

Sicher arbeiten bei Schlichter

Praxisnahe IT-Sicherheits- und Awareness-Inhalte für Mitarbeitende.

- [Warum IT-Sicherheit jeden betrifft](#)
 - [1.1 IT-Sicherheit ist keine reine IT-Aufgabe](#)
 - [1.2 Was eigentlich geschützt wird](#)
 - [1.3 Vertraulichkeit, Integrität und Verfügbarkeit](#)
- [Passwörter und Benutzerkonten](#)
 - [2.1 Warum Passwörter wichtig sind](#)
 - [2.2 Ein gutes Passwort](#)
 - [2.3 Passwortmanager](#)
 - [2.4 Passwörter niemals weitergeben](#)
 - [2.5 Was tun bei Verdacht auf ein gestohlenes Passwort?](#)
- [MFA – die zweite Schutzschicht](#)
 - [3.1 Was ist MFA?](#)
 - [3.2 Nur eigene Anmeldungen bestätigen](#)
 - [3.3 MFA-Müdigkeit](#)
- [Phishing und Social Engineering](#)
 - [4.1 Was ist Phishing?](#)
 - [4.2 Typische Warnzeichen](#)
 - [4.3 Gefälschte Absender](#)
 - [4.4 Zeitdruck und Autorität](#)
 - [4.5 QR-Code-Phishing](#)

- [E-Mail, Links und Anhänge](#)
 - [5.1 Links prüfen](#)
 - [5.2 Dateianhänge](#)
 - [5.3 Makros und ausführbare Dateien](#)
 - [5.4 Geschäftliche Daten an den richtigen Empfänger](#)
- [Sicherer Arbeitsplatz](#)
 - [6.1 Bildschirm sperren](#)
 - [6.2 Vertrauliche Informationen am Bildschirm](#)
 - [6.3 Clean Desk und Ausdrücke](#)
 - [6.4 Fremde Personen](#)
- [USB, Geräte und mobile Arbeit](#)
 - [7.1 Unbekannte USB-Sticks](#)
 - [7.2 Private Geräte](#)
 - [7.3 Notebook unterwegs](#)
 - [7.4 Öffentliches WLAN](#)
 - [7.5 VPN](#)
- [Daten und Datenschutz im Alltag](#)
 - [8.1 Nur notwendige Daten verwenden](#)
 - [8.2 Dateien nicht über beliebige Dienste versenden](#)
 - [8.3 Falscher Empfänger](#)
 - [8.4 Screenshots und Fotos](#)
- [Updates und Software](#)
 - [9.1 Warum Updates notwendig sind](#)
 - [9.2 Warum ein Neustart nötig sein kann](#)
 - [9.3 Software nicht selbst aus unbekannten Quellen installieren](#)
- [Sicherheitsvorfälle richtig melden](#)
 - [10.1 Was ist ein Sicherheitsvorfall?](#)
 - [10.2 Was tun nach einem falschen Klick?](#)
 - [10.3 Was tun nach Eingabe eines Passworts?](#)

- [10.4 Verlust eines Geräts](#)
- [10.5 Welche Informationen die IT braucht](#)
- [Kurze Alltagssituationen – Was würdest du tun?](#)
 - [11.1 Der Chef braucht dringend Gutscheinkarten](#)
 - [11.2 Microsoft fordert eine sofortige Anmeldung](#)
 - [11.3 Ein Lieferant schickt plötzlich neue Bankdaten](#)
 - [11.4 Ein Kollege braucht kurz dein Passwort](#)
 - [11.5 Du findest einen USB-Stick](#)

Warum IT-Sicherheit jeden betrifft

1.1 IT-Sicherheit ist keine reine IT-Aufgabe

Technische Schutzsysteme können viel abfangen, aber sie können nicht jede Entscheidung eines Menschen übernehmen. Deshalb gehört sicheres Verhalten genauso zur IT-Sicherheit wie Firewall, Updates oder Virenschutz.

Vergleich aus dem Alltag

Eine Alarmanlage hilft nur begrenzt, wenn jemand einem Fremden freiwillig die Tür öffnet.

Beispiel aus dem Arbeitsalltag

Eine täuschend echte E-Mail fordert zur Anmeldung auf. Die Technik kann verdächtige Merkmale erkennen, aber der Empfänger muss trotzdem aufmerksam bleiben.

“ **Merke:** IT-Sicherheit ist Teamarbeit: Technik schützt – Menschen entscheiden.

1.2 Was eigentlich geschützt wird

Geschützt werden nicht nur Computer. Wichtig sind vor allem Daten, Benutzerkonten, Kommunikation, Geschäftsprozesse und die Verfügbarkeit unserer Systeme.

Vergleich aus dem Alltag

Bei einem Büro schützt man nicht den Aktenschrank wegen des Schrankes, sondern wegen der Unterlagen darin.

Beispiel aus dem Arbeitsalltag

Ein gestohlenes E-Mail-Konto kann für Betrug, Datenzugriff oder weitere Angriffe genutzt werden.

“ **Merke:** Das wertvollste Ziel ist häufig die Information oder der Zugang – nicht das Gerät selbst.

1.3 Vertraulichkeit, Integrität und Verfügbarkeit

IT-Sicherheit lässt sich mit drei einfachen Zielen erklären: Informationen sollen nur von Berechtigten gelesen werden, sie sollen nicht unbemerkt verändert werden und sie sollen verfügbar sein, wenn sie gebraucht werden.

Vergleich aus dem Alltag

Ein Vertrag soll nicht von Fremden gelesen, nicht heimlich verändert und bei Bedarf wiedergefunden werden können.

Beispiel aus dem Arbeitsalltag

Eine Kundendatei muss vor unberechtigttem Zugriff geschützt sein, korrekt bleiben und für berechnigte Mitarbeiter erreichbar sein.

“ **Merke:** Vertraulich, unverändert und verfügbar – diese drei Ziele gehören zusammen.

