

# IT-Security

Sichere Nutzung der IKT im Alltag

# 1. Grundbegriffe zu Sicherheit

---

## 1.1. Datenbedrohung

### *Aus Daten werden Informationen*

*Beispiel: Wir messen die monatlichen Niederschlagsmengen innerhalb eines Jahres.*

*Unsere Messungen ergeben: 60 mm, 55 mm, 79 mm, 83 mm, 144 mm, 155 mm, 157 mm, 151 mm, 101 mm, 73 mm, 83 mm, 73 mm.*

*Mit Hilfe dieser Daten können verschiedene Fragen beantwortet werden:*

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

Die Antworten auf diese Fragen sind Informationen, die aus den Daten – nämlich den Messreihen - gewonnen wurden.

### **Cybercrime (Internetkriminalität)**

Internetkriminalität sind Straftaten, die auf dem Internet basieren oder mit den Techniken des Internets geschehen. Beispiele hierfür sind Internetbetrug, das Ausspähen von Daten, Identitätsdiebstahl, Urheberrechtsverletzung, Cyber-Terrorismus, Cyber-Mobbing, Volksverhetzung sowie das Verbreiten von Kinderpornographie.

### **Hacking oder Cracking?**

Hacker und Cracker umgehen Zugriffsbarrieren von Computer- und Netzwerksystemen. Der Begriff Hacker wird nicht einheitlich verwendet. Als Cracker werden Menschen bezeichnet, die in böswilliger Absicht in ein Computersystem eindringen. In den Medien wird zwischen den Begriffen Hacker und Cracker kaum unterschieden.

Es gibt auch Sicherheitsexperten, die Computersysteme auf Sicherheitslücken überprüfen, indem sie versuchen in das System einzubrechen (ethisches Hacking).

### **Daten können verloren gehen**

Computer können durch Feuer, Hochwasser und Erdbeben zerstört werden. Dabei werden auch wertvolle Daten vernichtet. Für viele Firmen würde der Kompletverlust ihrer Daten den Konkurs bedeuten: alle Kundenadressen wären verloren, ausstehende Zahlungen könnten nicht eingefordert werden, die Produktion könnte nicht mehr aufrecht erhalten werden...

Nur eine gut geplante Datensicherung (Backup) kann einen jederzeit möglichen Datenverlust verhindern:

Die Aufbewahrung von Datensicherungen sollte örtlich entfernt von der EDV-Anlage und in einer sicheren Umgebung erfolgen.

- Für Privatpersonen bieten sich externe Festplatten an. Diese lassen sich einfach an den Computer anschließen und ermöglichen so eine entfernte Aufbewahrung.
- Für kleinere Unternehmen eignen sich z. B. Bankschließfächer zur Datenträgeraufbewahrung. Eine Alternative dazu stellt Online Backup dar: die

Datensicherung erfolgt außer Haus, meist in einem Rechenzentrum, und es kann jederzeit darauf zugegriffen werden.

- Für größere Unternehmen (Banken, Versicherungen, Behörden etc.) können sich speziell gesicherte Safes oder Räumlichkeiten zur feuersicheren Unterbringung der Sicherungen lohnen. Auch können die gesicherten Daten auf mehrere Standorte oder Rechenzentren verteilt werden.

### **Die Bedrohung der Datensicherheit von innen!**

Mitarbeiter einer Firma geben interne Daten absichtlich oder unabsichtlich weiter.

- MitarbeiterInnen verraten ihre Passwörter, indem sie diese auf Klebezettel notieren.
- Frustrierte MitarbeiterInnen nehmen Daten aus der Firma mit.
- USB-Sticks und Notebooks gehen verloren
- verseuchte Datenträger (z.B. USB-Sticks) schleusen Malware in das Unternehmen ein.

Aktuelle Beispiele:

*Eine Bankmitarbeiterin will vertrauliche Unterlagen zu Hause weiter bearbeiten und schickt sich diese an die eigene E-Mail Adresse. Leider vertippt sie sich und wählt die falsche Adresse aus.*

*Ein Mitarbeiter bekommt als angebliches Werbegeschenk einen USB-Stick zugesandt. Er steckt ihn an seinem Arbeitsplatzcomputer an und installiert so unabsichtlich eine Spionageprogramm.*

## **1.2. Informationen sind wertvoll**

### **Sei sparsam bei der Weitergabe von personenbezogenen Daten**

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

Was kann passieren, wenn solche Daten in die falschen Hände gelangen?

- Unerwünschte Werbung wird an die persönliche Mailadresse geschickt (Spam)
- Über einmal veröffentlichte Daten hat man keine Kontrolle über deren Weiterverwendung und können später unerwünscht an anderen Stellen wieder auftauchen.
- Besonders Kinder sind oft leichtfertig bei der Veröffentlichung von Daten. Erwachsene mit schlechten Absichten können Kinder belästigen.

