Nicht lizensierter Ausdruck

Sicherer Umgang mit Daten, Geräten und dem Internet

1. Grundlagen & Datenschutz

Computer, Smartphones und das Internet gehören heute zum Alltag. Nutzerinnen und Nutzer speichern Fotos und Dokumente, verschicken Nachrichten, kaufen online ein und nutzen zahlreiche digitale Dienste.

Damit diese Möglichkeiten sicher bleiben, müssen Geräte, Daten und persönliche Informationen geschützt werden. IT-Sicherheit bedeutet deshalb nicht nur, Viren zu verhindern. Es geht auch darum, Betrug zu erkennen, Passwörter sicher zu verwenden, Daten zu schützen und Geräte richtig einzustellen.

1.1 Daten und Informationen

- **Daten** sind einzelne Werte oder Angaben. **Informationen** entstehen, wenn Daten in einen Zusammenhang gebracht werden und dadurch eine Bedeutung erhalten.
    - *Beispiel:* 12 – 08 – 15
- Erst wenn wir wissen, wofür die Zahlen stehen, erhalten wir eine nutzbare Information und können sie richtig verstehen.
    - *Beispiel:* „Am 12.08. findet um 15:00 Uhr eine Schulung statt.“

1.2 Die drei Grundbegriffe der IT-Sicherheit und wichtige Begriffe der IT-Sicherheit

- **Schwachstelle**: Eine Schwachstelle oder Lücke in einem System.
  Bedrohung: Etwas, das diese Schwäche ausnutzen und Schaden verursachen kann.
  Risiko: Die Wahrscheinlichkeit, dass tatsächlich ein Schaden entsteht.
    - Beispiel: Ein Computer hat ein veraltetes Programm (**Schwachstelle**). Ein Angreifer versucht, diese Schwäche auszunutzen (**Bedrohung**). Dadurch könnten Daten gestohlen oder das Gerät beschädigt werden (**Risiko**).
- **Cyber Security (Cyber-Sicherheit):** Alle Maßnahmen, die Computer, Netzwerke, Geräte und Daten vor Angriffen, Missbrauch und Schäden schützen.
    - *Beispiel:* Du schützt dein Smartphone mit einer PIN, installierst Sicherheitsupdates und verwendest eine Bildschirmsperre. Ein Unternehmen schützt seine Computer zusätzlich mit Firewalls, Sicherheitsprogrammen und Zugriffsrechten.
- **Cybercrime (Internetkriminalität):** Bezeichnet Straftaten, bei denen digitale Technologien oder das Internet genutzt werden. Beispiele sind Betrug, Erpressung und Datendiebstahl.
    - *Beispiel:* Eine gefälschte E-Mail sieht aus wie eine Nachricht der Bank. Wer auf den enthaltenen Link klickt und seine Zugangsdaten eingibt, kann Opfer eines Internetbetrugs werden.
- **Cyberattacke:** Ein gezielter digitaler Angriff auf ein Gerät, ein Netzwerk oder eine Organisation (z. B. Überlastung einer Website, sodass diese abstürzt.
    - *Beispiel:* Kriminelle greifen die Webseite eines Unternehmens mit sehr vielen Anfragen an. Der Server wird dadurch überlastet und die Webseite ist vorübergehend für Kunden nicht mehr erreichbar.

Nicht lizenzierter Ausdruck

- **Hacken:** Bedeutet, Sicherheitslücken eines Computersystems gezielt auszunutzen. Nicht jedes Hacken ist automatisch kriminell: Sicherheitsfachleute können Systeme auch mit Erlaubnis testen, um Schwachstellen zu finden. Kriminelles Hacken von Systemen erfolgt dagegen ohne Erlaubnis.
    - *Beispiel:* Ein Unternehmen beauftragt einen Sicherheitsexperten, sein Netzwerk zu überprüfen. Der Experte versucht, Sicherheitslücken zu finden, damit diese geschlossen werden können. Das ist ein erlaubter Sicherheitstest. Wer dagegen ohne Erlaubnis in ein fremdes Computersystem eindringt, handelt rechtswidrig.
- **Cyberwarfare (Cyber-Kriegsführung):** Digitale Angriffe im Rahmen von Konflikten zwischen Staaten, oft gerichtet auf kritische Infrastrukturen (z. B. Stromversorgung, Krankenhäuser).
    - *Beispiel:* In einem Konflikt könnte ein Staat versuchen, die Computersysteme eines anderen Staates anzugreifen und dadurch beispielsweise die Steuerung wichtiger Einrichtungen zu stören.

1.3 Ursachen von Bedrohungen

Daten können durch Menschen, technische Probleme oder Naturereignisse gefährdet werden:

1. **Menschliche Fehler (unbeabsichtigt)**
    - ***Beispiele***: Jemand gibt eine falsche E-Mail-Adresse ein und schickt vertrauliche Informationen an die falsche Person.
      Ein anderes Beispiel ist der Verlust eines unverschlüsselten USB-Sticks mit wichtigen Daten.
      Ein Mitarbeiter öffnet versehentlich einen gefährlichen Anhang.
2. **Böswillige Handlungen (absichtlich)**

    Kriminelle oder unzufriedene Mitarbeitende stehlen, verändern oder löschen Daten bewusst.
    - ***Beispiel***: Ein Mitarbeiter könnte beispielsweise vertrauliche Unternehmensdaten stehlen. Angreifer können versuchen, Schadsoftware auf Geräten einzuschleusen.
3. **Technische Probleme**

    Auch technische Defekte können Daten gefährden.
    - ***Beispiel*:** Eine Festplatte fällt aus und wichtige Dateien sind nicht mehr erreichbar.
4. **Naturereignisse und andere außergewöhnliche Ereignisse**

    Feuer, Überschwemmungen, Blitzschlag oder andere Ereignisse können Geräte und Server beschädigen.
    Deshalb ist es wichtig, wichtige Daten nicht nur am selben Ort wie das Original zu sichern.

1.4 Schutz von Arbeitsdaten und physischer Geräteschutz

- S**chutz von Arbeitsdaten:** Daten am Arbeitsplatz müssen besonders geschützt werden, um Diebstahl, betrügerische Verwendung, unbeabsichtigten Datenverlust und Sabotage zu verhindern.