Passwörter und Benutzerkonten

2.1 Warum Passwörter wichtig sind

Ein Passwort schützt den Zugang zu einem Benutzerkonto. Wer das Passwort kennt, kann gegenüber einem System möglicherweise so auftreten, als wäre er der eigentliche Benutzer.

Vergleich aus dem Alltag

Ein Passwort ist wie ein persönlicher Schlüssel. Wer eine Kopie besitzt, kann versuchen, dieselbe Tür zu öffnen.

Beispiel aus dem Arbeitsalltag

Mit einem gestohlenen Passwort könnte ein Angreifer versuchen, auf E-Mail oder andere Dienste zuzugreifen.

“ **Merke:** Passwörter sind geheim und werden nicht an Kollegen weitergegeben.

2.2 Ein gutes Passwort

Gute Passwörter sind vor allem lang und einzigartig. Kurze oder leicht erratbare Wörter sind ungeeignet. Dasselbe Passwort sollte nicht für mehrere wichtige Konten verwendet werden.

Vergleich aus dem Alltag

Wenn ein Schlüssel für Haus, Auto und Firma passt, ist sein Verlust besonders schlimm.

Beispiel aus dem Arbeitsalltag

Gerät ein Passwort eines fremden Onlineshops in falsche Hände, darf dieses Passwort nicht gleichzeitig das Firmenkonto öffnen.

Passwörter: lang und einzigartig

Schlecht

kurz · wiederverwendet
leicht zu erraten

Besser

lang · einzigartig
im Passwortmanager

“ **Merke:** Lang und einzigartig ist wichtiger als ein möglichst kompliziert aussehendes kurzes Passwort.

2.3 Passwortmanager

Ein Passwortmanager kann für verschiedene Konten unterschiedliche starke Passwörter speichern und erzeugen. Dadurch muss man sich nicht jedes einzelne Passwort merken.

Vergleich aus dem Alltag

Ein Passwortmanager ist wie ein gut geschützter Schlüsseltresor.

Beispiel aus dem Arbeitsalltag

Statt dasselbe Passwort an zehn Stellen zu verwenden, erzeugt der Passwortmanager zehn unterschiedliche Kennwörter.

“ **Merke:** Passwortmanager erleichtern sichere, einzigartige Passwörter.

2.4 Passwörter niemals weitergeben

Ein persönliches Passwort gehört ausschließlich zum eigenen Konto. Auch die IT sollte dein normales persönliches Kennwort nicht benötigen, um ein technisches Problem zu untersuchen.

Vergleich aus dem Alltag

Ein Techniker braucht für eine Reparatur nicht automatisch deinen persönlichen Haustürschlüssel für immer.

Beispiel aus dem Arbeitsalltag

Fordert jemand per Telefon oder E-Mail dein Passwort an, ist das ein Warnzeichen.

“ **Merke:** Persönliche Passwörter werden nicht per E-Mail, Chat oder Telefon weitergegeben.

2.5 Was tun bei Verdacht auf ein gestohlenes Passwort?

Wenn du glaubst, dass jemand dein Passwort kennt, zählt Zeit. Informiere die IT und ändere das betroffene Passwort nach den vorgesehenen Verfahren. Verschweige den Verdacht nicht.

Vergleich aus dem Alltag

Wenn ein Haustürschlüssel verschwunden ist, wartet man nicht erst ab, ob eingebrochen wird.

Beispiel aus dem Arbeitsalltag

Du hast dein Kennwort versehentlich auf einer verdächtigen Webseite eingegeben.

Was soll ich tun?

Ein möglicherweise gestohlenes Passwort ist bereits ein Sicherheitsvorfall.

“ **Merke:** IT unverzüglich informieren und den Vorfall genau beschreiben.

MFA – die zweite Schutzschicht

3.1 Was ist MFA?

Mehr-Faktor-Authentifizierung verlangt neben dem Passwort mindestens einen weiteren unabhängigen Nachweis. Dadurch reicht ein gestohlenes Passwort häufig nicht aus, um ein Konto zu übernehmen.

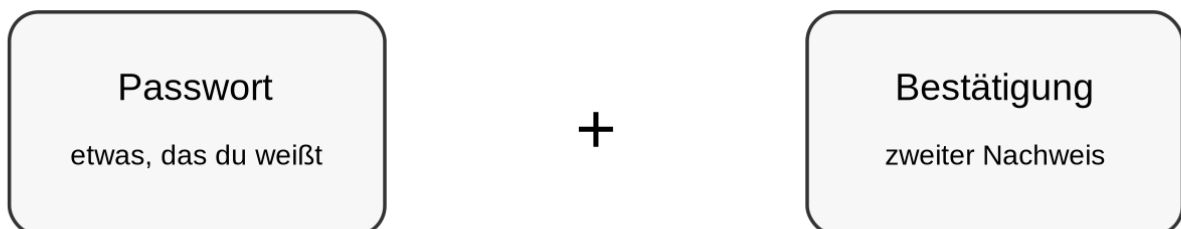
Vergleich aus dem Alltag

Eine Tür verlangt nicht nur einen Schlüssel, sondern zusätzlich einen passenden Ausweis.

Beispiel aus dem Arbeitsalltag

Nach dem Passwort muss eine Anmeldung auf einem registrierten Gerät bestätigt werden.

MFA: Zwei Nachweise statt nur eines



Nur bestätigen, wenn du die Anmeldung selbst gestartet hast.

“ **Merke:** MFA ist eine zusätzliche Schutzschicht, kein Ersatz für ein gutes Passwort.

3.2 Nur eigene Anmeldungen bestätigen

Eine MFA-Anfrage darf nur bestätigt werden, wenn du selbst gerade die dazugehörige Anmeldung gestartet hast. Eine unerwartete Anfrage kann bedeuten, dass jemand versucht, dein Konto zu verwenden.

Vergleich aus dem Alltag

Wenn jemand an der Tür klingelt, den du nicht bestellt hast, öffnest du nicht nur deshalb, weil er oft genug klingelt.

