IT-Sicherheit

Lern- und Trainingskapitel zum ICDL-Syllabus 2.0

Konrad Rennert
ECDL-Trainer & Autor

Erstellt mit Unterstützung durch KI
(ChatGPT-4 & DALLE)

Hinweise

1. Aktualität von Links und zur Verwendung der bereitgestellten Suchbegriffe

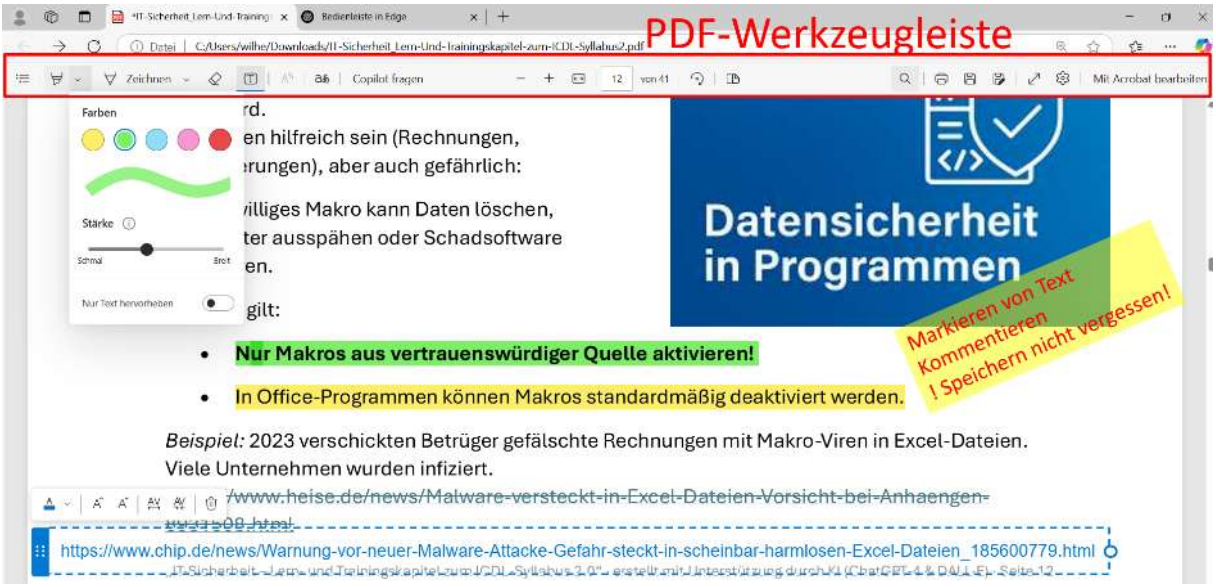
Die in diesem Werk enthaltenen Links wurden zum Zeitpunkt der Erstellung (2023/2024) von einer KI aus öffentlich zugänglichen Quellen vorgeschlagen. Viele waren damals gültig – doch da sich Webinhalte häufig ändern oder verschwinden, sind nicht mehr erreichbare Links durchgestrichen dargestellt.
Diese dienen weiterhin als Hinweis auf das ursprüngliche Thema oder die Quelle. Ergänzend habe ich als Autor ein alternatives Verfahren zur Aktualisierung eingeführt:

• An jeder Stelle mit ungültigem Link findet sich nun ein Suchvorschlag: [Begriff]
• Diese Begriffe wurden manuell ergänzt und ermöglichen durch Copy & Paste in jede Suchmaschine eine schnelle, tagesaktuelle Recherche.

Beispiel:
Durchgestrichener Link: ~~https://www.heise.de/news/LockBit...~~
→ Suchvorschlag: LockBit Ransomware Klinik 2024

2. Bearbeitung dieses Dokuments mit der PDF-Werkzeugleiste

In modernen Browsern wie **Microsoft Edge** kann man mit der automatisch eingeblendeten PDF-Werkzeugleiste eigene Notizen oder Ergänzungen direkt im PDF-Dokument hinterlegen – z. B. für Recherche-Ergebnisse oder alternative Quellen. Nach dem Speichern bleiben diese Ergänzungen erhalten. – Details dazu sind im Anhang zu finden



3. Einführungsvideo

https://youtube.com/watch?v=m_DzVfaya9w

Inhalt

1 Sicherheitskonzepte

1.1 Bedrohungen für Daten

1.1.1 Daten vs. Informationen

Daten sind rohe Fakten – etwa Zahlen, Texte oder Zeichen, die noch keine Bedeutung haben. Zum Beispiel: „2025“, „Müller“, „120 km/h“.

Informationen entstehen erst, wenn diese Daten in einen Zusammenhang gebracht werden:

„Herr Müller fuhr am 3. April 2025 mit 120 km/h durch eine 70er-Zone.“
Das ist eine verwertbare Information – eventuell auch für die Polizei. 😉

1.1.2 Cybercrime und Hacken

Cybercrime ist Kriminalität, die mit Computern oder über das Internet geschieht. Beispiele:

- Identitätsdiebstahl (jemand stiehlt deine Online-Daten)
- Online-Betrug (z. B. Fake-Shops)
- Ransomware (Erpressung durch Daten-Verschlüsselung)

Beispiel: Die „LockBit“-Ransomware-Gruppe griff 2023 gezielt deutsche Kliniken an, verschlüsselte Daten und verlangte Lösegeld.
~~https://www.heise.de/news/LockBit-Ransomware-Gruppe-Gefaehrliche-Cyberbande-ausgehoben-9574566.html~~

Suchvorschlag: LockBit Ransomware

Hacken ist das Eindringen in Computersysteme. Es gibt zwei Arten:

- **White Hat Hacker**: ethisch, decken Sicherheitslücken auf
- **Black Hat Hacker**: illegal, stehlen Daten oder richten Schaden an

1.1.3 Absichtliche und unbeabsichtigte Bedrohungen

Nicht jede Gefahr kommt von außen. Auch intern können Daten gefährdet sein:

- **Absichtlich**: Eine Mitarbeiterin kopiert sensible Kundendaten.
- **Unbeabsichtigt**: Ein IT-Techniker vergisst, ein wichtiges System zu sichern.

Beispiel: 2024 verlor ein Unternehmen durch einen Konfigurationsfehler Millionen von Kundendaten. Die Ursache: ein falscher Haken in der Cloud-Speichereinstellung.
~~https://www.zdnet.de/88395624/offene-cloud-eimer-uber-1-mrd-datensaetze-frei-zugaenglich/~~

Suchvorschlag: Konfigurationsfehler Datenverlust Kundendaten

1.1.4 Naturkatastrophen

Auch „höhere Gewalt“ kann Daten gefährden:

- Brände
- Überschwemmungen
- Erdbeben
- Krieg

Wichtig: Daten sollten nie nur an einem Ort gespeichert sein. Eine Kombination aus lokaler Sicherung und Cloud-Backup erhöht die Sicherheit.

Beispiel: Die Flutkatastrophe in Nordrhein-Westfalen 2021 zerstörte auch Rechenzentren. Firmen ohne externe Backups verloren wichtige Geschäftsdaten.
~~https://www.handelsblatt.com/technik/it-internet/it-sicherheit-die-flutkatastrophe-trifft-auch-serverzentren/27451598.html~~

Suchvorschlag: IT-Sicherheit Flutkatastrophe trifft Server-Zentren

1.1.5 Risiken durch Cloud-Computing

Cloud-Dienste wie Google Drive oder iCloud sind bequem – aber nicht ohne Risiko.
Mögliche Gefahren:

- **Datenschutzprobleme**: Wer kann mitlesen?
- **Kontrollverlust**: Was passiert mit gelöschten Daten?
- **Abhängigkeit**: Wenn der Anbieter offline ist, sind es auch deine Daten.

Beispiel: 2024 war Microsofts Cloud-Dienst „Azure“ stundenlang ausgefallen. Tausende Firmen hatten keinen Zugriff auf ihre Kundendaten.
~~https://www.spiegel.de/netzwelt/web/microsoft-azure-von-stoerung-betroffen-firmen-weltweit-betroffen-a-67b0f92b-5744-4c10-9bcb-6f7acdc62b4c~~

Suchvorschlag: Microsoft Azure Störung weltweit

Fazit: Was du tun kannst

Sicherheits-Tipps für alle:

- Nutze starke, einzigartige Passwörter
- Speichere wichtige Daten auch außerhalb der Cloud
- Achte auf aktuelle Sicherheitsupdates
- Überlege, wem du deine Daten gibst – online wie offline

Egal ob Schüler, Büroarbeiter oder Rentner – Datensicherheit geht uns alle an. Denn:
Informationen sind das neue Gold.

