IT-Security

Sichere Nutzung der IKT im Alltag

EASY4ME

1. Grundbegriffe zu Sicherheit

1.1. Aus **Daten** werden Informationen

Beispiel: Wir messen die monatlichen Niederschlagsmengen innerhalb eines Jahres.

Januar	60 mm
Februar	55 mm
März	79 mm
April	83 mm
Mai	144 mm
Juni	155 mm
Juli	157 mm
August	151 mm
September	101 mm
Oktober	73 mm
November	83 mm
Dezember	73 mm

Durch die Auswertung dieser **Daten** erhalten wir **Informationen**, z.B.:

- *Wie hoch ist die jährliche Niederschlagsmenge?*
- *In welchen Monaten gibt es besonders hohe/niedrige Niederschlagsmengen?*

Daten sind einzelne, noch nicht ausgewertete Werte.
Informationen entstehen, wenn diese Daten untersucht, in einen Zusammenhang gebracht und dadurch verständlich werden.

1.2. Datenbedrohung

Cybercrime (Internetkriminalität)

Als **Cybercrime** bezeichnet man strafbare Handlungen, die im Internet begangen werden:

- Internetbetrug
- Ausspähen von Daten
- Identitätsdiebstahl
- Eindringen in fremde Netzwerke (Hacking)
- Urheberrechtsverletzungen
- Cyber-Terrorismus
- Cyber-Mobbing
- Volksverhetzung
- Verbreitung von Kinderpornografie

1.3. Die Bedrohung der Datensicherheit von innen

Mitarbeiterinnen und Mitarbeiter können in bestimmten Situationen ein Sicherheitsrisiko für ein Unternehmen darstellen – sei es durch Fahrlässigkeit oder vorsätzliches Verhalten:

- Unsachgemäßer Umgang mit Passwörtern, etwa das Notieren auf Zetteln, die offen zugänglich sind.
- Unzufriedene Mitarbeitende, die sensible Unternehmensdaten absichtlich mitnehmen oder weitergeben.
- Verlust von mobilen Speichermedien oder Geräten, wie USB-Sticks oder Notebooks, die vertrauliche Informationen enthalten.
- Einschleusen von Schadsoftware durch infizierte Datenträger (z. B. USB-Sticks), die unbeabsichtigt ins Firmennetzwerk eingebracht werden.

Aktuelle Beispiele:

- *Eine Bankmitarbeiterin möchte vertrauliche Unterlagen zu Hause weiterbearbeiten und schickt sich diese an die eigene E-Mail-Adresse. Leider vertippt sie sich und wählt die falsche Adresse aus.*
- *Ein Mitarbeiter bekommt einen USB-Stick als „Werbegeschenk“. Beim Anschließen installiert er unabsichtlich ein Spionageprogramm.*
- *Ein E-Mail-Anhang enthält ein Word-Dokument. Beim Öffnen aktiviert der Mitarbeiter Makros, wodurch Malware installiert wird, die alle erreichbaren Daten verschlüsselt. Das Unternehmen wird anschließend erpresst und muss Geld für die Entschlüsselung zahlen.*

Prävention (Vorbeugung)

Um solche Fälle zu vermeiden, werden in firmeninternen Schulungen Mitarbeiter über **IT-Sicherheitsstrategien und Richtlinien zur sicheren Nutzung der EDV** informiert.

1.4. Informationen sind wertvoll

Personenbezogene Daten sind z. B. **Bankkonto-Daten, Geburtsdatum, Wohnadresse, E-Mailadresse, Telefonnummer, Einkommen, Beruf, Religionsbekenntnis.**

Risiken bei der Nutzung persönlicher Daten im Internet

- **Unerwünschte Werbenachrichten (Spam):** Persönliche E-Mail-Adressen können in den Umlauf geraten und für den massenhaften Versand von Werbemails genutzt werden.
- **Verlust der Kontrolle über veröffentlichte Daten:** Einmal online gestellte Informationen lassen sich kaum mehr vollständig entfernen und können an unerwünschten oder unkontrollierbaren Orten wieder auftauchen.
- **Gefährdung von Kindern und Jugendlichen:** Minderjährige sind besonders schutzbedürftig, da sie online leicht von Erwachsenen mit betrügerischen oder schädlichen Absichten kontaktiert und belästigt werden können.
- **Identitätsdiebstahl und -missbrauch:** Kriminelle können persönliche Daten stehlen und in fremdem Namen Waren bestellen, Kredite aufnehmen oder durch gefälschte Nachrichten (z. B. E-Mails) Rufschädigung betreiben.

Beispiele für Identitätsmissbrauch und Datenmissbrauch:

- ***Identitätsdiebstahl in sozialen Netzwerken:***
  Eine Frau wird von Freunden darauf hingewiesen, dass auf Facebook ein Profil mit ihrem Namen und ihren Fotos existiert. Auf dieser Seite werden rufschädigende Beiträge über sie und ihren Arbeitgeber veröffentlicht.

- ***Betrug durch gefälschte Bestellungen:***
  Eine Frau erhält Mahnungen von Inkassobüros für Online-Bestellungen, die sie nie getätigt hat. Erst durch Nachforschungen erfährt sie, dass Betrüger in ihrem Namen Waren bestellt und nicht bezahlt haben.
- ***Skimming am Bankomaten:***
  Herr S. stellt bei der Kontrolle seiner Kontoauszüge fest, dass im Ausland Bargeld mit seiner Bankomatkarte abgehoben wurde. Die Bank informiert ihn, dass seine Karte an einem manipulierten Geldautomaten kopiert (Skimming) und sein PIN bei der Eingabe ausgespäht wurde.

1.5. Wie kann ich meine Daten schützen?

- **Sichere Passwörter:**
  - Bestehen aus mindestens acht Zeichen, kombiniert aus Buchstaben, Zahlen und Sonderzeichen.
  - Keine leicht zu erratenden Passwörter wie Geburtsdaten, Namen von Angehörigen oder einfache Zahlenfolgen.