Beispiel aus dem Arbeitsalltag

Dein Smartphone fragt nach einer Anmeldebestätigung, obwohl du gerade kein neues Gerät oder Programm anmeldest.

Was soll ich tun?

Keine eigene Anmeldung = keine Bestätigung.

“ **Merke:** Anfrage ablehnen und bei Verdacht die IT informieren.

3.3 MFA-Müdigkeit

Angreifer können wiederholt Anmeldebestätigungen auslösen und hoffen, dass ein Benutzer irgendwann genervt auf „Bestätigen“ drückt. Dieses Vorgehen wird häufig als MFA-Fatigue oder MFA-Bombing bezeichnet.

Vergleich aus dem Alltag

Jemand klingelt hundertmal und hofft, dass du irgendwann aus Genervtheit die Tür öffnest.

Beispiel aus dem Arbeitsalltag

Innerhalb kurzer Zeit erscheinen mehrere unerwartete MFA-Anfragen.

Was soll ich tun?

Viele Anfragen machen eine Anmeldung nicht vertrauenswürdiger – sondern verdächtiger.

“ **Merke:** Nichts bestätigen und die IT informieren.

Phishing und Social Engineering

4.1 Was ist Phishing?

Phishing versucht, Menschen mit gefälschten Nachrichten oder Webseiten zu täuschen. Ziel können Passwörter, Zahlungsdaten, vertrauliche Informationen oder das Öffnen schädlicher Dateien sein.

Vergleich aus dem Alltag

Phishing ist Trickbetrug in digitaler Form.

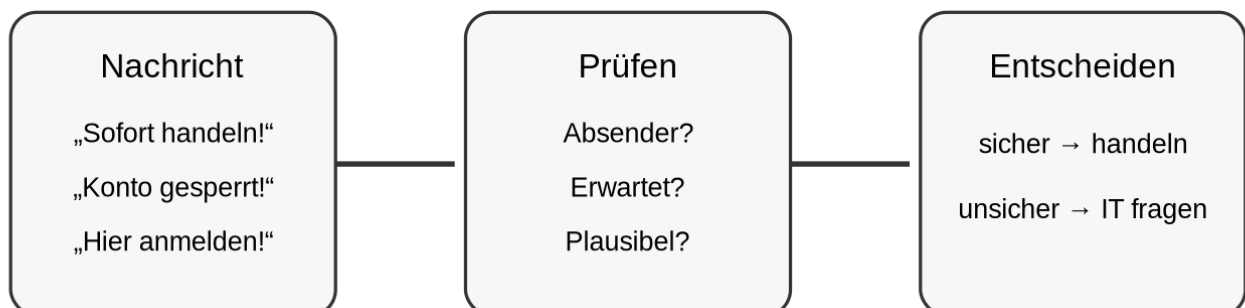
Beispiel aus dem Arbeitsalltag

Eine Nachricht behauptet, dein Postfach müsse sofort neu bestätigt werden und führt auf eine gefälschte Anmeldeseite.

Was soll ich tun?

Phishing greift zuerst deine Entscheidung an – nicht unbedingt deinen Computer.

Phishing: Erst prüfen, dann handeln



Merke: Nicht über den enthaltenen Link anmelden. Im Zweifel den bekannten normalen Weg zum Dienst verwenden.

4.2 Typische Warnzeichen

Ein einzelnes Merkmal beweist noch keinen Angriff. Mehrere Auffälligkeiten zusammen sollten dich aber besonders vorsichtig machen.

Vergleich aus dem Alltag

Bei einem gefälschten Ausweis kann ein Detail unauffällig sein. Mehrere falsche Details ergeben ein deutliches Bild.

Beispiel aus dem Arbeitsalltag

Ungewöhnlicher Absender, unerwartete Rechnung, großer Zeitdruck und Aufforderung zur sofortigen Anmeldung treten gemeinsam auf.

Was soll ich tun?

Überraschung + Zeitdruck + ungewöhnliche Handlung = besonders genau prüfen.

Warnzeichen

- ungewöhnlicher oder leicht veränderter Absender
- unerwarteter Anhang
- angebliche Kontosperrung
- ungewöhnliche Zahlungsanweisung
- Aufforderung zur Preisgabe von Zugangsdaten
- starker Zeitdruck

“ **Merke:** Absender, Anlass, Sprache, Linkziel und erwarteten Geschäftsprozess prüfen.

4.3 Gefälschte Absender

Ein sichtbarer Anzeigename ist kein sicherer Beweis für die Identität eines Absenders. Angreifer verwenden ähnlich aussehende Adressen oder Namen bekannter Personen und Firmen.

Vergleich aus dem Alltag

Auf einem Briefumschlag kann jemand ebenfalls einen bekannten Namen als Absender aufschreiben.

Beispiel aus dem Arbeitsalltag

Die Nachricht zeigt den Namen eines Kollegen, die tatsächliche Absenderadresse gehört aber zu einer fremden Domain.

Was soll ich tun?

Der angezeigte Name allein beweist nicht, wer eine Nachricht wirklich gesendet hat.

“ **Merke:** Bei ungewöhnlichen Anweisungen die vollständige Absenderadresse prüfen und über einen bekannten zweiten Weg rückfragen.

4.4 Zeitdruck und Autorität

Social Engineering nutzt menschliche Reaktionen. Besonders wirksam sind angebliche Dringlichkeit, Angst, Hilfsbereitschaft oder eine vermeintliche Anweisung einer Führungskraft.

Vergleich aus dem Alltag

Ein Betrüger will verhindern, dass du Zeit zum Nachdenken oder Nachfragen hast.

Beispiel aus dem Arbeitsalltag

Eine angebliche Führungskraft verlangt eine ungewöhnliche Zahlung und schreibt, sie sei gerade nicht telefonisch erreichbar.

Was soll ich tun?

Dringlichkeit ist kein Grund, Sicherheitsregeln zu überspringen.