1.2 Der Wert von digitalen Daten und Informationen

1.2.1 Vertraulichkeit, Integrität, Verfügbarkeit

Diese drei Begriffe sind das Fundament der **Informationssicherheit**:

- **Vertraulichkeit (Confidentiality)**: Nur berechtigte Personen dürfen auf Daten zugreifen.
- **Integrität (Integrity)**: Daten dürfen nicht unbemerkt verändert werden.
- **Verfügbarkeit (Availability)**: Daten sollen dann bereitstehen, wenn man sie braucht.

Beispiel: In einer Klinik müssen Patientendaten sicher (vertraulich), korrekt (integriert) und bei Notfällen abrufbar (verfügbar) sein – sonst kann das lebensbedrohlich werden.

1.2.2 Schutz persönlicher Informationen

Warum ist das wichtig?

- **Identitätsdiebstahl**: Betrüger nutzen gestohlene Daten, um auf deinen Namen einzukaufen oder Konten zu eröffnen.
- **Privatsphäre**: Jeder Mensch hat ein Recht darauf, dass private Informationen privat bleiben.

Beispiel: 2024 wurde eine große Dating-App gehackt. Millionen Nutzerprofile mit Fotos, Namen, sexuellen Vorlieben wurden veröffentlicht.
~~https://www.heise.de/news/Dating-App-Leck-Nutzerdaten-veroeffentlicht-9578317.html~~

Suchvorschlag: Dating App Leck Nutzerdaten veröffentlicht

1.2.3 Schutz von Unternehmensdaten

Am Arbeitsplatz sind sensible Daten oft noch wertvoller:

- Kundenlisten
- Angebote
- Finanzzahlen
- Betriebsgeheimnisse

Diese Daten müssen gegen **Diebstahl**, **Missbrauch**, **Verlust** und **Sabotage** geschützt sein.

Beispiel: 2023 verursachte ein ehemaliger Mitarbeiter durch Datenmanipulation Millionenverluste – das Unternehmen hatte keine Schutzmaßnahmen gegen Insider-Angriffe.
~~https://www.manager-magazin.de/unternehmen/it-sicherheit-und-insiderangriff-wie-mitarbeiter-firmen-in-gefahr-bringen-a-3458b03f-0002-0001-0000-000173241525~~

Suchvorschlag: Mitarbeiter IT Sabotage Insiderangriff

1.2.4 Datenschutz – Regeln und Prinzipien

Daten dürfen nur gesammelt und genutzt werden, wenn bestimmte Regeln eingehalten werden – z. B. laut DSGVO (Datenschutz-Grundverordnung):

- **Transparenz**: Nutzer müssen wissen, was mit ihren Daten passiert.
- **Zweckbindung**: Daten dürfen nur für den angegebenen Zweck genutzt werden.
- **Verhältnismäßigkeit**: Nur so viele Daten wie nötig dürfen gesammelt werden.

Beispiel: Webseiten müssen heute beim ersten Aufruf um Zustimmung zu Cookies fragen – ein direktes Ergebnis der DSGVO.
https://www.bfdi.bund.de/DE/Themen/Datenschutz/Datenschutz-Grundverordnung/Datenschutz-Grundverordnung.html

Suchvorschlag: Cookies Aufruf Datenschutz-Grundverordnung

1.2.5 Betroffene und datenverarbeitende Stellen

- **Betroffene Person**: Die Person, deren Daten gesammelt oder verarbeitet werden.
- **Verarbeitende Stelle**: Firmen oder Organisationen, die Daten erheben, speichern oder auswerten.

Beide Seiten müssen Rechte und Pflichten kennen.

Beispiel: Wenn ein Fitnessstudio Kundendaten an einen Werbepartner weitergibt, ohne Zustimmung – verletzt es die Rechte der betroffenen Person.

1.2.6 Richtlinien in der IT

Ohne klare Regeln geht es nicht. **IT-Sicherheitsrichtlinien** helfen, verantwortungsbewusst mit Daten umzugehen:

- Passwortrichtlinien
- Regeln zur Nutzung von USB-Sticks
- Schulungen zur IT-Sicherheit

Beispiel: Viele Unternehmen setzen auf verpflichtende Online-Trainings, in denen Mitarbeitende Phishing erkennen lernen.
https://www.handelsblatt.com/technik/it-internet/cybersecurity-wie-deutsche-firmen-ihr-personal-gegen-phishing-fit-machen/29287514.html

Suchvorschlag: Phishing Gefahren verpflichtende Online-Trainings für Mitarbeiter

Fazit: Daten sind wertvoll – schütze sie!

Daten sind heute oft wertvoller als Bargeld. Wer sie schützt, schützt nicht nur sich selbst, sondern auch andere.
Merke dir: Vertraulichkeit, Integrität und Verfügbarkeit sind keine Zauberwörter – sondern dein Werkzeugkasten für sicheres digitales Leben.

1.3 Persönliche Datensicherheit

1.3.1 Social Engineering – der Trick mit dem Vertrauen

Social Engineering ist, wenn jemand versucht, an deine Daten zu kommen – nicht durch Technik, sondern durch **Psychologie**.

Der Angreifer gibt sich z. B. als Kollege, Polizist oder IT-Support aus und fragt:

„Könnten Sie mir schnell mal Ihr Passwort geben? Ich muss was überprüfen."

Oder du bekommst eine E-Mail mit:

„Bitte bestätigen Sie Ihre Kontoinformationen – sonst wird Ihr Zugang gesperrt."

Beispiel: 2023 fielen Mitarbeitende eines Energieversorgers auf gefälschte IT-Mails herein – das Netz war tagelang gestört.
~~https://www.tagesschau.de/inland/gesellschaft/cyberangriff-rheinenergie-100.html~~

Suchvorschlag: Cyberangriff Rheinenergie

1.3.2 Methoden des Social Engineering

Hier sind die häufigsten Tricks:

- **Phishing**: Du bekommst eine gefälschte E-Mail oder Website, die aussieht wie deine Bank. Ziel: deine Daten.
- **Shoulder Surfing**: Jemand schaut dir beim Eintippen deines Passworts über die Schulter.
- **Telefonbetrug**: Der Anrufer behauptet, von Microsoft oder einer Versicherung zu sein.

Beispiel: Die Polizei warnt regelmäßig vor Anrufen angeblicher Bankberater, die nach PIN oder TAN fragen.
https://www.polizei-beratung.de/themen-und-tipps/betrug/

1.3.3 Identitätsdiebstahl – und seine Folgen

Wenn jemand deine persönlichen Daten nutzt, um sich als dich auszugeben, nennt man das **Identitätsdiebstahl**.

Folgen können sein:

- Kontoeröffnung in deinem Namen
- Online-Bestellungen auf deine Kosten
- Rufschädigung

Beispiel: Ein Schüler verlor durch eine geleakte E-Mail-Adresse seine Social-Media-Konten – und wurde dort durch einen Fake ersetzt.

https://www.verbraucherzentrale.de/wissen/digitale-welt/phishing-und-datenschutz/identitaetsdiebstahl-erkennen-und-verhindern-24120

Suchvorschlag: Identitätsdiebstahl erkennen und verhindern

1.3.4 Methoden des Identitätsdiebstahls

Wie klauen Kriminelle deine Identität?

- **Skimming**: Kartenleser an Geldautomaten speichern Daten deiner EC-Karte.
- **Pretexting**: Der Angreifer gibt sich als jemand Wichtiges aus (z. B. Steuerberater) und fragt Daten ab.
- **Information Diving**: Durchforsten von Papiermüll oder alten Handys nach persönlichen Informationen.

Beispiel: Ein Rentner wurde Opfer, weil er seine alten Kontoauszüge ungeschreddert im Müll entsorgte – jemand bestellte mit seinen Daten Elektronik.
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Identitaetsdiebstahl/identitaetsdiebstahl_node.html

Suchvorschlag: BSI, Identitätsdiebstahl

Fazit: Vertrauen ist gut – Vorsicht ist besser

Halte deine Augen und Ohren offen:

- Gib niemals Passwörter weiter
- Überprüfe Absender von E-Mails und Anrufen
- Zerstöre alte Dokumente oder sichere alte Geräte

Wer gut informiert ist, fällt nicht so leicht auf Betrüger herein – egal ob jung oder alt.

1.4 Datensicherheit in Programmen

1.4.1 Makros – kleine Helfer mit großem Risiko

Makros sind automatisierte Abläufe, z. B. in Excel oder Word.
Sie können hilfreich sein (Rechnungen, Formatierungen), aber auch gefährlich:

Ein böswilliges Makro kann Daten löschen, Passwörter ausspähen oder Schadsoftware installieren.

