsupdates, mit denen Schwachstellen im System geschlossen werden, die sonst Hacker für Angriffe nutzen. Checkliste:

- Liste der Programme, die eine Auto-Update-Funktion anbieten und eingeschaltet sind.
- Liste der Programme, die manuell aktualisiert werden müssen.
- Updates immer sofort installieren (!!!)
- „Vertrauen ist gut, Kontrolle ist besser“, informiert bleiben. Der BSI stellt verschiedene Newsletter zur Verfügung u. a. zu BCM (Betriebl. Kontinuitätsmanagement), Cloud-Computing, IT-Grundschutz, KMU und Verbraucherschutz⁴.

3. Virenschutz

Dass ein Schutzprogramm / Virenschanner unverzichtbar ist, zeigen die aktuellen bis täglichen Warnung und die Vielzahl der wichtigen „Systemupdates“ zum Schutz vor bekannten Schadprogrammen.

i. Gratis oder kostenpflichtig

Wie immer, ist es eine Frage der Anforderungen. Wie aktuelle Testbewertungen zeigen, kann eine Gratis - Version für einen Einzelplatzrechner oder Mobilgerät ausreichend sein. Ein Blick auf die Auswertungen des unabhängigen, Magdeburger AV - Test Instituts⁵ kann bei der Entscheidung hilfreich sein. Geht es an Mehrplatzrechner oder Client – Server – Strukturen mit Fernzugriff, vielleicht noch über Drittgeräte, sollte ein Spezialist mit entsprechendem Support hinzugezogen werden. Hilfestellung zum Einstieg gibt es auch vom BSI unter: „[Wie Sie Ihren Computer sicher einrichten](#)“.

ii. Online - Virenschanner

Es erscheint zunächst leichter, da keine Installation erforderlich und immer die aktuellste Prüfroutine genutzt wird. Allerdings fehlt der Wächter im Hintergrund, der jede aufgerufene Datei auf Signaturen prüft, er steht Offline nicht zur Verfügung, erfordert die Ausführung aktiver Inhalte (ActiveX) und muss möglicherweise über eine infizierte Onlineverbindung genutzt werden. Nützlich kann ein Onlinescanner helfen, wenn auf einem ungeschützten Rechner eine Infizierung vermutet wird oder für Einzelprüfungen, wie bei VirusTotal (Zusammenschluss von 70 Anbietern)⁶.

3 Link: PC-Welt: „[Die beste Backup-Software für Windows im Test \(2023\)](#)“

4 Link: BSI-Newsletter: „[BCM, Cloud-Computing, IT-Grundschutz, KMU, Verbraucherschutz](#)“

5 Quelle: AV Test GmbH: „[Testübersichten](#)“, für „[Privatanwender](#)“, für „[Unternehmen](#)“

6 LINK: [VIRUSTOTAL](#)



iii. Empfehlung(en)?

Ein Virens Scanner muss tief in die Systemarchitektur eingreifen können und sollte langfristig eingesetzt werden. Deshalb sind strenge Kriterien anzulegen und neben der Software sollte auch der Anbieter kritisch unter die Lupe genommen werden.



4. Firewall

Abgeleitet von der Brandschutzwand oder -tür, blockiert bzw. schützt es das Netzwerk (meist eine Kombination aus Hard- und Software) und/oder den einzelnen Rechner (Personal Firewall) vor allen Zugriffen von außen, wie vor anderen Geräten und Netzwerken (u. a. dem Internet). Die Firewall erkennt nicht, ob der Zugriff harmlos oder feindlich ist. Sie erlaubt oder verbietet den Datenverkehr mit der anderen Stelle. Deshalb ist die Kombination mit einem zuverlässigen Antivirenprogramm wichtig, dass installierte Anwendungen, wie dynamische Webseiteninhalte auf Gefahren prüft (Security Pakete).