“ **Merke:** Ungewöhnliche oder finanzielle Anweisungen über einen bekannten unabhängigen Kontaktweg bestätigen lassen.

4.5 QR-Code-Phishing

Auch QR-Codes können auf gefälschte Webseiten führen. Da das Ziel vor dem Scannen nicht immer sofort sichtbar ist, werden QR-Codes zunehmend für Phishing genutzt.

Vergleich aus dem Alltag

Ein QR-Code ist nur ein anderer Weg, eine Adresse zu verpacken. Er macht die Adresse nicht automatisch sicher.

Beispiel aus dem Arbeitsalltag

Eine E-Mail fordert dazu auf, einen QR-Code mit dem Smartphone zu scannen und das Firmenkonto anzumelden.

Was soll ich tun?

Ein QR-Code ist kein Vertrauensiegel.

“ **Merke:** Bei unerwarteten QR-Anmeldungen besonders vorsichtig sein und bekannte Zugangswege verwenden.

E-Mail, Links und Anhänge

5.1 Links prüfen

Ein Link kann anders aussehen als sein tatsächliches Ziel. Deshalb sollte bei unerwarteten Nachrichten nicht blind geklickt werden. Besonders Anmeldeseiten verdienen Aufmerksamkeit.

Vergleich aus dem Alltag

Ein Wegweiser kann „Bahnhof“ tragen und trotzdem in die falsche Richtung zeigen.

Beispiel aus dem Arbeitsalltag

Der sichtbare Text nennt Microsoft 365, das tatsächliche Ziel gehört aber zu einer unbekannten Domain.

Was soll ich tun?

Der Text eines Links und sein tatsächliches Ziel können verschieden sein.

“ **Merke:** Im Zweifel den Dienst über das bekannte Lesezeichen oder die selbst eingegebene Adresse öffnen.

5.2 Dateianhänge

Dateianhänge können normalen Inhalt, aber auch schädliche Programme oder präparierte Dokumente enthalten. Entscheidend ist deshalb nicht nur der Dateiname, sondern auch, ob die Nachricht und der Anhang erwartet wurden.

Vergleich aus dem Alltag

Ein Paket kann gefährlich sein, obwohl außen ein harmloser Aufkleber klebt.

Beispiel aus dem Arbeitsalltag

Eine unerwartete Bewerbung, Rechnung oder Versandinformation enthält eine ungewöhnliche Datei.

Was soll ich tun?

Erwartet und plausibel ist wichtiger als ein vertraut klingender Dateiname.

“ **Merke:** Bei Unsicherheit nicht öffnen und die Nachricht an die vorgesehene Supportstelle melden.

5.3 Makros und ausführbare Dateien

Bestimmte Dateien können Programmcode enthalten oder ausführen. Wenn ein Dokument unerwartet verlangt, Makros oder besondere Sicherheitsfunktionen zu aktivieren, ist Vorsicht geboten.

Vergleich aus dem Alltag

Ein normales Blatt Papier verlangt nicht, dass du zuerst die Alarmanlage abschaltest, bevor du es lesen kannst.

Beispiel aus dem Arbeitsalltag

Ein unbekanntes Office-Dokument fordert nach dem Öffnen dazu auf, Inhalte oder Makros zu aktivieren.

Was soll ich tun?

Sicherheitswarnungen nicht wegeklicken, nur damit ein Dokument funktioniert.

“ **Merke:** Nicht aktivieren und bei unerwarteten Dateien die IT fragen.

5.4 Geschäftliche Daten an den richtigen Empfänger

Ein Sicherheitsvorfall kann auch ohne Hacker entstehen: Eine E-Mail an den falschen Empfänger oder der falsche Anhang kann vertrauliche Informationen offenlegen.

Vergleich aus dem Alltag

Ein falsch adressierter Brief erreicht ebenfalls die falsche Person – nur lässt sich eine E-Mail oft noch schneller verschicken.

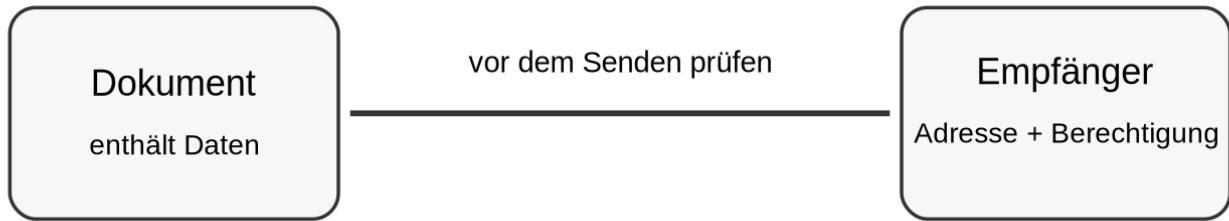
Beispiel aus dem Arbeitsalltag

Vor dem Versand enthält die Nachricht mehrere ähnlich klingende Empfänger oder einen automatisch ergänzten Kontakt.

Was soll ich tun?

Richtige Datei + richtiger Empfänger + richtiger Übertragungsweg.

Informationen nur an den richtigen Empfänger



Richtige Datei? Richtige Person? Richtiger Übertragungsweg?

“ **Merke:** Vor dem Senden Empfänger, CC-Feld und Anhänge noch einmal prüfen.

Sicherer Arbeitsplatz

6.1 Bildschirm sperren

Ein angemeldeter Computer besitzt bereits deine Berechtigungen. Verlässt du den Arbeitsplatz, sollte der Bildschirm deshalb gesperrt werden.