  Beispiele

  - **Gutes Passwort**: `mVi1982g!` (Merkhilfe: **m**ein **V**ater ist **19**82 **g**eboren**!**)
  - **Schlechte Passwörter**: `12345 qwertz geheim hallo boss passwort` …

  Eine Verschlüsselung ist nur so sicher wie das Passwort: Das Passwort soll geheim bleiben und regelmäßig geändert werden.

  Du kannst die Sicherheit eines Passworts z. B. hier online überprüfen:
  www.wiesicheristmeinpasswort.de

Tipps zum sicheren Umgang mit Passwörtern und sensiblen Daten

- **Verwende für jeden Zugang ein eigenes Passwort!** Wenn überall dasselbe Passwort genutzt wird, können Betrüger mit nur einem gestohlenen Passwort auf mehrere Konten zugreifen.
- **Nutze einen Passwort-Manager:**
  Passwort-Manager speichern Anmeldedaten wie Benutzernamen und Passwörter verschlüsselt auf deinem Gerät. Du musst dir nur ein einziges, starkes Master-Passwort merken – damit erhältst du Zugriff auf alle gespeicherten Zugangsdaten.
  Empfehlung: Der kostenlose Passwort-Manager **KeePass**.
- **Verschlüssle Daten auf mobilen Geräten:**
  Notebooks, Tablets und Smartphones können leicht verloren gehen oder gestohlen werden. **Oft ist der Verlust sensibler Daten schwerwiegender als der materielle Schaden des Geräts**. Eine Datenverschlüsselung schützt deine Informationen im Ernstfall.
- **Sicherer Umgang mit Cloud-Diensten:**
  Die Speicherung von Daten in der Cloud bietet Komfort, birgt jedoch auch Risiken. Gelangen Zugangsdaten in falsche Hände, sind unautorisierte Zugriffe möglich. Zudem gibst du mit der Cloud-Nutzung einen Teil der Kontrolle über deine Daten ab – daher sollten besonders sensible Informationen gut geschützt oder gar nicht erst in der Cloud gespeichert werden.

Beispiele aus den Schlagzeilen:

- *Persönliche Daten von acht Millionen Hotelgästen gestohlen*
- *Notebook-Schwund in Ministerien*
- *Britisches Verteidigungsministerium: wieder 28 Notebooks verschwunden*
- *Kontakt-App gehackt: Fotos, Führerscheine und private Chats veröffentlicht*

1.6. Datensicherheit

Für Unternehmen sind insbesondere **Kundendaten** und **Finanzdaten** von hoher Bedeutung:

- Gelangen Kundendaten in falsche Hände, können sie für Werbung missbraucht oder sogar für Betrug (z. B. Kreditkartendaten) verwendet werden.
- Finanzdaten können Konkurrenten wertvolle Einblicke in die wirtschaftliche Lage eines Unternehmens geben.

1.7. Die drei Schutzziele der Datensicherheit

1. Vertraulichkeit

Daten dürfen nur von autorisierten Personen eingesehen werden.

Maßnahmen:

- Verschlüsselung gespeicherter Daten
- Verschlüsselte Übertragung (z. B. E-Mail, Chat, Online-Banking)
- Zugriffsrechte für autorisierte Anwender.

Beispiele

- *Krankenakten: Zugriff nur für behandelndes medizinisches Personal, nicht für alle Beschäftigten eines Krankenhauses*
- *Adresslisten von Schülern: dürfen nicht an schulfremde Personen oder Firmen weitergegeben werden*
- *Notebooks: sollten stets verschlüsselt.*

2. Integrität

Daten müssen **vollständig und unverändert** bleiben.

- Veränderungen können unbeabsichtigt (z. B. technischer Fehler) oder absichtlich erfolgen.
- Unautorisierte Änderungen sind streng verboten**.**

Beispiel:

Eine Frau wurde versehentlich für tot erklärt. Nach dem Tod ihrer Mutter wurden in der Datenbank auch ihre eigenen Daten gelöscht – mit der Folge, dass ihre Pension ausblieb.

3. Verfügbarkeit

Daten müssen **zuverlässig zugänglich** sein, auch bei technischen Problemen. Systemausfälle sollen daher möglichst verhindert werden.

Beispiel:

Österreichweit kam es an einem Dienstag zu Ausfällen von Bankomaten. Elektronische Zahlungen waren stundenlang nicht möglich und konnten erst am Nachmittag wiederhergestellt werden.

1.8. Personenbezogene Daten sind gesetzlich geschützt

Die **EU-Datenschutz-Grundverordnung (DSGVO)** regelt den Schutz personenbezogener Daten wie z. B. **Adresse, Geburtsdatum, Telefonnummer, Religionsbekenntnis** etc.

In der DSGVO wird unterschieden:

Nicht besonders schutzwürdige Daten:

- Name
- Geburtsdatum
- Geburtsort
- Wohnort eines Menschen

Besonders schutzwürdige Daten:

- Rassische und ethnische Herkunft
- Politische Meinung
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheitsdaten, genetische und biometrische Daten
- Sexualleben oder sexuelle Orientierung

Diese besonders schutzwürdigen Daten dürfen nur mit ausdrücklicher Zustimmung verarbeitet werden (Ausnahmen für Behörden wie Polizei sind möglich).

1.9. Wichtige Rechte und Grundsätze der DSGVO

- **Datengeheimnis:**
  Personenbezogene Daten dürfen grundsätzlich nur mit ausdrücklicher Zustimmung der betroffenen Person weitergegeben werden – Ausnahmen gelten nur in gesetzlich genau geregelten Fällen.
- **Recht auf Auskunft:**
  Jede Person hat das Recht, Auskunft darüber zu erhalten, welche personenbezogenen Daten über sie gespeichert sind und wie diese verarbeitet werden
- **Grundsatz der Transparenz:**
  Betroffene müssen nachvollziehen können, welche Daten von welcher Organisation zu welchem Zweck und auf welche Weise verarbeitet werden.
- **Notwendigkeit und Verhältnismäßigkeit:**
  Es dürfen nur solche Daten erhoben und verarbeitet werden, die für den jeweiligen Zweck tatsächlich erforderlich sind. Der Umfang der Datenverarbeitung muss in einem angemessenen Verhältnis zum angestrebten Zweck stehen.