*Beispiel für einen Identitätsdiebstahl bzw. Identitätsmissbrauch: Eine junge Frau wird von Freunden darauf aufmerksam gemacht, dass auf ihrem Namen und mit ihren Fotos eine Facebookseite existiert. Auf dieser Seite werden rufschädigende Meldungen über sie und ihren Arbeitgeber gepostet. Nur eine sofortige Aussprache mit ihrem Chef und eine Anzeige bei der Polizei verhindern eine Entlassung.*

### **Was kann ich tun, um meine Daten zu schützen?**

- Sichere Passwörter haben mindestens acht Buchstaben, Zahlen und Sonderzeichen. Sie sollen nicht leicht zu erraten sein, also kein Geburtsdatum oder Name von Angehörigen verwenden.

- Verwende für jeden Zugang ein eigenes Passwort, besonders für wichtige Konten wie E-Mail und Onlinebanking. Wenn du immer dasselbe Passwort verwendest, können Betrüger mit einem erbeuteten Passwort auf mehrere wichtige Konten zugreifen.
- Wichtige Daten sollten verschlüsselt gespeichert werden. Notebooks können verloren gehen oder gestohlen werden. Oft wiegt der Verlust der Daten wesentlich schwerer als die Neubeschaffung des Notebooks.

*Schlagzeilen von Datendiebstählen: Persönliche Daten von acht Millionen Hotelgästen gestohlen. Notebookschwund in den Ministerien. Brite ersteigert Laptop mit Bankdaten bei Ebay. Britisches Verteidigungsministerium: wieder 28 Notebooks weg...*

## Datensicherheit

Daten sollen vor Verlust und unberechtigter Einsicht und Manipulation geschützt sein.

### Vertraulichkeit:

mehr oder weniger geheime Daten müssen geschützt werden:

*Krankenakten dürfen nur von behandelnden medizinischen Personal eingesehen werden. Nicht jeder Beschäftigte eines Krankenhauses hat Zugang zu allen Patientendaten.*

*Lehrer dürfen Adressenlisten von Schülern nicht an schulfremde Personen und Firmen weitergeben.*

### Integrität

Daten sollen vollständig und unverändert sein. Eine Veränderung könnte absichtlich (Sabotage), unabsichtlich oder durch einen technischen Fehler passieren.

*Zeitungsmeldung: Frau irrtümlich für tot erklärt: Drei Wochen nach dem Tod ihrer Mutter wurde auch deren 66-jährige Tochter für tot erklärt. Weil sie keine Pension mehr erhielt, meldete sich die Frau bei der Sozialversicherungsanstalt. Dort waren nach dem Tod der Mutter nicht nur deren Daten, sondern auch gleich alle Daten der Tochter aus dem Computer gelöscht worden.*

### Verfügbarkeit

Systemausfälle sollen verhindert werden, damit der Zugriff auf die Daten zuverlässig gewährleistet ist. Unser Leben ist in hohem Ausmaß auf die Zuverlässigkeit von Computersystemen angewiesen!

*Meldung 2009: In ganz Österreich ist es für drei Stunden zu einem Ausfall im gesamten Bankomatnetz gekommen. Ein Defekt sorgte dafür, dass Kunden in weiten Teilen kein Geld beheben oder in Geschäften mit Karte zahlen konnten. Kunden wurde teilweise auch Karten eingezogen...*

### Personenbezogene Daten werden gesetzlich geschützt!

Das Datenschutzgesetz 2000 regelt den Schutz personenbezogener Daten in Österreich wie z.B. E-Mail-Anschrift, Geburtsdatum oder Telefonnummer.

- Datengeheimnis: Personenbezogene Angaben dürfen ohne vorherige Zustimmung des Betroffenen nur in speziellen Fällen weitergegeben werden.
- Recht auf Auskunft: Jeder kann Auskunft über die zu seiner Person verarbeiteten Daten verlangen. Falls die Auskunft nicht erfolgt oder unvollständig ist, kann man sich an die Datenschutzkommission wenden.
- Recht auf Richtigstellung oder Löschung: Falls Daten unrechtmäßig oder unrichtig gespeichert worden sind, kann ihre Richtigstellung oder Löschung durchgesetzt werden.

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

- Jedes Unternehmen, das Daten verarbeitet, muss eine DVR-Nummer (Datenverarbeitungsregister-Nummer) angeben. Damit kann die Herkunft der Daten nachvollzogen werden.

