# IT Sicherheit

**IT Administration**

Marc Eugster
Obergütschrain 4
6003 Luzern

marc.eugster@eugster.net

BILDUNGSZENTRUM
GEOMATIK
SCHWEIZ

Baugewerbliche Berufsschule Zürich
Abteilung Planung und Rohbau
Lagerstrasse 55
8090 Zürich

# IT Sicherheit

**19**. & 20. Juni 2020

Marc Eugster, Luzern

Marc Eugster, Luzern
eidg. dipl. Informatiker PM
Leiter Marketing & Verkauf, Mitglied der Geschäftsleitung
Axians IT&T AG, Rotkreuz

marc.eugster@eugster.net

# EINFÜHRUNG

Als **Informationssicherheit** bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden (technischen oder nicht-technischen) Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem **Schutz vor Gefahren** bzw. Bedrohungen, der **Vermeidung von wirtschaftlichen Schäden** und der **Minimierung von Risiken**.

In der Praxis orientiert sich die Informationssicherheit im Rahmen des IT-Sicherheitsmanagements unter anderem an der internationalen ISO/IEC 27000-Reihe. Im deutschsprachigen Raum ist ein Vorgehen nach IT-Grundschutz verbreitet. Im Bereich der Evaluierung und Zertifizierung von IT-Produkten und -systemen findet die Norm ISO/IEC 15408 (Common Criteria) häufig Anwendung.

# Vorstellungsrunde

- Marc Eugster, Luzern
  - eidg. dipl. Informatiker PM
  - Leiter Marketing & Verkauf, Mitglied der Geschäftsleitung Axians Division Public Software Schweiz

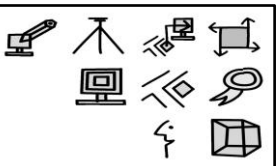
- marc.eugster@eugster.net

# Ziel des Kurses

- Schützende Daten identifizieren und deren Schutzbedarf bestimmen
- geeignete organisatorische, personelle, infrastrukturelle und technische Massnahmen beschreiben
- Sicherheitskonzepte für einen IT – Grundschutz (u.a. Notfall-Szenarium Virus) bestimmen
- Datenschutz und Sicherheitsmassnahmen für Personen- und Geschäftsdaten aufzeigen
- Momentane Sicherheitsstandards erklären

# Themen

- Tag 1
  - Einführung
  - Die Gefahr ist real …
  - Warum machen wir IT Sicherheit?
  - Risiken
  - Standards / Zertifizierungen
- Tag 2
  - Gruppenarbeit (Prüfung Teil 1)

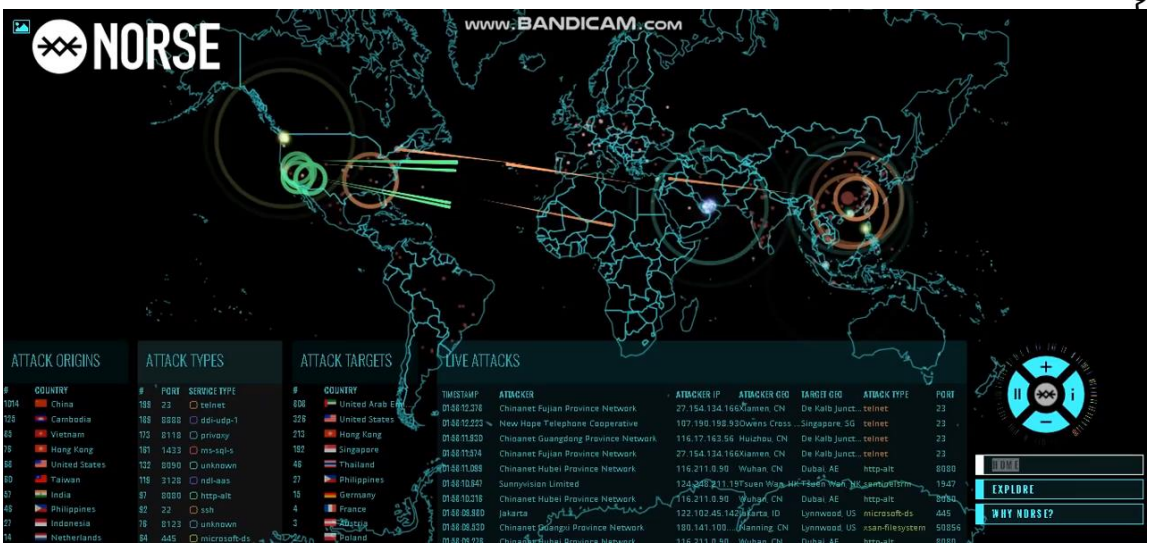


## DIE GEFAHR IST REAL …

Ich behaupte: Jeder von uns verlässt sich darauf, dass die IT sicher ist. Und zwar soweit, dass jeder von uns sein Leben darauf setzt. Oder wie seht Ihr das?

