

IT-Sicherheit

- [6.1 Warum IT-Sicherheit wichtig ist](#)
- [6.2 Viren, Trojaner und Ransomware](#)
- [6.3 Firewall](#)
- [6.4 Virenschutz und Endpunktschutz](#)
- [6.5 Sichere Passwörter](#)
- [6.6 Passwortmanager](#)
- [6.7 Mehr-Faktor-Authentifizierung](#)
- [6.8 Phishing](#)
- [6.9 Links und Anhänge prüfen](#)
- [6.10 Updates](#)
- [6.11 Backups](#)
- [6.12 Benutzerrechte](#)
- [6.13 Verschlüsselung](#)

6.1 Warum IT-Sicherheit wichtig ist

Computer enthalten wertvolle Daten und Zugänge. IT-Sicherheit soll verhindern, dass Informationen gestohlen, verändert, gelöscht oder unerlaubt genutzt werden. Dabei geht es nicht nur um Technik, sondern auch um Verhalten und klare Regeln.

Vergleich aus dem Alltag

Eine Firma schützt nicht nur ihre Eingangstür, sondern auch Schlüssel, Akten und Zugangsberechtigungen.

Beispiel

Ein gestohlenes Passwort kann ausreichen, um auf E-Mails oder Cloud-Daten zuzugreifen.

“ **Merke:** Sicherheit besteht aus Technik, Organisation und aufmerksamem Verhalten.

6.2 Viren, Trojaner und Ransomware

Schadprogramme gibt es in unterschiedlichen Formen. Ein Virus hängt sich an andere Dateien oder Programme, ein Trojaner tarnt sich als etwas Nützliches und Ransomware verschlüsselt häufig Daten, um Geld zu erpressen. Die Begriffe werden im Alltag oft ungenau verwendet.

Vergleich aus dem Alltag

Ein Trojaner ist wie ein Paket, das harmlos aussieht, aber etwas Gefährliches enthält.

Beispiel

Eine gefälschte Software kann im Hintergrund Zugangsdaten stehlen.

“ **Merke:** Der Oberbegriff für schädliche Software ist Malware.

6.3 Firewall

Eine Firewall kontrolliert Netzwerkverbindungen anhand von Regeln. Sie kann Verbindungen erlauben oder blockieren und dadurch Systeme voneinander abschirmen. Firewalls gibt es auf einzelnen Computern und als zentrale Netzwerkgeräte.

Vergleich aus dem Alltag

Eine Firewall ist wie ein Pförtner: Sie prüft, wer hinein oder hinaus darf.

Beispiel

Ein Server kann so konfiguriert sein, dass nur bestimmte Netzwerkdienste von außen erreichbar sind.

Firewall = Pförtner am Eingang



“ **Merke:** Eine Firewall ist ein wichtiger Schutz, ersetzt aber keine Updates und sicheren Konten.

6.4 Virenschutz und Endpunktschutz

Sicherheitssoftware kann bekannte und verdächtige Programme erkennen, blockieren oder untersuchen. Moderne Systeme verwenden neben klassischen Virensignaturen auch Verhaltensanalyse und weitere Schutzmechanismen. Trotzdem kann kein Programm jede Gefahr sicher erkennen.

Vergleich aus dem Alltag

Ein Virens Scanner ist wie eine Sicherheitskontrolle – hilfreich, aber nicht unfehlbar.

Beispiel

Eine verdächtige Datei kann beim Öffnen blockiert und in Quarantäne verschoben werden.

“ **Merke:** Virenschutz ist nur eine Schutzschicht von mehreren.

6.5 Sichere Passwörter

Ein gutes Passwort sollte lang, einzigartig und nicht leicht zu erraten sein. Für verschiedene wichtige Konten sollte nicht dasselbe Passwort verwendet werden. Lange Passphrasen sind oft leichter zu merken als kurze komplizierte Zeichenfolgen.

Vergleich aus dem Alltag

Ein Passwort ist wie ein Schlüssel. Wenn derselbe Schlüssel jede Tür öffnet, wird ein Verlust besonders gefährlich.

Beispiel

Ein langes einzigartiges Passwort für das E-Mail-Konto verhindert, dass ein bekannt gewordenes Shop-Passwort sofort auch dort funktioniert.

“ **Merke:** Wichtiger als möglichst viele Sonderzeichen ist vor allem: lang und für jedes Konto einzigartig.

6.6 Passwortmanager

Ein Passwortmanager speichert Zugangsdaten verschlüsselt und kann für jedes Konto ein langes, zufälliges Passwort erzeugen. Du musst dir dann hauptsächlich das starke Hauptpasswort merken und den Passwortmanager gut schützen.

Vergleich aus dem Alltag

Das ist wie ein sicherer Schlüsseltresor: Viele Schlüssel liegen geschützt an einer Stelle.

Beispiel

Der Passwortmanager erzeugt für jede Webseite ein anderes Passwort und füllt es beim Anmelden aus.

“ **Merke:** Ein Passwortmanager erleichtert einzigartige Passwörter für viele Konten.

6.7 Mehr-Faktor-Authentifizierung

Bei **MFA** reicht ein Passwort allein nicht. Zusätzlich wird ein zweiter unabhängiger Nachweis verlangt, zum Beispiel eine Bestätigung auf einem Gerät oder ein Sicherheitsschlüssel. Dadurch ist ein gestohlenes Passwort allein oft nicht genug.