Deshalb gilt:

- **Nur Makros aus vertrauenswürdiger Quelle aktivieren!**
- In Office-Programmen können Makros standardmäßig deaktiviert werden.

Beispiel: 2023 verschickten Betrüger gefälschte Rechnungen mit Makro-Viren in Excel-Dateien. Viele Unternehmen wurden infiziert.
https://www.heise.de/news/Malware-versteckt-in-Excel-Dateien-Vorsicht-bei-Anhaengen-8931508.html

Suchvorschlag: Malware in Excel Dateien

1.4.2 Daten verschlüsseln – und sicher aufbewahren

Verschlüsselung bedeutet: Deine Daten werden in eine Art Geheimcode verwandelt.
Nur mit dem richtigen **Passwort, Schlüssel oder Zertifikat** lassen sie sich wieder entschlüsseln.

Wichtige Hinweise:

- Den Schlüssel nie offen speichern!
- Passwörter gut aufbewahren – ohne Passwort kein Zugriff mehr!
- Zertifikate regelmäßig erneuern.

Beispiel: Die Stadtverwaltung von Witten hatte 2022 keinen Zugriff auf ihre verschlüsselten Backups – das Passwort war verloren gegangen.
~~https://www.derwesten.de/region/staedte-ohne-zugriff-datenverlust-witten-id234960837.html~~

Suchvorschlag: Cyberangriff in Witten

1.4.3 Dateien, Ordner und Laufwerke verschlüsseln

Du kannst nicht nur einzelne Dateien, sondern auch:

- **ganze Ordner** (z. B. mit Windows-Bordmitteln oder Tools wie VeraCrypt)
- **Laufwerke**, etwa USB-Sticks oder externe Festplatten, verschlüsseln.

So sind sensible Inhalte auch bei Diebstahl oder Verlust geschützt.

Programme wie:

- **BitLocker (Windows)**
- **FileVault (macOS)**
- **VeraCrypt (Open Source, kostenlos)**

1.4.4 Dokumente mit Kennwort schützen

Nicht immer braucht es eine vollständige Verschlüsselung. Oft reicht auch ein **Kennwortschutz**:

- Für Word-Dokumente
- Für Excel-Tabellen
- Für ZIP- oder RAR-Archive

Vorteil: Einfach umzusetzen, schnell eingerichtet
Nachteil: Schwache Passwörter können leicht geknackt werden.

Beispiel: Eine Schülerzeitung speicherte ihre Ausgaben passwortgeschützt auf Google Drive – doch das Passwort war „1234“… 🤦
~~https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Passwoerter/passwoerter_node.html~~

Suchvorschlag: BSI, Passwörter, passwoerter_node

Fazit: Programme sind mächtig – aber nicht immer sicher

Wenn du mit Programmen arbeitest, solltest du dir angewöhnen:

- Makros nur aktivieren, wenn du der Quelle vertraust
- Wichtige Dateien und Ordner regelmäßig sichern und verschlüsseln
- Starke Passwörter verwenden und gut aufbewahren

Ob Bewerbungsschreiben oder Geschäftsbericht – **Schutz deiner Daten beginnt im Programmfenster.**

2 Malware

2.1 Arten von Malware und ihre Funktionsweise

2.1.1 Was ist Malware?

Malware ist die Kurzform von „Malicious Software“, also **bösartige Software**.
Ziel: Schaden anrichten, Daten stehlen oder dich ausspionieren.

Malware versteckt sich oft im System, z. B. als:

- **Trojaner** – sieht nützlich aus, ist aber schädlich
- **Rootkits** – verschaffen dem Angreifer umfassende Kontrolle
- **Backdoors** – geheime Zugänge ins System

Beispiel: Ein scheinbar harmloses Spiel auf dem Handy installierte im Hintergrund einen Trojaner, der Daten an Dritte schickte.
~~https://www.kuketz-blog.de/android-trojaner-in-kinderspielen-im-play-store/~~

Suchvorschlag: Android Trojaner in Kinderspielen

2.1.2 Viren und Würmer – digitale Infektionen

- **Viren** hängen sich an Programme oder Dateien – sie verbreiten sich beim Öffnen.
- **Würmer** verbreiten sich selbstständig im Netzwerk.

Beide können:
❌ Dateien löschen
❌ Computer lahmlegen
❌ Systeme infizieren

Beispiel: Der Wurm „ILOVEYOU“ legte im Jahr 2000 Millionen Rechner lahm – über eine E-Mail mit dem Betreff „I love you“.
~~https://www.heise.de/news/ILOVEYOU-Wurm-verbreitete-sich-vor-20-Jahren-4706012.html~~

Suchvorschlag: ILOVEYOU Computer Wurm

2.1.3 Erpressung, Spionage, Werbung: Weitere Malware-Typen

- **Adware**: Zeigt dir ungewollte Werbung
- **Spyware**: Spioniert dich aus
- **Botnets**: Dein Gerät wird Teil eines „Zombie-Heeres“
- **Keylogger**: Zeichnet deine Tastatureingaben auf
- **Dialer**: Wählen teure Telefonnummern im Hintergrund

Beispiel: 2024 war eine bekannte Taschenlampen-App voller Spyware – Millionen Android-Geräte waren betroffen.
~~https://www.techbook.de/mobile/smartphones/handy-android-apps-spionieren~~

Suchvorschlag: Handy Android-Apps spionieren

2.2. Schutz vor Malware

2.2.1 Wie funktioniert Antiviren-Software?

Antivirenprogramme durchsuchen dein System nach bekannten Mustern und verdächtigem Verhalten. Sie vergleichen Dateien mit einer Datenbank, die ständig aktualisiert wird.

Wichtig:

- Antivirenprogramme erkennen *bekannte* Malware zuverlässig
- Neue („Zero-Day"-Angriffe) sind schwieriger zu erkennen
- Kein Schutz ist perfekt – der Mensch bleibt die beste Firewall

Beispiel: Beim Herunterladen eines vermeintlichen Updates schlug nur ein Antivirenprogramm Alarm – weil es eine neue Bedrohung noch nicht erkannte.
https://www.av-test.org/de/antivirus/

2.2.2 Installation auf allen Geräten

Ein Schutzprogramm gehört nicht nur auf den PC. Auch:

- **Smartphones**
- **Tablets**
- **Laptops**
- **IoT-Geräte (z. B. smarte Kameras)**

sind Ziele für Angriffe – oft sogar besonders anfällig!

Beispiel: 2023 wurden Hunderttausende Android-Handys durch infizierte Apps angegriffen, weil kein Schutz aktiv war.
~~https://www.heise.de/news/Sicherheitsluecken-bei-Android-Geraeten-9658704.html~~

Suchvorschlag: Sicherheitslücken bei Android

2.2.3 Updates – die wichtigste Verteidigungslinie

Veraltete Programme sind wie offene Türen. **Updates (Patches)** schließen Sicherheitslücken, bevor sie ausgenutzt werden.

Regelmäßig aktualisieren solltest du:
✔ Betriebssysteme (Windows, macOS, Android…)
✔ Browser (Chrome, Firefox, Edge…)
✔ Programme (z. B. Adobe, Zoom…)
✔ Antiviren-Software!

Beispiel: Die WannaCry-Ransomware 2017 nutzte eine alte Windows-Schwachstelle – obwohl es schon ein Update gab.
~~https://www.tagesschau.de/investigativ/ndr/chronologie-wannacry-101.html~~

Suchvorschlag: Cyberangriff WannaCry

2.2.4 Dateien regelmäßig prüfen

Du kannst bestimmte Dateien, Ordner oder ganze Laufwerke aktiv überprüfen – besonders bei:

- heruntergeladenen Dateien
- USB-Sticks

- verdächtigen E-Mail-Anhängen

Außerdem: **Zeitgesteuerte Scans** (z. B. täglich nachts) helfen, Infektionen frühzeitig zu entdecken.

Beispiel: Ein automatischer Wochenscan entdeckte Spyware auf einem Familienlaptop – nach dem Besuch einer vermeintlichen Rezept-Webseite.
~~https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Software-und-Einstellungen/Virenschutz/virenschutz_node.html~~

Suchvorschlag: BSI, Software und Einstellungen, Virenschutz

2.2.5 Alte Software = hohes Risiko

Programme, die nicht mehr gepflegt werden, sind gefährlich. Beispiele:

- Windows 7 (Support-Ende 2020)
- Adobe Flash Player
- Office 2010

Diese Software wird nicht mehr aktualisiert – Schwachstellen bleiben offen.