Zum Einstieg mal ein paar Beispiele, was denn alles so läuft bzw. wo wir uns überall in Gefahr bringen (teilweise auch ohne, dass wir uns dessen wirklich bewusst sind…)

# Die Gefahr ist Real …

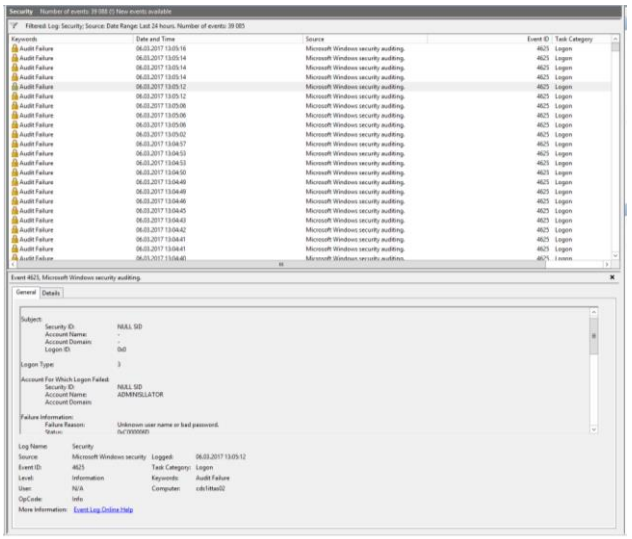



http://map.norsecorp.com/

## Die Gefahr ist Real …


http://map.norsecorp.com/

# Die Gefahr ist Real …

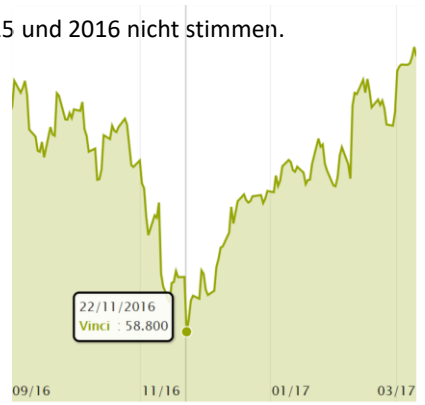


Serverattacken auf einen ‘ungesicherten’ Server anhand eines realen Beispiels …

Haupt-Ursache: Server (muss) vom Internet erreichbar sein

# Hacker lassen Aktie um 18 Prozent einbrechen

- 22.11.2016 - 16.08:
  "Baukonzern Vinci trennt sich von Finanzvorstand Christian Labeyrie“, berichteten die Nachrichtenagenturen.
- Später hiess es, dass die Geschäftszahlen von Vinci für 2015 und 2016 nicht stimmen.
- In der Folge verlor die Aktie des Baukonzerns 18 Prozent.




… eine Mischung aus Social Engineering und Fake News. Der Schaden war erheblich (18% Kursverlust innerhalb weniger Stunden). Es war eines der ersten Beispiele, wie anfällig unsere heutige Informations-Gesellschaft ist und wurden in Finanzkreisen mit entsprechend grosser Beachtung aufgenommen.

Auch hier gilt: Aus Fiktion wird Realität – in vielen Filmen wird dieses (bzw. ein ähnliches Szenario) als Basis genommen und dann Hollywood-mässig überspitzt dargestellt. Beispielsweise kämpft in Die Hard 4 Bruce Willis gegen Cyer-Attentäter, die mit erheblichem technischen Aufwand schlussendlich einfach Geld stehlen wollen. Das reale Beispiel ist nicht ganz so spektakulär in dessen Umsetzung, zeigt aber, dass auch mit weniger ‘Action, Special Effects’ und schlussendlich auch mit weniger Aufwand das gleiche Ergebnis erziehlt werden kann.

Der ganze Vorfall wurde mit einer gefälschten Website und entsprechender Pressemeldung durchgeführt.

