IT-Security

Sichere Nutzung der IKT im Alltag

EASY4ME

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: 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 z.B.:

- *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.

1.2. Datenbedrohung

Cybercrime (Internetkriminalität)

Der Begriff Internetkriminalität bezeichnet jedes Verbrechen, das mit Hilfe eines Computers mit Hilfe des Internets 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 Kinderpornographie.

Daten können verloren gehen

Computer können durch Feuer, Hochwasser und Erdbeben zerstört werden. Dabei werden auch wertvolle Daten vernichtet. Für viele Firmen würde der Komplettverlust ihrer Daten den Konkurs bedeuten: alle Kundenadressen wären verloren, ausstehende Zahlungen könnten nicht eingefordert werden, die Produktion könnte 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 ermöglichen so eine Aufbewahrung an einem sicheren Ort.
- 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.
- 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 ein Spionageprogramm.

Ein E-Mail enthält einen Anhang mit einer Worddatei. Ein Mitarbeiter will die Datei öffnen und aktiviert dabei die Ausführung von Makros. Dadurch wird Malware installiert.

1.3. Informationen sind wertvoll

Sei sparsam bei der Weitergabe von personenbezogenen Daten

Gib nur wirklich notwendige Daten an: Viele Gewinnspiele werden nur veranstaltet, um Adressen zu sammeln. Beim Download 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 Mailadresse 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 leichtfertig 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.

Identitätsmissbrauch Beispiel 1:
Eine Frau wird von Freunden darauf aufmerksam gemacht, dass auf ihrem Namen und mit ihren Fotos eine Facebookseite existiert. Auf dieser Seite 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.

Identitätsmissbrauch Beispiel 2:
Eine junge 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.
Nur mit Hilfe eines Anwalts kann sie ihren guten Ruf wieder herstellen.

Identitätsmissbrauch Beispiel 3:
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 die Eingabe des PIN-Codes beobachtet wurde.

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. Wird immer dasselbe Passwort verwendet, können Betrüger mit einem erbeuteten Passwort auf mehrere wichtige Konten zugreifen.
- **Passwort-Manager sind empfehlenswert:** Sie speichern sensible Daten wie Nutzernamen und Kennwörter verschlüsselt auf der Festplatte des Computers. Statt sich viele Passwörter merken zu müssen, genügt jetzt eines: Die Eingabe des Master-Passwortes gibt alle anderen frei.
- 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.
- Bei der Verwendung von Cloud-Computing sollte die Kontrolle über die Daten nicht verloren gehen: Man sollte sich immer im Klaren sein, wer Zugriffsrechte auf die Daten hat. Zudem besteht eine erhöhtes Risiko von unautorisierten Zugriffen, wenn Zugangsdaten in falsche Hände gelangen oder durch Hacking.

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 allen 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 könnte 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 hohen 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!

Das **Datenschutzgesetz** regelt den Schutz personenbezogener Daten wie z.B. Adresse, Geburtsdatum, Telefonnummer, Religionsbekenntnis etc.

- **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.

Fachbegriffe zum Datenschutzgesetz	**Auftraggeber** im Sinne des Datenschutzgesetzes ist eine Person oder Organisation, die personenbezogenen Daten speichert.
	Auskunftwerber ist die Person, die Auskunft verlangt.
	Betroffener: Person, deren Daten gespeichert wurden.

- **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.

- 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
  In Österreich kann man herausfinden, wem eine DVR-Nummer zugeordnet ist. Verwende eine Suchmaschine z.B. mit den Stichworten "DVR Recherche" und finde heraus, wem die DVR-Nummer 0103012 gehört!

Datensicherheit braucht Strategie, Backups eine Ablaufplanung!

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 (**u**nabhängige **S**tromver**s**orgung) 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.

  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 Richtlinien vorgeschrieben wie z.B.: keine USB-Sticks verwenden, keine Mails mit sensiblen Daten versenden, keinesfalls Zugangsdaten weiterzugeben etc.