Beispiel: Cyberangriffe auf Arztpraxen erfolgten über eine veraltete Windows-Version, für die es keine Sicherheitsupdates mehr gab.
~~https://www.aerzteblatt.de/nachrichten/139989/Cybersicherheit-Veraltete-Systeme-bedrohen-Arztpraxen~~

Suchvorschlag: Cybersicherheit veraltete Systeme bedrohen Arztpraxen

2.3 Problemlösung und Malware-Entfernung

2.3.1 Was bedeutet Quarantäne?

Antivirenprogramme verschieben verdächtige Dateien in die **Quarantäne**:

- Sie sind isoliert vom restlichen System
- Du kannst entscheiden: löschen oder wiederherstellen
- Kein Zugriff durch Schadsoftware möglich

Das ist nützlich, wenn du nicht sicher bist, ob eine Datei gefährlich ist.

2.3.2 Dateien löschen oder sichern

Wurde eine Datei eindeutig als gefährlich erkannt, solltest du sie:
dauerhaft löschen
Alternativ kannst du sie behalten – aber nur in Quarantäne

Nicht machen: Datei wieder öffnen, um „nur mal zu schauen“…

2.3.3 Hilfe im Netz finden

Falls du dir unsicher bist: Es gibt vertrauenswürdige Anlaufstellen:

- Webseiten deiner Antiviren-Software
- Microsoft / Apple Hilfeportale

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI)
- IT-Foren (z. B. Trojaner-Board, Heise Security)

Beispiel: Das BSI bietet konkrete Anleitungen zur Entfernung von Malware und zur Systemprüfung.
~~https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Software-und-Einstellungen/Virenschutz/virenschutz_node.html~~

Suchvorschlag: BSI Virenschutz_node

Fazit: Mit System gegen Schadsoftware

Deine Strategie gegen Malware:

1. Schutzprogramme nutzen
2. Immer aktuell bleiben
3. Misstrauisch sein – besonders bei Anhängen, Links, Apps
4. Bei Verdacht: schnell handeln und Hilfe holen

3 Netzwerksicherheit

3.1 Netzwerke und Netzwerkverbindungen

3.1.1 Netzwerkarten: LAN, WLAN, WAN und VPN

Ein **Netzwerk** verbindet zwei oder mehr Geräte miteinander, damit sie Daten austauschen können.

Die wichtigsten Netzwerkarten:

- **LAN (Local Area Network):** z. B. das Heimnetz mit PC, Drucker und NAS.
- **WLAN (Wireless LAN):** das gleiche – nur ohne Kabel.
- **WAN (Wide Area Network):** verbindet viele Netzwerke über große Entfernungen – das bekannteste ist das Internet.
- **VPN (Virtual Private Network):** eine **verschlüsselte Verbindung** durch das Internet, damit niemand mitlesen kann.

Beispiel: Viele Unternehmen verlangen heute bei Homeoffice einen VPN-Zugang, damit interne Daten geschützt übertragen werden.
https://de.wikipedia.org/wiki/Virtual_Private_Network

3.1.2 Sicherheitsrisiken in Netzwerken

Ein Netzwerk ist praktisch – aber auch ein Einfallstor für Gefahren:

- **Malware-Verbreitung:** Ist ein Gerät infiziert, kann es andere anstecken.
- **Unautorisierter Zugriff:** Hacker könnten ins Netzwerk eindringen.
- **Datenschutzverletzung:** Unverschlüsselte Datenübertragung ist wie eine Postkarte – jeder kann mitlesen.

Beispiel: 2023 wurde eine große deutsche Schule durch eine veraltete WLAN-Konfiguration Opfer eines Cyberangriffs – persönliche Daten von Lehrern und Schülern waren betroffen.
~~https://www.tagesschau.de/investigativ/wdr/hackerangriff-schulen-101.html~~

Suchvorschlag: Hackerangriff Schule

3.1.3 Aufgaben von Netzwerk-Admins

Ein **Netzwerkadministrator** kümmert sich um:

- Rechtevergabe: Wer darf auf was zugreifen?
- Benutzerkonten: Einrichten, ändern, löschen
- Schutzmaßnahmen: z. B. Virenschutz im Netzwerk, Updates einspielen
- Zugriffsprotokolle und Überwachung

Beispiel: Der Admin eines mittelständischen Betriebs konnte dank zentraler Netzwerküberwachung eine Malware-Ausbreitung früh stoppen.
https://de.wikipedia.org/wiki/Systemadministrator

3.1.4 Die Firewall als digitale Schutzmauer

Firewalls sind Programme oder Geräte, die den Datenverkehr filtern – wie ein Türsteher für dein Netzwerk.

- Sie blockieren verdächtigen Datenverkehr
- Sie schützen vor einfachen Angriffen aus dem Internet
- **Private Firewalls (z. B. Windows-Firewall)** bieten Grundschutz

Aber: Gegen **komplexe Hackerangriffe** reichen sie oft nicht – dafür braucht man professionelle Sicherheitslösungen.

Beispiel: Die Firewall eines Smart-TVs war deaktiviert – ein Sicherheitsexperte konnte aus dem Auto darauf zugreifen.
~~https://www.heise.de/news/Smart-TV-ohne-Firewall-Hackbar-vom-Parkplatz-aus-9001149.html~~

Suchvorschlag: Smart TV ohne Firewall hacken

3.1.5 Firewall richtig nutzen

Du kannst deine Firewall:

Aktivieren/Deaktivieren (aber bitte nur mit Bedacht)
Anpassen:

- Anwendungen erlauben oder blockieren
- Regeln für eingehende und ausgehende Verbindungen setzen

Tipp: Bei Windows geht das unter → Systemsteuerung → Windows Defender Firewall → „Eine App durch die Firewall zulassen“

Beispiel: Ein Nutzer ließ versehentlich eine Schadsoftware durch, weil er die Firewall-Regel falsch gesetzt hatte.
https://de.wikipedia.org/wiki/Firewall

3.2 Absicherung von drahtlosen Netzwerken

3.2.1 WLAN absichern: Verschlüsselung & Filter

Drahtlose Netzwerke (WLANs) brauchen besonderen Schutz, weil jeder in Reichweite sie nutzen *könnte*.

Verschlüsselungsstandards:

- **WEP:** sehr unsicher – nicht mehr verwenden!
- **WPA / WPA2:** heute Standard
- **WPA3:** moderner, sicherer – aber noch nicht überall verfügbar

Weitere Sicherheitsmaßnahmen:

- **SSID (Name des WLANs):** besser nicht „FritzBox123“ nennen
- **MAC-Filter:** Nur bestimmte Geräte dürfen rein

Beispiel: Ein Café wurde 2022 Opfer eines WLAN-Angriffs, weil es noch WEP benutzte. Kundendaten wurden abgegriffen.
https://de.wikipedia.org/wiki/Wireless_Local_Area_Network#Sicherheitsaspekte

3.2.2 Gefahren ungesicherter Netzwerke

Wer ungeschützte WLANs nutzt, riskiert viel:

Lauschangriffe: Angreifer lesen mit
Hijacking: Dein Gerät wird aus der Verbindung geworfen – Angreifer übernimmt
Man-in-the-Middle: Der Hacker steht „zwischen dir und dem Internet"

Beispiel: In mehreren ICE-Zügen wurden 2023 gefälschte WLAN-Zugänge entdeckt – die Passwörter der Nutzer wurden abgefangen.
https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff

3.2.3 Persönlicher Hotspot

Ein **Hotspot** ist ein mobiler Zugangspunkt zum Internet – etwa dein Handy, das als WLAN-Router für andere Geräte dient.

Wichtig:

- **Sicheres Passwort wählen!**
- **WPA2 oder WPA3 verwenden**
- Nur freigeben, wenn wirklich nötig

🔹 3.2.4 Hotspot steuern

Du kannst deinen Hotspot:

- ✔ **Ein- und ausschalten**
- ✔ **Geräte verbinden oder trennen**
- ✔ **SSID und Passwort ändern**

Tipp: Nutze Hotspots nie dauerhaft – je kürzer offen, desto sicherer.

Fazit: Netzwerke verbinden – und müssen geschützt werden

Ob zu Hause, in der Schule oder im Urlaub: Wer ein Netzwerk nutzt, **trägt Verantwortung**.
Je besser es abgesichert ist, desto sicherer sind deine Daten – und die deiner Mitmenschen.

