

IT-Security

Sichere Nutzung der IKT im Alltag - IT Security

1. Grundbegriffe zu Sicherheit

1.1. Daten und Informationen – was ist der Unterschied?

Aus Daten werden Informationen

Beispiel: Wir messen die monatlichen Niederschlagsmengen innerhalb eines Jahres.

*Unsere Messungen für die Monate ergeben diese **Daten**:*

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.

*Mit diesen **Daten** können Fragen beantwortet werden:*

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

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

1.2. Datenbedrohung

Cybercrime (Internetkriminalität)

Der Begriff Internetkriminalität bezeichnet jedes Verbrechen, das mit Hilfe eines Computers im Internet begangen wird.

Beispiele hierfür sind Internetbetrug, das Ausspähen von Daten, Identitätsdiebstahl (Pretexting), Eindringen in fremde Netzwerke, Urheberrechtsverletzung, Cyber-Terrorismus, Cyber-Mobbing, Volksverhetzung sowie das Verbreiten von Kinderpornografie.

Datensicherung – Backup

Computer können durch Feuer, Hochwasser und Erdbeben zerstört werden. Dabei werden auch wertvolle Daten vernichtet. Für viele Firmen hat der Verlust ihrer Daten schwerwiegende Folgen: Kundenadressen sind verloren, ausstehende Zahlungen können nicht eingefordert werden, die Produktion kann nicht mehr aufrechterhalten werden...

Nur eine gut geplante Datensicherung (Backup) kann einen jederzeit möglichen Datenverlust verhindern. Dazu gehört auch eine **Ablaufplanung für die Datensicherung**, in der der Ablauf der Datensicherung und die Vorgangsweise beim Schadensfall beschrieben wird.

Damit bei einem Unglück nicht auch das Backup zerstört wird, sollte die Aufbewahrung von Datensicherungen 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 können an einem sicheren Ort aufbewahrt werden.
- 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.

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

Die Bedrohung der Datensicherheit von innen!

Mitarbeiter einer Firma können in manchen Fällen ein Sicherheitsrisiko sein! Sie geben interne Daten absichtlich oder unabsichtlich weiter:

- MitarbeiterInnen verraten ihre Passwörter, indem sie diese auf Klebezettel notieren.
- Unzufriedene MitarbeiterInnen nehmen Daten aus der Firma mit.
- USB-Sticks und Notebooks mit wichtigen Daten 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 „Werbegeschenk“ einen USB-Stick zugesandt. Er steckt ihn an seinem Arbeitsplatzcomputer an und installiert so unabsichtlich ein Spionageprogramm.

Ein E-Mail enthält im Anhang ein Worddokument. Ein Mitarbeiter will die Datei öffnen und aktiviert dabei die Ausführung von Makros. Dadurch wird Malware installiert, die alle erreichbaren Daten verschlüsselt und dadurch unlesbar macht. Die Firma wird dann erpresst und eine hohe Summe für die Wiederherstellung der Daten verlangt.

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

1.3. Informationen sind wertvoll

Sei sparsam bei der Weitergabe von personenbezogenen Daten

Gib nur wirklich notwendige Daten weiter: Viele Gewinnspiele werden nur veranstaltet, um Informationen zu sammeln. Beim Download oder der Installation eines kostenlosen Programms sollte keine Angabe von persönlichen Daten notwendig sein.

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 E-Mail-Adresse geschickt (Spam)
- Sind Daten einmal veröffentlicht, hat man keine Kontrolle über deren Weiterverwendung. Sie können später unerwünscht an anderen Stellen wieder auftauchen.
- Kinder sind oft unvorsichtig bei der Veröffentlichung von Daten. Erwachsene mit schlechten Absichten können Kinder belästigen.
- Bei einem Identitätsdiebstahl bzw. Identitätsmissbrauch verwendet jemand die persönlichen Daten einer anderen Person z.B. zum Einkauf von Waren, Erlangung von Krediten oder Verleumdung durch Versenden Mails etc.

Beispiele für Identitätsmissbrauch:

Eine Frau wird von Freunden darauf aufmerksam gemacht, dass eine Facebookseite mit ihrem Namen und ihren Fotos existiert. Dort werden unter ihrem Namen rufschädigende Meldungen über sie und ihren

Arbeitgeber gepostet. Nur eine sofortige Aussprache mit ihrem Chef und eine Anzeige bei der Polizei verhindern eine Entlassung.

Eine Frau erhält Mahnungen von Inkassounternehmen für Bestellungen, die sie nie gemacht hat. Sie erfährt, dass gegen sie bereits ein Haftbefehl wegen Betrugs besteht.

Betrüger haben unter ihrem Namen umfangreiche Bestellungen getätigt, die nicht bezahlt wurden.

Herr S. bemerkt bei der Kontrolle der Kontoauszüge, dass mit seiner Bankomatkarte im Ausland Geld abgehoben wurde. Er erfährt von der Bank, dass mit Hilfe eines manipulierten Bankomaten seine Bankomatkarte kopiert wurde (Skimming!) und er bei der Eingabe des PIN-Codes beobachtet wurde.

Wie kann ich meine Daten 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.