**Hauptursache**: Vermutlich die Aussicht auf Gewinne mit Börsen-Geschäften

# Virenbefall – ein reales Beispiel

- **Tag 1**
  - 11.33 – Mitarbeiterin öffnet einen Anhang einer E-Mail
  - 11.40 – erste Meldung, dass ein Word-Dokument nicht geöffnet werden kann
  - 11.45 – Verdacht auf Virenbefall erhärtet sich
  - 11.55 – Server werden vom Netz genommen
  - 12.03 – Schadensausmass bekannt:
    Alle Office-Dokumente auf allen der bei der Mitarbeiterin gemappten Laufwerke sind infiziert
  - 13.04 – Entscheid für die Recovery-Massnahme 'Full-Restore'
  - 13.15 – Restore gestartet
- **Tag 2**
  - Restore läuft seit 24 Stunden – 78% der Daten sind wieder verfügbar
  - 18.39 – Meldung: Restore abgeschlossen

- Geschätzter finanzieller Schaden aufgrund von Unproduktivität während des Restores:
  ca. 60'000 Fanken!

**Schadenberechnung**
25 Mitarbeiter – 12 Stunden (Arbeits-)Ausfall – Vollkosten pro Mitarbeiter 180 Franken

Beim beschriebenen Beispiel handelte es sich um eine Abart des *XDocCrypt* Virus, bzw. einem Verschlüsselungstrojaner. Nach der Ausführung, z.B. beim Klick auf einen verseuchten E-Mail-Anhang verschlüsselt diese Art des Angriffs alle auf den lokal gemappten Laufwerken die gefundenen Office-Dateien. Ziel dieses Angriffs ist, dass nach dem Befall der Betroffene eine Information erhält, dass nach Zahlung eines entsprechenden 'Entgelds' eine Entschlüsselungsroutine zur Verfügung gestellt wird, damit die Dateien wieder genutzt werden können.

Anmerkung: In unserem Fall haben wir nie eine entsprechende Information erhalten – somit währen ohne Backup unsere gesamten Office-Dateien zerstört gewesen. Dies kann je nachdem dazu führen, dass eine Unternehmung handlungsunfähig wird und im Schlimmsten Fall seine Geschäftstätigkeit nicht mehr ausführen kann.

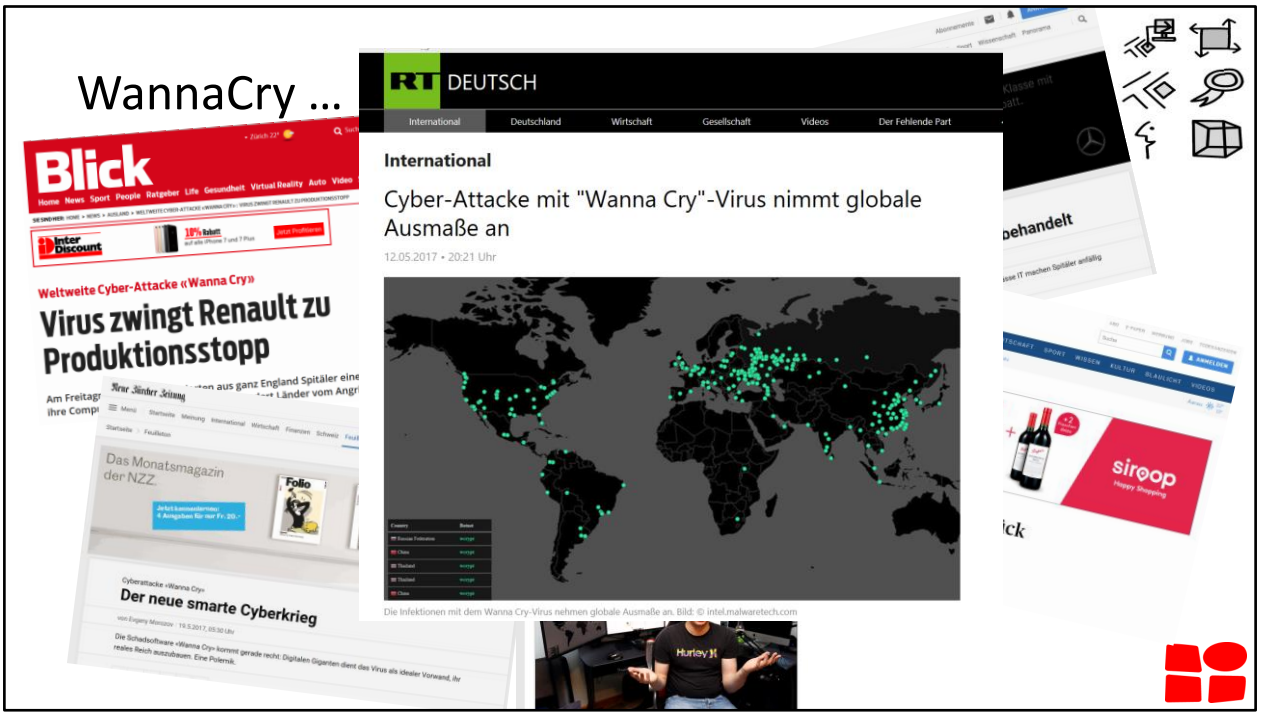
**Trojaner legt tausende Büros lahm**
http://www.t-online.de/computer/sicherheit/id_58584044/office-trojaner-legt-tausende-bueros-lahm.html

**Gefährlicher Virus steckt in Word-Dateien**
http://www.recklinghaeuser-zeitung.de/ratgeber/digitales/Vorsicht-bei-E-Mails-Gefaehrlicher-Virus-steckt-in-Word-Dateien;art348541,1693902

Hauptursache: menschliches Fehlverhalten


**Mai 2017**

- Wer erinnert sich?
- War jemand betroffen?