4 Zugangskontrolle

4.1 Methoden

4.1.1 Maßnahmen gegen unbefugten Zugriff

Um deine Daten zu schützen, brauchst du eine **Zugangskontrolle** – vergleichbar mit einem Türsteher, der nur autorisierte Gäste reinlässt.
Wichtige Mittel dafür:

- **Benutzername & Passwort**
- **PIN (z. B. am Handy oder Bankautomat)**
- **Verschlüsselung** (macht Daten für Fremde unlesbar)
- **Multi-Faktor-Authentifizierung (MFA)**: zusätzlich z. B. SMS-Code oder Fingerabdruck

Beispiel: Die Zwei-Faktor-Anmeldung bei Google verhindert, dass jemand dein Konto übernimmt – selbst, wenn er dein Passwort kennt.
https://safety.google/authentication

4.1.2 Einmalpasswort – der flüchtige Schlüssel

Ein **Einmalpasswort (One-Time Password / OTP)** ist nur für eine kurze Zeit gültig – und wird dann ungültig. Du bekommst es:

- per SMS
- über eine App (z. B. Authenticator)
- auf ein Gerät wie ein TAN-Generator

Anwendungsbeispiele:

- Online-Banking
- Login bei sensiblen Diensten
- Fernzugang zu Systemen

Beispiel: Viele Banken setzen heute auf mobileTAN oder pushTAN, um Online-Banking abzusichern.
~~https://www.verbraucherzentrale.de/wissen/geld-versicherungen/banken-und-sparkassen/die-verschiedenen-tanverfahren-im-vergleich-60575~~

Suchvorschlag: mobileTAN pushTAN Tan-Verfahren

4.1.3 Netzwerkkonto – digitaler Ausweis

Ein **Netzwerkkonto** ist ein Benutzerkonto, mit dem man sich in einem Unternehmens- oder Schulnetzwerk anmeldet. Es dient zur:

- **Identifikation:** Wer bist du?
- **Autorisierung:** Was darfst du tun?
- **Nachvollziehbarkeit:** Was hast du wann gemacht?

Beispiel: In Schulen oder Firmen melden sich Nutzer am PC mit einem Netzwerkkonto an, das Zugriff auf persönliche Dateien, Drucker oder E-Mail gewährt.

4.1.4 Anmelden und abmelden – klingt banal, ist essenziell

Wenn du an einem Gerät angemeldet bist, kann jeder, der es benutzt, auf **dein Konto und deine Daten** zugreifen. Deshalb:

- Immer mit **Benutzername & Passwort** anmelden
- Bei Verlassen: **Sperren oder abmelden**

Beispiel: In einem Co-Working-Space wurde eine Dropbox geöffnet, weil der Vorbenutzer sich nicht ausgeloggt hatte – der neue Nutzer hatte unbeabsichtigt Zugriff.
~~https://www.dropboxforum.com/t5/Sicherheit-und-Konto/Wichtige-Sicherheitstipps-für-geteilte-Geräte/td-p/662901~~

Suchvorschlag: Dropbox Wichtige Sicherheitstipps für geteilte Geräte

4.1.5 Biometrie – der Körper als Schlüssel

Moderne Geräte erkennen uns am Körper:

- **Fingerabdruckscanner**
- **Iris- oder Netzhautscanner**
- **Gesichtserkennung**
- **Handgeometrie (z. B. Handvenenscanner)**

Vorteil: bequem und sicher
Nachteil: Wenn diese Daten kompromittiert werden, kann man sie **nicht einfach ändern** wie ein Passwort

Beispiel: Apples Face ID kombiniert Kamera- und Tiefensensoren – das macht sie sicherer als einfache Foto-Erkennung.
https://support.apple.com/de-de/HT208109

4.2 Passwort Management

4.2.1 Gute Passwörter – deine erste Verteidigung

Ein gutes Passwort ist wie ein starker Schlüssel. Es sollte:

- **mind. 12 Zeichen lang** sein
- **Zahlen, Groß-/Kleinbuchstaben und Sonderzeichen** enthalten
- **nicht** aus dem Wörterbuch stammen
- **regelmäßig geändert** werden
- **nicht mehrfach verwendet** werden

Niemals Passwörter weitergeben – auch nicht an Kolleg*innen oder Support!

Beispiel: Laut einer Studie 2023 war „123456“ noch immer eines der häufigsten Passwörter…
~~https://www.sicherheit.info/die-haeufigsten-passwoerter-2023~~

Suchvorschlag: häufigste-passwörter Fehler 123

4.2.2 Passwortmanager – digitale Tresore

Ein **Passwortmanager** hilft dir, viele sichere Passwörter zu erstellen und zu speichern. Du brauchst nur noch **ein einziges Master-Passwort**.

Beliebte Tools:

- Bitwarden
- KeePass
- 1Password
- LastPass

Aber: Wenn dein Master-Passwort kompromittiert ist, sind alle Passwörter in Gefahr. Deshalb: **Zusätzliche Absicherung per MFA nutzen!**

Beispiel: Immer mehr Unternehmen verpflichten Mitarbeitende zur Nutzung von Passwortmanagern mit Cloud-Synchronisierung.
~~https://www.verbraucherzentrale.de/wissen/digitale-welt/passwoerter/passwortmanager-sinnvoll-oder-nicht-33036~~

Suchvorschlag: Passwort-Manager sinnvoll Risiko

Fazit: Nur autorisierte Personen dürfen rein

So wie du dein Haustürschloss niemandem gibst, solltest du auch mit digitalen Schlüsseln verantwortungsvoll umgehen.
Denn: **Daten haben einen Wert – und sie verdienen Schutz.**

5 Internetdienste

5.1 Browsereinstellungen

5.1.1 Formulardaten im Browser

Webbrowser wie Chrome oder Firefox bieten an, deine Eingaben zu speichern:

- **Automatisches Speichern:** z. B. Name, Adresse, E-Mail
- **Auto-Vervollständigung:** Vorschläge erscheinen beim Tippen

Bequem – aber auch ein Risiko, wenn Dritte Zugriff auf dein Gerät haben.

Du kannst das deaktivieren unter:
Einstellungen → Datenschutz → Formulardaten speichern (deaktivieren)

Beispiel: In einem Internetcafé konnte ein Fremder auf gespeicherte Login-Daten zugreifen, weil der vorherige Nutzer Auto-Vervollständigung nicht deaktiviert hatte.

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Software-und-Einstellungen/Webbrowser/webbrowser_node.html

Suchvorschlag: BSI, Webbrowser, webbrowser_node

5.1.2 Browserdaten löschen

Ein Browser merkt sich viel:

- **Verlauf:** welche Seiten du besucht hast
- **Cache:** gespeicherte Inhalte von Webseiten
- **Cookies:** kleine Dateien mit Infos über dich
- **Passwörter:** gespeicherte Logins
- **Formulardaten**

Diese Daten kannst du löschen – regelmäßig empfohlen!

In Chrome: **Einstellungen → Datenschutz → Browserdaten löschen**
In Firefox: **Einstellungen → Datenschutz → Chronik löschen**

5.2.1 Nur auf sicheren Webseiten einkaufen & bankieren

5.2 Sicheres Surfen

Beim Online-Shopping oder Banking gilt: **Nur auf sicheren Seiten aktiv sein!**

Erkennbar an:
„https://“ (das „s“ steht für „secure“)
Schlosssymbol in der Adresszeile

Keine Daten auf Seiten eingeben, die nur „http://“ anzeigen!

Beispiel: Eine gefälschte Online-Banking-Seite ohne https sammelte Zugangsdaten – über 500 Nutzer waren betroffen.
https://www.verbraucherzentrale.de/wissen/digitale-welt/phishing-und-datenschutz/sichere-webseiten-erkennen-41586

Suchvorschlag: Phishing Datenschutz http

5.2.2 Wie erkennt man eine echte Webseite?

Eine echte Seite erkennst du an mehreren Punkten:

- ✔ **Inhalt wirkt professionell**
- ✔ **Aktualisierungen sind sichtbar**
- ✔ **Impressum & Kontaktinformationen vorhanden**
- ✔ **Sicherheitszertifikat (durch Klick aufs Schloss)**
- ✔ **Domain passt (z. B. amazon.de, nicht amaz0n-login.com)**

Beispiel: 2024 wurde eine Phishing-Seite entdeckt, die Amazon täuschend echt nachbildete – bis auf ein fehlendes SSL-Zertifikat und eine merkwürdige Domain.
https://www.heise.de/news/Phishing-Angriff-mit-faelschter-Amazon-Webseite-9657824.html

Suchvorschlag: Phishing Angriff mit falscher Amazon-Webseite

5.2.3 Pharming – das heimliche Umlenken

Pharming ist gefährlicher als Phishing. Dabei wirst du heimlich auf eine gefälschte Webseite umgeleitet – auch wenn du die richtige Adresse eintippst!