Fachbegriffe

- **Verantwortlicher** ist eine Person oder Organisation, die darüber entscheidet, welche personenbezogenen Daten gespeichert werden (z.B. der Firmenchef).
- **Auftragsverarbeiter**: Person oder Organisation, die die Daten speichert (z.B. Buchhalter).
- **Betroffener**: Person, deren Daten gespeichert wurden und die Auskunft verlangen kann.

Recht auf Richtigstellung oder Löschung:

Wenn Daten falsch oder unrechtmäßig gespeichert wurden, kann deren Korrektur oder Löschung verlangt werden.

***Beispiel**: Herr X möchte einen Handyvertrag abschließen, der ihm verweigert wird. Er nützt sein Recht auf Auskunft und erfährt, dass er durch eine Verwechslung als unzuverlässiger Schuldner in einer Datenbank eingetragen ist. Er beantragt die Löschung dieses Eintrags.*

Verarbeitung von Daten

„**Verarbeitung von Daten**“ bedeutet jede Handlung, die mit personenbezogenen oder anderen Daten vorgenommen wird – egal ob automatisch (z. B. per Computer) oder manuell (z. B. auf Papier).

Verarbeitung umfasst vor allem:

- **Erheben** (z. B. Online-Formular ausfüllen)
- **Speichern** (z. B. in einer Datenbank)
- **Ordnen und Strukturieren**
- **Ändern oder Anpassen**
- **Abrufen** oder **Abfragen**
- **Verwenden** (z. B. zur Kundenbetreuung)
- **Übermitteln** (z. B. an andere Firmen)
- **Löschen oder Vernichten**

Alles, was mit Daten passiert - von der Erfassung bis zur Löschung - ist eine Verarbeitung.

1.10. Datensicherheit – Strategien, Backups und Schutzmaßnahmen

Warum braucht Datensicherheit Strategie und Planung?

Datenverarbeiter müssen sicherstellen, dass Daten

- sicher gespeichert werden und
- vor unbefugtem Zugriff geschützt sind

Dazu braucht es technische Vorkehrungen und organisatorische Maßnahmen:

Datensicherung (Backup): Schutz vor Datenverlust

Unvorhersehbare Ereignisse wie Brand, Hochwasser, Erdbeben, Diebstahl oder Schadsoftware (z. B. Ransomware) können IT-Systeme und wichtige Daten zerstören.
Besonders für Unternehmen kann der Verlust von Daten schwerwiegende Folgen haben:

- Verlust von Kunden- und Geschäftsdaten
- Zahlungsrückstände können nicht eingefordert werden
- Produktionsausfälle und Betriebsunterbrechungen

Nur eine durchdachte **Backup-Strategie** schützt vor dauerhaftem Datenverlust.
Bestandteile einer Backup-Strategie:

- **regelmäßige Datensicherungen** nach einem festgelegten Zeitplan
- **dokumentierte Ablaufpläne**, die festlegen, wie Sicherungen erstellt und im Notfall wiederhergestellt werden
- **räumlich getrennte Aufbewahrung der Backups**, um diese vor denselben Gefahren wie die Originaldaten zu schützen

Backup-Methoden:

- **Herkömmliche Backups**: Speichern auf externen Datenträgern (z. B. SSDs, Festplatten), die sicher aufbewahrt werden
- **Online-Backups (Cloud-Backup):** Verschlüsselte Datenübertragung an Backup-Server in Rechenzentren

Aufbewahrung der Backups je nach Nutzergruppe:

- **Privatpersonen**: Externe Festplatten, sicher verstaut
- **Kleine Unternehmen**: z. B. Bankschließfächer oder Cloud-Dienste
- **Große Organisationen**: Feuersichere Datensafes, redundante (mehrfache) Speicherung an verschiedenen Standorten oder Rechenzentren

Unterbrechungsfreie Stromversorgung (USV): Schutz bei Stromausfall

Eine USV stellt bei einem Stromausfall kurzfristig Energie bereit, damit Systeme ordnungsgemäß heruntergefahren oder weiter betrieben werden können.

- **Server**: Weiterbetrieb durch USV
- **Notebooks**: Stromversorgung über den Akku

1.11. IT-Sicherheitsstrategie

IT-Sicherheitskonzept – Grundlage für den Schutz von Systemen und Daten
Ein IT-Sicherheitskonzept ist der übergeordnete Plan eines Unternehmens zum langfristigen Schutz seiner IT-Infrastruktur und sensiblen Daten.

Es umfasst:

- Beschreibung möglicher Risiken und Bedrohungen,
- **geeignete Schutzmaßnahmen**,
- **Maßnahmen im Notfall** (z. B. bei Cyberangriffen oder Systemausfällen).

Ziel:

Den sicheren, zuverlässigen und unterbrechungsfreien Betrieb der IT-Systeme sicherstellen sowie vertrauliche Informationen vor unbefugtem Zugriff, Verlust oder Missbrauch schützen.

1.12. IT-Sicherheitsrichtlinie und -plan

- **IT-Sicherheitsrichtlinie:** legt allgemeine Ziele, Regeln und Verantwortlichkeiten fest
- **IT-Sicherheitsplan:** beschreibt konkrete Maßnahmen, z. B. Regeln für Mitarbeiter

Beispiele für Maßnahmen:

- Passwörter müssen mindestens 12 Zeichen haben und Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen enthalten.
- Die Verwendung privater USB-Sticks ist nicht erlaubt.
- Zugangsdaten dürfen nicht weitergegeben werden. Jeder Mitarbeiter meldet sich nur mit eigenem Login an.