*Beispiel: Eine Schülerliste wird aus der Schulverwaltung ausgedruckt – in der Fußzeile wird die DVR-Nummer angegeben z.B. DVR: 0103012*

### **Datensicherheit braucht Strategie!**

Datenverarbeiter müssen darauf achten, dass ihre Daten sicher gespeichert werden und dass keine Unbefugten zu den Daten Zugang haben. Dazu müssen Vorkehrungen getroffen werden:

- Backups dienen zur Wiederherstellung von Daten im Falle von Zerstörung (Brand, Hochwasser, Diebstahl etc.). Herkömmliche Backups erfolgen auf Datenträger, die örtlich entfernt von z.B. einer Firma aufbewahrt werden. Online Backups werden über das Internet zu einem Backupserver übertragen.
- Eine USV (unabhängige Stromversorgung) sichert bei Stromausfall den unterbrechungsfreien Betrieb eines Servers.  
*Genau besehen hat ein Notebook eine USV in Form eines Akkus!*
- Weiter Sicherungsmaßnahmen für Server sind beispielsweise Datenspeicherung auf mehreren Festplatten (RAID-Systeme), doppelt vorhandene Server etc.
- Nicht jeder Mitarbeiter hat Zugriff auf alle Daten. Der Datenbankadministrator teilt den Mitarbeitern abgestufte Zugriffsrechte zu. Nach der Angabe von Benutzername und Passwort weist das Computersystem dem Benutzer entsprechende Zugangsrechte zu.
- Mitarbeiter müssen für den sicheren Umgang mit Daten geschult werden. Es werden Richtlinien vorgeschrieben wie z.B.: keine USB-Sticks verwenden, keine Mails mit sensiblen Daten versenden, keinesfalls Zugangsdaten weiterzugeben etc.

### **Persönliche Sicherheit**

- **Social Engineering** ist eine Methode von Betrügern durch Ausnutzung von zwischenmenschlichen Beeinflussungen unberechtigt an Daten zu kommen.  
*Beispiel: Ein Mitarbeiter erhält einen Anruf eines angeblichen Technikers, der vorgibt für einen Test die geheimen Zugangsdaten zu benötigen.*
- **Phishing**  
*Beispiel: ein gefälschtes E-Mail fordert auf, einen Link auf eine gefälschte Webseite anzuklicken und dort die geheimen Zugangsdaten (z.B. für Ebay, Paypal, E-Mail, Bank, etc.) einzugeben.*
- **Shoulder Surfing**: an Geldautomaten, in Internetcafés, beim Arbeiten in der Öffentlichkeit am Notebook kann die Eingabe von Zugangsdaten beobachtet werden.
- Als **Identitätsdiebstahl bzw. Identitätsmissbrauch** wird die missbräuchliche Verwendung personenbezogener Daten bezeichnet.
- **Information Diving**: oft landen sensible Informationen durch Achtlosigkeit im Papiermüll wie z.B. Akten, Adressenlisten, Kontoauszüge, Briefe etc.

- Beim **Pretexting** besorgt sich jemand unter Vorspiegelung einer fremden Identität Informationen sensible Daten eines Dritten. 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:*

DiesisteinKlartextunderwirdnunverschlüsselt  
GLHVLVWHLQNODUWHAWXQGHUZLUGQXQYHUVFKOXHVVHOW

Verschlüsselung kann auf Datei- bzw. Datenträgerebene stattfinden:

- **Verschlüsselung auf Dateiebene:** Dateien werden beim Speichern oder beim Komprimieren mit einem Passwort verschlüsselt. Nachteil: umständlich bei vielen Dateien.
- **Verschlüsselung auf Datenträgerebene:** auf dem Computer wird die Festplatte erst nach Eingabe eines Passwortes entschlüsselt. Der Benutzer merkt nichts von der Verschlüsselung, da diese im Hintergrund geschieht. Beim Diebstahl eines verschlüsselten Datenträgers sind alle Dateien für den Dieb unleserlich. Die Professionalversionen von Windows bieten eine derartige Verschlüsselung. Alternativ gibt es kostenlos das Programm Truecrypt.

Eine Verschlüsselung ist so sicher wie das Passwort: man muss es geheim halten, regelmäßig ändern, das Passwort soll aus Buchstaben, Ziffern und Sonderzeichen zusammengesetzt sein und eine angemessene Mindestlänge aufweisen.

## 2. Malware sind Schadprogramme

---

Der Begriff Malware setzt sich aus den englischen Begriffen **malicious**, „böartig“ und **Software** zusammen. Malware ist ein Überbegriff für unerwünschte und schädliche Software, die ohne Wissen des Benutzers im Hintergrund auf dem Rechner läuft.