Das geschieht z. B. durch:

- Manipulierte Router
- DNS-Vergiftungen
- Trojaner auf deinem Gerät

Schutz:

- Router regelmäßig aktualisieren
- Antivirenprogramm verwenden
- DNS-Server bei Bedarf manuell einstellen

https://de.wikipedia.org/wiki/Pharming_(Internet)

5.2.4 Webseiten filtern – besonders für Kinder wichtig

Inhaltskontrollprogramme (Webfilter) helfen, schädliche oder unerwünschte Inhalte zu blockieren:

Für Familien:

- Kinderschutzfilter (z. B. „JusProg“)
  https://www.jugendschutzprogramm.de/
- Google SafeSearch
- Einschränkungen direkt am Gerät

Für Unternehmen:

- Surfkontrolle für Produktivität & Sicherheit

Beispiel: Schulen nutzen Filtersoftware, um Gewalt- und Glücksspielseiten automatisch zu sperren.
https://www.klicksafe.de/ueber-klicksafe/aktuelles/news/detail/kindersicheres-internet-filterprogramme-im-vergleich

Suchvorschlag: Klicksafe kindersicheres Internet

Fazit: Surfen mit Köpfchen

Ob Browser, Online-Shop oder E-Mail: Wer **sicher surfen** will, sollte Technik verstehen – und die Augen offenhalten.
Vertrauen ist gut – Zertifikat prüfen ist besser.

6 Kommunikation

6.1 E-Mail

🔹 6.1.1 E-Mail-Verschlüsselung – Briefe im digitalen Umschlag

Wenn du eine E-Mail schreibst, reist sie normalerweise **unverschlüsselt** durch das Internet – wie eine Postkarte. Jeder auf dem Weg könnte mitlesen.

Verschlüsselung bedeutet:

- Deine Nachricht wird in einen geheimen Code umgewandelt
- Nur der Empfänger kann sie lesen

Tools dafür:

- PGP (Pretty Good Privacy)
- S/MIME
- Viele Mailprogramme wie Thunderbird oder Outlook bieten Verschlüsselung

Beispiel: Journalisten nutzen Verschlüsselung, um Whistleblower zu schützen.
https://www.kuketz-blog.de/mailverschluesselung-mit-pgp-die-anleitung/

Suchvorschlag: Mailverschlüsselung PGP

6.1.2 Digitale Signatur – der elektronische Ausweis

Eine **digitale Signatur** zeigt:

- Diese Nachricht stammt **wirklich von der Person**, die sie verschickt hat
- Der Inhalt wurde **nicht verändert**

Sie funktioniert wie eine **unterschriebene Nachricht** mit **Sicherheitscode**

Nützlich z. B. für:

- Verträge
- Angebote
- Unternehmenskommunikation

Beispiel: In der E-Beschaffung der öffentlichen Verwaltung ist eine digitale Signatur oft Pflicht.
https://www.bundesdruckerei.de/de/Serviceportal/Themenwelten/Elektronische-Signatur

Suchvorschlag: öffentliche Verwaltung digitale Signatur

6.1.3 Betrügerische E-Mails erkennen

Unerwünschte und gefährliche E-Mails sind oft:

- **Spam**: Werbung, die keiner will
- **Phishing**: Täuschung, um Passwörter zu stehlen
- **Malware-Träger**: z. B. infizierte Anhänge

Merkmale:
❌ Dringlichkeit („Letzte Mahnung!“)

❌ Rechtschreibfehler
❌ Verdächtige Anhänge (.exe, .zip, .docm)

~~https://www.verbraucherzentrale.de/phishingradar~~

Suchvorschlag: Phishing Radar

6.1.4 Phishing erkennen und melden

Phishing-E-Mails sehen täuschend echt aus – von Amazon, PayPal, deiner Bank. Aber sie wollen nur **deine Zugangsdaten**.

Erkennungszeichen:
⚠️ Gefälschte Logos
⚠️ Verdächtige Links
⚠️ Bitte um Eingabe sensibler Daten
⚠️ Ungewöhnlicher Absender

💡 Immer direkt über die offizielle Webseite einloggen – **niemals über E-Mail-Links!**

Phishing melden:

- an deine Bank
- oder an: **phishing@verbraucherzentrale.de**

~~https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Phishing/phishing_node.html~~

Suchvorschlag: BSI, Phishing, phishing_node

6.1.5 Gefährliche Dateianhänge erkennen

Anhänge können **Malware enthalten**. Besonders gefährlich sind:

- **.exe** (Programme)
- **.zip / .rar** (komprimiert)
- **.docm / .xlsm** (Office-Dateien mit Makros)

Öffne Anhänge nur, wenn du dem Absender vertraust – und sicher bist, dass du den Anhang erwartet hast.

6.2 Soziale Netzwerke

6.2.1 Keine sensiblen Infos in sozialen Netzwerken

Auch wenn Facebook & Co. vertraut wirken:
Keine Passwörter, Adressen oder Bankdaten öffentlich posten
Vorsicht mit Fotos von Ausweisen, Tickets, Kindern

Denke daran: Was einmal gepostet ist, **bleibt oft für immer auffindbar.**

6.2.2–6.2.3 Einstellungen für Privatsphäre & Standort

Dein Konto sollte nur zeigen, was du freigeben willst. Prüfe regelmäßig:

- Wer darf was sehen? (Freunde, öffentlich, individuell)

- Standortfreigabe?
- Sichtbarkeit von Posts, Freundeslisten, Geburtstagen etc.

Beispiel: Meta (Facebook/Instagram) steht immer wieder wegen übergriffiger Standard-Einstellungen in der Kritik.
~~https://www.heise.de/news/Facebook-und-Co-Datenschutzverstoesse-der-grossen-Plattformen-9648236.html~~

Suchvorschlag: Facebook und Co Datenschutzverstösse der grossen Plattformen

6.2.4 Gefahren in sozialen Netzwerken

Soziale Netzwerke sind nicht nur Spiel & Spaß:

⚠️ **Cybermobbing**
⚠️ **Grooming** (Anbahnung sexuellen Missbrauchs)
⚠️ **Falsche Profile**
⚠️ **Fake News**
⚠️ **Schadlinks** in Kommentaren oder Nachrichten

6.2.5 Missbrauch melden

Melden hilft allen! Auf jeder Plattform gibt es Möglichkeiten, Inhalte zu melden – oft über:

📍 Drei Punkte-Menü
📍 „Inhalt melden"-Funktion
📍 Hotline der Plattform
📍 Polizei, wenn Gefahr besteht

In Deutschland hilft auch **jugendschutz.net** bei Fällen mit Kindern:
https://www.jugendschutz.net

6.3 VoIP und Instant Messaging

6.3.1 Risiken bei VoIP & Instant Messaging

VoIP (z. B. Skype) und Messenger (z. B. WhatsApp) sind beliebt – aber auch angreifbar:

- **Malware-Anhänge**
- **Backdoors** (versteckter Zugang)
- **Lauschangriffe**
- **Datenlecks**

6.3.2 Schutz bei Chat & VoIP

So bleibst du sicher:

✔ Verschlüsselte Dienste (z. B. Signal, Threema)
✔ Keine sensiblen Daten im Chat
✔ Gemeinsame Nutzung von Dateien begrenzen

Beispiel: WhatsApp nutzt standardmäßig Ende-zu-Ende-Verschlüsselung – Meta sieht aber trotzdem viele Metadaten.
https://www.datenschutz.org/whatsapp-datenschutz

6.4 Mobile Geräte

6.4.1 Vorsicht mit Apps aus dubiosen Quellen

Nur Apps aus **offiziellen Stores** (Google Play, Apple App Store) installieren.

Gefahr bei Drittanbietern:

⚠️ Malware

⚠️ Spionage

⚠️ Datenklau

⚠️ Fake-Apps mit Abo-Fallen

6.4.2 Berechtigungen verstehen

Apps fragen oft nach Zugriff auf:
📷 Kamera
📍 Standort
📁 Dateien
📞 Kontakte

Nur Berechtigungen erlauben, die **für die App-Funktion wirklich nötig sind.**

6.4.3 Was Apps wirklich sammeln können

Viele Apps senden Daten an Werbenetzwerke – darunter:

- Adressbuch
- Fotos
- Standort
- Surfverhalten
- Nutzungsdauer

Beispiel: Wetter-Apps stehen immer wieder in der Kritik – sie wollen deinen Standort, auch wenn du ihn nicht brauchst.
~~https://www.tagesschau.de/investigativ/wdr/datensammlung-apps-101.html~~

Suchvorschlag: Datensammlung Apps Gefahr

6.4.4 Handy verloren – was tun?

📱 Sofortmaßnahmen:

1. **Ortungsfunktion aktivieren (Android/iOS)**
2. **Fernsperrung und Fernlöschung starten**
3. **SIM-Karte sperren** lassen

4. **Passwörter ändern** (z. B. Google, E-Mail, Bank)

Fazit: Kommunikation braucht Vertrauen – und Vorsicht

Ob E-Mail, WhatsApp oder Facebook – digitale Kommunikation kann sicher sein, wenn wir **unsere Werkzeuge kennen und mitdenken**.