1.13. Zugriffsrechte

Nicht jeder Mitarbeiter hat Zugriff auf alle Daten: Nach der Anmeldung weist das Computersystem dem Benutzer entsprechende Zugangsrechte zu.

Beispiele:

- Lagerarbeiter: Zugriff auf Lagerbestand, aber keine Preisänderungen
- Personalchef: Zugriff auf Mitarbeiterdaten, aber nicht auf den Lagerbestand

Der Datenbankadministrator vergibt **abgestufte Zugriffsrechte** an die Mitarbeiter.

1.14. Persönliche Sicherheit – Methoden von Angreifern

Social-Engineering und Pretexting

Angreifer manipulieren Menschen oder geben sich gezielt als jemand anderes aus, um Informationen zu erschleichen.

Beispiele:

- *Ein angeblicher Techniker ruft an und verlangt geheime Zugangsdaten.*
- *Die Buchhaltung erhält eine gefälschte E-Mail vom „Chef“ mit der Anweisung, Geld ins Ausland zu überweisen. (Signierte E-Mails würden solche Betrugsversuche verhindern.)*

1.15. Phishing

Gefälschte E-Mails fordern zur Eingabe von Zugangsdaten auf einer falschen Website auf.

Beispiel:

Frau X erhält ein E-Mail von ihrer Bank, dass ihr Konto gesperrt wird. Sie soll sich mit ihren Zugangsdaten anmelden, um diese Sperre aufzuheben.

Weitere Bedrohungen:

- **Shoulder Surfing**:
  Beobachtung von Passworteingaben oder anderen sensiblen Informationen in der Öffentlichkeit – z. B. über die Schulter oder durch versteckte Kameras.
- **Identitätsdiebstahl:**
  Missbrauch personenbezogener Daten, z. B. durch Phishing oder gestohlene Dokumente, um sich als eine andere Person auszugeben.
- **Information Diving** (auch: Dumpster Diving): Entnahme sensibler Informationen aus ungesichertem Müll – z. B. ungeschredderte Akten, Adresslisten, Kontoauszüge oder Briefe.
- **Man-in-the-Middle-Angriff**:
  Angreifer schalten sich unbemerkt zwischen Nutzer und Website, um Daten zu manipulieren oder auszuspähen – z. B. beim Online-Banking, um Überweisungen zu ändern.
- **Browser-Hijacker:**
  Schädliche Programme, die Browser-Einstellungen verändern und Nutzer auf unerwünschte Webseiten umleiten.

  ***Beispiel**: AnySearchManager:*

  ***Funktion**: Ändert die Standardsuchmaschine und Startseite des Browsers auf eigene Dienste wie search.anysearchmanager.com.*

  ***Verbreitung**: Häufig über kostenlose Software-Downloads.*

  ***Ziel**: Erzeugung von Werbeeinnahmen durch manipulierte Suchergebnisse und Verfolgung des Nutzerverhaltens.*

  Entfernung:
  - *Alle zugehörigen Programme deinstallieren*
  - *Verdächtige Browser-Erweiterungen entfernen*

- *Browser-Einstellungen (Startseite, Suchmaschine) zurücksetzen*
- *Hinweise zur Rücksetzung finden sich auf den offiziellen Webseiten der Browserhersteller.*

1.16. Sicherheit für Dateien durch Verschlüsselung

Eine Verschlüsselung macht Dateien unleserlich. Nur wer den Schlüssel kennt, kann die Datei wieder lesbar machen.

Beispiel für die *Verschlüsselung* eines Klartextes in einen Geheimtext:

```
Dies ist ein Klartext und er wird nun verschluesselt
GLHVLVWHLQNODUWHAWXQGHUZLUGQXQYHUVFKOXHVVHOW
```

Arten der Verschlüsselung

1. Verschlüsselung auf Dateiebene

Beschreibung: Einzelne Dateien werden beim Speichern oder Komprimieren mit einem Passwort geschützt.
Nachteil: Sehr umständlich bei einer großen Anzahl von Dateien.

***Beispiele**:*

- **Microsoft Office**
  1. Datei > Speichern unter
  2. Schaltfläche „Tools“ > Allgemeine Optionen
  3. Passwort vergeben
- **Ordner-Verschlüsselung in Windows**
  1. Rechtsklick auf den gewünschten Ordner
  2. Eigenschaften > Allgemein > Erweitert
  3. Häkchen bei „Inhalt verschlüsseln, um Daten zu schützen“ setzen

Hinweis: Windows verwendet die Benutzeranmeldung zur Verschlüsselung. Andere Benutzer desselben PCs haben keinen Zugriff auf diese Daten.

2. Laufwerks- bzw. Festplattenverschlüsselung

- **Beschreibung**: Ganze Laufwerke oder Partitionen werden verschlüsselt. Der Zugriff ist nur nach Eingabe des Passworts oder mit der richtigen Benutzeranmeldung möglich.
- **Vorteile**:
  - Läuft im Hintergrund, ohne den Benutzer im Alltag einzuschränken.
  - Bei Diebstahl bleiben die Daten unlesbar.
- **Beispiele**:
  - **BitLocker**: In Windows Pro, Enterprise und Education integriert.
  - **VeraCrypt**: Kostenlose, leistungsstarke Open-Source-Alternative.

2. Malware (Schadsoftware)

2.1. Computervirus

Verbreitet sich über infizierte Programme, Dokumente oder Datenträger. Aktiviert sich meist erst, wenn die infizierte Datei geöffnet oder ausgeführt wird.

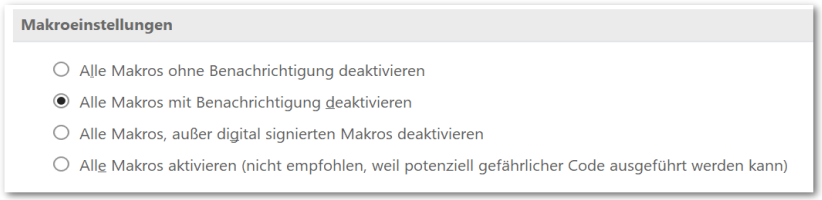
2.2. Wurm

Breitet sich selbstständig über Netzwerke aus und versucht, in andere Computer einzudringen – ohne Benutzerinteraktion.