Nicht lizensierter Ausdruck

- **Drei Regeln für physische Sicherheit:** Geräte müssen physisch vor Diebstahl und unbefugtem Zugriff geschützt werden:
    - **Abschließen**: Räume und Schränke beim Verlassen abschließen.
    - **Anketten**: Laptops mit einem Sicherheitskabel (Kensington-Schloss) sichern.
    - **Beaufsichtigen**: Geräte an öffentlichen Orten niemals unbeaufsichtigt lassen.

1.5 Cloud-Dienste

Beim Cloud-Computing werden Daten auf externen Servern eines Anbieters gespeichert (z. B. OneDrive, Google Drive, iCloud).

Vorteil: Flexibler, ortsunabhängiger Zugriff von verschiedenen Endgeräten.

Zu beachten: Vertrauen in den Anbieter, Einhaltung der Datenschutzregeln und Erstellung von Backups.

1.6 Schutzziele und Datenschutz

Informationen können sehr wertvoll sein. Ein Unternehmen muss beispielsweise Kundendaten schützen. Eine Privatperson möchte vielleicht verhindern, dass jemand auf Fotos, Nachrichten oder Bankdaten zugreift.

Die 3 Schutzziele der IT-Sicherheit (CIA-Prinzip)

Schutzziel	Bedeutung	Beispiel aus der Praxis
C – *Confidentiality* **(Vertraulichkeit)**	Nur berechtigte Personen dürfen Daten einsehen.	Patientenakten dürfen nur vom behandelnden Arzt gelesen werden.
I – *Integrity* **(Integrität)**	Daten müssen korrekt sein und dürfen nicht unbefugt geändert werden.	Der Geldbetrag bei einer Überweisung darf unterwegs nicht verändert werden.
A – *Availability* **(Verfügbarkeit)**	Daten und Systeme müssen bei Bedarf erreichbar sein.	Ein Online-Shop muss rund um die Uhr für Kunden erreichbar sein.

1.7 Datenschutz-Grundverordnung (DSGVO)

Der Datenschutz schützt Menschen, nicht Daten. Er sorgt dafür, dass personenbezogenen Daten (z. B. Name, Adresse, Fotos, Standortdaten, Bankdaten, Kaufhistorie) nicht missbraucht werden.

Die **Datenschutz-Grundverordnung (DSGVO)** enthält Regeln für die Verarbeitung personenbezogener Daten. Datenschutz begegnet uns im Alltag zum Beispiel bei Online-Einkäufen, Apps, sozialen Netzwerken und Kundenkarten.

Nicht lizensierter Ausdruck

Vier Grundprinzipien der DSGVO:

- **Transparenz:** Du musst klar erkennen können, wer deine Daten sammelt und was damit geschieht.
    - *Beispiel:* Eine App möchte auf den Standort zugreifen. Es sollte erkennbar sein, warum sie diese Berechtigung benötigt.
- **Zweckbindung:** Daten dürfen nur für den ursprünglichen Zweck verwendet werden (z. B. Lieferadresse nur für die Paketzustellung, nicht für Werbung).
    - *Beispiel:* Eine Lieferadresse wird benötigt, um ein Paket zuzustellen. Sie sollte nicht einfach für einen völlig anderen Zweck verwendet werden.
- **Datenminimierung:** Es werden nur so viele Daten erhoben wie unbedingt nötig (z. B. für einen Newsletter braucht man keine Wohnadresse).
- **Verhältnismäßigkeit:** Die Verarbeitung personenbezogener Daten muss in einem angemessenen Verhältnis zum Ziel stehen und darf die Rechte der betroffenen Person nicht übermäßig einschränken.
    - *Beispiel*: Eine *Videoüberwachung* im Büro zur Arbeitszeiterfassung wäre unverhältnismäßig, da z. b. eine Anwesenheitsliste reicht.

Rollen beim Datenschutz

- **Betroffene Person:** Die Person, um deren Daten es geht, z. B. ein Kunde, eine Mitarbeiterin oder ein Schüler.
- **Verantwortlicher:** Entscheidet, warum und wie personenbezogene Daten verarbeitet werden, z. B. ein Unternehmen, eine Behörde oder eine Schule.
- **Auftragsverarbeiter:** Verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen, z. B. z. B. ein externer Cloud-Anbieter oder IT-Dienstleister.

Beispiel Online-Einkauf

Bestellung eines Laptops in einem Online-Shop:

- **Betroffene Person:** Kunde – die Bestell- und Kontaktdaten werden verarbeitet.
- **Verantwortlicher:** Der Online-Shop entscheidet, welche Daten für die Bestellung benötigt werden und wie sie verarbeitet werden.
- **Auftragsverarbeiter:** Ein beauftragter IT- oder Cloud-Dienstleister verarbeitet die Daten im Auftrag des Shops.
- **Zweckbindung:** Die Lieferadresse wird für die Zustellung benötigt.
- **Datenminimierung:** Der Shop erhebt nur Daten, die für die Bestellung tatsächlich benötigt werden.

Nichtlizensierter Ausdruck

1.8 IT-Richtlinien

IT-Richtlinien sind Verhaltensregeln in Schulen oder Unternehmen. Sie legen fest, wie Geräte und Daten sicher genutzt werden.

> **Typische Richtlinie**: Nutzung der Mehrfach-Authentifizierung (MFA), Verbot von privaten USB-Sticks an Dienst-PCs und Pflicht zum Sperren des Bildschirms beim Verlassen des Platzes.

2. Schutz persönlicher Daten, Social Engineering und Programme

2.1 Grundbegriffe

Social Engineering: Die gezielte menschliche Beeinflussung und Täuschung, um Vertrauen zu erschleichen und an vertrauliche Daten oder Geld zu gelangen.

- *Beispiel:* Ein angeblicher IT-Mitarbeiter fordert einen Mitarbeiter auf, sein Passwort zu nennen, und versucht damit, Zugriff auf ein Computersystem zu erhalten.

Identitätsdiebstahl: Der Missbrauch gestohlener persönlicher Daten, um sich als eine andere Person auszugeben oder in deren Namen zu handeln. (*z. B. Erstellen eines Fake-Profils auf Social Media*).