7 Sicheres Daten-Management

7.1 Datensicherung

7.1.1 Geräte physisch schützen

Nicht nur Hacker sind eine Gefahr – auch **Diebstahl oder Verlust**.
So schützt du deine Geräte **physisch**:

- ✔ **Nie unbeaufsichtigt lassen** – weder Laptop noch Smartphone
- ✔ **Gerätestandorte abschließen** (z. B. Serverräume)
- ✔ **Sicherheitskabel** für Laptops in öffentlich zugänglichen Bereichen
- ✔ **BIOS/UEFI-Passwort** & automatische Sperrbildschirme

Beispiel: 2023 wurden vertrauliche Patientendaten öffentlich, weil ein Laptop aus einem Auto gestohlen wurde – unverschlüsselt und nicht gesperrt.
~~https://www.datenschutz-notizen.de/datenschutz-unterm-sitz-0712025/~~

Suchvorschlag: vertrauliche Patientendaten aus einem Auto gestohlen

7.1.2 Warum regelmäßige Backups wichtig sind

Datenverlust passiert häufiger als man denkt – durch:

- Hardwarefehler
- Malware
- Fehlbedienung
- Diebstahl

Backups retten Existenzen! Ein Unternehmen ohne Backup nach einem Angriff steht schnell vor dem Aus.

7.1.3 Regeln für eine gute Datensicherung

Ein gutes Backup ist:

🗓️ **Regelmäßig** (z. B. täglich, wöchentlich)
🗄️ **Gesichert gelagert** (z. B. externer Speicher oder Cloud)
🗜️ **Komprimiert**, um Platz zu sparen
🔐 **Verschlüsselt**, damit niemand mitlesen kann

Es gilt das **3-2-1-Prinzip**:

- 3 Kopien
- 2 unterschiedliche Medien
- 1 davon **außerhalb des Standorts**

~~https://www.heise.de/tipps-tricks/Backup-Strategien-Daten-sichern-wie-die-Profis-5034715.html~~

Suchvorschlag: Tipps Tricks, Backup Strategien Daten sichern

7.1.4 Backup erstellen

Du kannst ein Backup anlegen auf:

- 🖥️ **Lokalem Laufwerk** (z. B. zweite Festplatte)
- 💾 **Externe Medien** (z. B. USB, externe SSD, NAS)
- ☁️ **Cloud-Dienste** (z. B. Google Drive, Dropbox, OneDrive)

Programme:

- Windows-Sicherung
- Time Machine (Mac)
- Acronis, Veeam, Cobian

7.1.5 Daten wiederherstellen

Ein Backup ist **nur dann sinnvoll**, wenn es im Ernstfall **funktioniert**.
Deshalb: Regelmäßig testen!

Du kannst Daten wiederherstellen von:

- ✔ **lokaler Festplatte**
- ✔ **externer Sicherung**
- ✔ **Cloud-Backup**

Viele Tools bieten eine Vorschaufunktion oder Wiederherstellung nur einzelner Dateien.

7.2 Daten richtig löschen und vernichten

7.2.1 Löschen bedeutet nicht vernichten

Wenn du eine Datei „löschst“, landet sie oft nur im **Papierkorb** – oder wird als „frei verfügbarer Speicherplatz“ markiert.

Daten können mit Tools wie **Recuva** oder **Photorec** wiederhergestellt werden – auch nach Monaten!

7.2.2 Warum Daten endgültig gelöscht werden müssen

Manchmal reicht es nicht, Daten „zu löschen“ – etwa bei:

- Verkauf von Geräten
- Ende eines Arbeitsverhältnisses
- Auslauf von Verträgen
- Schutz sensibler Kunden- oder Patientendaten

Beispiel: 2024 kaufte ein Journalist ein gebrauchtes Smartphone – mit gespeicherten Kundendaten eines Logistikunternehmens.
~~https://www.spiegel.de/netzwelt/gadgets/gebrauchte-handys-oft-mit-privaten-daten-a-974489.html~~

Suchvorschlag: gebrauchtes Smartphone Gefahr durch nicht gelöschte Daten

7.2.3 Online gelöscht bedeutet nicht wirklich gelöscht

Was im Internet war, **bleibt oft auffindbar** – selbst, wenn du es „löschst“:

- Beiträge in Foren
- Fotos in der Cloud
- Social-Media-Inhalte

Auch Google & Co. speichern Inhalte länger als dir lieb ist.

~~https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Loeschen-von-Daten/loeschen-node.html~~

Suchvorschlag: BSI, Löschen von Daten

7.2.4 Daten sicher und dauerhaft vernichten

Richtig löschen geht so:

🧨 **Shreddern:** Daten mehrfach überschreiben (z. B. mit „Eraser“ oder „DBAN“)
🧲 **Entmagnetisieren (Degaussen):** für Festplatten
🪓 **Physisch zerstören:** z. B. durch Zerkleinerung
🔧 **Spezialsoftware:** z. B. Blancco, CCleaner, Secure Erase

Besonders bei Altgeräten wichtig – auch Drucker, Router und Smart-TVs speichern Daten!

Fazit: Daten schützen – von Anfang bis Ende

Daten verdienen **Sorgfalt** – von der Erstellung bis zur endgültigen Löschung.

Denn: Was ungewollt offenbleibt, kann **ernste Folgen** haben – für dich, deine Arbeit oder deine Kunden.

Anhang

Mein Angebot

Frei verfügbare eBooks: https://news.konrad-rennert.de/ebook-support

Optionaler Support:

- Durchführung von Schulungen auf Basis dieses E-Books zur IT-Sicherheit
- Workshops und Videokonferenzen mit interaktiven Aufgaben und Fallbeispielen
- Bereitstellung von bearbeitbaren PDFs, Kursmaterialien und Lernvideos
- Didaktische Beratung für Lehrkräfte, z. B. zu Moodle, WordPress, alfaview, MS Teams, Zoom

Zielgruppen

- Lehrkräfte und Bildungseinrichtungen
- Multiplikatoren in der Erwachsenenbildung
- IT-Beauftragte in Initiativen, Vereinen und Organisationen

Kontakt & Umsetzung

Alle Angebote sind modular, flexibel und individuell anpassbar – vom einstündigen Impuls bis zur mehrtägigen Fortbildung.

- Für Schulungen: **flipped-classroom@konrad-rennert.de**
- Allgemeine Anfragen: info@konrad-rennert.de
- Weitere Informationen: https://konrad-rennert.de/?s=learninglounge

Spendenbasierter Zugang zur erweiterten Lernplattform

Die Teilnahme erfolgt spendenbasiert:

- Ab 10 € Spende erhalten Sie eine Benutzerrolle und 3 Monate Zugriff auf geschützte Inhalte auf news.konrad-rennert.de mit weiteren Materialien zum Computerführerschein.
- Eine gültige E-Mail-Adresse genügt – kein Account, kein Passwort
- Die Spende gilt gleichzeitig als Identitätsnachweis

Bearbeitbare PDF-Dokumente für Bildung und Weiterbildung

Wie können Lernende das meiste aus einem bearbeitbaren PDF herausholen – insbesondere mit den Werkzeugen, die direkt im Edge-Browser oder im PDF-Viewer zur Verfügung stehen?

Die KI ChatGPT-4 erklärt die Symbole in der Werkzeugleiste Schritt für Schritt – jeweils mit einer praxisbezogenen Anwendung für Weiterbildung oder Videokonferenzen:

🧰 **Symbolleiste – Funktionen & Anwendungsbeispiele**

🖍️ **Zeichnen (Freihand-Werkzeug)**

🖍️ Damit kannst du per Maus, Stift oder Finger **direkt ins PDF schreiben oder skizzieren**.

🧠 *Anwendung:*
Markiere mit einem Tablet-Stift zentrale Begriffe während einer Live-Erklärung in der Videokonferenz – wie auf einem Whiteboard.

🖊️ **Text hervorheben (Markieren)**

📒 Zum **Hervorheben wichtiger Textstellen**, wie mit einem Textmarker auf Papier.

🧠 *Anwendung:*
Lernende markieren z. B. Begriffe wie „Vertraulichkeit“ oder „Pharming“ und notieren in einer separaten Datei eine Definition – ideal zur Prüfungsvorbereitung.

📝 **Textfeld hinzufügen**

📄 Mit einem Klick kannst du **eigene Notizen als Textbox direkt ins PDF einfügen**.