SRF Mediathek:
**Weltweite Cyber-Attacke Schlägt «Wanna Cry» nochmal zu?**
https://www.srf.ch/news/international/schlaegt-wanna-cry-nochmal-zu


Haupt-Ursache: kein aktuelles Betriebssystem installiert.
Dieser Virus kommt bei WannaCry offensichtlich sogar ohne ‘Interaktion’ durch den Benutzer auf die Systeme

März 2018

- Facebook-Skandal mit durch Cambridge Analytica (inzwischen Konkurs) missbräuchlich verwendeten Daten

Juni 2018
- Facebook gab User-Daten auch an Huawei und andere Chinesen (Siehe https://www.inside-it.ch/articles/51286)

# Facebook …

- Die Analysefirma Cambridge Analytica verschaffte sich über Facebook Zugriff auf Millionen Nutzerdaten und manipulierte mutmasslich weltweite Wahlen.


**Darum geht's:**
«Ein Datenskandal bei Facebook hat weltweit für Aufruhr gesorgt. Die britische Analysefirma Cambridge Analytica (CA) verschaffte sich über das soziale Netzwerk Zugriff auf Daten von Millionen von Nutzern. Dabei handelt es sich aber nicht um ein Datenleck im eigentlichen Sinne, sondern CA hat das App-System von Facebook ausgenutzt, um an die Daten zu kommen. …»
Weiterlesen: http://www.20min.ch/finance/news/story/So-schuetzen-Sie-Ihre-Daten-auf-Facebook-25746820

## Aber auch ganz nahe …

20 minuten

de fr it Zürich 9°

Schweiz Ausland Wirtschaft Sport People Entertainment Digital Wisse

News Taschengeldrechner Börse Grow Up

Ihre Story, Ihre Informationen, Ihr Hinweis? feedback@20minuten.ch

Leser-Kritik 14. März 2019 20:34; Akt: 14.03.2019 20:52

**Der neue Migros-Shop ist vielen nicht geheuer**

*von Dominic Benz - Von Datenmissbrauch bis Bevormundung – 20-Minuten-Leser kritisieren die Online-Plattform My Migros. Der Detailhändler nimmt Stellung.*

März 2019

Der neue Migros-Shop ist vielen nicht geheuer
*von Dominic Benz - Von Datenmissbrauch bis Bevormundung – 20-Minuten-Leser kritisieren die Online-Plattform My Migros. Der Detailhändler nimmt Stellung.*

Die Migros testet das personalisierte Einkaufen. Dafür lanciert der Detailhändler den Onlineshop My Migros. Es handelt sich um ein Pilotprojekt der Migros Aare.

Der Shop schlägt dem Kunden gezielt seine häufig gekauften Produkte vor – aufgrund der gesammelten Cumulus-Daten. Auch teilt er ihm mit, wann ein Produkt wie etwa WC-Papier wieder gekauft werden sollte. Das soll laut Migros das Einkaufen vereinfachen und schneller machen.
Das Konzept ist vielen Lesern von 20 Minuten nicht geheuer. Sie wittern eine andere Absicht hinter dem Shop oder sehen darin gar einen Missbrauch der Cumulus-Daten. Das antwortet die Migros auf die häufigsten Kritikpunkte:

**Dynamische Preise**
**Personalisierte Auswertung**

**Daten sammeln**
**Bevormundung**
**Produkte aufschwatzen**

## Pandemie …


Wenn, wie während des Corona Lockdowns im Frühling 2020, plötzlich viel mehr Arbeitnehmende von zu Hause aus Arbeiten zeigen sich schnell mögliche Sicherheitslücken. Seien dies unzureichend geschützte Zugänge zu den Firmen IT-Systemen oder auch ‘grössere’ Probleme, welche die verteilte Kommunikation untereinander betreffend.