2.3. Makroviren

Eingebettet in Office-Dokumente wie Word oder Excel.
Makros sind eigentlich harmlose Hilfsprogramme zur Automatisierung von Aufgaben.
Makroviren nutzen diese Funktionen jedoch aus, um weitere Schadsoftware aus dem Internet herunterzuladen und zu installieren.

Tipp: Die Ausführung von Makros lässt sich über die Makro-Sicherheitseinstellungen in Office gezielt steuern.



2.4. Trojaner (kommt von Trojanisches Pferd)

Tarnen sich als nützliche Programme, installieren im Hintergrund jedoch Malware.

Beispiel:
Herr L. lädt ein vermeintlich hilfreiches Tool von einer Webseite herunter, das angeblich die PC-Leistung verbessert. Tatsächlich installiert es heimlich Schadsoftware.

2.5. Ransomware (Erpressungs- oder Kryptotrojaner)

Verschlüsselt Dateien auf dem Gerät und fordert ein Lösegeld zur Entschlüsselung.

***Beispiel*:**
Herr S. erhält eine E-Mail mit einer gefälschten Rechnung eines Energieunternehmens. Nach dem Öffnen des Anhangs erscheinen zunächst nur Fehlermeldungen. Wenige Tage später sind alle seine Dateien verschlüsselt – er soll mehrere hundert Euro für den Zugriff zahlen.

2.6. Rootkit

Versteckt Malware vor dem Benutzer und sogar vor Antivirenprogrammen, um deren Entdeckung und Entfernung zu verhindern.

2.7. Keylogger

Zeichnen alle Tastatureingaben auf – einschließlich Passwörtern und sensibler Daten.

2.8. Backdoor (Hintertür)

Ermöglicht Angreifern den Fernzugriff auf das infizierte System.
Typische Funktionen:

- Dateien versenden oder löschen
- Programme ausführen
- Daten ausspähen
- Computeraktivitäten protokollieren

2.9. Spyware

Spioniert das Verhalten der Nutzer aus und sendet die gesammelten Daten an Dritte – meist ohne Wissen des Betroffenen.

2.10. Adware

Blendet unerwünschte Werbung ein, häufig in Form von Pop-ups oder Weiterleitungen.

2.11. Scareware

Täuscht dem Nutzer eine Bedrohung (z. B. Virenbefall) vor, um ihn zu einem Kauf oder Download (meist unnützer Software) zu bewegen.

2.12. Dialer

Wählen unbemerkt teure Sonderrufnummern, was zu hohen Kosten führen kann – besonders bei alten Modem- oder ISDN-Verbindungen.

2.13. Botnets

Von Malware infizierte Computer werden heimlich zu einem Netzwerk zusammengeschlossen und vom Angreifer ferngesteuert – oft ohne Wissen der Besitzer. Sie werden für Zwecke wie Spamversand, DDoS-Angriffe oder Datenklau missbraucht.

2.14. Schutz vor Malware

Antivirenprogramme – Schutz vor bekannter Schadsoftware

Funktionen:

- Erkennen, blockieren und entfernen bekannter Schadsoftware

Regelmäßige Updates:

- Da täglich neue Viren entstehen, lädt die Software aktuelle Virensignaturen vom Hersteller herunter
- Nur durch Updates bleibt der Schutz wirksam.

Einschränkung:

- Erkennung in der Regel nur bei bereits bekannten Bedrohungen
- Vorsichtiges Nutzerverhalten bleibt daher unerlässlich

Umgang mit infizierten Dateien:

- **Reinigung**: Versuch, befallene Dateien zu reparieren
- **Quarantäne**: Falls Reinigung nicht möglich ist, werden Dateien isoliert, um Schaden zu verhindern

Fehlalarme:

- Gelegentlich werden harmlose Dateien fälschlich als Bedrohung erkannt

Software-Updates

- Programme und Betriebssysteme immer **aktuell** halten.
- **Veraltete Software** (z. B. Windows 7) birgt hohe Sicherheitsrisiken.

3. Sicherheit im Netzwerk

3.1. Netzwerke verbinden Computer

Netzwerktypen

- **LAN** (Local Area Network): verbindet Rechner in einem Netz. Typisch für Schulen, Firmenstandorte und Heimnetzwerke.
- **WLAN**: **W**ireless **L**ocal **N**etwork: kabelloses lokales Funknetzwerk. Viele mobile Geräte wie Smartphones, Tabletts oder Notebooks werden über WLAN mit dem Internet verbunden.
- **WAN** (Wide Area Network) ist ein Rechnernetz, das sich im Unterschied zu einem LAN über einen sehr großen geografischen Bereich erstreckt.
- **VPN** (**V**irtual **P**rivate **N**etwork) ist eine verschlüsselte Verbindung über das Internet (z. B. für Firmenzugriff von zuhause).

3.2. Datensicherheit im Netzwerk

Ein Netzwerkzugang bietet den Zugriff auf gemeinsame Ressourcen wie Daten, Netzwerkdrucker und andere Serverdienste. Eine Authentifizierung ermöglicht nur berechtigten Benutzern den Zugang.

- **Authentifizierung**: Benutzername + Passwort.
  Multi-Faktor-Authentifizierung kombiniert:
- **Wissen** (Passwort)
- **Besitz** (Smartphone, Token)
- **Biometrie** (Fingerabdruck, Gesicht).
- **Benutzerrechte**: legen fest, was ein User sehen oder bearbeiten darf.
- **Nutzungsdokumentation:** Zugriffe auf sensible Daten werden protokolliert.
  ➔ Bsp.: *Polizist in Österreich wegen unbefugter Datenabfrage verurteilt*

Sicherheitstipp: Verlässt man den Computerarbeitsplatz, sollte man sich entweder abmelden oder den Zugang sperren (unter Windows: mit Win + l).