2.2 Digitale Täuschungs- und Angriffsmethoden

Methode	**Kanal / Medium**	**Angriffsform / Beispiel**
Phishing	E-Mail	Gefälschte E-Mails locken auf gefälschte Bank-Websites und man wird aufgefordert über einen Link die Zugangsdaten zu bestätigen.
Smishing	SMS / Messenger / E-Mail	Nachricht über angebliche Paketprobleme mit schädlichem Link.
Vishing (von Voice + Phishing)	Anruf (Voice)	Angeblicher Support-Mitarbeiter fordert am Telefon Passwörter an.
Quishing (von QR-Code und Phishing)	QR-Code	Präparierter QR-Code auf einem Plakat führt zu Zahlungsbetrug.
Pharming *(von **Ph**ishing und F**arming**)*	Web-Umleitung	Opfer wird trotz richtiger Adresseingabe unbemerkt auf gefälschte Website umgeleitet. Eine Person möchte die Webseite ihrer Bank

Nicht lizensierter Ausdruck

Methode	Kanal / Medium	Angriffsform / Beispiel
		aufrufen, landet aber unbemerkt auf einer gefälschten Kopie.
Watering-Hole	Bestimmte Websites	Benannt nach Raubtieren, die an einer Wasserstelle auf ihre Beute lauern. Eine von Zielgruppen häufig besuchte Website wird präpariert. Besucher könnten dadurch auf eine schädliche Website weitergeleitet oder mit Schadsoftware angegriffen werden.
Web-Scraping (engl. scraping = auskratzen/abschöpfen)	Bot-Software	Automatisierte Massen-Abschöpfung von Daten aus Websites. Dies ist grundsätzlich nicht verboten, doch werden dabei ohne Erlaubnis große Mengen personenbezogener Daten gesammelt, kann dies problematisch sein.

2.3 Physische und analoge Angriffe

- **Shoulder Surfing:** Heimliches Beobachten bei der Eingabe eines Passworts, einer PIN oder anderen vertraulichen Informationen.
    - *Beispiel:* Jemand beobachtet im Zug, wie eine Person ihre PIN am Smartphone eingibt.
- **Tailgating:** *(engl. Tailgate = Heckklappe, im Autoverkehr wird zu dichtes Auffahren auf das vorausfahrende Auto Tailgating genannt)*
  Beim **Tailgating** verschafft sich eine unbefugte Person Zugang zu einem geschützten Bereich, indem sie direkt hinter einer berechtigten Person durch eine Tür geht.
    - *Beispiel:* Ein Mitarbeiter öffnet mit seiner Zugangskarte die Bürotür. Eine fremde Person geht unbemerkt oder unter einem Vorwand direkt hinter ihm durch die Tür.
- **Baiting (Köder):** Ein Angreifer verwendet einen attraktiven Köder, um Neugier zu wecken.
    - *Beispiel:* Ein präparierter USB-Stick mit Schadsoftware wird an einem öffentlichen Ort liegen gelassen. Eine Person findet ihn und steckt ihn aus Neugier in den Computer.
- **Information Diving:** Durchsuchen von weggeworfenen Unterlagen oder Datenträgern nach vertraulichen Informationen.
    - *Beispiel:* Jemand durchsucht einen Papierkorb nach Rechnungen oder anderen Dokumenten mit persönlichen Daten.

Nicht lizensierter Ausdruck

- **Skimming:** Bezeichnet das unerlaubte Auslesen von Daten von Zahlungskarten, beispielsweise mit manipulierten Geldautomaten-Kartenlesern.
    - *Beispiel:* Ein manipulierter Geldautomat liest Kartendaten aus. Eine zusätzliche versteckte Kamera könnte versuchen, die Eingabe der PIN aufzuzeichnen.

2.4 Manipulative Techniken und KI

- **Pretexting** (engl. Pretext = Vorwand, Ausflucht): Der Angreifer erfindet eine glaubwürdige Geschichte oder gibt sich als eine andere Person aus, um Vertrauen zu gewinnen und an Informationen zu gelangen.
    - *Beispiel:* Jemand gibt sich als Mitarbeiter der IT-Abteilung aus und behauptet, wegen eines technischen Problems das Passwort zu benötigen.
- **Deepfakes und KI-Imitation:** Künstliche Intelligenz kann verwendet werden, um sehr realistische Bilder, Videos oder Stimmen zu erzeugen oder zu verändern.

  Dadurch können Angreifer versuchen, eine andere Person zu imitieren.
    - *Beispiel:* Ein Angreifer erzeugt mit KI eine Stimme, die wie die eines Vorgesetzten klingt, und fordert telefonisch eine dringende Überweisung.

Wichtiger Sicherheitstipp: *Bei ungewöhnlichen Anweisungen oder Geldforderungen immer über einen zweiten, bekannten Kommunikationsweg (z. B. offizielle Telefonnummer) zurückrufen!*

2.5 Datensicherheit in Programmen

Makros: Kleine Zusatzprogramme, die Abläufe z. B. in Word oder Excel automatisieren (z. B. Tabellen automatisch formatieren und berechnen).

> **Risiko:** Kriminelle können Schadcode in Makros verstecken. Makros sollten daher nur aktiviert werden, wenn die Datei und ihre Quelle vertrauenswürdig sind.

Verschlüsselung: Wandelt Klartext in unlesbaren Zeichencode um. Ohne den passenden Schlüssel bleiben die Daten unlesbar.

- Beispiel*:* Eine E-Mail mit Gehaltsabrechnungen wird verschlüsselt gesendet. Fängt ein Angreifer die Datei ab, sieht er nur unlesbaren Zeichencode statt des eigentlichen Inhalts. Ohne den passenden Schlüssel kann er den Inhalt nicht lesen.

Laufwerksverschlüsselung: Schützt gespeicherte Daten, wenn ein Gerät verloren geht oder gestohlen wird. Ohne den erforderlichen Schlüssel können die gespeicherten Daten nicht einfach ausgelesen werden.

> *Wichtig:* Geht das Passwort oder der Wiederherstellungsschlüssel verloren, ist der Zugriff auf die Daten möglicherweise dauerhaft nicht mehr möglich.

Passwortschutz von Dokumenten

- **Funktion:** Schützt einzelne Dateien, z. B. PDF- oder Word-Dokumente, durch ein Kennwort vor unbefugtem Zugriff.