Ein gross in den Medien verbreitetes Beispiel sind die vielfältigen Sicherheits-Probleme von Zoom.us: *https://www.watson.ch/digital/coronavirus/106601868-zoom-hat-s-vermasselt-die-unglaubliche-chronologie-der-zoom-fails*

Im Prinzip geht es immer darum,

**RISIKEN** ZU MINIMIEREN

# Risiko-Management

- Formel zur Risikoberechnung

$$R = W \; x \; A$$

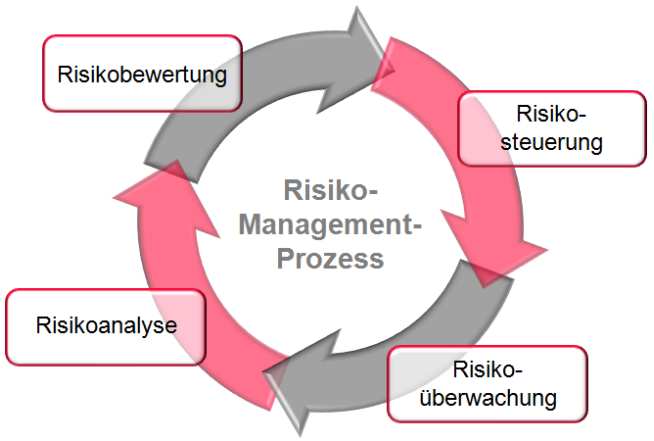
$R_{isiko}$ = $W_{ahrscheinlichkeit\ des\ Schadenereignisses}$ x $A_{usmass\ des\ Schadens}$

- Einfache Risiko-Berechnung:

| Beschreibung | Wahrschein-lichkeit | Ausmass des Schadens | Risiko |
|---|---|---|---|
| Feuer im Serverraum | 2 | 9 | 18 |
| Wasserschaden im Serverraum | 3 | 9 | 27 |
| Diebstahl eines Servers | 1 | 10 | 10 |
| Stromausfall Serverraum | 6 | 6 | 36 |

Der Anwendungsbereich dieser Formel bezieht sich auf Schäden mittleren Ausmasses. Für Bagatellschäden, wie auch für Grosskatastrophen, ist die Formel nicht anwendbar.

# Risiko-Management




**Begriffe des Risikomanagements**[Bearbeiten | Quelltext bearbeiten]

**Risikoanalyse** – wird zur Identifikation und Bewertung von Risiken eingesetzt. Im technischen Bereich kommt die probabilistische Sicherheitsanalyse zur Anwendung.

**Identifikation von Risiken** – ist Teil der Risikoanalyse, es wird eine Liste der verschiedenen Risiken erstellt, im Fall von technischen Systemen anhand der Funktionsanforderungen (unabhängig von einer technischen Ausführung). Hilfsmittel sind: Szenario-Technik, Post-Mortem-Analyse, Expertenbefragungen, Delphi-Methode, Kreativitätstechniken, Checklisten (Gefährdung: Liste der Gefährdungen im Arbeitsschutz), Analyse möglicher Gefährdungen (Hazard and Operability Study),[7] Auswertung der Erfahrungen (industrielle Unfälle, Insolvenzen) aus vergleichbaren Unternehmensbereichen.

Beispiel für eine Risikomatrix

**Risikomatrix**: – wird zur detaillierten Erfassung und Bewertung des Gesamtrisikos eines Unternehmens, einer technischen Anlage oder eines Unternehmens- oder technischen Prozesses verwendet, indem die ermittelten Risikofaktoren in eine Matrix (Risikoportfolio, Risikomatrix) mit den Dimensionen Eintrittswahrscheinlichkeit und Schadensausmaß eingetragen werden.[5][8]

**Risikovermeidung** – durch Unterlassung einer risikobehafteten Aktivität.

**Risikominderung** – reduziert das Risikopotenzial auf ein akzeptables Maß.

**Risikobegrenzung** – durch Festlegung definierter Obergrenzen von Risiken.

**Risikokommunikation** – der Risikoergebnisse – in transparenter und nachvollziehbarer Weise – für die Entscheidungsfindung über die Vertretbarkeit des Risikos durch den Betreiber, der Behörde unter Einbeziehung von Sachverständigen sowie für die durch das Risiko betroffenen Personen in der Anlage und in der Anlagenumgebung.[5]

**Risikoakzeptanz** – wird erreicht, wenn das Risiko unter den gegebenen gesellschaftlichen Rahmenbedingungen und unter Beachtung eventueller Restrisiken als vertretbar bewertet wird.