### 2.1. Definition und Funktionsweise und Typen

**Computerviren** sind die älteste Art der Malware, sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben.

Ein **Computerwurm** ähnelt einem Computervirus, verbreitet sich aber direkt über Netze wie das Internet und versucht, in andere Computer einzudringen.

**Makroviren** sind Computerviren, die nicht als eigenständiges Programm vorliegen, sondern in Form eines Makros. Ein Makro ist ein Programm, das in einem Dokument eingebettet ist. So kann zum Beispiel ein Excel-Dokument ein Programm enthalten, das bestimmte Vorgänge automatisiert und dem Benutzer Arbeit abnimmt. Ein Makrovirus ist so programmiert, dass er sich selbst in andere Dokumente einnistet und schädliche Funktionen aufruft z.B. ein Rootkit aus dem Internet herunterlädt und installiert.

Mit den Makro-Sicherheitseinstellungen kann man die Ausführung von Makros steuern.

Ein **Trojanisches Pferd** (kurz Trojaner) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, böartigen Teil. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Ein **Rootkit** ist ein Programm, das die Kommunikation zwischen Anwendern und dem Betriebssystem manipuliert. So werden z.B. Virendateien für den Benutzer und unsichtbar gemacht und dadurch

**Keylogger** sind Programme, die Tastatureingaben mitprotokollieren. Damit können Betrüger z.B. Passwörter herausfinden.

Eine **Backdoor** ist eine verbreitete Schadfunktion, die üblicherweise durch Viren, Würmer oder Trojanische Pferde eingebracht und installiert wird. Sie ermöglicht Dritten einen Zugang („Hintertür“) zum Computer unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft genutzt, um den kompromittierten (befallenen) Computer als Spamverteiler oder für Angriffe auf andere Computersysteme (Denial-of-Service-Angriffe) zu missbrauchen.

**Spyware** und **Adware** (zusammengesetzt aus **advertisement** und **Software**) forschen den Computer und das Nutzerverhalten aus und senden die Daten an den Hersteller oder andere Quellen, um diese entweder zu verkaufen oder um gezielt Werbung zu platzieren. Diese Form von Malware wird häufig zusammen mit anderer, nützlicher Software installiert, ohne den Anwender zu fragen und bleibt auch häufig nach deren Deinstallation weiter tätig.

**Scareware** ist darauf angelegt, den Benutzer zu verunsichern und ihn dazu zu verleiten, schädliche Software zu installieren oder für ein unnützes Produkt zu bezahlen. Beispielsweise werden gefälschte Warnmeldungen über angeblichen Virenbefall des Computers angezeigt, den eine käuflich zu erwerbende Software zu entfernen vorgibt.

Teils werden auch **Dialer** (Einwahlprogramme auf Telefon-Mehrwertnummern) unter Malware genannt. Dialer-Programme führen die Einwahl heimlich, d. h. im Hintergrund und vom Benutzer unbemerkt, durch und fügen dem Opfer finanziellen Schaden zu, der etwa über die Telefonrechnung abgerechnet wird. Mit der großen Verbreitung von Breitbandanschlüssen sind Dialerprogramme heute kaum von Bedeutung.

## 2.2. Schutz vor Malware

### Antiviren-Software

Ein Antivirenprogramm sollte Vireninfectionen verhindern bzw. entdecken und entfernen. Da täglich neue Viren auftauchen, lädt das Antivirenprogramm laufend automatisch die neuesten Vireninformationen (Virensignaturen) von der Herstellerseite herunter. Nur ein aktuelles Antivirenprogramm kann seine Aufgaben erfüllen!

Antivirensoftware überprüft laufend aktuelle Dateioperationen und in regelmäßigen Zeitabständen werden die Laufwerke auf Virenbefall durchsucht (gescannt).

Verdächtige oder infizierte Dateien werden entweder gelöscht oder in den Quarantäneordner verschoben, wo sie keinen Schaden anrichten können.

## 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.
- **WAN** (Wide Area Network) ist ein Rechnernetz, das sich im Unterschied zu einem LAN über einen sehr großen geografischen Bereich erstreckt.
- **VPN** (Virtual Private Network) verbindet (meist verschlüsselt) Netzwerke über Internet  
Beispiel: Ein Datenbankadministrator greift per VPN auf die Dateien eines Servers zu und kann sie auf seinen Rechner kopieren, löschen etc.

#### Datensicherheit im Netzwerk

Ein Netzwerk ermöglicht vielen Computern den Zugriff auf Daten. Beim Zugriff auf diese Daten muss gewährleistet sein, dass nur berechtigte Benutzer die ihnen zustehenden Daten verwenden dürfen.