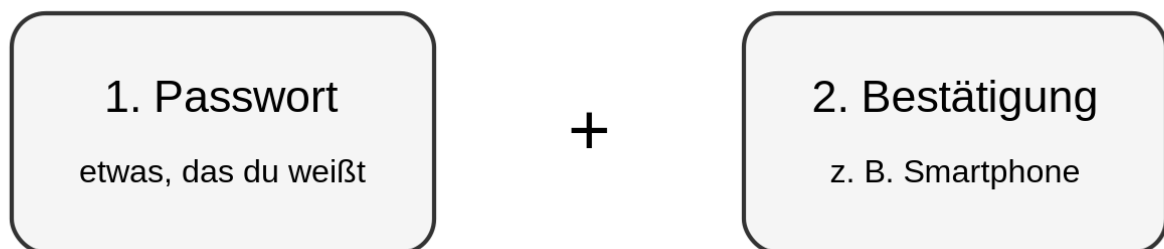
Vergleich aus dem Alltag

Es ist wie eine Tür mit Schlüssel und zusätzlichem Ausweis.

Beispiel

Nach Eingabe des Passworts musst du die Anmeldung auf deinem Smartphone bestätigen.

Mehr-Faktor-Anmeldung



Zwei unabhängige Nachweise sind sicherer als nur einer.

“ **Merke:** MFA schützt Konten deutlich besser als ein Passwort allein.

6.8 Phishing

Beim Phishing versuchen Angreifer, Menschen zu täuschen. Gefälschte E-Mails, Webseiten oder Nachrichten sollen dazu bringen, Passwörter einzugeben, Dateien zu öffnen oder Geld zu überweisen. Häufig wird Zeitdruck erzeugt.

Vergleich aus dem Alltag

Phishing ist digitaler Trickbetrug: Der Angreifer versucht nicht zuerst den Computer, sondern den Menschen zu überlisten.

Beispiel

Eine Nachricht behauptet, dein Konto werde in 30 Minuten gesperrt und fordert dich auf, sofort einen Link anzuklicken.

“ **Merke:** Zeitdruck, ungewöhnliche Absender und überraschende Anfragen sind Warnzeichen.

6.9 Links und Anhänge prüfen

Links und Dateianhänge können gefährlich sein. Vor dem Öffnen sollte geprüft werden, ob die Nachricht erwartet wurde, ob Absender und Ziel plausibel sind und ob die Datei wirklich benötigt wird. Bei Unsicherheit lieber über einen bekannten Kontaktweg nachfragen.

Vergleich aus dem Alltag

Ein unbekannter Anhang ist wie ein Paket ohne erwarteten Absender: Erst prüfen, dann öffnen.

Beispiel

Eine angebliche Rechnung kommt überraschend von einer fremden Adresse und enthält eine ausführbare Datei – das ist verdächtig.

“ **Merke:** Nicht aus Neugier klicken. Erst prüfen, dann handeln.

6.10 Updates

Sicherheitslücken sind Fehler oder Schwächen in Software. Hersteller schließen viele davon mit Updates. Deshalb sollten Betriebssysteme, Browser, Programme und Geräte regelmäßig aktualisiert werden.

Vergleich aus dem Alltag

Ein Update ist wie das Reparieren eines kaputten Fensters, bevor jemand hindurchklettert.

Beispiel

Ein Browser erhält ein Sicherheitsupdate, das eine bekannte Angriffsmöglichkeit schließt.

“ **Merke:** Updates gehören zu den wichtigsten Grundlagen der IT-Sicherheit.

6.11 Backups

Ein **Backup** ist eine zusätzliche Kopie wichtiger Daten. Es hilft bei defekten Datenträgern, versehentlichem Löschen, Diebstahl oder Schadsoftware. Ein gutes Backup liegt nicht nur auf demselben Gerät wie die Originaldaten und muss im Ernstfall wiederherstellbar sein.

Vergleich aus dem Alltag

Ein Backup ist wie eine Ersatzkopie eines wichtigen Dokuments, die an einem anderen sicheren Ort liegt.

Beispiel

Wenn eine SSD ausfällt, können Dateien aus einer getrennten Sicherung wiederhergestellt werden.

Backup = Sicherheitskopie



Geht das Original verloren, kann die Kopie helfen.

“ **Merke:** Eine Kopie ist erst dann wirklich nützlich, wenn die Wiederherstellung funktioniert.

6.12 Benutzerrechte

Benutzer sollten nur die Rechte besitzen, die sie für ihre Aufgaben benötigen. Dieses Prinzip nennt man **Least Privilege** oder minimale Rechte. Dadurch kann ein Fehler oder ein kompromittiertes Konto weniger Schaden anrichten.

Vergleich aus dem Alltag

Nicht jeder Mitarbeiter eines Gebäudes braucht einen Generalschlüssel für alle Räume.

Beispiel

Ein normaler Benutzer kann Programme verwenden, aber keine sicherheitskritischen Systemeinstellungen ändern.

“ **Merke:** So viele Rechte wie nötig, aber so wenige wie möglich.

6.13 Verschlüsselung

Verschlüsselung verwandelt lesbare Daten mit einem mathematischen Verfahren in eine Form, die ohne passenden Schlüssel nicht verständlich ist. Sie schützt zum Beispiel Daten auf Geräten und Verbindungen im Internet.

Vergleich aus dem Alltag

Verschlüsselung ist wie ein Tresor: Die Daten sind vorhanden, aber ohne Schlüssel nicht sinnvoll lesbar.

Beispiel

HTTPS verschlüsselt die Verbindung zwischen Browser und Webseite.

“ **Merke:** Verschlüsselung schützt Daten, wenn Schlüssel und Zugangsdaten ebenfalls geschützt werden.