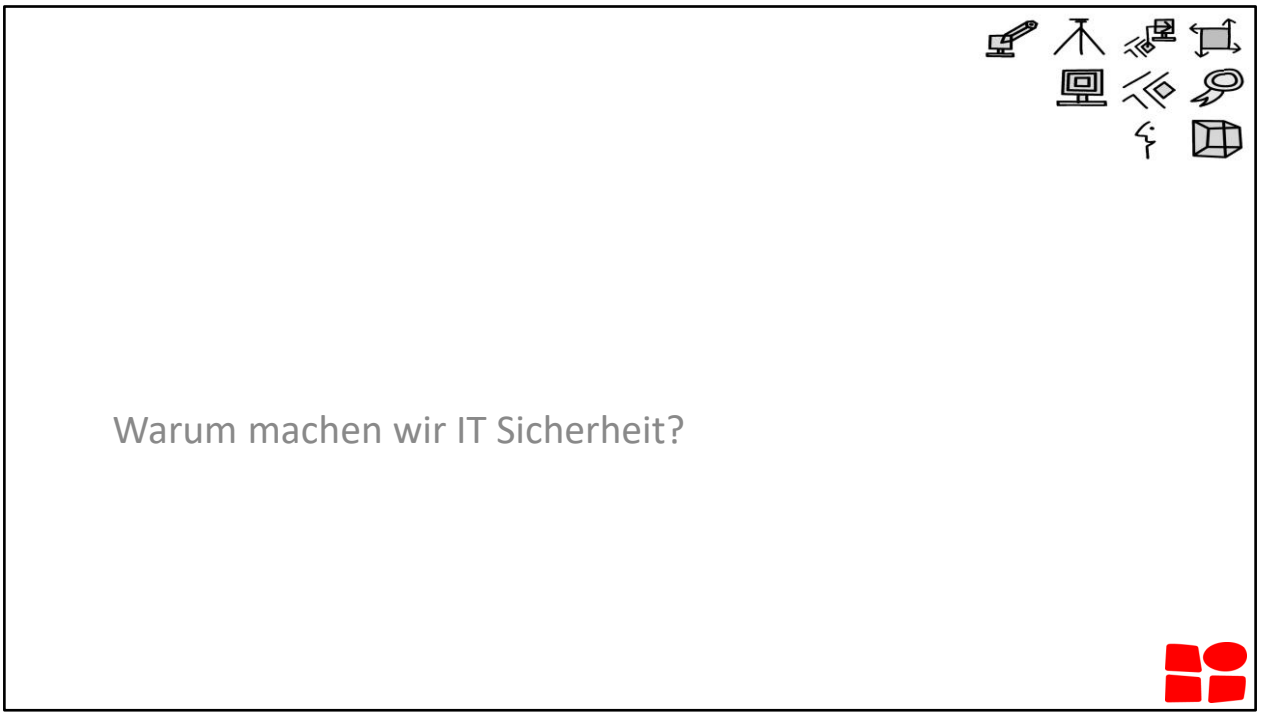
**Restrisiko** – ist das Risiko, welches nach der Anwendung von Schutzmaßnahmen verbleibt.[5] (Siehe auch die Aussage des Bundesverfassungsgerichts von 1978 im Kalkar-Urteil zum Restrisiko.[9])
**Grenzrisiko** – ist das größte noch vertretbare Risiko bei Einhaltung vorgegebener Standards (Stand der Technik / Sicherheitstechnik)[5] (Siehe auch Minimale endogene Mortalität ist ein Maß für das akzeptierte - unvermeidliche - Risiko.)
**Risikowahrnehmung** – wird entsprechend der Einflussgrößen von Freiwilligkeit, Kontrolle, Vertrauen und Katastrophenpotential (nach den Grundannahmen der Psychologie) als inhärent subjektiv empfunden.[5]
**Risikodiversifikation** – durch die Aufteilung des Vermögens auf verschiedene Vermögenswerte.
**Risikotransfer** – durch Übertragung des Risikos auf Dritte, indem der Risikoträger wechselt (z. B. auf ein Versicherungsunternehmen).
**Risikokontrolle** – durch Überwachung der identifizierten, aktuellen Risiken (Risiko-Indikatoren) und Einhaltung vorgegebener Grenzwerte.
**Risikoindikatoren** – Messung von Systemgrößen, die Aufschluss über die Risiken (Risikokennzahlen) geben (Empfindlichkeit / Sensitivität eines Systems gegenüber äußeren Einflüssen). In der Sicherheitstechnik wird der Begriff Sicherheitsindikator verwendet. In der Finanzwirtschaft werden die Indikatoren unterschieden:[10]
*Lagging indicators*, die sich verändern, nachdem sich die Finanzwirtschaft als Ganzes verändert hat.
*Leading indicators*, die sich verändern, bevor sich die Finanzwirtschaft als Ganzes verändert.
**Risikoaggregation** – ist eine Zusammenfassung aller Einzelrisiken, wobei die Einzelrisiken entsprechend ihrer relativen Bedeutung auf die Unternehmensentwicklung gewichtet werden, und nicht durch deren einfache Addition der Einzelrisiken. Dieses kann durch Simulation der Faktoren zur Ermittlung des Gesamtrisikos des Systems erfolgen (Verwendung z. B. zur Bestimmung des „Marktpreisrisikos“).
**ALARP-Prinzip** (ALARP *As Low As Reasonably Practicable*) bedeutet, die Risiken sollen auf ein vernünftiges und durchführbares Maß minimiert werden. In einer Risiko-Nutzen-Analyse kann abgeschätzt werden, ob der Nutzen des Produkts das Restrisiko überwiegt.
**RAMS**-Management stellt sicher, dass Systeme definiert, Risikoanalysen durchgeführt, Gefährdungsraten ermittelt, detaillierte Prüfungen gemacht und Sicherheitsnachweise erstellt werden (im englischen RAMS: Reliability, Availability, Maintainability, Safety / Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit).