3.3. Firewall

- Schutz vor Angriffen aus dem Netzwerk.
- Blockiert unerwünschte Datenpakete, lässt nur angeforderte durch.
- **Standardmäßig aktiv** in modernen Betriebssystemen.
- Nur begrenzt wirksam bei bereits infiziertem System (z. B. Spyware)

3.4. Netzwerkverbindungen

- Verbindung per Kabel oder WLAN, Funkverbindung.
- Jede Netzwerkanbindung ist potenzielles Angriffsziel – Angriff von außen.

3.5. Drahtlose Netzwerke – Sicherheit und Verschlüsselung (WLAN)

Grundprinzip

Drahtlose Netzwerke sollten **immer verschlüsselt** werden, um unbefugten Zugriff zu verhindern.

- Der Benutzer meldet sich mit einem Passwort an und wird mit dem Funknetz verbunden.
- Nur autorisierte Personen haben Zugang.
- Durch die Verschlüsselung können Dritte keine Informationen aus dem Datenverkehr auslesen.

Zur Absicherung von WLANs stehen verschiedene Sicherheitsprotokolle zur Verfügung:

- **WPA (veraltet) / WPA2 (Wi-Fi Protected Access):** Verschlüsseln den Datenverkehr und bieten grundlegenden Schutz.
- **WPA3:** Aktuellster Standard, höhere Sicherheit und einfachere Handhabung
- **Offene Netzwerke (z. B. in Flughäfen oder Cafés):** Jeder kann sich verbinden, daher besonders unsicher.
    - HTTPS (erkennbar an *https://* in der Browserzeile) bietet eine gewisse Absicherung.
    - Trotzdem: In öffentlichen WLANs keine sensiblen Aktivitäten (z. B. Online-Banking) durchführen.

Zusätzliche Absicherung: MAC-Filter

- Zugriff nur für Geräte mit zugelassener **MAC-Adresse** (eindeutige Hardwarekennung, z. B. CC-52-AF-40-A0-1F).
- *Vorteile*: Geräte lassen sich eindeutig identifizieren.
- *Nachteile*: Verwaltung aufwendig, zudem können MAC-Adressen relativ leicht gefälscht werden.

- **MAC-Filter** **MAC-Filter** können den Zugang zum Netzwerk auf Geräte mit bestimmten MAC-Adressen (Media Access Control) beschränken.
  Jede Netzwerkschnittstelle besitzt eine eindeutige MAC-Adresse (*z. B. CC-52-AF-40-A0-1F)*. Diese Methode identifiziert Geräte im Netzwerk eindeutig, ist jedoch umständlich zu verwalten – zudem lassen sich MAC-Adressen relativ leicht fälschen.

3.6. Man-in-the-Middle-Angriffe:

- Angreifer lesen oder manipulieren Datenverkehr zwischen Benutzer und Website.
- **Schutz:** Verwendung sicherer Verbindungen über **HTTPS**.
- **Hinweis:** Browser warnen, wenn unsichere Umleitungen oder Verbindungen bestehen.

4. Sichere Web-Nutzung

Einkaufen im Internet

Beim Online-Einkauf werden häufig sensible Zahlungsdaten wie Kreditkartennummern übermittelt. Zudem kann es zu Problemen mit dem gekauften Produkt kommen, etwa bei einer fehlenden oder mangelhaften Lieferung."

4.1. Seriöse Webshops erkennen

- **Impressum prüfen:** vollständige Kontaktangaben (Telefon, E-Mail, Adresse)
  Kein Einkauf ohne vollständiges Impressum!
- Klare Produkt-, Versand- und Zahlungsinformationen
- Die **Webseite soll sicher** sein, das **Sicherheitszertifikat** (links neben der URL) aufrufen.
- Positive Bewertungen

4.2. Vertrauenswürdigkeit einer Website überprüfen:

- URL genau prüfen
- Sicherheitszertifikat (Schloss-Symbol links neben URL) anzeigen
- Domain-Inhaberschaft abfragen (z. B. ***www.whois.com***)

Sichere Webseiten

- Beginnen mit **https**:// (Hypertext Transfer Protocol Secure).
- Schloss-Symbol vor der URL zeigt verschlüsselte Datenübertragung an.
- Digitale Zertifikate von unabhängigen Zertifizierungsstellen (z. B. GlobalSign, Verisign) bestätigen Identität und Gültigkeit.
  Klicke auf das Vorhangschloss, um Informationen über die Webseite zu erhalten!

4.3. Begriffe zur Sicherheit im Internet:

- **Einmal-Kennwörter (z. B. TAN):** Nur einmal nutzbar, z. B. für Online-Banking (2-Faktor-Authentifizierung).
  ***Beispiel**: Beim Online-Banking wird eine TAN (Transaktionsnummer) per SMS auf das Handy des Bankkunden gesandt. Dies erhöht die Sicherheit wesentlich, weil zwei voneinander unabhängige Übertragungswege – Internet und Handynetz – verwendet werden.*
- **Pharming:** DNS-Manipulation, um Nutzer trotz richtiger Adresse auf gefälschte Seiten umzuleiten.
- **Cross Site Scripting (XSS):** Manipulierte Webseitendaten, die Benutzereingaben umleiten oder ausspionieren.

4.4. Browser-Funktionen & Sicherheit

- **Automatisches Ausfüllen von Formulardaten:** Praktisch, aber Risiko bei fremden Geräten (z. B. Kreditkartendaten, Passwörter).

  Edge: Einstellungen → Profile
  Firefox: Einstellungen → Datenschutz & Sicherheit

- **Cookies**: Speichern z. B. Login-Informationen. Sinnvoll, aber auf fremden PCs sollten Cookies gelöscht werden:

  Edge: Einstellungen → Datenschutz, Suche und Dienste → Browserdaten löschen
  Firefox: Einstellungen → Datenschutz & Sicherheit → Cookies und Website-Daten

- **Verlauf & temporäre Dateien:**
  Speichern besuchte Seiten, Passwörter und Formulardaten → bei Nutzung fremder PCs unbedingt löschen.
- **Blockieren/Zulassen von Cookies**:
  Edge: Einstellungen → Cookies und Websiteberechtigungen
  Firefox: Einstellungen → Datenschutz & Sicherheit → Cookies und Website-Daten
- **Kinderschutz:**
  Um Kinder vor ungeeigneten Inhalten im Internet zu schützen und ihre Online-Zeit zu begrenzen, können Inhaltefilter und Kindersicherungen verwendet werden.