*Beispiele: die Lohnabrechnung dürfen nur Mitarbeiter der Lohnverrechnung sehen, Dokumente des Chefs sollen für andere Mitarbeiter nicht zugänglich sein.*

- **Authentifizierung:** ein Benutzer muss sich mit Benutzerkennung und Passwort anmelden. Damit „weiß“ das System, auf welche Daten der Benutzer und wie (z.B. nur lesend) zugreifen darf.
- **Benutzerrechte:** sie geben an, welche Daten der Benutzer bearbeiten, welche er nur sehen darf und auf welche er nicht zugreifen kann.
- **Nutzung dokumentieren:** Jeder, der auf sensible Daten zugreift, muss damit rechnen, dass diese Zugriffe registriert und gespeichert werden. Damit kann gegebenenfalls nachvollzogen werden, wer bestimmte Daten abgerufen hat.

*Österreich: Weil er die Adresse seines Nebenbuhlers über den Dienstcomputer im zentralen Melde-register (ZMR) abgefragt hatte, wurde ein Polizist wegen Amtsmissbrauchs zu einer bedingten Geldstrafe von 4000 Euro verurteilt.*

#### Wozu braucht man eine Firewall?

- Die **externe Firewall** befindet sich zwischen verschiedenen Rechnernetzen. Sie schützt das interne Netzwerk, Sie tut dies, indem sie beispielsweise (Antwort-)Pakete durchlässt, die aus dem internen Netz heraus angefordert wurden und alle anderen Netzwerkpakete blockiert.
- Eine **Personal Firewall** ist eine Software, die auf dem zu schützenden Rechner installiert ist. Alle aktuellen Betriebssysteme haben eine Firewall, die standardmäßig aktiviert ist.

Firewalls bieten nur einen Schutz, wenn der Rechner nicht kompromittiert ist, da vor allem Datenpakete, die der Rechner nicht angefordert hat, abgewiesen werden. Ein Rechner mit z.B. einem Spywareprogramm fordert selbständig Daten aus dem Internet an und versendet auch

Daten. Hier kann eine Firewall nicht unterscheiden, ob der Datenverkehr erwünscht ist oder nicht<sup>1</sup>. Es ist daher wichtig, alle Programme (vor allem Browser und Betriebssystem) auf dem neuesten Stand zu halten, damit keine Sicherheitslöcher ausgenutzt werden können.

## 3.2. Netzwerkverbindungen

Der Anschluss ans Netzwerk kann per Netzkabel oder drahtlos per Funkverbindung erfolgen. Jede Verbindung mit einem Netzwerk bedeutet, dass der Rechner dem Risiko eines Angriffs von außen ausgesetzt ist.

## 3.3. Sicherheit im drahtlosen Netz

Drahtlose Netzwerke sollten aus Sicherheitsgründen verschlüsselt werden. Der Benutzer gibt bei der Anmeldung ein Passwort ein und wird dann mit dem Funknetz verbunden. Damit ist der Zugang zum Netzwerk nur berechtigten Nutzern möglich und aus dem verschlüsselten Netzwerkverkehr können keine Informationen entnommen werden.

Es gibt verschiedene Verfahren zum Schutz von drahtlosen Netzwerken:

- **Wired Equivalent Privacy (WEP)**: unsicher und daher nicht zu empfehlen. WEP-Verbindungen können ohne großen Aufwand abgehört werden.
- **Wi-Fi Protected Access (WPA bzw. WPA2)** bieten eine nach heutigem Stand eine sichere Verschlüsselung.

Offene Netzwerke erlauben jedem den Zugang zum Internet (z.B. in öffentlichen Räumen wie Flughäfen). Man sollte aber wissen, dass in offenen Netzwerken unverschlüsselter Datenverkehr abgefangen werden kann. Nur wenn im Browser vor der URL **https** aufscheint, werden die Daten verschlüsselt.

## 3.4. Zugriffskontrolle

Ein Netzwerkzugang bietet den Zugriff auf gemeinsame Ressourcen wie Daten, Netzwerkdrucker und andere Serverdienste. Benutzername und Passwort ermöglichen nur befugten Benutzern den Zugang.

Ein gutes Passwort sollte

- aus Klein und Großbuchstaben, Ziffern und Sonderzeichen bestehen
- eine Mindestlänge von 8 Zeichen haben und nicht in einem Wörterbuch stehen
- keine persönlichen Bezug haben wie Geburtsdatum, Namensteile etc.
- regelmäßig geändert werden

Gutes Passwort: `mVi1963g` (Merkhilfe: **mein Vater ist 1963 geboren**)

Schlechte Passwörter: `12345 qwertz geheim hallo boss password ...`

Biometrische Verfahren nutzen körpereigene unverwechselbare Merkmale zur Personenidentifikation: Fingerabdruck, Handgeometrie, Auge (Iris-Scanner), Gesichtserkennung, Stimmerkennung.