Nicht lizensierter Ausdruck

- **Pfad in Word:** *Datei > Informationen > Dokument schützen > Mit Kennwort verschlüsseln*

3. Gefahren durch Schadsoftware (Malware)

3.1 Arten von Malware

Malware ist ein Sammelbegriff für Schadsoftware. Dabei handelt es sich um Programme oder Skripte, die Geräte, Daten oder Systeme schädigen oder unerwünschte Aktionen ausführen.

Schadsoftware-Typ	Funktionsweise	Praxisbeispiel
Virus	Hängt sich an bestehende Dateien oder Programme an und wird häufig durch das Ausführen der infizierten Datei aktiviert.	Eine infizierte Word-Datei wird geöffnet und der Schadcode kann weitere Dateien infizieren.
Wurm	Verbreitet sich selbstständig über Netzwerke und Sicherheitslücken – ganz ohne Zutun des Nutzers.	Ein Wurm nutzt eine Sicherheitslücke im Betriebssystem und infiziert automatisch weitere Computer im Netzwerk.
Fileless Malware	Arbeitet weitgehend direkt im Arbeitsspeicher (RAM) und hinterlässt dabei möglichst wenige schädliche Dateien auf dem Datenträger.	Schadcode wird über eine Sicherheitslücke oder ein manipuliertes Dokument gestartet und führt Befehle direkt im Arbeitsspeicher aus.
Trojaner	Tarnt sich als nützliches Programm (z. B. Gratis-Spiel), führt im Hintergrund aber Schadfunktionen aus.	Ein kostenloser Videoplayer wird installiert, lädt aber heimlich weitere Schadsoftware aus dem Internet nach.
Ransomware	Verschlüsselt Dateien oder sperrt den Zugriff auf ein System und fordert für die Freigabe meist Lösegeld.	Unternehmensdaten werden verschlüsselt; eine Erpressernachricht fordert Kryptowährung für den Entschlüsselungsschlüssel.
Spyware & Keylogger	Spyware spioniert Nutzeraktivitäten aus. Keylogger zeichnen gezielt Tastatureingaben auf.	Ein Keylogger zeichnet beim Online-Banking heimlich eingegebene Zugangsdaten auf.

Nicht lizenzierter Ausdruck

Schadsoftware-Typ	Funktionsweise	Praxisbeispiel
Adware	Spielt ohne Zustimmung des Nutzers ungewollte Werbeeinblendungen (Pop-ups, Banner) aus oder leitet Suchanfragen um, um Werbeeinnahmen für den Angreifer zu generieren.	Nach der Installation eines Gratis-Programms öffnen sich im Browser ständig ungefragt Werbefenster und die Startseite wurde eigenmächtig geändert.
Bots & Botnetze	Ein **Bot** ist ein infizierter Computer oder ein anderes Gerät, das von Angreifern ferngesteuert werden kann. Mehrere solcher Bots bilden zusammen ein **Botnetz**.	Tausende Bots überlasten gleichzeitig die Server einer Website (DDoS-Angriff).
Cryptojacking	Zweigt heimlich Rechenleistung ab, um im Hintergrund Kryptowährungen zu schürfen.	Ein PC wird plötzlich langsam und der Lüfter läuft ständig, weil der Prozessor im Hintergrund für Cryptomining genutzt wird.
KI-gestützte Malware	Nutzt KI, um Angriffe anzupassen, Schadcode zu verändern oder Sicherheitsmaßnahmen zu umgehen.	Schadsoftware verändert ihr Erscheinungsbild kontinuierlich, um Antiviren-Scans zu umgehen.

3.2 Schutz vor Malware

Antiviren- & Anti-Malware-Software: Scannt Dateien auf bekannte Muster sowie verdächtiges Verhalten.

> *Wichtig:* Kein 100%iger Schutz! Völlig neue oder gezielt veränderte Schadsoftware kann von Schutzprogrammen zunächst übersehen werden.

Regelmäßige Updates: Regelmäßige Updates schließen Sicherheitslücken im Betriebssystem, in Browsern und Apps und können dadurch Angriffe verhindern.

> *Risiko veralteter Software (End of Life):* Programme, die keine Updates mehr vom Hersteller erhalten, können bekannte Sicherheitslücken enthalten und dadurch Angreifern Einfallstore bieten.

Quarantäne-Funktion: Verdächtige Dateien werden vom Schutzprogramm isoliert, damit sie keinen Schaden anrichten können.

Nicht lizensierter Ausdruck

Manuelle Scans und Zeitplanung: Neben dem automatischen Echtzeitschutz können einzelne Ordner oder USB-Sticks jederzeit manuell überprüft werden (z. B. Rechtsklick > *Mit Microsoft Defender überprüfen*).

4. Netzwerke, WLAN, IoT und Sicherheit

4.1 Netzwerke und Verbindungen

- **LAN (Local Area Network):** Netzwerk in einem begrenzten Bereich, z. B. in einer Wohnung, Schule oder einem Büro. Die Verbindung kann über Kabel oder Funk erfolgen.
- **WLAN (Wireless LAN):** Drahtlose Netzwerkverbindung über Funk. Ein WLAN ermöglicht beispielsweise Smartphones, Tablets und Laptops den kabellosen Zugang zu einem lokalen Netzwerk.
- **WAN (Wide Area Network):** Verbindet Netzwerke über große Entfernungen, z. B. verschiedene Unternehmensstandorte. Das Internet ist das bekannteste Beispiel für ein sehr großes WAN.
- **VPN (Virtual Private Network):** Stellt über ein öffentliches Netzwerk, meist das Internet, eine **verschlüsselte Verbindung** zu einem anderen Netzwerk oder Dienst her. Dadurch werden die übertragenen Daten auf dem Weg dorthin besser vor dem Mitlesen geschützt.
    - *Beispiel:* Ein Außendienstmitarbeiter greift auf Reisen im Hotel über eine VPN-Verbindung auf das interne Firmennetz zu.
- **Cloud- & hybride Netzwerke:** Verbinden eigene Systeme mit externen Cloud-Diensten.
    - *Beispiel:* Ein Betrieb speichert bestimmte Daten auf einem eigenen Server vor Ort, nutzt für E-Mail und Videokonferenzen aber Cloud-Dienste im Internet.
- **Netzwerkadministrator:** Verantwortlich für Verwaltung, Zugriffsrechte, Updates und Sicherheit des Netzwerks.
    - *Beispiel:* Die IT-Abteilung richtet Zugänge für neue Mitarbeiter ein, vergibt Berechtigungen für Ordner und installiert Sicherheitsupdates.
- **Firewall:** Überwacht den ein- und ausgehenden Netzwerkverkehr und kann unerlaubte Verbindungen blockieren. Sie schützt Geräte oder Netzwerke beispielsweise vor unerwünschten Zugriffen aus dem Internet.