Gutes Passwort: mVi1982g! (Merkhilfe: **mein Vater ist 1982 geboren!**)

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

Eine Verschlüsselung ist nur so sicher wie das Passwort: Das Passwort soll geheim und regelmäßig geändert werden. Es soll aus Buchstaben, Ziffern und Sonderzeichen bestehen und eine angemessene Mindestlänge mit mindestens 8 Zeichen aufweisen.

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

www.wiesicheristmeinpasswort.de

- Verwende für jeden Zugang ein eigenes Passwort, besonders für wichtige Konten wie E-Mail und Onlinebanking. Wird immer dasselbe Passwort verwendet, können Betrüger mit einem erbeuteten Passwort auf mehrere wichtige Konten zugreifen.
- **Passwort-Manager** speichern sensible Daten wie Nutzernamen und Kennwörter verschlüsselt auf der Festplatte des Computers. Man muss sich nur ein einziges Passwort merken. Die Eingabe dieses Haupt-Passwortes gibt alle anderen Passwörter frei.
Ein empfehlenswerter kostenloser Passwort-Manager ist das Programm **KeyPass**.
- Besonders auf mobilen Geräten sollten Daten verschlüsselt gespeichert werden: Notebooks können verloren gehen oder gestohlen werden. Oft wiegt der Verlust der Daten wesentlich schwerer als die Kosten der Neubeschaffung des Notebooks.
- Bei der Datenspeicherung im Internet (Cloud-Computing) darf die Kontrolle über die Daten nicht verloren gehen: Es besteht ein erhöhtes Risiko von unautorisierten (unerlaubten) Zugriffen, wenn Zugangsdaten in falsche Hände gelangen.

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.

Für Firmen sind Kundendaten und Finanzdaten wertvoll. Wenn Kundendaten in falsche Hände kommen, können sie z. B. für Werbung oder sogar für Betrug (Daten von Kreditkarten) verwendet werden. Finanzdaten können Konkurrenten Einblicke in die Firma geben.

Vertraulichkeit:

Daten müssen vor unbefugter Einsichtnahme geschützt werden:

- Verschlüsselung von gespeicherten Daten.
- Verschlüsselte Datenübertragung bei E-Mail, Chat (Instant Messaging), Online-Banking ...
- Datenzugriff nur für autorisierte Anwender.

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

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

Daten auf Notebooks sollten verschlüsselt sein.

Integrität

Daten sollen vollständig und unverändert sein.

Eine Veränderung kann unabsichtlich oder durch einen technischen Fehler passieren.

Die Daten dürfen nicht durch einen unautorisierten Zugriff geändert werden.

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 1.1.2017: Eine technische Störung hat am Neujahrstag österreichweit Bankomatkassen lahmgelegt. Die Zahlung mit Karte war stundenlang nicht möglich. Erst am Nachmittag konnte die Betreiberfirma den Ausfall beheben.

Personenbezogene Daten werden 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:

Daten, die **keiner besonderen Schutzwürdigkeit** unterliegen:

- der Name
- das Geburtsdatum
- und der Geburtsort
- oder der Wohnort eines Menschen

und **besonders schutzwürdiger** Daten:

- die rassische und ethnische Herkunft eines Menschen
- seine politische Meinung
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Angaben zur Gesundheit, genetische und biometrische Daten, die zu einer eindeutigen Identifikation einer natürlichen Person führen
- das Sexualleben oder die sexuelle Orientierung eines Menschen

Diese Daten dürfen **eigentlich grundsätzlich nicht verarbeitet werden** (Behörden wie die Polizei unterliegen Ausnahmen), es sei denn, die Betroffenen stimmen der Verarbeitung ausdrücklich zu .

- **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. Ein wichtiges Element der Datenschutz-Grundverordnung (DSGVO) ist der **Grundsatz der Transparenz**. Nach diesem Grundsatz soll **jede Betroffene** Kenntnis davon haben, welches Unternehmen bzw. welche Organisation, welche personenbezogenen Daten, auf welche Art und Weise verarbeitet.

Fachbegriffe:

Verantwortlicher ist eine Person oder Organisation, die darüber entscheidet, welche personenbezogenen Daten gespeichert werden.

Das kann zum Beispiel der Chef einer Firma sein.

Auftragsverarbeiter ist eine Person oder Organisation, die diese Daten speichert. Das kann z. B. der Buchhalter sein, der Daten von einem Unternehmer für die Lohnverrechnung erhält.

Betroffener ist eine Person, deren Daten gespeichert wurden und darüber Auskunft verlangen kann.

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 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.

Datensicherheit braucht Strategie, Backups eine Ablaufplanung!

Datenverarbeiter müssen darauf achten, dass 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, krimineller Verschlüsselung etc.). Herkömmliche Backups erfolgen auf Datenträger, die an einem anderen Ort sicher aufbewahrt werden. Online Backups werden über das Internet zu einem Backupserver übertragen. Eine **Ablaufplanung** beschreibt die nötigen Schritte zur Erstellung von Backups und die Wiederherstellung der Daten aus einem Backup.
- Eine USV (unabhängige Stromversorgung) sichert bei Stromausfall den unterbrechungsfreien Betrieb eines Servers.
Bei einem Notebook ist der Akku eine USV!
- Weitere 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.
Ein Lagerarbeiter wird nur Zugriff auf den Lagerbestand haben. Er darf keine Preise ändern. Ein Personalchef hat Zugriff auf alle Mitarbeiterdaten, benötigt aber keinen Lagerbestand.
- Mitarbeiter müssen für den sicheren Umgang mit Daten geschult werden: Es werden **Sicherheitsstrategien** und **Richtlinien** vorgeschrieben wie z. B.: keine USB-Sticks verwenden, keine E-Mails mit sensiblen Daten versenden, keinesfalls Zugangsdaten weitergeben ...