---

<sup>1</sup> Es gibt allerdings professionelle Firewalls, die versuchen, verdächtigen Datenverkehr zu blockieren.

Beispiele: Viele Notebooks haben einen Fingerabdruckscanner, Arbeitszeiterfassung ist möglich durch Fingerscan, Serverraumabsicherung durch Gesichtserkennung...

## 4. Sichere Web-Nutzung

---

### 4.1. Browser verwenden

#### Einkaufen im Internet

Kaufe nur bei seriösen Shops! Seriöse Firmen erkennt man z.B. durch positive Bewertungen im Internet, klare Produkt-, Versand- und Bezahlinformationen und Angabe von Kontaktmöglichkeiten durch Telefon, E-Mail und Adresse.

Bei Einkauf und Online-Banking ist die Übermittlung von wichtigen persönlichen Daten notwendig. Achte darauf, dass dies auf einer sicheren Webseite erfolgt.

Sichere Webseiten erkennt man am Protokoll <https://> (*hypertext transfer protocol secure*) und an einem geschlossenen Vorhangschloss. Die Daten werden verschlüsselt übertragen.



Begriffe zur Sicherheit im Internet:

- **Digitales Zertifikat:** Geschützte Webseiten besitzen ein **digitales Zertifikat**, das von verschiedenen unabhängigen Zertifizierungsstellen (z.B. *GlobalSign, Verisign, Trust Center u.a.*) ausgegeben wird. Ein digitales Zertifikat enthält Informationen über den Namen des Inhabers der Webseite.

*Beispiel: <https://www.sparkasse.at>. Klick auf das Vorhangschloss, um Informationen über die Webseite zu erhalten!*

- **Einmal-Kennwörter** werden z.B. zur Autorisierung von Bezahlvorgängen verwendet. Sie sind nur für einen Vorgang gültig und können nicht wieder verwendet werden.

*Beispiel: beim Online-Banking wird eine Transaktionsnummer per SMS auf das Handy des Bankkunden gesandt. Dies erhöht die Sicherheit wesentlich, weil zwei voneinander unabhängige Übertragungswege - Internet bzw. Handynetz – verwendet werden.*

**Beim Onlinebanking mit einem Smartphone sollte man sich deshalb die Transaktionsnummer (TAN) per SMS an ein zweites Handy senden lassen.**

- **Pharming** ist eine Betrugsmethode, die durch das Internet verbreitet wird. Sie basiert auf einer Manipulation der DNS-Anfragen von Webbrowsern um den Benutzer auf gefälschte Webseiten umzuleiten. Dies setzt voraus, dass auf dem Rechner ein Schadprogramm aktiv war oder noch ist.
- Im Browser gibt es Einstellungen, die das **Ausfüllen von Formulardaten** erleichtern, indem sie persönliche Daten bereits in die Felder einfügen. Die Funktion **AutoVervollständigen** schlägt bei Eingaben in der Adressleiste passende URLs vor. Diese Funktionen sind zwar praktisch, können aber ein Sicherheitsrisiko darstellen.

*Probiere selbst: im Internet Explorer aktiviert bzw. deaktiviert man die Einstellungen so:  
Extras → Internetoptionen → Registerkarte Inhalte → AutoVervollständigen → Einstellungen.*

- **Cookies** sind Dateien, die auf dem Computer durch Webseiten abgespeichert werden, um Einstellungen wie z. B. Anmeldeinformationen zu speichern. Diese werden beim erneuten Besuchen dieser Webseiten wieder verwendet. Das kann für den Nutzer des Internets beim neuerlichen Besuch einer Webseite sinnvoll sein und das Surfen erleichtern. Surft man auf einem fremden PC, sollten die persönlichen Einstellungen und Eingaben gelöscht werden:

*Extras → Internetoptionen → Registerkarte Allgemein → Browserverlauf → Löschen → Cookies löschen.*

Das **Blockieren oder Zulassen von Cookies** kann im Internet Explorer gesteuert werden:  
*Extras → Internetoptionen → Registerkarte Datenschutz. Durch das Verschieben des Schiebereglers kann die Behandlung von Cookies beeinflusst werden.*

- Während der Verwendung des Browsers werden die besuchten Seiten (der Verlauf), temporäre Internetdateien und je nach Einstellung Passwörter, Cookies und Formulardaten gespeichert. Diese Daten, mit der Hilfe man die Internetnutzung nachvollziehen kann, sollten auf fremden Rechnern entfernt werden:

*Extras → Internetoptionen → Registerkarte Allgemein → Löschen.*

- Um Kinder vor ungeeigneten Webinhalten und unkontrollierter Internetnutzung zu schützen, gibt es Inhaltfilter und Kindersicherungen. Der Internet Explorer bietet dazu Einstellungen:

*Internetoptionen → Inhalte → Inhaltsratgeber...*

## 4.2. Soziale Netzwerke

Fallbeispiele für Missbrauch von sozialen Netzwerken:

- *A. hat ihre Emailadresse in Facebook bekannt gegeben. Jetzt erhält sie lästige E-Mails von ihr unbekanntenen Personen.*
- *W. hat auf seinem Facebookprofil Fotos von einer Party eingestellt, die ihm später peinlich sind. Leider haben seine „Freunde“ schon diese Fotos kopiert und an anderen Stellen veröffentlicht.*
- *N. wird bei einer Stellenbewerbung trotz bester Aussichten überraschend abgelehnt. Auf Umwegen erfährt sie, dass ein Foto von ihr in lockerer Bekleidung mit einer Bierflasche in der Hand, das sie vor einiger Zeit auf Facebook veröffentlicht hatte, den Grund für die Ablehnung lieferte.*
- *J. wird per Facebook von seinen Mitschülern gemobbt. Jeden Tag muss er abfällige Bemerkungen in Facebook lesen. Zusätzlich wird er mit bearbeiteten Fotos lächerlich gemacht.*

Wir wollen hier nicht Facebook nur negativ darstellen. Facebook ermöglicht es, Kontakte über Kontinente hinweg zu führen, Freunde an seinem Leben teilhaben zu lassen oder Erfahrungen und Tipps auszutauschen.

### Tipps für den sicheren Umgang mit sozialen Netzwerken:

- Sei vorsichtig mit der Angabe von persönlichen Daten wie Adresse, Telefonnummer, Geburtsdatum, Emailadresse usw.
- Überlege dir, welche Fotos du einstellst. Sie könnten dir später peinlich sein.

- Prüfe Freundschaftsanfragen und wähle nur Menschen, die du auch kennst.
- Überprüfe deine Sicherheitseinstellungen zum Schutz der Privatsphäre. Wer Inhalte für Freunde von Freunden frei gibt, macht sie für fast alle sichtbar!

### Fachbegriffe

- **Cyber-Mobbing:** Mobbing mit Hilfe von elektronischen Medien.
- **Cyber-Grooming:** gezieltes Ansprechen von Kindern und Jugendlichen im Internet mit dem Ziel der Anbahnung sexueller Kontakte.
- **Falsche Identität:** nicht jeder ist der, der er zu sein vorgibt. Es ist relativ einfach, eine falsche Identität vorzuspielen.
- **Arglistige Links oder Nachrichten** führen zu problematischen Webseiten, die z.B. versuchen, Malware zu installieren.

## 5. Kommunikation

---

### 5.1. E-Mail

E-Mails werden standardmäßig unverschlüsselt versandt, ihre Sicherheit entspricht also eher einer Ansichtskarte.

Auch der Absender kann einfach geändert werden: wenn man eine E-Mail von einer Firma erhält, kann nicht mit Sicherheit ausgeschlossen werden, dass dieses Mail gefälscht wurde.

#### E-Mails verschlüsseln

Aktuelle Emailprogramme bieten eine **Verschlüsselung** an. Die Nachricht wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Der Empfänger entschlüsselt die Mail mit seinem geheimen privaten Schlüssel. Der öffentliche Schlüssel kann aus dem Internet von einem Keyserver abgerufen werden.

#### Digitale Signatur für E-Mails

Eine **digitale Signatur** stellt sicher, dass die E-Mail vom angegebenen Absender stammt und unverändert übermittelt wurde.

Optimale Sicherheit wird durch verschlüsselte und digital signierte E-Mails erreicht.

#### Unerwünschte E-Mails

**Spam bzw. Junk E-Mails:** sind unerwünschte Werbemails für zweifelhafte Produkte wie Medikamente, Aktien oder vorgetäuschte Lottogewinne.

**Phishing** (von engl. **password fishing**) E-Mails geben vor, von einer seriösen Quelle wie z.B. einer Bank zu stammen. Der Empfänger wird aufgefordert auf einer gefälschten Webseite geheime Zugangsdaten einzugeben. Damit können dann Betrüger Geld abheben.

E-Mailanhänge können auch Malware enthalten. Beim Öffnen eines Attachments kann der Computer infiziert werden, beispielsweise durch ein Dokument, das ein Makro enthält oder durch eine ausführbare Datei.