Persönliche Sicherheit

- **Social-Engineering** bzw. **Pretexting** ist eine Methode 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.

- **Phishing**

  Beispiel: ein 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.

  Phishing ist auch ein Beispiel für Sozial-Engineering, da ein Phishing-Mail vorgibt, von einem vertrauenswürdigen Absender zu stammen.
- **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.
- **Man-in-the-Middle-Angriff**: Ein Hacker platziert sich bzw. seine Software zwischen dem Opfer und und einer aufgerufenen Internetseite, wie z.B. eine Bank oder Webmail. So können z. B. Überweisungen abgeändert oder Rechnungen gefälscht werden.
- **Browser-Hijacker** bzw. **Browserentführer** sind kleine Programme, welche die Einstellungen des Browsers manipulieren, um Seitenaufrufe (etwa die Startseite) und Suchanfragen auf bestimmte Webseiten umzuleiten. Browser-Hijacker installieren sich häufig ohne Wissen des Benutzers, oft durch Ausnutzung von Sicherheitslücken in der Browsersoftware.

  Beispiel für einen Browser-Hijacker: Awesomehp
  Awesomehp verbreitet sich über scheinbar kostenfrei heruntergeladene Vollversionen von Software und über vermeintliche Aktualisierungspakete bekannter Windows-Erweiterungen (z.B. Java, Flash). 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.

Sicherheit für Dateien durch Verschlüsselung

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

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

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

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 *Veracrypt*.

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

2. Malware sind Schadprogramme

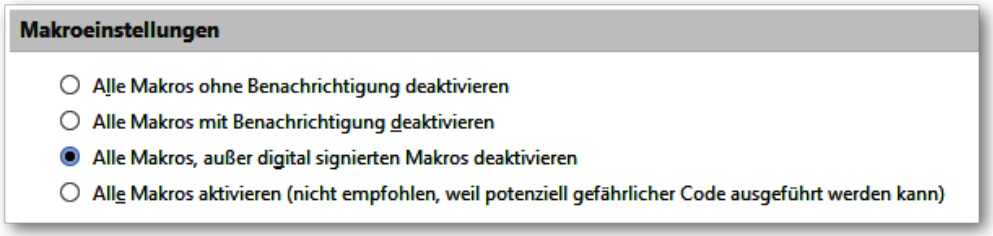
Der Begriff **Malware** setzt sich aus den englischen Begriffen **mal**icious, „bösartig“ und Soft**ware** zusammen. Malware ist ein Überbegriff für unerwünschte und schädliche Software, die ohne Wissen des Benutzers im Hintergrund auf dem Rechner läuft.

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 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:



Makroeinstellungen in Word

Ein **Trojanisches Pferd** (kurz Trojaner) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Programms mit einem versteckt arbeitenden, bösartigen 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, E-Mails von Zustelldiensten mit einem Link auf auf Zustellungsdaten, Rechnungen von Energieunternehmen etc. Werden Daten über den angebotenen Link heruntergeladen und geöffnet, 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 **ad**vertisement und Soft**ware**) 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.

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.

Virenscanner können trotzdem nur bekannte Schadprogramme (Viren, Würmer, Trojaner etc.) erkennen und somit nicht vor allen Viren und Würmern schützen. Daher können Virenscanner nur als Ergänzung zu allgemeinen Vorsichtsmaßnahmen betrachtet werden. Vorsicht und aufmerksames Handeln bei der Internetnutzung ist notwendig!

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

Die Antivirensoftware kann Dateien von Viren reinigen. Ist das nicht möglich, werden verdächtige oder infizierte Dateien in einen **Quarantäneordner**[1] 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. Veraltete und nicht mehr unterstützte Software wie z. B. Windows XP 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**: **W**ireless **L**ocal **N**etwork: Ist ein lokales Funknetzwerk. Viele mobile Geräte wie Smartphones, Tabletts oder Notebooks werden über WLAN mit dem Internet verbunden.
- **WAN** (Wide Area Network) ist ein Rechnernetz, das sich im Unterschied zu einem LAN über einen sehr großen geografischen Bereich erstreckt.
- **VPN** (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 des Chefs 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.