4.2 Sicherheit von WLANs

WLAN-Sicherheitsstandards

Die **WLAN-Verschlüsselung** schützt die übertragenen Daten vor dem einfachen Mitlesen durch andere Personen im selben WLAN. Welche Sicherheit erreicht wird, hängt unter anderem vom verwendeten **Sicherheitsstandard** und einer sicheren Konfiguration ab.

- **WEP & WPA:** Veraltete Sicherheitsstandards, die heute nicht mehr verwendet werden sollten.
- **WPA2:** Weit verbreiteter Sicherheitsstandard. Bietet bei starkem Passwort guten Schutz.

Nicht lizensierter Ausdruck

- **WPA3:** Moderner WLAN-Sicherheitsstandard mit verbessertem Schutz gegenüber WPA2. Er bietet unter anderem einen besseren Schutz gegen das Erraten von WLAN-Passwörtern und verwendet moderne Verschlüsselungsverfahren.

Zusätzliche WLAN-Schutzmaßnahmen (kein wirksamer Schutz vor Angriffen)

- **MAC-Filterung (veraltet)**: Erlaubt nur Geräten mit festgelegter Hardware-Adresse (MAC-Adresse) den Zugriff.
  Wichtig für die Praxis: **Kein echter Schutz**. MAC-Adressen werden unverschlüsselt übertragen und können von Angreifern leicht herausgefunden und gefälscht werden.
- **SSID verbergen**: Der Name des WLAN-Netzwerks wird unsichtbar geschaltet.
  Bietet keine Sicherheit. Der Netzwerkname lässt sich mit einfachen Werkzeugen innerhalb von Sekunden ermitteln, sobald ein Gerät mit dem WLAN verbindet.

Risiken öffentlicher / ungeschützer WLANs

- **Eavesdropping (Lauschangriff):** Angreifer versuchen, Datenverkehr im selben Netzwerk heimlich mitzulesen. Besonders gefährdet sind Daten, die **nicht verschlüsselt** übertragen werden.

  *Der Begriff **Eavesdropping** stammt vom englischen Wort **„eaves“** (Dachtraufe). Ursprünglich bezeichnete er das heimliche Lauschen unter der Dachtraufe eines Hauses. In der IT steht **Eavesdropping** für das heimliche Abhören oder Mitlesen von Datenverkehr in einem Netzwerk.*

- **Man-in-the-Middle-Angriff:** Ein Angreifer bringt sich unbemerkt zwischen zwei Kommunikationspartner (z. B. dein Smartphone und eine Website) und kann dabei Daten abfangen oder verändern.
  - *Beispiel:* Ein Angreifer stellt ein gefälschtes WLAN mit einem ähnlichen Namen wie das offizielle Hotel-WLAN bereit (Evil Twin). Verbindet sich ein Nutzer damit, kann der Angreifer den gesamten Datenverkehr mitlesen.
- **Code-Injektion** (über unsichere Verbindungen): Der Angreifer nutzt eine unverschlüsselte Verbindung, um bösartigen Code direkt in die übertragenen Webinhalte einzuschleusen.
  - *Beispiel für Code-Injektion***:** Du rufst eine normale Nachrichten-Website auf. Ein Angreifer schleust über das unsichere Netzwerk Schadcode ein, der deinen Browser dazu bringt, gefälschte Werbe-Pop-ups anzuzeigen oder Schadsoftware auf deinen PC herunterzuladen.
- **Netzwerk-Übernahme (Session Hijacking):** Ein Angreifer übernimmt eine bestehende, ungeschützte Sitzung (z. B. eine bestehende Anmeldung auf einer Website), um sich als der berechtigte Nutzer auszugeben und Befehle im fremden Namen auszuführen.
  - *Beispiel*: Ein Nutzer meldet sich im WLAN eines Cafés bei einem Dienst an. Der Angreifer übernimmt diese aktive Sitzung und kann im Namen des Nutzers Nachrichten versenden oder vertrauliche Daten einsehen – ohne das Passwort zu besitzen.

4.3 Persönlicher Hotspot (Tethering)

Das Smartphone stellt seine mobile Internetverbindung anderen Geräten, z. B. einem Laptop, über WLAN zur Verfügung und funktioniert dabei wie ein mobiler WLAN-Router.

Nicht lizensierter Ausdruck

Wichtig: Der persönliche Hotspot sollte immer mit einem **starken Passwort** geschützt sein. Moderne Smartphones verwenden in der Regel **WPA2 oder WPA3**.

4.4 Geräte- und IoT-Sicherheit (Internet of Things)

- **IoT (Internet of Things)** bezeichnet Alltagsgeräte, die mit dem Internet oder einem Netzwerk verbunden sind und Daten austauschen können. Dazu gehören beispielsweise **Smart-TVs, Saugroboter, Fitness-Tracker und Überwachungskameras**.

Schlecht geschützte IoT-Geräte können für Angreifer ein **Einfallstor in das Heim- oder Firmennetzwerk** sein. Werden solche Geräte übernommen, können beispielsweise Daten ausgelesen, Einstellungen verändert oder weitere Geräte im Netzwerk angegriffen werden.

Schutzmaßnahmen:

1. **Standard-Passwörter ändern**: Werkseinstellungen des Herstellers direkt nach der Einrichtung durch ein starkes, individuelles Passwort ersetzen.
2. **Firmware-Updates installieren**: Regelmäßig Firmware- und Sicherheitsupdates installieren. Sie können bekannte Sicherheitslücken schließen und die Sicherheit des Geräts verbessern.
3. **Unnötige Schnittstellen abschalten**: Funktionen wie WLAN, Bluetooth oder Fernzugriff deaktivieren, wenn sie nicht benötigt werden. Dadurch werden unnötige Zugriffsmöglichkeiten für Angreifer vermieden.