🧠 *Anwendung:*
Schreibe unter jeden Abschnitt deine eigene Zusammenfassung – oder eine Frage, die du im nächsten Online-Treffen stellen willst.

🗣️ **Vorlesen lassen (z. B. mit Immersive Reader in Edge)**

📢 Edge bietet eine **Vorlesefunktion**, die Texte in natürlicher Sprache wiedergibt.

🧠 *Anwendung:*
Perfekt für DaF-Lernende oder Menschen mit Sehschwäche: Lass dir Inhalte auf Deutsch oder Englisch **abschnittsweise vorlesen**, um Aussprache und Verständnis zu trainieren.

🌐 **Übersetzen (via Kontextmenü oder Microsoft Edge-Add-on)**

🈶 Rechtsklick → „Übersetzen in…“ oder Browsererweiterung nutzen.

🧠 *Anwendung:*
Markiere ein schwieriges Wort oder einen Absatz – und lasse dir die Bedeutung in deiner Muttersprache anzeigen, z. B. als Unterstützung für DaF-Lernende in Videokursen.

📎 **Kommentar hinzufügen**

💬 Kommentare einfügen wie in Word – **ohne das Original zu verändern.**

🧠 *Anwendung:*
Trainer*innen können individuelle Hinweise oder Reflexionsfragen einfügen („Was bedeutet dieser Begriff für deine tägliche Online-Nutzung?“). Oder: Teilnehmende kommentieren gegenseitig.

🔍 **Suchen (Suchfeld rechts oben)**

🔎 **Volltextsuche** durch das gesamte Dokument.

🧠 *Anwendung:*
Schnell nach „Verschlüsselung“ oder „Passwort“ suchen – ideal, wenn du ein Thema wiederholen willst.

🔄 **Drucken & Speichern (Diskette/Druckersymbol)**

💾 Änderungen speichern oder direkt **mit eigenen Ergänzungen ausdrucken**.

🧠 *Anwendung:*
Fertig bearbeitetes Arbeitsblatt ausdrucken oder zur Hausaufgabenkontrolle im Online-Kurs einsenden.

📄 **Seitenanzeige (z. B. „9 von 41“)**

➞ Navigation durch das Dokument.

🧠 *Anwendung:*
Ermöglicht gezielten Zugriff auf das gerade im Online-Meeting besprochene Kapitel – z. B. „Gehe bitte alle auf Seite 12“.

🧑‍🏫 **Online-Kurs-Szenario: Das PDF im Einsatz**

- 🔹 *Vorbereitung:* Teilnehmer laden das PDF im Browser, markieren und kommentieren vor dem Meeting
- 🔹 *Live:* Trainer teilt Bildschirm und erklärt Inhalte – Teilnehmer ergänzen Notizen direkt ins PDF
- 🔹 *Nachbereitung:* Lernende senden ihre Version mit Kommentaren oder Rückfragen ein oder tauschen sich in Gruppenräumen (Breakout-Rooms) aus

✅ **Fazit**

Ein bearbeitbares PDF ist **viel mehr als ein statisches Dokument**. In Verbindung mit den integrierten Werkzeugen – insbesondere in Microsoft Edge – wird es zum **interaktiven Arbeits- und Lernheft**. Es fördert:

- Selbstständiges Arbeiten
- Sprachliches Verständnis
- Digitale Kompetenz
- Kollaboratives Lernen im Online-Unterricht

Zusammenfassung der Funktionen in der Werkzeugleiste

Symbol / Funktion	Einsatz im Bildungsalltag
Zeichnen	Freihand schreiben oder skizzieren – ideal für Hervorhebungen mit einem Stift.
Text markieren	Wichtige Begriffe oder Definitionen hervorheben wie mit einem Textmarker.
Textfeld	Eigene Notizen direkt ins Dokument einfügen – z. B. Zusammenfassungen oder Rückfragen.
Vorlesen	Texte automatisch vom System vorlesen lassen – ideal für DaF-Lernende.
Übersetzen	Abschnitte in deine Muttersprache übersetzen lassen – per Rechtsklick oder Add-on.
Kommentar	Kommentare einfügen, ohne das Original zu verändern – ideal zur Reflexion.
Suchen	Begriff im gesamten Dokument finden – z. B. „Phishing" oder „Verschlüsselung".
Speichern & Drucken	Bearbeitete Seiten sichern oder als Lernnachweis ausdrucken.
Navigation	Gezielt zu Kapiteln springen – z. B. für Besprechung im Online-Meeting.

Haftungsausschluss für Schulungsformate

Die Inhalte aller Webinare, Online-Kurse und Workshops dienen ausschließlich der allgemeinen Information und Weiterbildung. Trotz sorgfältiger Vorbereitung übernehmen Referenten und Veranstalter keine Gewähr für die Aktualität, Richtigkeit oder Vollständigkeit der vermittelten Informationen.

Die Veranstaltungen stellen keine individuelle Rechts-, IT- oder Sicherheitsberatung dar. Die Teilnehmenden sind selbst verantwortlich für die Umsetzung der vermittelten Inhalte in ihrer jeweiligen Organisation oder Praxis.

Für etwaige Schäden oder Verluste, die durch die Anwendung von Inhalten aus der Schulung entstehen, wird keine Haftung übernommen.

Impressum

Titel des Werks:
IT-Sicherheit – Lern- und Trainingskapitel zum ICDL-Syllabus 2.0

Autorenschaft & Projektverantwortung:
Dieses Werk wurde fachlich konzipiert und inhaltlich betreut von:
Konrad Rennert, ECDL-Trainer, Diplom-Physiker, E-Learning-Trainer

https://konrad-rennert.de/profil

E-Mail: info@konrad-rennert.de

Redaktionelle und visuelle Ausarbeitung mit Unterstützung künstlicher Intelligenz:
Die Erstellung der Inhalte, Illustrationen und didaktischen Aufbereitung erfolgte unter aktiver Einbindung von **ChatGPT-4** und **DALL·E**, zwei KI-gestützten Tools der Firma OpenAI.

Was wurde erstellt?

- Kapiteltexte gemäß ICDL-IT-Sicherheit Syllabus 2.0

- Fallbeispiele und Quellenverweise
- Infografiken und Titelbilder im einheitlichen Layout
- Vereinfachte Erklärungen für die Zielgruppen und Altersklassen von älteren Schülern bis zu Senioren

Wie wurde es erstellt?

- Fachlich begleitet durch einen zertifizierten ECDL/ICDL-Trainer
- Unterstützt durch generative KI (Text & Bild) mit manuellem Feinschliff
- Quellen aus öffentlicher Berichterstattung und Behördenportalen (z. B. BSI, Verbraucherzentralen, Heise, Tagesschau, Wikipedia)
- Struktur und Tiefe orientieren sich am ICDL Syllabus IT-Sicherheit 2.0
  Zitat: Copyright © 1997 – 2019 ICDL Foundation / ICDL Germany In Zweifelsfällen gilt die Version der ICDL Foundation (www.icdl.org). … Der Syllabus darf nur in Zusammenhang mit der ICDL Initiative verwendet werden…

Wann wurde es erstellt?
Erarbeitet und aktualisiert im Zeitraum: **März – April 2025**

Warum wurde es erstellt?
Zur Vorbereitung auf das ICDL-Modul *IT-Sicherheit* sowie zur Sensibilisierung für digitale Risiken in Alltag, Schule, Beruf und Gesellschaft.
Das Werk richtet sich ausdrücklich an alle Lernenden – unabhängig von Alter oder Vorwissen – und versteht sich als Beitrag zur digitalen Grundbildung.

Wo darf das Werk verwendet werden?

- Im Rahmen des ICDL/EDCL-Trainings
- Für schulische und berufliche Bildungsmaßnahmen
- In nicht-kommerziellen Weiterbildungsprojekten

Rechtlicher Hinweis zur Verwendung generativer KI:
Die Texte und Bilder in diesem Werk wurden unter aktiver redaktioneller Aufsicht mit Unterstützung künstlicher Intelligenz erzeugt. Eine eigenständige urheberrechtliche Schutzfähigkeit gemäß §2 UrhG besteht, da die Inhalte menschlich kuratiert, strukturiert und finalisiert wurden.

Haftungsausschluss:
Trotz größter Sorgfalt bei der Erstellung übernimmt der/die Herausgeber/in keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte. Die Nutzung erfolgt auf eigene Verantwortung.

Bildnachweise & Tools:
Titel- und Kapitelbilder erstellt mit **DALL·E (OpenAI)**
Inhalte erstellt mit **ChatGPT-4 (OpenAI)**
ICDL-Referenz: ▶ https://www.icdl.de

Lizenzhinweis (CC BY 4.0)