Persönliche Sicherheit

- **Social-Engineering** und **Pretexting** sind Methoden von Betrügern durch Ausnützung von zwischenmenschlichen Beeinflussungen oder unter Vorspiegelung einer fremden Identität unberechtigt an Daten zu kommen.

Beispiel 1: Ein Mitarbeiter erhält einen Anruf eines angeblichen Technikers, der vorgibt für einen Test die geheimen Zugangsdaten zu benötigen.

Beispiel 2: Die Buchhaltung erhält ein Mail des Firmenchefs mit der Aufforderung, sofort eine hohe Geldmenge an ein bestimmtes Konto im Ausland zu überweisen. Das E-Mail erscheint auf den ersten Blick echt – erst eine telefonische Nachfrage beim Chef ergibt, dass es gefälscht ist.

*Hinweis: Würde die Firma nur **signierte E-Mails** versenden, wäre der Betrug sofort aufgefallen!*

- **Phishing**

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.

Gefälschte E-Mails verleiteten Anwender, geheime Zugangsdaten für Ebay, PayPal, E-Mail, Online-Banking etc. auf einer gefälschten Webseite einzugeben.

Phishing ist ein Beispiel für Sozial-Engineering, da ein Phishing-Mail vorgibt, von einem vertrauenswürdigen Absender zu stammen.

- **Shoulder Surfing:** An Geldautomaten, 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 wichtige (sensible) Informationen durch Achtlosigkeit im Papiermüll wie z.B. Akten, Adressenlisten, Kontoauszüge, Briefe etc.
- **Man-in-the-Middle-Angriff:** Ein Hacker platziert sich bzw. seine Software zwischen dem Opfer und einer aufgerufenen Internetseite, wie z. B. eine Bank oder Webmail. So können Überweisungen abgeändert oder Rechnungen gefälscht werden.
- **Browser-Hijacker** bzw. **Browserentführer** sind kleine Programme, welche die Einstellungen des Browsers manipulieren, um auf bestimmte Webseiten umzuleiten.

Beispiel für einen Browser-Hijacker: Awesomehp

Awesomehp verbreitet sich über kostenfrei heruntergeladene Software und über vermeintliche Aktualisierungspakete. Nach der ungewollten Installation dieser Adware werden in allen installierten Webbrowsern die Startseite, die Neuer-Tab-Seite und die Standard-Suchmaschine so verändert, dass diese auf www.awesomehp.com verweisen. Diese optisch an bekannte Suchmaschinen angepasste Website verweist auf weitere Adware und Spyware, speichert Werbe-Cookies und blendet überflüssige Anzeigen ein. Dieser Hijacker lässt sich mit Hilfe entsprechender Software wieder entfernen.

Auf den Webseiten der Browserhersteller findet man Informationen, wie der Webbrowser auf die Standardeinstellungen zurückgesetzt werden kann.

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:

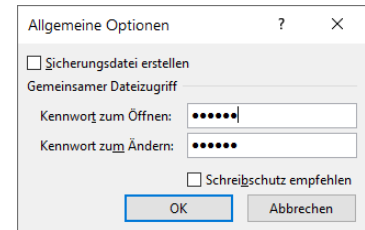
Dies ist ein Klartext und er wird nun verschlüsselt
GLHVLVWHLQNODUWHAWXQGHUZLUGQXQYHUVFKOXHVHWHOW

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.

In Microsoft Office werden Dateien so verschlüsselt:

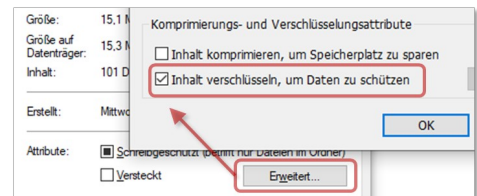
- Datei **speichern unter**
- Schaltfläche **Tools**
- **Allgemeine Optionen**



Datei verschlüsseln in Excel

Auch Windows kann Ordner verschlüsseln:

- **Rechter Mausklick auf Ordner**
- **Eigenschaften > Allgemein**
- Schaltfläche **Erweitert**
- Häkchen bei **Inhalt verschlüsseln um Daten zu schützen**.



Ordner verschlüsseln mit Windows

Windows verwendet für die Verschlüsselung die Benutzeranmeldung. Andere Benutzer auf dem PC können diese Daten nicht lesen.

- **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 Windows-Version Pro bietet eine derartige Verschlüsselung an. Alternativ gibt es kostenlos das Programm *Veracrypt*.

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

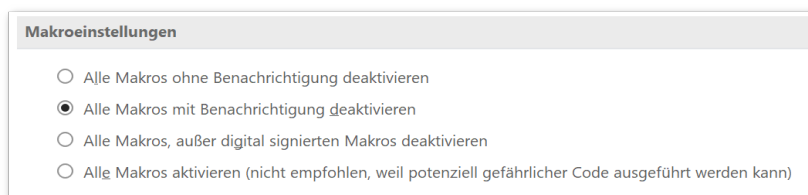
Computerviren verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben.