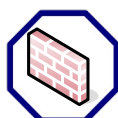
i. Software Firewall

Für einen ersten Eindruck der Funktionsweise rufen Sie z. B. in Windows die Einstellungen zur Firewall auf. In Windows über die Suche (🔍) und Eingabe „Firewall“ mit der Auswahl „Windows Defender ...“ In der folgenden Übersicht erscheinen 3 Kategorien mit unterschiedlichem Sicherheitsniveau.

- ▶ „Domänenprofil“, für Netzwerke mit Kontoauthentifizierung.
 - ▶ „Privates Profil“, für Heimnetzwerke u. ä.
 - ▶ „Öffentliches Profil“, für öffentliche Netzwerke wie Hotspots in Cafés, Hotel, Geschäften u.s.w.
- In den empfohlenen Einstellungen sollte:

- ✔ Die Firewall aktiviert sein
- ✗ Eingehende Verbindungen ohne Regel werden blockiert
- ✔ Ausgehenden Verbindungen ohne Regel werden zugelassen.

➔ Über Firewall Eigenschaften werden die Einstellung dazu angezeigt. Hinweis: In den Einstellungen sollte „Benachrichtigungen anzeigen“ auf „Ja“ eingestellt sein. Wenn die Firewall eingehende, wie auch ausgehende Verbindungen je nach Einstellung blockiert, wird eine Nachricht angezeigt und je Einzelfall kann mit Rechten als Administrator eine Freigaberegeln für vertrauensvolle Verbindungen erstellt werden.



ii. Hardware Firewall

Die Bezeichnung ist nicht ganz korrekt, ohne Software funktioniert keine Firewall, diese Bezeichnung besagt lediglich, dass die Firewall (Software) unabhängig vom Client / Server auf einem externen Gerät (z. B. Router) läuft und den gesamten Datenverkehr kontrolliert. So liegen z. B. die Zugangsdaten für die Netzwerke separat auf dem externen Gerät. Die Funktionen sind⁷:

- **Paketfilter:** Prüft die Header – Informationen und lässt das Paket durch, oder eben nicht.
- **Stateful – Packet – Inspection:** Eine dynamische Filtertechnik, bei der jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird.
- **Proxyfilter:** Als „Stellvertreter“ wird neben Adress- und Protokolldaten auch der Datenverkehr auf Anwendungsebene analysiert. Ergänzt um einen „Contentfilter“ können auch unerwünschte Inhalte aus Webseiten (z. B. ActiveX, JavaScript u.ä.) einschließlich ganzer Webseiten herausgefiltert werden.
- **Deep Packet Inspection:** Hier werden nicht nur Ursprung und Ziel (Header), sondern auch der Inhalt analysiert, wodurch sich intelligentere Regeln aufstellen lassen. Um verschlüsselte Pakete analysieren zu können, ist zusätzlich eine SSL-/TLS-Termination erforderlich, die das Paket anhält, entschlüsselt und nach Analyse wieder eine verschlüsselte Verbindung zur Zieladresse aufbaut.

⁷ Quelle: Wikipedia: „Firewall“



iii. Und jetzt?

Eine Empfehlung kann ich natürlich nicht aussprechen, da dies von der jeweiligen Konstellation abhängig ist. Einen IT – Spezialisten um Rat fragen, kann sicher nicht schaden. Hilfreich ist ggf.:

- **Anleitung:** „Bewährte Methoden zum Konfigurieren von Windows Defender Firewall“ Microsoft.⁸
- **Zur einfachen Konfiguration** der Personal Firewall mit einer gut verständlichen und deutschsprachigen Oberfläche empfiehlt chip.de, z. B. die „Free Firewall“⁹ der IT-Beratung Steinmiller aus Kraichtal.
- **Vergleich Security Pakete:** Firewall Vergleich 2023 mit Erläuterungen auf vergleich.org¹⁰
- **BSI:** Basis zur IT-Sicherheit: „Firewall“ und der Baustein NET.3.2: Firewall (Edition 2021)