## 5.2. Instant Messaging (webchat, icq, windows live messenger...)

**Instant Messaging** (kurz **IM**, englisch für „sofortige Nachrichtenübermittlung“) oder Nachrichtensofortversand ist eine Kommunikationsmethode, bei der sich zwei oder mehr Teilnehmer per Textnachrichten unterhalten (chatten). Dabei geschieht die Übertragung so, dass die Nachrichten unmittelbar beim Empfänger ankommen. Die Teilnehmer müssen dazu mit einem Computerprogramm (genannt Client) über ein Netzwerk wie das Internet direkt oder über einen Server miteinander verbunden sein. Viele Clients unterstützen zusätzlich die Übertragung von Dateien und Audio- und Video-Streams.

Benutzer können sich gegenseitig in ihrer Kontaktliste führen und sehen dann an der Präsenzinformation, ob der andere zu einem Gespräch bereit ist.

### Tipps für sicheres Chatten

- In Chats kann man sich nie sicher sein, ob das Gegenüber auch wirklich der ist, wofür er oder sie sich ausgibt. Scheinbar persönliche Informationen und Fotos brauchen nicht unbedingt mit der realen Person übereinzustimmen. So kann es zum Beispiel vorkommen, dass man mit einem Mann chattet, der sich für eine Frau ausgibt.
- Beim Chatten mit Menschen, die dir persönlich unbekannt sind, sei freundlich aber bleibe misstrauisch. Gib keine persönlichen Daten wie Adresse, Telefonnummern, Nachnamen und E-Mailadressen preis.
- Solltest du unangenehm belästigt werden, brich den Chat ab und sprich darüber mit Menschen, denen du vertraust.
- Chatprogramme bieten zusätzliche Funktionen zur Übermittlung von Dateien an. Hier sind dieselben Vorsichtsmaßnahmen sinnvoll wie auch sonst im Internet z.B. keine Programmdateien unbekannter Herkunft starten, da diese Malware aller Art enthalten können.
- Grundsätzlich muss man sich bewusst sein, dass bei *icq* und *windows live messenger* die Übertragung nicht verschlüsselt wird. Es allerdings Möglichkeiten verschlüsselt zu kommunizieren wie z.B. mit der Chatfunktion von *Skype* oder mit alternativen IM-Clients wie *Pidgin*.

## 6. Sicheres Daten-Management

---

Daten sind auf Datenträgern in Computern gespeichert. Um diese vor Diebstahl zu sichern sollten Maßnahmen ergriffen werden:

- **Zugangsbeschränkungen** zu den Räumlichkeiten
- **Sicherungskabel** (*Kensington*) aus Stahl für Notebooks an öffentlich zugänglichen Orten wie z.B. Messveranstaltungen verwenden.
- **Inventarisierung** von Datenträgern ermöglicht die Kontrolle über Vorhanden- bzw. Nichtvorhandensein von Geräten.

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

- Sicherungskopien (Backups) müssen regelmäßig nach Plan erstellt werden, damit immer aktuelle Daten verfügbar sind.

- Backups müssen sicher an verschiedenen Orten aufbewahrt werden, damit z.B. bei einer Zerstörung eines Gebäudes immer noch Backups vorhanden sind. Online-Backups ermöglichen eine Sicherung über das Internet auf einen Server einer Spezialfirma.
- Die Rücksicherung von Backups sollte getestet werden. *Es gab Fälle, bei denen erst im Schadensfall erkannt wurde, dass die Wiederherstellung der Daten aus der Sicherung nicht funktionierte.*

## 6.1. Sichere Datenvernichtung

Auf ausrangierten Computern befinden sich häufig noch persönliche Daten wie E-Mails, Zugangsdaten, geschäftliche und private Dokumente, Bilder und Videos etc.

Diese Daten sollten vor der Weitergabe **so gelöscht werden, dass eine Wiederherstellung nicht mehr möglich ist**. Es ist nicht ausreichend, die Daten z.B. im Explorer zu löschen und den Papierkorb zu leeren. Auch eine Formatierung der Festplatte kann rückgängig gemacht werden.

Es gibt verschiedene Möglichkeiten, Daten unwiederbringlich zu löschen:

- Physikalische Zerstörung des Datenträgers: CDs und DVDs können geshreddert werden, Festplatten durch Magneteinwirkung oder Zerstörung unlesbar gemacht werden.
- Die Daten von Festplatten werden durch Überschreiben mit einem speziellen Programm vernichtet.

---

Anmerkung:

In diesem Skriptum wird die Schriftfamilie Liberation verwendet. Diese Fonts sind frei verfügbar und können z.B. hier heruntergeladen werden:

<https://fedorahosted.org/releases/l/l/liberation-fonts/Liberation-1.02.zip>