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

Makroviren sind Computerviren, die als Makro in ein Dokument (z.B. in Excel, Word oder in PowerPoint) eingebettet sind. Makros sind im Normalfall nützliche Programme, die bestimmte Vorgänge automatisieren und dem Benutzer so Arbeit abnehmen.

Ein Makrovirus ist so programmiert, dass z. B. ein Rootkit oder Ransomware aus dem Internet heruntergeladen und installiert wird.

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



Ein **Trojanisches Pferd** (kurz Trojaner) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Programms mit einem versteckt arbeitenden, böartigen Teil. Ein Trojanisches Pferd verbreitet sich nicht selbst, wird durch den Benutzer unabsichtlich installiert.

Herr L. lädt von einer Webseite ein Programm herunter, das verspricht, den Computer schneller und sicherer zu machen. Es stellt sich später heraus, dass das Programm nicht nützlich war und zusätzlich Malware installiert hat.

Krypto-/Erpressungstrojaner bzw. **Ransomware** verschlüsseln alle erreichbaren Dateien auf dem Computer und macht sie dadurch unlesbar. Der Anwender wird aufgefordert „Lösegeld“ für seine Daten zu zahlen.

Ransomware nutzt zur Verteilung häufig gefälschte E-Mails: angebliche Bewerbungsschreiben, Mitteilungen von Zustelldiensten mit einem Link auf Zustellungsdaten, Rechnungen von Energieunternehmen etc.

Wenn man solche Dokumente herunterlädt und öffnet, wird die Schadsoftware aktiv.

Herr S. erhält ein E-Mail von einem Energieunternehmen mit einer hohen Rechnungssumme. Sofort klickt er auf den Link, lädt die Rechnung herunter und öffnet sie. Der Computer zeigt eine Fehlermeldung an. Einige Tage später kann er nicht mehr auf seine Dateien zugreifen, da sie verschlüsselt und daher unlesbar sind. Er wird aufgefordert, mehrere hundert Euro für die Entschlüsselung zu bezahlen.

Ein **Rootkit** ist ein Programm, das die Kommunikation zwischen Anwendern und dem Betriebssystem manipuliert. So werden z. B. Virenprogramme und die von ihnen ausgeführten Prozesse vor dem Benutzer versteckt und so ihre Entdeckung und Entfernung erschwert bzw. verhindert.

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

Ein **Backdoor** erlaubt die Fernsteuerung des Computers durch den Urheber der Malware. Im Gegensatz zu den normalen Fernadministrationsprogrammen wie z. B. Teamviewer sind die Backdoor-Trojaner für den Computernutzer unsichtbar.

Ein Backdoor ermöglicht Dritten einen Zugang („Hintertür“) zum Computer unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoorprogrammen steht der Computer völlig offen: sie können Dateien versenden, empfangen, ausführen, löschen oder vertrauliche Daten ausspionieren, Computeraktivitäten protokollieren und mehr. Backdoors werden auch 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.

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.

Dialer-Programme wählen in computergesteuerten Telefonanlagen unbemerkt teure Mehrwertnummern und verursachen so finanziellen Schaden.

Botnets: Infizierte Computer werden ohne Wissen der Eigentümer zu einem Netzwerk (Botnet) zusammengeschlossen. Die Betreiber von Botnets missbrauchen die Computer z. B. für den Versand von Spam- oder Phishingmails.

2.2. Schutz vor Malware

Antiviren-Software

Ein Antivirenprogramm sollte Vireninfektionen verhindern bzw. entdecken und entfernen.

Nur ein laufend aktualisiertes Antivirenprogramm kann seine Aufgaben erfüllen! Da täglich neue Viren auftauchen, lädt das Antivirenprogramm automatisch die neuesten Vireninformationen (Virensignaturen) von der Herstellerseite herunter.

Virens Scanner können nur bekannte Schadprogramme und ihre Varianten erkennen. Ganz neue Schadprogramme bleiben manchmal unerkannt. Daher ist Vorsicht und aufmerksames Handeln bei der Internetnutzung notwendig!

Eine Antiviren-Software überprüft laufend aktuelle Dateioperationen und in regelmäßigen Zeitabständen werden die Laufwerke auf Virenbefall durchsucht (gescannt).

Die Antiviren-Software kann Dateien von Viren reinigen. Ist das nicht möglich, werden verdächtige oder infizierte Dateien in einen **Quarantäneordner** verschoben, wo sie keinen Schaden anrichten können.

Antiviren-Software kann auch Fehlalarme erzeugen und harmlose Dateien in die Quarantäne verschieben.

Software immer aktualisieren!

Die auf dem Computer installierte Software sollte immer aktuell sein, Updates heruntergeladen und installiert werden. Veralterte und nicht mehr unterstützte Software wie z. B. Windows 7 oder veraltete Browserversionen sollte nicht mehr verwendet werden.

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: Wireless Local Network**: Ist ein lokales Funknetzwerk. Viele mobile Geräte wie Smartphones, Tablets 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** (Virtual Private Network) verbindet (meist verschlüsselt) Netzwerke über das 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 der ChefIn sollen für andere Mitarbeiter nicht zugänglich sein.