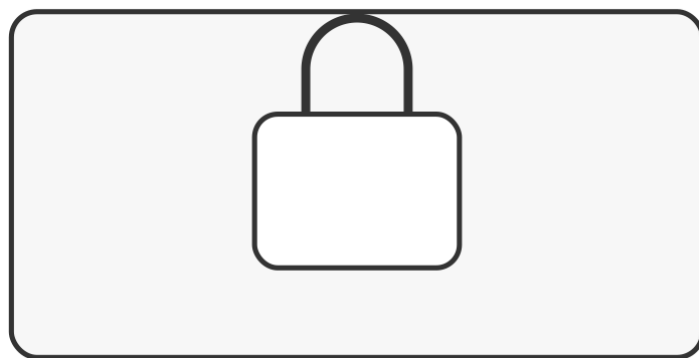
Vergleich aus dem Alltag

Ein offener Computer ist wie ein Büro, in dem dein Ausweis und deine Schlüssel unbeaufsichtigt auf dem Tisch liegen.

Beispiel aus dem Arbeitsalltag

Auch für einen kurzen Gang zum Drucker kann der Bildschirm mit `Windows-Taste + L` gesperrt werden.

Arbeitsplatz verlassen? Bildschirm sperren.



Windows-Taste + L

“ **Merke:** Arbeitsplatz verlassen = Bildschirm sperren.

6.2 Vertrauliche Informationen am Bildschirm

Nicht jede Information ist für jede Person bestimmt. Achte darauf, wer deinen Bildschirm sehen kann – besonders in Besprechungsräumen, öffentlichen Bereichen oder beim Teilen des Bildschirms.

Vergleich aus dem Alltag

Ein vertrauliches Dokument legst du auch nicht offen in einen Besucherbereich.

Beispiel aus dem Arbeitsalltag

Bei einer Videokonferenz wird der gesamte Bildschirm geteilt und im Hintergrund ist eine vertrauliche E-Mail sichtbar.

Was soll ich tun?

Bildschirmfreigabe kann mehr zeigen, als du eigentlich präsentieren wolltest.

“ **Merke:** Wenn möglich nur das benötigte Fenster teilen und nicht benötigte Anwendungen schließen.

6.3 Clean Desk und Ausdrucke

Vertrauliche Ausdrucke sollten nicht unbeaufsichtigt an Druckern oder auf Schreibtischen liegen bleiben. Papier ist ebenfalls ein Datenträger.

Vergleich aus dem Alltag

Datenschutz endet nicht, sobald eine Information ausgedruckt wurde.

Beispiel aus dem Arbeitsalltag

Eine Liste mit Kunden- oder Personaldaten bleibt über längere Zeit offen am gemeinsam genutzten Drucker liegen.

Was soll ich tun?

Papierdaten sind Daten.

“ **Merke:** Ausdrucke zeitnah abholen und vertrauliche Unterlagen passend aufbewahren oder entsorgen.

6.4 Fremde Personen

Physische Sicherheit gehört zur IT-Sicherheit. Unbekannte Personen sollten nicht allein aufgrund eines selbstbewussten Auftretens Zugang zu geschützten Bereichen oder Geräten erhalten.

Vergleich aus dem Alltag

Eine Warnweste oder ein Werkzeugkoffer macht jemanden nicht automatisch zum berechtigten Techniker.

Beispiel aus dem Arbeitsalltag

Eine unbekannte Person behauptet, einen PC oder Netzwerkanschluss prüfen zu müssen.

Was soll ich tun?

Freundlich sein bedeutet nicht, Zugang ungeprüft zu erlauben.

“ **Merke:** Im Zweifel Zuständigkeit über einen bekannten internen Kontakt prüfen.

USB, Geräte und mobile Arbeit

7.1 Unbekannte USB-Sticks

USB-Sticks können Dateien und in bestimmten Fällen auch schädliche Inhalte enthalten. Ein gefundener oder unbekannter Datenträger sollte deshalb nicht aus Neugier an einen Firmencomputer angeschlossen werden.

Vergleich aus dem Alltag

Ein gefundener Schlüssel wird auch nicht nacheinander in alle Türen gesteckt, um herauszufinden, wo er passt.

Beispiel aus dem Arbeitsalltag

Auf dem Parkplatz liegt ein USB-Stick mit der Aufschrift „Löhne 2026“.

Was soll ich tun?

Neugier ist kein Grund, unbekannte Datenträger anzuschließen.

bekannte Datenträger sind nicht automatisch vertrauenswürdig



Merke: Nicht anschließen. An die zuständige Stelle oder IT geben.

7.2 Private Geräte

Private Geräte und Firmen-IT haben unterschiedliche Sicherheits- und Verwaltungsanforderungen. Nicht jedes private Gerät oder Zubehör sollte ohne Freigabe mit Firmensystemen verbunden werden.

Vergleich aus dem Alltag

An eine Produktionsmaschine schließt man ebenfalls nicht beliebige private Erweiterungen an.

Beispiel aus dem Arbeitsalltag

Ein privater Datenträger soll für die schnelle Übertragung geschäftlicher Dateien verwendet werden.

Was soll ich tun?

Bequem ist nicht automatisch sicher oder zulässig.

“ **Merke:** Für Datenaustausch die vorgesehenen Firmenwege verwenden und im Zweifel die IT fragen.

7.3 Notebook unterwegs

Firmen-Notebooks enthalten Zugänge und möglicherweise lokale Daten. Unterwegs müssen sie vor Verlust, Diebstahl und neugierigen Blicken geschützt werden.

Vergleich aus dem Alltag

Ein Notebook ist nicht nur ein Gegenstand, sondern kann ein Schlüssel zu weiteren Firmensystemen sein.

Beispiel aus dem Arbeitsalltag

Das Notebook bleibt sichtbar im geparkten Auto oder unbeaufsichtigt in einem öffentlichen Bereich liegen.

Was soll ich tun?

Ein verlorenes Arbeitsgerät ist ein Sicherheitsereignis und sollte schnell gemeldet werden.

“ **Merke:** Gerät möglichst bei sich behalten, Bildschirm sperren und Verlust sofort melden.

7.4 Öffentliches WLAN

Öffentliche WLANs werden von vielen unbekannten Geräten genutzt. Für geschäftliche Arbeit sollten nur vorgesehene und abgesicherte Verbindungswege verwendet werden.