**UND JETZT …?**

Wir machen vermeintlich sehr viel im Bereich Informatik-Sicherheit. Leider sehr oft ohne wirkliches Konzept, also ohne, dass wir wissen, vor was wir uns eigentlich schützen müssen und welche Massnahmen wirklich sinnvoll sind.

Das Bild zeigt überspitzt die Funktionalität der mit Windows XP neu eingeführte Windows-Firewall. Diese ‘gaukelte’ die vermeintlich absolute Sicherheit vor, deckte jedoch nur einen geringen Anteil der Angriffsmöglichkeiten ab.

**Nun wollen wir uns anschauen, was wir tun können, um unsere IT sicher(er) zu machen …**




Warum machen wir überhaupt IT Sicherheit?

Die Antworten dazu können in die folgenden Haupt-Themen gruppiert werden:

- Um die Informationssicherheit zu gewährleisten
- Aus Betriebsüberlegungen
- Aus rechtlichen Gründen

- Die schlechte Nachricht zuerst:
  **Eine 100%tige Sicherheit gibt es nicht!**

- **Aber**:
  - Wir wollen ohne Störungen arbeiten
  - Wir wollen uns vor Bedrohungen schützen
  - Wir sollten für den Notfall vorsorgen
  - Wir müssen Haftungsrisiken ausschliessen

**Schutz vor Bedrohung**
Da Unternehmen in ihrer Geschäftstätigkeit von den Systemen der Informations- und Kommunikationstechnologie abhängig sind, ist der Schutz elektronisch verarbeiteter Daten und Ihrer Datenverarbeitungsanlagen vor Bedrohungen wie technischen Systemausfällen, Systemmissbrauch (z.B. unbefugte oder unbemerkte Veränderung), Spionage, Verlust oder Diebstahl, besonders bedeutend. Der Schutz vor Bedrohungen gewinnt immer mehr an Bedeutung. Die ungewollte Bekanntgabe oder auch der ungewollte Verlust von Informationen eines Unternehmens kann den Fortbestand beeinflussen bzw. erschweren.

**Arbeiten ohne Störungen**
Ohne ein gut durchdachtes, konsistentes System ist ein reibungsloses Arbeiten nicht möglich, durch Ausfälle ist der Zugriff auf Daten nicht gewährleistet.

**Für den Notfall vorsorgen**
Um Schäden und Risiken in der IT zu vermeiden bzw. zu minimieren, müssen Massnahmen eingerichtet und aufrechterhalten werden. Eine funktionierende Hard-und Software, eingerichtete Sicherheitstechniken (Zugriffsschutz, Firewall, Netzwerksicherheit usw.), ein Berechtigungskonzept und Notfallpläne bei Störungen sind wichtige Vorsorge-Massnahmen.

**IT-Sicherheit nach Störungen gewährleisten**
Daten sollten regelmässig gesichert werden, damit bei einer möglichen Störung der Zugriff auf die Daten gewährleistet ist.

**Haftungsrisiken**
Geschäftsführer und leitende Angestellte, die für die IT-Technik zuständig sind, sind der Gefahr ausgesetzt, für entstandene Schäden Dritter oder dem Unternehmen gegenüber persönlich haftbar gemacht zu werden.

IT Sicherheit für KMUs

# DAS WICHTIGSTE IM ÜBERBLICK:

Für die IT Sicherheit in KMUs gibt es sehr viele Bereiche, die Berücksichtigt werden müssen. Auf der folgenden Folie ein (nicht abschliessender) Überblick über die Themen, die in der IT Sicherheit zu berücksichtigen sind. Viele dieser Themen werden in den folgenden Folien näher beleuchtet.