- **Authentifizierung:** Ein Benutzer muss sich mit Benutzerkennung und Passwort anmelden. Das System erkennt damit den Benutzer und „weiß“, auf welche Daten und mit welchen Rechten (z. B. Lesen/Schreiben/Löschen oder nur Lesen) er darauf zugreifen darf.

In vielen Unternehmen setzt sich die **Multi-Faktor-Authentifizierung** durch.

Der Benutzer muss sich mehrfach identifizieren:

- **durch Wissen:** z. B. Benutzername und Passwort
- **durch Besitz:** z. B. Bankomatkarte, Token, Smartphone-App
- **durch biometrische Merkmale:** z. B. Fingerabdruck, Gesichtserkennung, Irisscan

Die Authentifizierung sichert den Zugriff auf Daten, schützt die Identität des Benutzers und identifiziert diesen.

- **Benutzerrechte** legen fest, 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 ein Polizist die Adresse des neuen Freundes seiner Ex-Freundin über den Dienstcomputer im zentralen Melderegister (ZMR) abgefragt hatte, wurde dieser wegen Amtsmissbrauchs zu einer bedingten Geldstrafe von 4000 Euro verurteilt.

Wozu braucht man eine Firewall?¹

Eine **Firewall** schützt Computer vor Angriffen aus dem Netzwerk. Sie nur lässt nur Daten durch, die angefordert wurden. Andere Daten werden blockiert. Damit schützt sie den Computer vor Angreifern.

- Alle aktuellen Betriebssysteme haben eine Firewall, die standardmäßig aktiviert ist. Die Konfiguration der Firewall findet man in den Einstellungen.
- Sollte in seltenen Fällen die Firewall eine gewünschte Software, eine App oder einen Dienst **blockieren** (man erhält eine Meldung auf dem Computer bei der Installation), kann diese vorübergehend oder dauerhaft deaktiviert werden.

Firewalls bieten nur begrenzten Schutz, wenn der Computer bereits von Malware betroffen ist. Eine Firewall blockiert nur Datenpakete, die nicht explizit vom Computer angefordert wurden. Wenn ein Computer jedoch mit Spyware oder ähnlichen Programmen infiziert ist, können diese eigenständig Daten aus dem Internet abrufen und senden, ohne dass die Firewall eingreifen kann. Es ist daher entscheidend, alle Programme, insbesondere den Browser und das Betriebssystem, stets auf dem neuesten Stand zu halten, um potenzielle Sicherheitslücken zu schließen und das Risiko von Angriffen zu minimieren.

3.2. Netzwerkverbindungen

Der Anschluss an ein 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.

¹ Brandmauern (Firewalls) werden zwischen Gebäuden errichtet, damit sich Brände nicht auf andere Gebäude ausbreiten können.

3.3. Sicherheitsprotokolle WPA2 und WPA3 - Sicherheit im WLAN

Drahtlose Netzwerke (WLAN) sollten aus Sicherheitsgründen verschlüsselt werden. Der Benutzer gibt bei der Anmeldung ein Passwort ein und wird 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 (**Sicherheitsprotokolle**) zum Schutz von drahtlosen Netzwerken:

- **WPA und WPA2: Wi-Fi Protected Access** bieten eine sichere Verschlüsselung.
- **WPA3** – seit 2018 - soll WLAN noch sicherer und einfacher bedienbar machen.

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 über WLAN übertragen. Ganz sicher geht man, wenn man im offenen/unverschlüsselten WLAN auf sicherheitsrelevante Zugriffe wie Online-Banking verzichtet.

MAC-Filter lassen nur Geräte mit bestimmten MAC-Adressen in das Netzwerk.

Die **MAC-Adresse** (**M**edia-**A**ccess-**C**ontrol-Adresse – *Beispiel: CC-52-AF-40-A0-1FA*) dient dazu, einen Computer im Netzwerk eindeutig zu identifizieren.

MAC-Filter sind umständlich zu verwalten, weil jedes neue Gerät eingetragen werden muss. Zudem lassen sich MAC-Adressen auch fälschen.

Man-in-the-Middle-Angriffe: Ein Hacker platziert sich oder seine Software zwischen dem Opfer und einer aufgerufenen Internetseite. Dadurch erlangt er vollständige Kontrolle über den Datenverkehr und kann die Informationen nach Belieben einsehen und sogar manipulieren.

Auf diese Weise können z. B. Banküberweisungen verfälscht oder E-Mails abgefangen werden.

Die Verwendung von sicheren Verbindungen (HTTPS) erschwert Man-in-the-Middle-Angriffe deutlich.

Aktuelle Browser warnen Anwender, wenn eine gesicherte Verbindung umgeleitet wird!

3.4. Zugriffskontrolle

Ein Netzwerkzugang bietet den Zugriff auf gemeinsame Ressourcen wie Daten, Netzwerkdrucker und andere Serverdienste. Eine Authentifizierung mit z. B. Benutzername und Passwort ermöglicht nur befugten Benutzern den Zugang.

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

4. Sichere Web-Nutzung

4.1. Browser verwenden

Einkaufen im Internet

Ein Einkauf im Internet erfordert sehr oft, dass Kreditkartendaten eingegeben werden, damit der Kauf abgeschlossen ist. Weiters kann es mit dem erworbenen Produkt Probleme geben. Das erfordert Vorsichtsmaßnahmen.