  Unter Windows lässt sich für jedes Kind ein eigenes Benutzerkonto einrichten, in dem sowohl inhaltliche als auch zeitliche Beschränkungen festgelegt werden können.

5. Soziale Netzwerke

5.1. Fallbeispiele für Missbrauch & Fehlverhalten

- **Bekanntgabe der E-Mail-Adresse:** führt zu unerwünschten Nachrichten (Spam, Belästigung).
- **Peinliche Fotos** in sozialen Netzwerken können kopiert und weiterverbreitet werden.
- **Negative Auswirkungen bei Bewerbungen**: Unvorteilhafte Fotos führen zu Ablehnungen.
- **Cyber-Mobbing:** Beleidigungen, Gerüchte, bearbeitete Fotos.
- **Verbreitung intimer Fotos** ist strafbar (Kinderpornografie, sexuelle Belästigung).
- **Rassistische Äußerungen & Drohungen**.

5.2. Sicherer Umgang mit sozialen Netzwerken

- Persönliche Daten (Adresse, Tel., Geburtsdatum) sparsam angeben.
- Keine peinlichen Fotos posten.
- Inhalte sind oft nicht endgültig löschbar.
- Freundschaftsanfragen prüfen (nur echte Bekannte).
- Privatsphäre-Einstellungen regelmäßig prüfen.
- Missbrauch und Fehlverhalten immer melden (Provider/Behörden).

5.3. Fachbegriffe

- **Cyber-Mobbing:** Mobbing über elektronische Medien.
- **Cyber-Grooming:** Kontaktaufnahme mit Kindern/Jugendlichen mit sexuellen Absichten.
- **Falsche Identität:** Personen geben sich als jemand anderes aus.
- **Arglistige Links/Nachrichten** führen zu Malware-Seiten.

Mit etwas Vorsicht lassen sich die Vorteile sozialer Netzwerke sinnvoll nutzen: Plattformen wie Facebook und WhatsApp ermöglichen es, Kontakte über Kontinente hinweg zu pflegen, Freunde am eigenen Leben teilhaben zu lassen oder Erfahrungen und Tipps auszutauschen.

5.4. Verlust oder Diebstahl von Geräten

Notebooks, Smartphones und Tablets können verloren gehen oder gestohlen werden. Dabei wiegt der potenzielle Missbrauch persönlicher oder vertraulicher Daten häufig schwerer als der materielle Verlust. Gelangen sensible Informationen in falsche Hände, kann dies erhebliche Konsequenzen nach sich ziehen – weit über den reinen Gerätewert hinaus.

- **Gerätesicherung:** Schutz durch PIN, Muster, Passwort oder Fingerabdruck.
- **Datenverschlüsselung:** Aktiviere in den Sicherheitseinstellungen die Geräteverschlüsselung. So können fremde Personen auf die gespeicherten Inhalte nicht zugreifen.
- **Fernzugriff bei Verlust:** Sollte ein Smartphone, Tablett oder Notebook abhandenkommen, gibt es die Möglichkeiten der Fernsperre, Fernlöschung und Geräteortung mittels GPS.

5.5. Anwendungs- bzw. App-Berechtigungen:

Beim Installieren von Apps wird abgefragt, auf welche Funktionen oder Daten (z. B. Mikrofon, Kontakte, Standort, Bilder) die App zugreifen möchte. Es ist wichtig, sorgfältig zu prüfen, ob diese Zugriffsrechte wirklich notwendig sind, bevor man sie erlaubt.

Diese Anwendungsberechtigungen können in den Einstellungen überprüft und geändert werden.

Apps aus unsicheren Quellen können Probleme verursachen!
Gefahren: Spionage, hohe Kosten, Malware, hoher Strom- oder Datenverbrauch, schlechte Qualität

6. Kommunikation

6.1. E-Mail

Sicherheitsaspekte

Der Absender einer E-Mail kann gefälscht werden!

Herr S. erhält ein E-Mail – angeblich von seinem Stromanbieter – mit einem Link zum Download der Rechnung. Es stellt sich heraus, dass der Absender falsch angegeben ist und die Rechnung einen Virus enthält.

Eine Gemeinde erhält eine E-Mail mit einer Rechnung. Als Absender ist eine Baufirma angegeben, die gerade den Kindergarten baut. Der Rechnungsbetrag wird an das angegebene Konto überwiesen. Später stellt sich heraus, dass Absender und Rechnung gefälscht waren.

Schutzmaßnahmen

Verschlüsselte Übertragung

So gut wie alle E-Mail-Anbieter wie Google, Microsoft oder GMX übertragen E-Mails verschlüsselt, damit sie nicht abgefangen und gelesen werden können.

6.2. Digitale Signatur – der elektronische Ersatz der Unterschrift

Die digitale Signatur erfüllt denselben Zweck wie eine handschriftliche Unterschrift: Sie bestätigt, dass eine elektronische Information tatsächlich von der Person stammt, die sie signiert hat (**Authentizität**) und dass der Inhalt seitdem nicht verändert wurde (**Integrität**).

Im Gegensatz zur eigenhändigen Unterschrift bietet die digitale Signatur sogar ein höheres Maß an Sicherheit – insbesondere, weil sie nachträglich nicht abgestritten werden kann.

Programme, Dokumente und auch E-

Beispiel für eine digitale Signatur eines PDF-Dokuments

Mails lassen sich digital signieren. Eine digital signierte E-Mail gewährleistet, dass sie vom angegebenen Absender stammt und während der Übertragung nicht manipuliert wurde.