5. Anmeldesicherheit und Authentifizierung (Syllabus Modul 4)

5.1 Authentifizierung und Zugangskontrolle

Bei einer Authentifizierung wird die Identität einer Person überprüft – also nachgewiesen, ob jemand tatsächlich derjenige ist, für den er sich ausgibt.

Die 3 Anmelde-Faktoren

- **Wissen** *(Was man weiß):* Passwort, PIN, Sicherheitsfrage.
- **Besitz** *(Was man hat):* Smartphone, Hardware-Token, Chipkarte.
- **Biometrie** *(Was man ist):* Fingerabdruck, Gesichtserkennung, Iris-Scan.

Sicherheitskonzepte & Maßnahmen:

- **Mehrfaktor-Authentifizierung (MFA):** Kombination aus mindestens zwei verschiedenen Anmeldefaktoren. Dadurch erhöht sich die Sicherheit deutlich: Kennt jemand beispielsweise das Passwort, reicht dieses allein nicht für die Anmeldung.
    - Beispiel*:* **Passwort + Bestätigung auf dem Smartphone** = Wissen + Besitz = MFA.
- **Passkeys:** Eine moderne Anmeldemethode, bei der kein herkömmliches Passwort eingegeben werden muss. Ein digitaler Sicherheitsschlüssel auf dem Gerät ermöglicht die Anmeldung. Die Freigabe erfolgt einfach per **Fingerabdruck**, **Gesichtserkennung** oder **Geräte-PIN**.

Nicht lizensierter Ausdruck

- ***Beispiel***: Große Anbieter wie PayPal, Amazon oder Google unterstützen bereits Passkeys. Beim Login entfällt das Passwort komplett: Man bestätigt die Anmeldung einfach per Fingerabdruck, Gesichtserkennung oder Geräte-PIN auf dem Smartphone.

- **Bildschirm sperren:** Beim Verlassen des Arbeitsplatzes das Gerät immer sofort sperren. Unter Windows geht das schnell mit **Windows-Taste + L**.

5.2 Sichere Passwörter und Passwort-Manager

Passwort-Regeln

- **Länge & Komplexität:** Mindestens 12–16 Zeichen nutzen; Kombination aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen wählen.
- **Typische Fallen vermeiden:** Keine Namen, Geburtsdaten, einfachen Zahlenfolgen oder leicht erratbaren Wörter verwenden.

  Unsichere Passwörter: Passwort123, Sommer2026, Klaus1980

- **Einzigartigkeit:** Für jeden Dienst und jedes Konto ein **eigenes Passwort** verwenden. Wird ein Passwort gestohlen, sind andere Konten dadurch nicht automatisch gefährdet.
- **Geheimhaltung:** Passwörter niemals mit anderen Personen teilen – auch nicht mit Kollegen oder Freunden.
- **Zusätzlicher Schutz:** Wo immer möglich, **Mehrfaktor-Authentifizierung (MFA)** aktivieren. Dadurch reicht ein gestohlenes Passwort allein nicht für die Anmeldung.

Ein gutes Passwort ist **lang, einzigartig und geheim** und wird, wenn möglich, durch **Mehrfaktor-Authentifizierung (MFA)** zusätzlich geschützt.

Passwort-Manager

Ein Passwort-Manager verwaltet Passwörter und Zugangsdaten **zentral** und speichert sie verschlüsselt in einem **digitalen Tresor**.

Vorteil: Er generiert für **jeden Dienst** lange, **einzigartige Passwörter** und speichert diese sicher ab.

Bedienung: Man muss sich nur noch ein starkes **Master-Passwort** merken. Dieses darf für keinen anderen Dienst verwendet werden.

Wichtig: Das Master-Passwort darf nicht vergessen oder weitergegeben werden (bei Verlust gibt es meist keine „Passwort vergessen“-Funktion!). Der Passwort-Manager sollte nach Möglichkeit immer zusätzlich mit **MFA** geschützt werden.

- ***Beispiel aus dem Alltag***: Viele Browser (wie Chrome, Firefox oder Edge) und eigene Programme (wie Bitwarden) haben solche Tresore eingebaut.
  Nach dem Entsperren (z. B. mit Passwort, PIN oder Fingerabdruck) werden Zugangsdaten auf Websites automatisch eingetragen.

Nicht lizensierter Ausdruck

6. Sicher im Internet, per E-Mail und mit mobilen Geräten

6.1 Browser und sicheres Surfen

Autovervollständigung: Auf fremden oder öffentlichen Geräten niemals Passwörter oder Formulardaten im Browser speichern.

Sichere Webseiten und Echtheitsprüfung

- **Sicherheitszertifikat (HTTPS) und Inhaber-Prüfung (Validierung):**
    - **Verschlüsselung (HTTPS)**: Sorgt dafür, dass deine Daten verschlüsselt übertragen werden und niemand im Netzwerk mitlesen kann.

      Neu bei modernen Browsern: Das Kürzel https:// und das klassische Schlosssymbol werden in aktuellen Browsern meist ausgeblendet. Stattdessen warnen Browser nur noch aktiv vor unsicheren Seiten (z. B. mit dem Hinweis „Nicht sicher“).
    - **Domain-Inhaber-Prüfung (Validierung)**: Vor der Ausstellung prüft eine unabhängige Zertifizierungsstelle (eine digitale „Passbehörde“), wer der echte Besitzer der Webadresse ist.
    - **WICHTIG**: HTTPS schützt zwar vor dem Mitlesen, garantiert aber nicht, dass die Website ehrlich ist (auch Betrüger nutzen HTTPS-Verschlüsselung).
- **Adresszeile prüfen:** Die Webadresse genau kontrollieren und auf Tippfehler, Buchstabendreher oder ungewöhnliche Domainnamen achten.
    - *Beispiel:* Eine gefälschte Website könnte statt ***bank.at*** eine ähnlich aussehende Adresse verwenden. Exakt auf Buchstabendreher oder Tippfehler prüfen (z. B. Fake-Domains).
- **Anbieter prüfen:** Bei unbekannten oder wichtigen Websites Impressum, Kontaktdaten und andere Angaben zum Anbieter überprüfen.
- **Qualität und Aktualität des Inhalts**:
    - Auf Rechtschreibung, funktionierende Links und ein professionelles Erscheinungsbild achten.
- **Privater Modus (Inkognito):** Speichert den Verlauf und bestimmte andere Browserdaten, wie Cookies, nach dem Schließen des privaten Fensters nicht dauerhaft im normalen Browserprofil auf dem Gerät.