1 **Quarantäne**: Menschen mit ansteckenden Krankheiten werden isoliert untergebracht, damit andere Menschen nicht angesteckt werden.

In vielen Unternehmen setzt sich die **Multi-Faktor-Authentifizierung** durch.
Der Benutzer muss sich mehrfach identifizieren:

- **Etwas, das er weiß**: Passwort oder Pin
- **Etwas, das er hat**: Token (kontaktlos, per USB angesteckt oder ein kleines Gerät zur Erzeugung eines Einmalpassworts)
- **Etwas, das er ist**: Biometrie wie Fingerabdruck, Augen- bzw. Irisscan, Handgeometrie (misst die individuellen Abmessungen der Hand), ...

Die Authentifizierung sichert den Zugriff auf Daten, schützt die Identität von Benutzern und identifiziert den Benutzer.

- **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 Melderegister (ZMR) abgefragt hatte, wurde ein Polizist wegen Amtsmissbrauchs zu einer bedingten Geldstrafe von 4000 Euro verurteilt.

Wozu braucht man eine Firewall?[2]

- 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. Zu finden sind die Einstellungen der Firewall in der Systemsteuerung.
- Sollte in seltenen Fällen die Personal Firewall eine gewünschte Software oder einen Dienst **blockieren** (man erhält eine Meldung auf dem Computer bei der Installation), kann diese vorübergehend ausgeschaltet werden oder (besser!) so eingestellt werden, dass die Firewall diesen Datenverkehr durchlässt.

Firewalls bieten nur einen Schutz, wenn der Rechner nicht kompromittiert (= von Malware befallen) 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 ohne weiteres unterscheiden, ob der Datenverkehr erwünscht ist oder nicht. Es ist daher wichtig, alle Programme (vor allem Browser und Betriebssystem) auf den neuesten Stand zu halten, damit keine Sicherheitslücken ausgenutzt werden können.

3.2. Netzwerkverbindungen

Der Anschluss an ein Netzwerk kann per Netzwerkkabel oder drahtlos per Funkverbindung erfolgen.

Jede Verbindung mit einem Netzwerk bedeutet, dass der Rechner dem Risiko eines Angriffs von außen ausgesetzt ist.

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

3.3. Sicherheit im drahtlosen Netz

Drahtlose Netzwerke (WLAN) 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:

- **WPA bzw. WPA2: W**i-Fi **P**rotected **A**ccess bieten eine nach heutigem Stand eine sichere Verschlüsselung.
- **WEP**: **W**ired **E**quivalent **P**rivacy: unsicher und daher **nicht zu empfehlen**.
  WEP-Verbindungen können ohne großen Aufwand abgehört werden.

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 http**s** 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.

Die Einrichtung eines **MAC-Filters** ist eine weitere Möglichkeit, den Zugang zu einem Netzwerk zu beschränken:

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. Ein **MAC-Filter** gibt den Zugang zu einem Netzwerk nur für bestimmte MAC-Adressen frei - allen anderen ist der Zugang verwehrt. So können sich nur bestimmte Computer mit dem WLAN verbinden. *MAC-Filter sind umständlich zu verwalten, weil jedes neue Gerät eingetragen werden muss. MAC-Adressen lassen sich auch fälschen.*

Man-in-the-Middle-Angriffe können auch bei gesicherten Verbindungen ein Problem sein: 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.

3.4. Zugriffskontrolle

Ein Netzwerkzugang bietet den Zugriff auf gemeinsame Ressourcen wie Daten, Netzwerkdrucker und andere Serverdienste. Eine Authentifzierung mit z.B. Benutzername und Passwort ermöglicht 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,
- keinen persönlichen Bezug haben wie Geburtsdatum, Namensteile etc.,
- regelmäßig geändert werden.