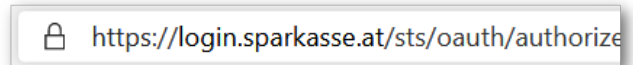
Seriöse Firmen erkennt man z.B. durch positive Bewertungen im Internet, klare Produkt-, Versand- und Bezahlinformationen und einem Impressum, das eine Angabe von Kontaktmöglichkeiten durch Telefon, E-Mail und Postadresse beinhaltet.

Wie kann man die Echtheit bzw. Vertrauenswürdigkeit einer Webseite bzw. Webshops beurteilen?

- Die URL der Website einer Firma überprüfen.
- Die **Webseite soll sicher** sein, das **Sicherheitszertifikat** (links neben der URL) aufrufen.
- Nachsehen, wer die Webseite registriert hat (Domain-Inhaberschaft): z. B. auf www.whois.com
- Das **Impressum der Webseite** kontrollieren – bei einem Webshop ohne oder unvollständigem Impressum soll man nicht einkaufen.

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.

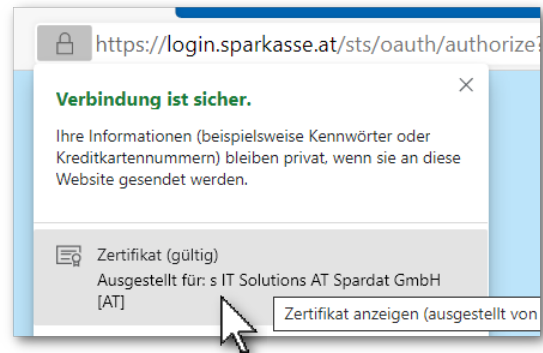


Adresse einer sicheren Webseite

Begriffe zur Sicherheit im Internet:

- **Digitales Zertifikat:** Geschützte Websites besitzen ein **digitales Zertifikat**, das von verschiedenen unabhängigen Zertifizierungsstellen wie *GlobalSign, Verisign, Trust Center* und anderen ausgegeben wird. Ein digitales Zertifikat enthält Informationen über den Namen des Inhabers der Webseite und Gültigkeitsdauer.

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



Digitales Zertifikat einer Webseite

- **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 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** ist eine Betrugsmethode, die auf einer Manipulation der DNS-Anfragen von Webbrowsern basiert. Ein Benutzer wird so auf gefälschte Webseiten umgeleitet, obwohl die Adresse korrekt eingegeben wurde.
- **Cross Site Scripting** Angriffe: Durch einen Angreifer werden Daten einer Webseite so verändert, dass Eingaben eines Anwenders umgeleitet und ausspioniert werden.

Beispiel: Die Webseite einer Zeitung infiziert unabsichtlich durch Werbeanzeigen, die automatisch von Werbeanbietern bezogen wird, die Rechner der Besucher.

- Im Browser kann man sich das **Ausfüllen von Formulardaten** erleichtern, indem persönliche Daten automatisch in die passenden Felder eingefügt werden. Auch **Passwörter** und **Zahlungsinformationen** wie Kreditkartendaten können automatisch eingefügt werden. Diese Funktionen sind zwar praktisch, können aber ein Sicherheitsrisiko darstellen.

*Im Browser Microsoft Edge kann man das in den Einstellungen unter **Profile** ändern.*

*Im Browser Firefox findet man das in den Einstellungen unter **Datenschutz & Sicherheit**.*

- **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 in den Einstellungen des Browsers gelöscht werden:

***Microsoft Edge:** Einstellungen → Datenschutz, Suche und Dienste → Browserdaten löschen*

***Firefox:** Einstellungen → Datenschutz & Sicherheit → Cookies und Website-Daten*

Das **Blockieren oder Zulassen von Cookies** kann im Browser gesteuert werden:

***Microsoft Edge:** Einstellungen → Cookies und Websiteberechtigungen...*

***Firefox:** Einstellungen → Datenschutz & Sicherheit → Cookies und Website-Daten*

- 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 deren Hilfe man eine Internetnutzung nachvollziehen kann, sollten auf fremden Rechnern entfernt werden:

Microsoft Edge: Einstellungen → Datenschutz, Suche und Dienste → Browserdaten löschen

Firefox: Einstellungen → Datenschutz & Sicherheit → Cookies und Website-Daten

- Um Kinder vor ungeeigneten Webinhalten zu schützen und die Internetnutzung zeitlich zu beschränken, gibt es Inthaltefilter und Kindersicherungen.

In Windows muss man dafür ein Konto für jedes Kind einrichten und inhaltliche und zeitliche Zugangsbeschränkungen festlegen.