Vergleich aus dem Alltag

Ein öffentliches WLAN ist wie ein Gespräch in einer Bahnhofshalle: Viele unbekannte Personen befinden sich in derselben Umgebung.

Beispiel aus dem Arbeitsalltag

Ein Notebook wird im Hotel oder Café mit einem öffentlichen Funknetz verbunden.

Was soll ich tun?

Öffentliches WLAN ist nicht automatisch gefährlich, aber auch nicht automatisch vertrauenswürdig.

“ **Merke:** Vorgesehene Sicherheitsverfahren und gegebenenfalls den Firmen-VPN verwenden.

7.5 VPN

Ein VPN baut einen verschlüsselten Verbindungstunnel zu einem vorgesehenen Firmennetz auf. Es ermöglicht den Zugriff auf dafür freigegebene interne Dienste.

Vergleich aus dem Alltag

Ein VPN ist wie ein geschützter Tunnel durch öffentliches Gelände.

Beispiel aus dem Arbeitsalltag

Außerhalb des Unternehmens wird zuerst die VPN-Verbindung aufgebaut, bevor ein interner Dienst verwendet wird.

Was soll ich tun?

VPN schützt die Verbindung, ersetzt aber keine sichere Arbeitsweise.

“ **Merke:** Nur die bereitgestellte VPN-Lösung und die vorgesehenen Zugänge verwenden.

Daten und Datenschutz im Alltag

8.1 Nur notwendige Daten verwenden

Geschäftliche und personenbezogene Daten sollten nur für den vorgesehenen Zweck und von berechtigten Personen verwendet werden. Nur weil eine Information technisch erreichbar ist, bedeutet das nicht, dass sie für jede Aufgabe benötigt wird.

Vergleich aus dem Alltag

Ein Schlüssel zum Archiv ist keine Einladung, jede Akte aus Neugier zu lesen.

Beispiel aus dem Arbeitsalltag

Ein Mitarbeiter kann technisch auf einen Ordner zugreifen, benötigt dessen Inhalt aber nicht für seine Aufgabe.

Was soll ich tun?

Technischer Zugriff und dienstliche Berechtigung sind nicht dasselbe.

“ **Merke:** Nur die Daten öffnen und verwenden, die für die eigene Arbeit erforderlich sind.

8.2 Dateien nicht über beliebige Dienste versenden

Geschäftliche Dateien sollten über die dafür vorgesehenen Systeme übertragen werden. Private Cloudspeicher, private Mailkonten oder beliebige Dateitransferdienste können Datenschutz- und Sicherheitsprobleme verursachen.

Vergleich aus dem Alltag

Firmenpost wird auch nicht einfach über einen unbekannten privaten Kurierdienst verschickt.

Beispiel aus dem Arbeitsalltag

Eine große Datei passt nicht in eine E-Mail und soll deshalb spontan über einen privaten Onlinedienst geteilt werden.

Was soll ich tun?

Für Geschäftsdaten nur freigegebene Übertragungswege verwenden.

“ **Merke:** Die vorgesehenen Unternehmenslösungen verwenden oder bei der IT nach einer passenden Möglichkeit fragen.

8.3 Falscher Empfänger

Eine falsch adressierte E-Mail kann ein Datenschutz- oder Sicherheitsvorfall sein. Wichtig ist, nicht zu versuchen, das Problem stillschweigend zu lösen.

Vergleich aus dem Alltag

Ein vertraulicher Brief im falschen Briefkasten wird nicht richtiger, wenn niemand darüber spricht.

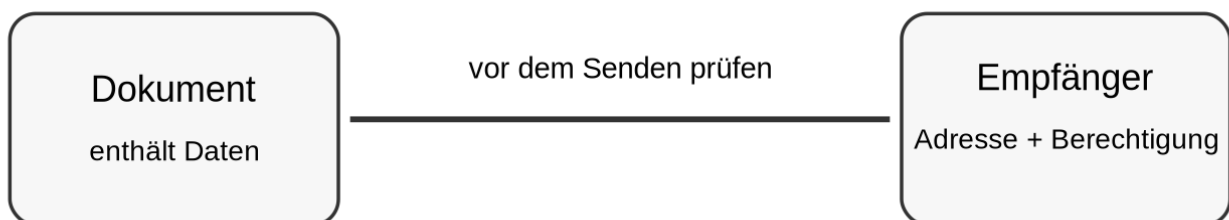
Beispiel aus dem Arbeitsalltag

Eine Nachricht mit vertraulichem Anhang wurde versehentlich an einen falschen externen Empfänger gesendet.

Was soll ich tun?

Fehler schnell melden – Zeit kann bei der Schadensbegrenzung entscheidend sein.

Informationen nur an den richtigen Empfänger



Richtige Datei? Richtige Person? Richtiger Übertragungsweg?

Merke: Unverzüglich die zuständige interne Stelle informieren und die Situation genau beschreiben.

8.4 Screenshots und Fotos

Auch Screenshots und Fotos können vertrauliche Informationen enthalten. Vor dem Teilen sollte geprüft werden, was im gesamten Bild sichtbar ist.

Vergleich aus dem Alltag

Ein Foto vom Schreibtisch kann unbeabsichtigt Unterlagen im Hintergrund zeigen.

Beispiel aus dem Arbeitsalltag

Ein Screenshot einer Fehlermeldung zeigt gleichzeitig Kundendaten, E-Mail-Adressen oder andere nicht benötigte Informationen.

Was soll ich tun?

Ein Screenshot ist eine Kopie von Informationen und muss entsprechend behandelt werden.

“ **Merke:** Nur den relevanten Bereich teilen oder nicht benötigte Daten vorher unkenntlich machen.

Updates und Software

9.1 Warum Updates notwendig sind

Software enthält Fehler und manchmal Sicherheitslücken. Hersteller veröffentlichen Updates, um solche Probleme zu beheben. Deshalb gehören regelmäßige Aktualisierungen zum Schutz der IT.