5. „Makros“

Makros können ein Segen sein, um sich wiederholende, regelmäßige Vorgänge mit einem Klick (Makro) auszuführen. Leider können solche Makros auch ein Fluch sein, denn es lassen sich auch ganze Programme darin „verstecken“. Wie dem ESET Threat Report H1 2023¹¹ zu entnehmen, gehörten Office-Makros über viele Jahre zu den größten Cyberbedrohungen global. Mittlerweile hat Microsoft in den Standardeinstellungen Makros deaktiviert. Neben den selbst erstellen Makros besteht die Gefahr, schädliche Makros von Dritten über E-Mail und Dateianhängen, Download, Erweiterungen (Addons), Programminstallation u. ä. zu erhalten. Makros können auch in anderen Dateien (z.B. PDF) versteckt sein. Wie immer ist die Konfiguration ein Kompromiss aus Sicherheit versus Komfort und Funktionalität.



i. Sicherheitseinstellungen einordnen



Sehr hoch

Nur Makros aus vertrauenswürdigen Dateiquellen werden ausgeführt. Alle anderen Makros werden deaktiviert, unabhängig von einer Signatur.



Hoch

Nur signierte Makros aus vertrauenswürdigen Quellen werden ausgeführt. Nicht signierte Makros werden deaktiviert.



Mittel

Bestätigung vor dem Ausführen von Makros aus nicht vertrauenswürdigen Quellen.



Niedrig

Alle Makros ausführen ist nicht empfehlenswert, nur wenn sichergestellt ist, dass nur sichere Dokumente geöffnet werden können.



ii. Und jetzt?

Gute und vertrauenswürdige Programmanbieter haben die Ausführung von Makros bereits in den Voreinstellungen deaktiviert und geben einen Warnhinweis vor Aktivierung aus. Ein Blick in Office und Kommunikationsanwendungen ist sicher hilfreich und beruhigend (meist unter „Trust Center, Sicherheit und Datenschutz u. ä.).

Für mittelgroße und große Organisationen, die Endsysteme mit Gruppenrichtlinien in einer Active – Directory - Umgebung verwalten, gibt die BSI Empfehlungen mit Schwerpunkt auf Microsoft Office Anwendungen¹². Die zur Weitergabe an den IT – Service (bzw. Dienstleister) sehr zu empfehlen sind.



6. Schulen & Sensibilisieren

Ein wichtiger Sicherheitsfaktor zur Abwehr von Cyberangriffen ist der Mensch (*und nicht das Problem, um es mal deutlich zu sagen, denn nur Mensch kann noch verhindern, was die IT-*

⁸ Quelle: Microsoft / Learn / Sicherheit: „[Bewährte Methoden zum Konfigurieren von Windows Defender Firewall](#)“

⁹ Quelle: Chip.de: „[Free Firewall](#)“

¹⁰ Quelle: Vergleich.org: „[Firewall Vergleich 2023](#)“

¹¹ Quelle: eset: „[Threat Report H1 2023 December 2022 – May 2023 \(PDF\)](#)“

¹² Quelle: BSI: „[Empfehlungen: IT in Unternehmen, Sichere Konfiguration von MS Office...](#)“

Sicherheit nicht kann.). Damit er diese Anforderung meistern kann, sollte der Mensch regelmäßig sensibilisiert und geschult werden.



i. Information & Unterstützung durch:

- ✓ Verständliche Information über die technischen Sicherheitsvorkehrungen, deren Schutzwirkung und vor allem über deren Grenzen!
- ✓ Vermittlung eines guten Gefühls bei verdächtigen Aktivitäten (z. B. E-Mail) lieber eine Anfrage zu viel den IT-Verantwortlichen vorzustellen, als genau die „EINE“ zu wenig.
- ✓ Einfache Tipps, wie z.B. den 3-Sekunden-Sicherheits-Check¹³ des BSI zu E-Mails (1. Kenne ich den Absender? 2. Ist der Betreff sinnvoll? 3. Erwarte ich den Anhang?) PLUS: 4.) Fehler im Text und sichtbare Links weichen von echtem Link ab (z.B. „google.com“ zu „goooogle.com“).
- ✓ Wenige Grundregeln in der E-Mail Kommunikation erhöhen nicht nur die Effizienz, sondern auch die Sicherheit zur Erkennung korrekter E-Mails. Zum Beispiel die Vermeidung unnötiger „Empfänger in „cc & bcc“, ein kurzer Betreff beginnend mit dem Grund (INFO: AUFGABE: ANTWORT: EILT: ERLEDIGT:) „|“ Termin(e) „|“ mit Stichwort zum Thema und bei jeder E-Mail vom Absender im 1. Absatz eine kurze Zusammenfassung der Erwartung an den / die Empfänger zur Mail.

✓ ...



ii. Informationen zu Angriffsflächen


- ✓ Um eine möglichst realitätsnahe Nachricht zu erstellen, sammeln Betrüger Informationen in sozialen Netzwerken und auf Plattformen. Deshalb ist mit persönlichen und geschäftlichen Informationen dort sehr verantwortungsvoll umzugehen. Keine Veröffentlichung von vertraulichen Informationen in sozialen – Netzwerken und überhaupt in der Kommunikation mit Dritten über den Arbeitgeber, die Organisation und die Arbeit.
- ✓ Zugangsdaten, Passwörter oder Kontoinformation niemals per Mail, Telefon oder Konferenzsystemen weitergeben, da die Gefahr des Mitlesens oder Mithörens besteht.
- ✓ Betrüger nutzen auch gerne Fernwartungssoftware (Remote – Services), um sich auf den eigenen Rechner aufzuschalten und durch Ablenkung Schadsoftware aufspielen zu können. Der 3-Punkte-Check vor Einsatz von Fernwartungssoftware 1.) Ist der Anbieter bekannt? 2.) Besteht eine Vereinbarung mit dem Serviceanbieter? 3.) Ist die Rechtmäßigkeit einer Ankündigung auf unabhängigem Kommunikationsweg bestätigt?
- ✓ „Wie Hacker Ihre Psyche entschlüsseln ... und wie Sie sich davor schützen können. Psychotricks und Phishing-Maschen“ ein DIN A3 Poster der Allianz-für-Cybersicherheit¹⁴ zeigt kurz und übersichtlich die Tricks und Maschen der Kriminellen. Ein Aushang kann die Aufmerksamkeit hochhalten.

✓ ...



iii. „Outdoor – Office“

Auch wenn hinlänglich beschrieben, geschrieben, gesagt und gezeigt, fällt mir beim Reisen doch immer wieder auf, dass ein Minimum an Grundregeln nicht beachtet wird.

- SPERREN: Geräte sollten zwar nie unbeaufsichtigt sein, aber sobald man es „aus der Hand“ legt ist die Sperre (Passwort oder biometrische Sperren u. ä.) auf Smartphone, Laptop umgehend zu aktivieren (z. B. +L).
- NETZ: Öffentliche WLAN – Netze sind immer ein Risiko für und mit sensiblen Daten. „Wenn es denn sein muss, nie ohne VPN (Virtual Privat Network; verschlüsselte Verbindung zwischen zwei Beteiligten). Im Zweifel lieber auf das Mobilfunknetz setzen, z. B. über die einen WLAN - Hotspot vom Smartphone mit VPN. Anleitung zur Ersteinrichtung von chip.de¹⁵


¹³ Quelle: BSI „Spam-Phishing & Co. So erkennen Sie gefälschte und schadhafte E-Mails“

¹⁴ Quelle. Allianz-für-Cybersicherheit: „Awareness-Poster „Psychotricks und Phishing-Maschen“