4.2. Soziale Netzwerke

Fallbeispiele für missbräuchliche Verwendung oder Fehlverhalten in sozialen Netzwerken:

- *A. hat ihre E-Mail-Adresse in Facebook bekannt gegeben. Jetzt erhält sie unerwünschte E-Mails von ihr unbekannten Personen.*
- *W. hat auf seiner Facebookseite Fotos von einer Party eingestellt, die ihm später peinlich sind. Seine „Freunde“ haben diese Fotos kopiert und an anderen Stellen veröffentlicht.*
- *Frau N. wird bei einer Stellenbewerbung trotz bester Aussichten überraschend abgelehnt. Auf Umwegen erfährt sie, dass ein Foto von ihr in lockerer Bekleidung in angeheiterter Stimmung 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.*
- *Schüler X. schickt ein Nacktfoto von sich an Y, das dieser per WhatsApp an seine Freunde weiter leitet. Die Folge sind Ermittlungen der Polizei gegen X., Y. und seine Freunde wegen Kinderporno-graphie.*
- *S erhält von einem Mitglied in dem Sozialen Netzwerk, dem er angehört, rassistische Äußerungen und Drohungen.*

Mit etwas Vorsicht kann man die guten Seiten von sozialen Netzwerken sinnvoll nutzen: Facebook und WhatsApp ermöglichen 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, E-Mail-Adresse usw.
- Überlege dir, welche Fotos du einstellst. Sie könnten dir später peinlich sein.
- Sei dir im Klaren, dass das Löschen von Inhalten in manchen sozialen Netzwerken, Blogs, Internetforen, Cloud-Diensten nicht endgültig ist!
- Prüfe Freundschaftsanfragen und wähle nur Menschen, die du kennst.
- Überprüfe deine Sicherheitseinstellungen zum Schutz der Privatsphäre. Wer Inhalte für Freunde von Freunden oder öffentlich freigibt, macht sie viele Personen sichtbar!
- Eine missbräuchliche Verwendung oder Fehlverhalten in sozialen Netzwerken kann dem jeweiligen Service-Provider und Behörden bzw. Organisationen gemeldet werden. Viele Plattformen haben Richtlinien und Meldesysteme, um solches Verhalten zu melden und zu sanktionieren.

Fachbegriffe

- **Cyber-Mobbing:** Mobbing mithilfe 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. Mobile Geräte

Notebooks, Smartphones und Tablets können verloren gehen oder entwendet werden. Oft ist es viel schlimmer, wenn Daten in falsche Hände gelangen als die Kosten für ein neues Gerät.

Einige Vorkehrungen:

- Den Zugriff auf das Gerät durch PIN, Muster, Passwort oder Fingerabdruckscan sichern.
- In den Sicherheitseinstellungen die Verschlüsselung aktivieren. Beim Einschalten wird die Entschlüsselung mittels PIN, Muster, Passwort oder Fingerabdruckscan aktiviert.
- Sollte ein Smartphone, Tablett oder Notebook abhanden kommen, gibt es die Möglichkeiten der Fernsperre, Fernlöschung und Geräteortung mittels GPS.

Apps aus **nicht offiziellen Appstores** können gefährlich sein:

- Sie können Malware enthalten,
- hohen Stromverbrauch erzeugen oder hohen Datenverkehr verursachen,
- Daten ausspionieren,
- schlechte Qualität haben und unnötige Kosten verursachen.

5.1. Anwendungsberechtigungen bzw. App-Berechtigung:

Bei der Installation von Apps wird angefragt, auf welche Ressourcen die App zugreifen darf: Ist der Zugriff auf Mikrofon, Kontaktdaten, Standortverlauf, Bilder etc. notwendig?

Unter Windows können diese Anwendungsberechtigungen in den Einstellungen geändert werden.

6. Kommunikation

6.1. E-Mail

E-Mails werden mittlerweile verschlüsselt versandt. **Der Absender kann einfach 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.

E-Mails verschlüsseln

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

Digitale bzw. elektronische Signatur

Die digitale Signatur erfüllt den gleichen Zweck wie eine eigenhändige Unterschrift. Sie bestätigt, dass eine elektronische Information von der Person stammt, die sie signiert hat (**Authentizität**) und dass diese Information nicht mehr verändert wurde (**Integrität**).

Sie ist sogar sicherer als eine eigenhändige Unterschrift, weil sie später nicht mehr bestritten werden kann.

Programme, Dokumente und auch **E-Mails** können signiert werden. Eine **digital signierte** E-Mail stellt sicher, dass die E-Mail vom angegebenen Absender stammt und unverändert übermittelt wurde.

Bei E-Mails wird optimale Sicherheit durch **verschlüsselte Übertragung** und **digitale Signierung** erreicht.



Beispiel für eine digitale Signatur eines PDF-Dokuments

Unerwünschte E-Mails

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

Phishing (von engl. password **fish**ing) 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-Mail-Anhänge 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.

6.2. Instant Messaging (Skype, WhatsApp, Facebook Messenger...)

Instant Messaging (kurz **IM**, englisch für „sofortige Nachrichtenübermittlung“) oder Nachrichten-sofortversand ist eine Kommunikationsmethode, bei der sich zwei oder mehr Teilnehmer per Textnachrichten chatten (plaudern, unterhalten). Die Nachrichten kommen sofort beim Empfänger an.

Auch Dateien wie Bilder, Audio-Nachrichten und Videos können übertragen werden.

Mit Instant Messaging können Dateien übermittelt werden! Keine Dateien von unbekannten Personen annehmen, da diese Malware enthalten können.

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.
- Sei vorsichtig bei der Herausgabe von persönlichen Daten!
- Chatprogramme wie Facebook Messenger oder WhatsApp bieten die Übermittlung von Dateien an. Vorsicht! Diese Dateien könnten Malware enthalten.
- Bei Skype, WhatsApp und Facebook Messenger ist die Übertragung sicher verschlüsselt.