Gutes Passwort: `mVi1963g!` (Merkhilfe: **m**ein **V**ater **i**st **1963 g**eboren**!**)

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

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

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

4. Sichere Web-Nutzung

4.1. Browser verwenden

Einkaufen im Internet

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.

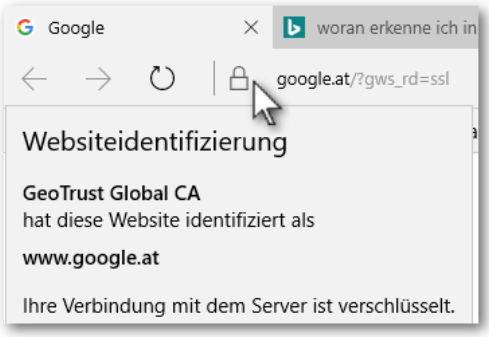
Wie kann man die Echtheit bzw. Vertrauenswürdigkeit einer Website beurteilen?

- Die URL der Website einer Firma überprüfen
- 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 – eine Webshop ohne Impressum ist so gut wie sicher illegal oder es besteht die Gefahr, dass man betrogen wird.

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

Sichere Websites erkennt man am Protokoll **https://** (**h***ypertext* **t***ransfer* **p***rotocol* ***secure***) und an einem geschlossenen Vorhangschloss. Die Daten werden verschlüsselt übertragen.

Begriffe zur Sicherheit im Internet:



Digitales Zertifikat für google.at

- **Digitales Zertifikat:** Geschützte Websites 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. Klicke 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 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 vermeintlich sicheren 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. Die Funktion **AutoVervollständigen** schlägt

auch bei Eingaben in der Adressleiste passende URLs vor. Diese Funktionen sind zwar praktisch, können aber ein Sicherheitsrisiko darstellen.

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

  IE: Extras → Internetoptionen → Registerkarte Allgemein → Löschen.
  Firefox: Chronik → Neueste Chronik löschen

- Um Kinder vor ungeeigneten Webinhalten zu schützen und die Internetnutzung zeitlich zu beschränken, gibt es Inhaltefilter und Kindersicherungen.
  Der Internet Explorer bietet dazu Einstellungen:

  Internetoptionen → Inhalte → Inhaltsratgeber...

4.2. Soziale Netzwerke

Fallbeispiele für Missbrauch von sozialen Netzwerken:

- *A. hat ihre E-Mail-Adresse in Facebook bekannt gegeben. Jetzt erhält sie lästige E-Mails von ihr unbekannten Personen.*
- *W. hat auf seinem Facebookprofil Fotos von einer Party eingestellt, die ihm später peinlich sind. Seine „Freunde“ haben schon 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.*

Mit etwas Vorsicht kann man die guten Seiten von Facebook – ohne Überraschungen – nutzen: 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, 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 auch kennst.
- Überprüfe deine Sicherheitseinstellungen zum Schutz der Privatsphäre. Wer Inhalte für Freunde von Freunden frei gibt, macht sie viele Personen 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. Mobile Geräte

Notebooks, Smartphones und Tabletts können verloren gehen oder entwendet werden. Oft ist der Verlust der Daten wesentlich schwerwiegender als Kosten für die Neuanschaffung.

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 das Smartphone abhanden kommen, gibt es die Möglichkeiten der Fernsperre, Fernlöschung und Geräteortung.

Apps aus nicht offiziellen Appstores bergen Risiken:

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

Bei der Installation von Apps sollte man die Anwendungsberechtigungen prüfen: Ist der Zugriff auf Kontaktdaten, Standortverlauf, Bilder etc. notwendig?

6. Kommunikation

6.1. E-Mail

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

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

E-Mails verschlüsseln

Aktuelle E-Mailprogramme bieten eine **Verschlüsselung** an. Die Nachricht wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Der Empfänger entschlüsselt die Mail mit seinen 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. **p**assword f**ishing**) 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 (webchat, Skype, WhatsApp...)

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.