  Aufruf: In den meisten Browsern über das Menü oben rechts (drei Punkte/Striche) oder per Tastenkombination (Strg + Umschalt + N bzw. P bei Firefox) aufrufbar.

  Wichtig: Der private Modus macht nicht anonym im Internet. Beispielsweise können besuchte Websites, der Internetanbieter oder der Betreiber eines Netzwerks Aktivitäten weiterhin erfassen.

6.2 E-Mail-Sicherheit

- **Verschlüsselung:** Verhindert das Mitlesen von Nachrichten auf dem Übertragungsweg.

Nicht lizensierter Ausdruck

- **Digitale Signatur:** Ermöglicht die Prüfung, ob eine Nachricht oder ein Dokument tatsächlich vom angegebenen Absender stammt und ob der Inhalt nach der Signierung verändert wurde.

- Phishing-Checkliste

Bei verdächtigen oder unerwarteten E-Mails besonders aufmerksam sein:

1. **Absenderadresse:** Die vollständige E-Mail-Adresse prüfen – nicht nur den angezeigten Namen. Eine Adresse wie service@beispiel-bank.com kann beispielsweise auf eine gefälschte Website hinweisen.

2. **Dringlichkeit hinterfragen:** Vorsicht bei künstlich erzeugtem Zeitdruck, z. B. *„Ihr Konto wird in 24 Stunden gesperrt!“* Kriminelle wollen dadurch verhindern, dass man in Ruhe nachdenkt.

3. **Links prüfen:** Mit dem **Hover-Effekt** den Mauszeiger über einen Link bewegen, ohne ihn anzuklicken. So lässt sich das tatsächliche Linkziel anzeigen. Bei einer unbekannten oder verdächtigen Adresse den Link nicht öffnen.

   Wichtig: Auch wenn der Inhalt einer E-Mail plausibel erscheint, kann sie gefälscht sein. Eine erwartete Nachricht ist nicht automatisch eine echte Nachricht. Beispielsweise kann eine Nachricht über eine **tatsächlich erwartete Paketsendung** einen gefälschten Link enthalten, über den persönliche Daten oder Zahlungsinformationen gestohlen werden sollen. Bei wichtigen Vorgängen die Website des Anbieters **direkt über die bekannte Adresse oder eine offizielle App** aufrufen, statt den Link in der E-Mail zu verwenden.

4. **Anhänge:** Unerwartete Anhänge nicht öffnen. Besonders vorsichtig bei **ausführbaren Dateien** wie .exe und bei Office-Dokumenten, die zum Aktivieren von **Makros** auffordern.

Meldewege*:* Phishing-Versuche an die betroffene Organisation, den E-Mail-Anbieter oder zuständige Behörden melden.

6.3 Soziale Netzwerke und Mobile Schnittstellen

Soziale Netzwerke: Keine wichtigen persönlichen Daten offenlegen; Datenschutz-, Standort- und Freigabeeinstellungen regelmäßig prüfen. Unangemessenes Verhalten (Cybermobbing, Grooming, Desinformation/Fake News) dem Anbieter oder Behörden melden.

Löschen von Online-Konten: Nicht mehr genutzte Konten (Foren, Social Media) aktiv schließen und Daten löschen. (Wichtig: Das bloße Löschen von Inhalten führt meist nicht zur sofortigen physischen Vernichtung auf den Servern des Betreibers!)

Gefahren in Netzwerken, Begriffe

- **Cybermobbing:** Absichtliches und wiederholtes Beleidigen, Bloßstellen, Belästigen oder Bedrohen einer Person über digitale Medien, z. B. über soziale Netzwerke oder Messenger.

- **Cyber-Grooming:** Gezieltes Kontaktsuchen von Erwachsenen zu Minderjährigen im Internet mit der Absicht, ihr Vertrauen zu erschleichen und sie sexuell zu missbrauchen.

- **Desinformation / Fake News:** Falsche oder irreführende Informationen, die gezielt verbreitet werden, um Menschen zu täuschen, Meinungen zu beeinflussen oder Verunsicherung zu erzeugen.

Nicht lizensierter Ausdruck

Wichtig: Nicht jede falsche Information ist Desinformation. Falsche Informationen können auch **unabsichtlich** weiterverbreitet werden.

Mobile Schnittstellen (GPS, Bluetooth, NFC)

- **GPS:** Ermöglicht die Bestimmung des Standorts eines Geräts und kann dadurch die Erstellung von **Bewegungsprofilen** ermöglichen. App-Zugriffe auf den Standort sollten nur erlaubt werden, wenn sie für die jeweilige Funktion benötigt werden.
- **Bluetooth:** Ermöglicht die drahtlose Verbindung mit Geräten über kurze Entfernungen, z. B. mit Kopfhörern oder einer Smartwatch.
  Bluetooth sollte ausgeschaltet oder für andere Geräte nicht sichtbar sein, wenn es nicht benötigt wird. Unbekannte Kopplungsanfragen niemals annehmen.
- **NFC (Near Field Communication):** Ermöglicht die drahtlose Kommunikation über kurze Entfernungen, z. B. für kontaktloses Bezahlen.
  NFC sollte nur mit vertrauenswürdigen Geräten und Anwendungen verwendet werden.

Notfallplan bei Smartphone-Verlust

1. **Geräteortung:** Über die Ortungsfunktion des Geräts den aktuellen oder zuletzt bekannten Standort auf einer Karte anzeigen lassen. Wenn das Gerät vermutlich gestohlen wurde, nicht selbst zum Standort gehen, sondern die Polizei informieren.
2. **Fernsperrung:** Das Smartphone über einen anderen Computer oder ein anderes Gerät aus der Ferne sperren. Dadurch wird der Zugriff auf die persönlichen Daten erschwert.
3. **Fernlöschung (Remote Wipe):** Dabei werden die auf dem Gerät gespeicherten Daten aus der Ferne gelöscht. Je nach Gerät kann es anschließend auf die Werkseinstellungen zurückgesetzt werden.
4. **SIM-Karte sperren**: Die SIM-Karte beim Mobilfunkanbieter sperren lassen, damit sie nicht für Telefonate, SMS oder mobile Daten missbraucht werden kann.