7. Sicheres Daten-Management

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

- **Zugangsbeschränkungen** und -kontrollen zu den Räumlichkeiten.
- **Sicherungskabel** aus Stahl für Notebooks an öffentlich zugänglichen Orten wie Messveranstaltungen verhindern Diebstahl.
- **Inventarisierung** von Datenträgern ermöglicht die Kontrolle über Vorhanden- bzw. Nichtvorhandensein von Geräten.



Diebstahlsicherung durch Stahlseil

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

- Sicherungskopien (Backups) müssen regelmäßig nach Ablaufplan erstellt werden, damit immer aktuelle Daten verfügbar sind.
- Backups müssen sicher aufbewahrt werden, damit z. B. bei einer Zerstörung eines Gebäudes immer noch Backups vorhanden sind.
- Online-Backups bzw. die Sicherung in der Cloud ermöglichen eine Sicherung über das Internet auf einen Server. Mit der Sicherung in der Cloud entfallen Bereitstellung und Betreuung von Speichersystemen im eigenen Betrieb. Anbieter von Cloud-Speicher bieten eine hohe Sicherheit.
- Die Rücksicherung von Backups muss getestet werden. *Es gab Fälle, bei denen erst im Schadensfall erkannt wurde, dass die Wiederherstellung der Daten aus der Sicherung nicht funktionierte.*

7.1. Sichere Datenvernichtung

Vor der Entsorgung oder Weitergabe von Computern, Tablets oder Smartphones sollten gespeicherte persönliche Daten wie E-Mails, Zugangsdaten, geschäftliche und private Dokumente, Bilder und Videos unbedingt entfernt werden.

Diese Daten sollten vor der Weitergabe **so gelöscht werden, dass eine Wiederherstellung nicht mehr möglich ist:**

- Die Daten von Festplatten werden durch Überschreiben mit einem speziellen Programm vernichtet.
- DVDs oder Festplatten werden geschreddert (in kleine Teile zerbrochen).
- Smartphones und Tablets sollten auf die Werkseinstellungen zurückgesetzt werden.

Du willst deinen alten Computer weiter geben und möchtest deine persönlichen Daten löschen:

- ➔ Wähle in den Einstellungen **System** und dann **Wiederherstellung**.
- ➔ Bei **Diesen PC zurücksetzen** klicke auf **Los geht's**.
- ➔ Klicke auf **Alles entfernen**.
- ➔ **Nur Dateien entfernen:** löscht persönliche Dateien.
Festplatte säubern: die Daten werden gelöscht **und** zusätzlich überschrieben.
Sie sind dann sicher nicht mehr wiederherstellbar.

Inhaltsverzeichnis

1. Grundbegriffe zu Sicherheit.....	2
1.1. Daten und Informationen – was ist der Unterschied?.....	2
Aus Daten werden Informationen.....	2
1.2. Datenbedrohung.....	2
Cybercrime (Internetkriminalität).....	2
Datensicherung – Backup.....	2
Die Bedrohung der Datensicherheit von innen!.....	3
1.3. Informationen sind wertvoll.....	3
Sei sparsam bei der Weitergabe von personenbezogenen Daten.....	3
Wie kann ich meine Daten schützen?.....	4
Datensicherheit.....	4
Vertraulichkeit:.....	5
Integrität.....	5
Verfügbarkeit.....	5
Personenbezogene Daten werden gesetzlich geschützt!.....	5
Datensicherheit braucht Strategie, Backups eine Ablaufplanung!.....	6
Persönliche Sicherheit.....	6
Sicherheit für Dateien durch Verschlüsselung.....	7
2. Malware sind Schadprogramme.....	8
2.1. Definition und Funktionsweise und Typen.....	8
2.2. Schutz vor Malware.....	10
Antiviren-Software.....	10
Software immer aktualisieren!.....	10
3. Sicherheit im Netzwerk.....	10
3.1. Netzwerke verbinden Computer.....	10
Netzwerktypen.....	10
Datensicherheit im Netzwerk.....	10
Wozu braucht man eine Firewall?.....	11
3.2. Netzwerkverbindungen.....	11
3.3. Sicherheitsprotokolle WPA2 und WPA3 - Sicherheit im WLAN.....	12
3.4. Zugriffskontrolle.....	12
4. Sichere Web-Nutzung.....	12
4.1. Browser verwenden.....	12
Einkaufen im Internet.....	12
Begriffe zur Sicherheit im Internet:.....	14
4.2. Soziale Netzwerke.....	15
Tipps für den sicheren Umgang mit sozialen Netzwerken:.....	15
5. Mobile Geräte.....	16
5.1. Anwendungsberechtigungen bzw. App-Berechtigung:.....	16
6. Kommunikation.....	16
6.1. E-Mail.....	16
E-Mails verschlüsseln.....	16
Digitale bzw. elektronische Signatur.....	17
Unerwünschte E-Mails.....	17
6.2. Instant Messaging (Skype, WhatsApp, Facebook Messenger...).....	17
Sicheres Chatten:.....	17
7. Sicheres Daten-Management.....	18
7.1. Sichere Datenvernichtung.....	18