Als Vorsichtsmaßnahme sollten die Sicherheitseinstellungen aktiviert, bzw. hoch gesetzt werden: z. B. keine Nachrichten von Fremden annehmen, Aufnahme in die Kontaktliste nur mit Erlaubnis zulassen.

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

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 vorsichtig. Gib keine persönlichen Daten wie Adresse, Telefonnummern, Nachnamen und E-Mail-Adressen her.
- 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.
- Es gibt Möglichkeiten verschlüsselt zu kommunizieren wie z.B. mit der Chatfunktion von *Skype*, oder *WhatsApp*.

7. Sicheres Daten-Management

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

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

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 an verschiedenen Orten 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 einer Spezialfirma.
  Mit der Sicherung in der Cloud entfallen die Bereitstellung und Betreuung von Speichersystemen im eigenen Betrieb. Die Kosten sind kalkulierbarer und Anbieter von Cloud-Speicher bieten für die Daten eine hohe Sicherheit.
  Allerdings, es gibt Fragen wie: Wo sind meine Daten? Sind sie noch in Europa? Wird es den Anbieter nächstes Jahr noch geben? Ist die Datenübertragung sicher? Können die Daten in falsche Hände gelangen?
- 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

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:**

- Zerstörung des Datenträgers: DVDs oder Festplatten werden geschreddert.
- Die Daten von Festplatten werden durch Überschreiben mit einem speziellen Programm vernichtet.
- Festplatten können durch starke Magnetisierung gelöscht werden.

*Du willst deinen alten Computer weiter geben und möchtest deine persönlichen Daten so löschen, dass sie **nicht wiederherstellbar** sind:*

➔ *Erstelle einen neuen Benutzer mit Administratorrechten*

- ➔ *Lösche dein altes Benutzerkonto samt allen dazu gehörigen Dateien - du hast bereits deine Daten auf den neuen Rechner übertragen!*
- ➔ *Leere den Papierkorb*
- ➔ *Installiere das kostenlose Programm CCleaner (achte darauf, dabei keine zusätzlichen Programme zu installieren!) und überschreibe mit der Funktion "Festplatten Wiper" den **freien Platz** auf der Festplatte – 1x überschreiben reicht.*

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
Daten können verloren gehen....2
Die Bedrohung der Datensicherheit von innen!....2
1.3.Informationen sind wertvoll....3
Sei sparsam bei der Weitergabe von personenbezogenen Daten....3
Was kann ich tun, um meine Daten zu schützen?....4
Datensicherheit....4
Vertraulichkeit:....4
Integrität....4
Verfügbarkeit....5
Personenbezogene Daten werden gesetzlich geschützt!....5
Datensicherheit braucht Strategie, Backups eine Ablaufplanung!....5
Persönliche Sicherheit....6
Sicherheit für Dateien durch Verschlüsselung....7
2.Malware sind Schadprogramme....7
2.1.Definition und Funktionsweise und Typen....7
2.2.Schutz vor Malware....8
Antiviren-Software....8
Software immer aktualisieren!....9
3.Sicherheit im Netzwerk....9
3.1.Netzwerke verbinden Computer....9
Netzwerktypen....9
Datensicherheit im Netzwerk....9
Wozu braucht man eine Firewall?....10
3.2.Netzwerkverbindungen....10
3.3.Sicherheit im drahtlosen Netz....11
3.4.Zugriffskontrolle....11
4.Sichere Web-Nutzung....12
4.1.Browser verwenden....12
Einkaufen im Internet....12
Begriffe zur Sicherheit im Internet:....12
4.2.Soziale Netzwerke....13
Tipps für den sicheren Umgang mit sozialen Netzwerken:....14
Fachbegriffe....14
5.Mobile Geräte....14
6.Kommunikation....14
6.1.E-Mail....14
E-Mails verschlüsseln....15
Digitale Signatur für E-Mails....15
Unerwünschte E-Mails....15
6.2.Instant Messaging (webchat, Skype, WhatsApp...)....15
Tipps für sicheres Chatten:....15
7.Sicheres Daten-Management....16
7.1.Sichere Datenvernichtung....16