Vergleich aus dem Alltag

Ein bekannt defektes Türschloss sollte repariert werden, bevor jemand die Schwachstelle ausnutzt.

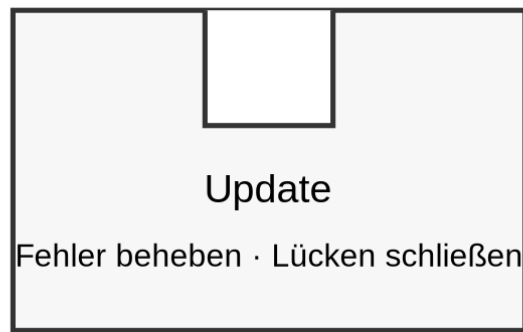
Beispiel aus dem Arbeitsalltag

Ein Browser erhält ein Update, das eine bekannte Sicherheitslücke schließt.

Was soll ich tun?

Updates sind Wartung und Sicherheitsmaßnahme zugleich.

Updates schließen bekannte Lücken



Manchmal ist danach ein Neustart nötig.

“ **Merke:** Updates nicht ohne Grund dauerhaft aufschieben.

9.2 Warum ein Neustart nötig sein kann

Manche Systembestandteile können erst vollständig ersetzt werden, wenn Windows oder ein anderes Betriebssystem neu gestartet wird. Deshalb verlangen bestimmte Updates einen Neustart.

Vergleich aus dem Alltag

Eine laufende Maschine kann nicht an jeder Stelle repariert werden, während sie weiterläuft.

Beispiel aus dem Arbeitsalltag

Windows meldet nach einem Update, dass ein Neustart erforderlich ist.

Was soll ich tun?

Ein Neustart kann Teil des Updates sein – nicht nur eine lästige Zusatzfrage.

“ **Merke:** Arbeit speichern und den vorgesehenen Neustart nicht unbegrenzt verschieben.

9.3 Software nicht selbst aus unbekannten Quellen installieren

Programme aus unbekannten Quellen können Schadsoftware, unerwünschte Zusatzprogramme oder ungeklärte Lizenzbedingungen enthalten. Auf Firmengeräten gelten deshalb Vorgaben für Softwareinstallation.

Vergleich aus dem Alltag

Du würdest auch kein unbekanntes Ersatzteil in eine Firmenmaschine einbauen, nur weil es kostenlos angeboten wird.

Beispiel aus dem Arbeitsalltag

Eine Webseite verspricht ein kostenloses Werkzeug und fordert zum Herunterladen einer ausführbaren Datei auf.

Was soll ich tun?

Kostenlos und nützlich bedeutet nicht automatisch sicher oder lizenzrechtlich erlaubt.

“ **Merke:** Benötigte Software über die vorgesehenen Wege beziehen oder mit der IT abstimmen.

Sicherheitsvorfälle richtig
melden

10.1 Was ist ein Sicherheitsvorfall?

Ein Sicherheitsvorfall ist nicht nur ein erfolgreicher Hackerangriff. Auch ein verlorenes Gerät, ein versehentlich weitergegebenes Passwort, eine falsche E-Mail oder ein verdächtiger Anmeldeversuch können relevant sein.

Vergleich aus dem Alltag

Ein Brandmelder wird nicht erst benutzt, wenn das ganze Gebäude brennt.

Beispiel aus dem Arbeitsalltag

Du bemerkst eine unbekannte Anmeldung, hast auf einen verdächtigen Link geklickt oder ein Firmen-Notebook verloren.

Was soll ich tun?

Lieber einen Verdacht einmal zu viel melden als einen echten Vorfall zu spät.

„ **Merke:** Bei begründetem Verdacht frühzeitig die zuständige Stelle informieren.

10.2 Was tun nach einem falschen Klick?

Ein Klick allein bedeutet nicht automatisch, dass ein Schaden entstanden ist. Trotzdem sollte der Vorgang ernst genommen werden. Entscheidend ist, was danach passiert ist.

Vergleich aus dem Alltag

Wenn du eine falsche Tür geöffnet hast, ist wichtig, ob du nur hineingeschaut oder anschließend Schlüssel und Unterlagen abgegeben hast.

Beispiel aus dem Arbeitsalltag

Du hast einen Link geöffnet, aber keine Zugangsdaten eingegeben. Oder du hast zusätzlich Benutzernamen und Passwort eingegeben.

Was soll ich tun?

Nicht verheimlichen und nicht auf eigene Faust „aufräumen“ – genaue Informationen helfen der IT.

Bei einem Sicherheitsvorfall

1. Nicht
weiterklicken

2. Situation
merken

3. IT sofort
informieren

4. Anweisungen
befolgen

Frühe Meldung ist wichtiger als die Frage, wer einen Fehler gemacht hat.

“ **Merke:** Nicht weiter experimentieren. Merken, was genau passiert ist, und die IT mit diesen Informationen kontaktieren.

10.3 Was tun nach Eingabe eines Passworts?

Wenn ein Passwort auf einer verdächtigen Seite eingegeben wurde, muss davon ausgegangen werden, dass es bekannt geworden sein könnte. Jetzt zählt eine schnelle Reaktion.

Vergleich aus dem Alltag

Ein Schlüssel, den ein Fremder kopiert haben könnte, gilt nicht mehr als zuverlässig geheim.

Beispiel aus dem Arbeitsalltag

Nach dem Klick auf einen Link sah die Anmeldeseite echt aus. Erst danach bemerkst du, dass die Webadresse falsch war.

Was soll ich tun?

Ein eingegebenes Passwort kann kompromittiert sein, auch wenn die Webseite danach einen Fehler gezeigt hat.

“ **Merke:** IT sofort informieren und das Passwort nach dem vorgesehenen Verfahren ändern. Unerwartete MFA-Anfragen nicht bestätigen.

10.4 Verlust eines Geräts

Der Verlust eines Smartphones, Tablets oder Notebooks sollte unverzüglich gemeldet werden. Je früher die zuständigen Stellen davon wissen, desto schneller können Zugänge bewertet oder Schutzmaßnahmen eingeleitet werden.