Die höchste Sicherheit bei der E-Mail-Kommunikation wird durch die Kombination aus **verschlüsselter Übertragung** und **digitaler Signatur** erreicht.

6.3. Spam- und Phishing-E-Mails sowie gefährliche Anhänge

Spam- bzw. **Junk-E-Mails** sind unerwünschte Werbenachrichten, die häufig zweifelhafte Produkte oder Dienstleistungen bewerben – etwa Medikamente, Aktien, fragwürdige Krypto-Investments mit unrealistischen Gewinnversprechen oder angebliche Lottogewinne.

Phishing-E-Mails (vom englischen password fishing) geben sich als Nachrichten vertrauenswürdiger Absender aus, etwa von Banken oder Paketdiensten. Sie fordern den Empfänger dazu auf, persönliche Zugangsdaten auf einer gefälschten Webseite einzugeben. Die so erbeuteten Informationen werden von Kriminellen genutzt, um z. B. Konten zu plündern.

E-Mail-Anhänge können Schadsoftware (Malware) enthalten. Bereits das Öffnen eines infizierten Dokuments – z. B. mit Makros – oder einer ausführbaren Datei (.exe) kann den Computer mit Viren, Trojanern oder Ransomware infizieren.

6.4. Instant Messaging (WhatsApp, Facebook Messenger, Signal...)

Instant Messaging (kurz **IM**, deutsch: Nachrichtensofortversand) ist eine Kommunikationsform, bei der sich zwei oder mehr Personen in Echtzeit über Textnachrichten unterhalten. Die Nachrichten werden sofort beim Empfänger angezeigt. Neben Text können auch **Dateien** wie Bilder, Sprachnachrichten oder Videos übertragen werden.

Wichtige Hinweise zum sicheren Umgang mit Chatdiensten:

- **Dateien übertragen – aber mit Vorsicht:**
  Instant-Messaging-Apps ermöglichen den Austausch von Dateien. Nimm keine Dateien von unbekannten Personen an! Sie könnten Schadsoftware (Malware) enthalten.
- **Verschlüsselte Übertragung:**
  Bei Diensten wie WhatsApp, Signal oder Facebook Messenger erfolgt die Kommunikation **Ende-zu-Ende-verschlüsselt**. Das bedeutet, dass die Nachrichten unterwegs nicht mitgelesen werden können – nicht einmal vom Anbieter.
- **Achtung bei Kontakten:**
  In Chats kann man sich nicht sicher sein, wer am anderen Ende wirklich sitzt. Personen können sich online anders ausgeben – z. B. als jemand jüngeren Alters, als eine andere Identität oder mit gefälschten Bildern. **Sei misstrauisch bei scheinbar persönlichen Informationen oder Profilbildern**!
- **Persönliche Daten schützen**:
  Gib **niemals leichtfertig persönliche Daten** (Adresse, Telefonnummer, Schule, Fotos etc.) weiter – auch nicht, wenn dir jemand im Chat „vertraut“ vorkommt.

7. Sicheres Daten-Management

Wichtige Daten, wie beispielsweise Kundendaten, werden auf Computern gespeichert. Um sie vor Diebstahl oder Missbrauch zu schützen, müssen Sicherheitsmaßnahmen getroffen werden.

Diebstahlsicherung durch Stahlseil

7.1. Datenschutzmaßnahmen

- **Zugangsbeschränkungen** zu den Räumen mit Datenträgern
- **Sicherungskabel** aus Stahl für Notebooks an öffentlich zugänglichen Orten wie Messeveranstaltungen.
- Die **Inventarisierung** von Datenträgern zur Bestandskontrolle

Backups

Datenträger können durch Defekte unlesbar werden oder können abhandenkommen. Eine Sicherungskopie ermöglicht die Wiederherstellung der Daten:

- **Regelmäßig** nach Ablaufplan erstellen.
- **Sicher aufbewahren:** geschützt vor Feuer, Wasser, Zerstörung und Diebstahl.
- **Cloud-Backups**: sicher, wartungsfrei, Anbieter sorgt für Sicherheit.
- **Rücksicherung testen**, um im Notfall funktionsfähige Backups zu haben. Sicherungskopien (Backups) müssen nach Ablaufplan erstellt werden

8. Sicheres Löschen persönlicher Daten vor der Weitergabe oder Entsorgung

Bevor ein **Computer**, **Tablet** oder **Smartphone** weitergegeben oder entsorgt wird, müssen alle persönlichen Daten wie E-Mails, Zugangsdaten (z. B. für Online-Konten), Geschäfts- und Privatdokumente, Bilder und Videos **vollständig gelöscht** werden.

⚠️ Diese Daten dürfen nicht einfach nur gelöscht, sondern müssen so entfernt werden, dass sie nicht wiederhergestellt werden können!

Möglichkeiten zur sicheren Datenlöschung:

- **Festplatten überschreiben:**
  Mit speziellen Programmen werden Daten mehrfach überschrieben – so sind sie nicht wiederherstellbar.
- **Physische Zerstörung:**
  Alte Datenträger können auch geschreddert oder mechanisch zerstört werden.
- **Smartphones/Tablets zurücksetzen:**
  Stelle das Gerät auf Werkseinstellungen zurück, damit alle persönlichen Daten gelöscht werden.

PC sicher zurücksetzen und alle persönlichen Daten löschen

Wenn du deinen alten Computer weitergeben möchtest, gehe folgendermaßen vor:

- Öffne die **Einstellungen**.
- Wähle **System → Wiederherstellung**.
- Klicke bei „**Diesen PC zurücksetzen**“ auf „**Los geht’s**“.

- Wähle „Alles entfernen“.

Dann:

- „**Nur Dateien entfernen**“: löscht persönliche Dateien, aber nicht sicher.
- „**Laufwerk bereinigen**“ (Festplatte säubern): löscht und überschreibt die Daten – sie sind dann dauerhaft gelöscht.

Inhalt