6.4 Datensicherung und sicheres Löschen

Die 3-2-1-Backup-Regel

- **3 Kopien:** Drei Kopien wichtiger Daten besitzen (1 Original + 2 Backups).
- **2 Medien:** Die Daten auf mindestens zwei unterschiedlichen Speichermedien oder Speichersystemen sichern, z. B. auf einer externen Festplatte und in der Cloud.
- **1 externer Ort:** Mindestens eine Sicherung sollte **an einem anderen Ort** aufbewahrt werden. So geht sie beispielsweise bei einem Brand, Diebstahl oder einer Überschwemmung nicht gleichzeitig mit dem Original verloren.

Backup-Bedingungen & Begriffe:

- Regelmäßige zeitgesteuerte Sicherung.
- Datenkomprimierung: Verringert die Speichergröße der Sicherung.
- Datendeduplizierung: Vermeidet das doppelte Speichern identischer Dateien.

Nicht lizensierter Ausdruck

- Wiederherstellungstest: Regelmäßige Prüfung, ob gesicherte Daten auch tatsächlich wiederhergestellt werden können.

Wichtig: Eine Sicherung ist nur dann hilfreich, wenn sich die Daten im Notfall auch wiederherstellen lassen. Deshalb sollte die Wiederherstellung regelmäßig getestet werden.

Daten löschen vs. vernichten

- **Normales Löschen / Papierkorb leeren:** Die Datei wird in der Regel nicht sofort physisch vom Speichermedium entfernt. Die Daten können unter bestimmten Umständen wiederhergestellt werden.
- **Sicheres Überschreiben:** Der Speicherbereich wird gezielt mit anderen Daten überschrieben. Dieses Verfahren eignet sich insbesondere für Festplatten **(HDDs)**.
- **Degaussieren (Entmagnetisieren):** Ein starkes Magnetfeld löscht die magnetisch gespeicherten Daten auf geeigneten magnetischen Datenträgern, z. B. HDDs. Die Festplatte ist danach in der Regel nicht mehr nutzbar.

  Einschränkung: Funktioniert nur bei magnetischen Medien (nicht bei SSDs, USB-Sticks oder Speicherkarten, da diese Flash-Speicher nutzen).
- **Physische Zerstörung:** Der Datenträger wird geschreddert oder mechanisch zerstört. Dieses Verfahren kann insbesondere bei **defekten Datenträgern oder Datenträgern mit vertraulichen oder besonders sensiblen Daten** eingesetzt werden.

7. Die wichtigsten Grundregeln der IT-Sicherheit

- **1. Starke Passwörter nutzen:** Für jeden Dienst ein eigenes Passwort verwenden (am besten mit einem Passwort-Manager).
- **2. MFA aktivieren:** Wo immer möglich, die Mehr-Faktor-Authentifizierung nutzen.
- **3. Systeme aktuell halten:** Betriebssysteme, Browser und Apps regelmäßig aktualisieren, damit bekannte Sicherheitslücken geschlossen werden.
- **4. Skepsis bei Links & Anhängen:** Keine verdächtigen Links, E-Mails, Nachrichten oder Dateien unüberlegt öffnen. Auch eine Nachricht, die auf den ersten Blick plausibel erscheint, kann gefälscht sein.
- **5. Absender und URLs prüfen:** E-Mail-Adressen und Internetadressen genau kontrollieren und auf Tippfehler, ungewöhnliche Domains oder andere Auffälligkeiten achten.
- **6. Datensparsamkeit:** Persönliche und vertrauliche Informationen nur weitergeben, wenn dies wirklich notwendig ist.
- **7. Vorsicht bei öffentlichem WLAN:** Bei öffentlichen WLANs besonders vorsichtig sein. Für sensible Vorgänge möglichst ein vertrauenswürdiges Netzwerk oder ein VPN verwenden und auf eine verschlüsselte Verbindung achten.
- **8. Backups erstellen:** Wichtige Daten regelmäßig nach der **3-2-1-Regel** sichern.

Nicht lizensierter Ausdruck

- **9. Bildschirm sperren:** Beim Verlassen des Arbeitsplatzes den Computer oder das Smartphone sperren. Unter Windows geht das schnell mit **Windows-Taste + L**.

Denke daran: IT-Sicherheit entsteht durch das Zusammenspiel aus aktueller Technik, sicheren Einstellungen, starken Passwörtern und deiner eigenen Aufmerksamkeit.

Inhalt

1. Grundlagen & Datenschutz 1
1.1 Daten und Informationen 1
1.2 Die drei Grundbegriffe der IT-Sicherheit und wichtige Begriffe der IT-Sicherheit 1
1.3 Ursachen von Bedrohungen 2
1.4 Schutz von Arbeitsdaten und physischer Geräteschutz 2
1.5 Cloud-Dienste 3
1.6 Schutzziele und Datenschutz 3
1.7 Datenschutz-Grundverordnung (DSGVO) 3
1.8 IT-Richtlinien 5
2. Schutz persönlicher Daten, Social Engineering und Programme 5
2.1 Grundbegriffe 5
2.2 Digitale Täuschungs- und Angriffsmethoden 5
2.3 Physische und analoge Angriffe 6
2.4 Manipulative Techniken und KI 7
2.5 Datensicherheit in Programmen 7
3. Gefahren durch Schadsoftware (Malware) 8
3.1 Arten von Malware 8
3.2 Schutz vor Malware 9
4. Netzwerke, WLAN, IoT und Sicherheit 10
4.1 Netzwerke und Verbindungen 10
4.2 Sicherheit von WLANs 10
4.3 Persönlicher Hotspot (Tethering) 11
4.4 Geräte- und IoT-Sicherheit (Internet of Things) 12
5. Anmeldesicherheit und Authentifizierung (Syllabus Modul 4) 12
5.1 Authentifizierung und Zugangskontrolle 12
5.2 Sichere Passwörter und Passwort-Manager 13
6. Sicher im Internet, per E-Mail und mit mobilen Geräten 14
6.1 Browser und sicheres Surfen 14
6.2 E-Mail-Sicherheit 14

6.3 Soziale Netzwerke und Mobile Schnittstellen 15
6.4 Datensicherung und sicheres Löschen 16
7. Die wichtigsten Grundregeln der IT-Sicherheit 17

Nicht lizensierter Ausdruck