¹⁵ Link: chip.de: „Anleitung für die Ersteinrichtung im Praxistipp > Android von chip.de.“


- **VERSCHLÜSSELN:** Damit im „Fall der Fälle“ kein unerlaubter Zugriff auf Rechner oder Smartphone erfolgt, ist eine Verschlüsselung angebracht, die meistens schon „an Board“ ist, mit BitLocker bei Windows, FileVault bei Mac-OS. Die Smartphones, iPhones wie Android ab Version 10 sind standardmäßig verschlüsselt.
- **DISKRETION:** „Mithören“ und „Mitsehen“ lässt sich in öffentlichen Räumen auch für Dritte meist schlecht vermeiden. Deshalb keine Telefonate oder Videokonferenzen zu vertraulichen Themen und Nennung von Namen / Daten / Fakten. Hilfreich ist auch eine Blickschutzfolie zur Vermeidung neugieriger Blicke.
- **NIE KIOSK-PCs:** ... an Flughäfen oder in Hotels, wie unbekannte Hardware Dritter für Dienste mit sensiblen Inhalten und Zugangsdaten nutzen (z. B. Online-Banking). PS: Öffentliche Ladestationen über USB statt Netzstecker sind beliebte Angriffspunkte für Hacker.

7. Passwörter¹⁶

 Mit den Passwörtern ist es so eine Sache, am besten ein einfaches Passwort für alles, dann ist es aber auch einfach zu knacken und eröffnet den Kriminellen schnell „Tür und Tor“. Ein komplexes Passwort (Zeichenarten mit: „a“, „A“, „1“, „\$“ + „ä“) und für jedes Konto ein anderes, kann sich keiner mehr merken. Und dann gibt es ja noch die Konten, die in regelmäßigen Abständen ein neues Passwort erbitten. Passwort-Manager können da Abhilfe schaffen, aber sind eben auch Anwendungen, die für eine komfortable Nutzung über eine Cloud synchronisiert werden. Die Empfehlungen des BSI:

- ✓ Im Standard eingestellte Passwörter umgehend ändern.
- ✓ Für jedes Konto ein anderes Passwort
- ✓ Entweder ein kurzes, komplexes Passwort aus mindestens 8 Zeichen und vier Zeichenarten, oder ein langes Passwort mit mindestens 25 Zeichen, z. B. als ganzer Satz. Man sollte es sich gut merken können.
- ✓ Passwörter NIE an Dritte weitergeben, bzw. einsehen lassen.
- ✓ Passwortwechsel, sobald ein unsicheres Gefühl aufkommt.
- ✓ Nutzung eines Passwortmanagers, „dem man vertraut“.

8. Zwei-Faktor Authentisierung¹⁷

 „2FA“ oder Zwei – Faktor Authentisierung kombiniert zwei unterschiedliche Zugangskanäle zur Authentisierung oder Login. Faktor 1: ist meist der klassische Zugang mit Benutzer und (starkem) Passwort. Faktor 2: ist dann z. B. eine Transaktionsnummer per SMS oder E-Mail an eine zuvor hinterlegte Mobilfunknummer bzw. Mail-Adresse. Alternativ bietet sich auch eine „Authenticator-App“ an, wie z. B. von Microsoft, Google, Apple oder eine herstellernunabhängige, wie von Sophos mit Intcept X, über ein zuvor ausgetauschtes Schlüsselpaar.

Bei Bedarf, einfach einmal sprechen!



Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtigkeit und Vollständigkeit übernehmen kann. Aus Gründen der besseren Lesbarkeit Verwendung der männlichen Form, die alle Geschlechter mit einbezieht.

¹⁶ Quelle: BSI – DINA4 Merkblatt: „BSI - Basisschutz: Sichere Passwörter (PDF)“

¹⁷ Quelle: BSI: „Zwei-Faktor-Authentisierung. Mehr Sicherheit für Online-Konten und vernetzte Geräte“