Vergleich aus dem Alltag

Bei einer verlorenen Schlüsselkarte meldest du den Verlust ebenfalls, damit sie gesperrt werden kann.

Beispiel aus dem Arbeitsalltag

Ein Firmen-Smartphone bleibt im Zug liegen oder ein Notebook wird gestohlen.

Was soll ich tun?

Nicht erst bis zum nächsten Arbeitstag warten, wenn ein Firmenzugang verloren gegangen ist.

“ **Merke:** IT bzw. die dafür vorgesehene interne Stelle sofort informieren und Ort, Zeitpunkt und Gerät möglichst genau nennen.

10.5 Welche Informationen die IT braucht

Für die Untersuchung sind konkrete Fakten wichtig: Was ist passiert? Wann? Welches Gerät oder Konto? Welche Nachricht oder Webseite? Wurden Zugangsdaten eingegeben? Wurde etwas heruntergeladen oder geöffnet?

Vergleich aus dem Alltag

Ein Feuerwehrmann kann besser reagieren, wenn er weiß, wo Rauch gesehen wurde und was dort gelagert ist.

Beispiel aus dem Arbeitsalltag

„Ich glaube, ich habe etwas Falsches angeklickt“ ist ein Anfang. Noch hilfreicher sind Zeitpunkt, Screenshot, Absender und die Information, was anschließend eingegeben oder geöffnet wurde.

Was soll ich tun?

Genaue Informationen helfen mehr als Vermutungen.

“ **Merke:** Situation möglichst unverändert lassen und die bekannten Fakten weitergeben.

Kurze Alltagssituationen –
Was würdest du tun?

11.1 Der Chef braucht dringend Gutscheinkarten

Du erhältst eine Nachricht von einer angeblichen Führungskraft. Sie brauche sofort Gutscheinkarten oder eine ungewöhnliche Zahlung und könne gerade nicht telefonieren. Solche Geschichten sind ein bekanntes Muster beim Social Engineering.

Vergleich aus dem Alltag

Der Betrüger nutzt Autorität und Zeitdruck, damit normale Kontrollwege übersprungen werden.

Beispiel aus dem Arbeitsalltag

Die Nachricht klingt persönlich und nennt sogar echte Namen, verlangt aber einen ungewöhnlichen Ablauf.

Was soll ich tun?

Ungewöhnliche Zahlungsanweisung + Geheimhaltung oder Zeitdruck = stoppen und prüfen.

“ **Merke:** Nicht ausführen. Die Person über einen bekannten unabhängigen Kontaktweg erreichen und die Anweisung bestätigen lassen.

11.2 Microsoft fordert eine sofortige Anmeldung

Eine E-Mail behauptet, dein Microsoft-365-Konto werde gesperrt, wenn du dich nicht innerhalb kurzer Zeit über einen Link anmeldest.

Vergleich aus dem Alltag

Angst vor Arbeitsausfall soll dich zum schnellen Handeln bringen.

Beispiel aus dem Arbeitsalltag

Die Mail sieht professionell aus, enthält aber einen Link zu einer fremden Adresse.

Was soll ich tun?

Eine professionell aussehende Nachricht kann trotzdem gefälscht sein.

“ **Merke:** Nicht über den Link anmelden. Den bekannten normalen Zugang verwenden und bei Unsicherheit die IT fragen.

11.3 Ein Lieferant schickt plötzlich neue Bankdaten

Änderungen von Zahlungsdaten sind besonders sensibel. Eine E-Mail allein sollte bei ungewöhnlichen Änderungen nicht automatisch als ausreichender Nachweis betrachtet werden.

Vergleich aus dem Alltag

Wenn jemand per Brief behauptet, dein Vermieter habe ab morgen ein völlig anderes Konto, würdest du ebenfalls nachprüfen.

Beispiel aus dem Arbeitsalltag

Ein bekannter Lieferant nennt überraschend eine neue Bankverbindung und drängt auf schnelle Änderung.

Was soll ich tun?

Finanzdaten nicht allein aufgrund einer unerwarteten E-Mail ändern.

“ **Merke:** Die Änderung nach dem vorgesehenen Geschäftsprozess und über einen bekannten unabhängigen Kontaktweg verifizieren.

11.4 Ein Kollege braucht kurz dein Passwort

Auch wenn die Bitte von einem Kollegen kommt, bleibt ein persönliches Passwort persönlich. Gemeinsame Arbeit wird über Berechtigungen, Freigaben oder dafür vorgesehene Konten gelöst.

Vergleich aus dem Alltag

Du verleihst deinen persönlichen Firmenausweis nicht, damit jemand unter deinem Namen eine Tür öffnet.

Beispiel aus dem Arbeitsalltag

Ein Kollege muss dringend an eine Datei und bittet deshalb um dein Kennwort.

Was soll ich tun?

Kollegialität bedeutet nicht, persönliche Zugangsdaten zu teilen.

“ **Merke:** Passwort nicht weitergeben. Stattdessen eine passende Freigabe oder Unterstützung durch die IT organisieren.

11.5 Du findest einen USB-Stick

Ein unbekannter USB-Stick kann absichtlich platziert worden sein, um Neugier auszunutzen. Selbst wenn das selten vorkommt, gibt es keinen guten Grund, ihn an einen Firmencomputer anzuschließen.

Vergleich aus dem Alltag

Eine unbekannte Flasche würdest du auch nicht probieren, nur um herauszufinden, was darin ist.

Beispiel aus dem Arbeitsalltag

Vor dem Gebäude liegt ein USB-Stick mit einer interessant klingenden Beschriftung.

Was soll ich tun?

Unbekannter Datenträger: nicht testen, sondern melden.

bekannte Datenträger sind nicht automatisch vertrauenswürdig



“ **Merke:** Nicht anschließen. An die IT oder die zuständige interne Stelle geben.