# IT Sicherheit für KMUs

**Organisatorisches & Rechtliches**

- Informationssicherheit / Datenschutz- und Sicherheit
- Verantwortlichkeiten
- Mitarbeitende schulen
- Risiken überprüfen
- Passwort-Policy

**Technisches**

- Virenschutz, Spam-Filter, Firewall
- Regelmässige (täglich) ein Backup
- Aktivitäten aufzeichnen (Logdateien)
- Strikte Rechte-Vergabe („least privilege“ Prinzip)
- Segmentieren Sie Ihr Netzwerk
- Passwort-Policy technisch umsetzen
- Remote-Zugänge stark authentisieren
- Sicherheitsupdates automatisch einspielen

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

**10 Goldene Regeln**
www.itmagazine.ch/Artikel/art_details.cfm?aid=16572&fnc=pdf

Organisatorische Massnahmen
- IT-Sicherheit ist ‘Chef-Sache’
- Sicherheitskonzept
- Überwachung

Technische Massnahmen

Informationssicherheit

## Definition Informationssicherheit

- Wir wollen die Schutzziele/Grundwerte **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** sicherstellen.

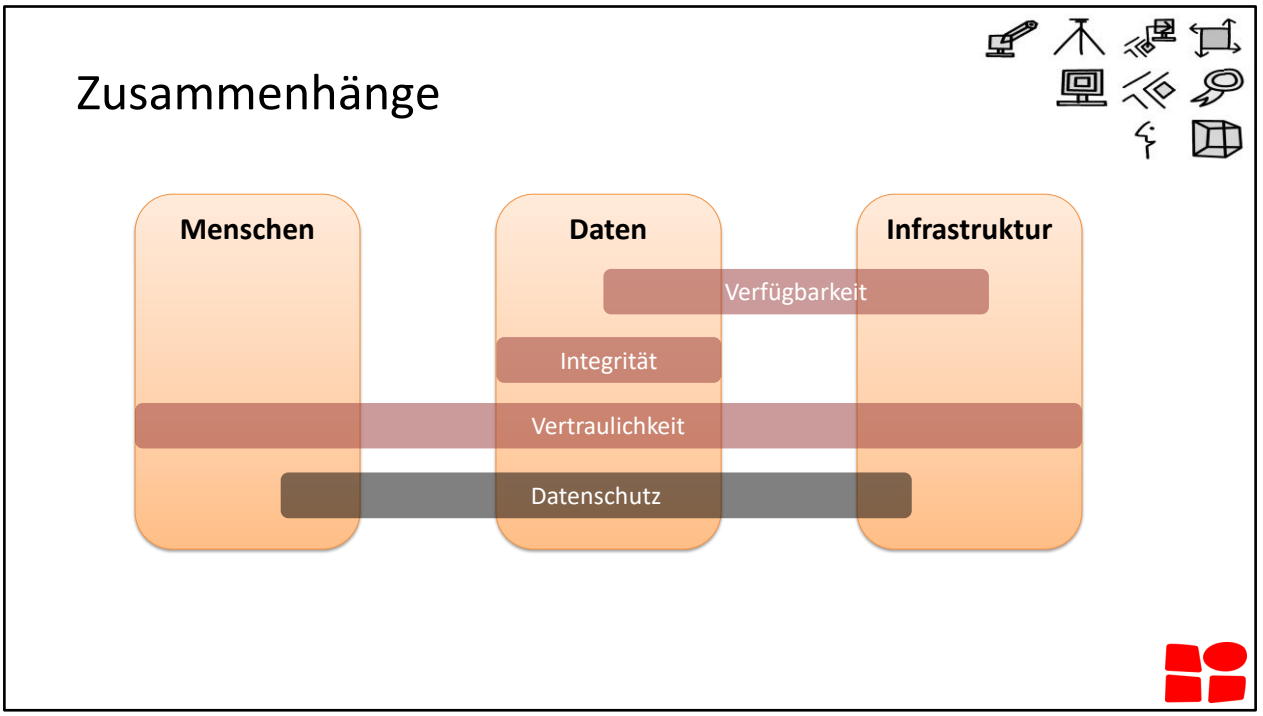
- Informationssicherheit dient dem **Schutz vor Gefahren** bzw. Bedrohungen, der **Vermeidung von wirtschaftlichen Schäden** und der **Minimierung von Risiken**.

Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden (technischen oder nicht-technischen) Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. **Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken**.

In der Praxis orientiert sich die Informationssicherheit im Rahmen des IT-Sicherheitsmanagements unter anderem an der internationalen ISO/IEC 27000-Reihe. In Deutschland ist ein Vorgehen nach IT-Grundschutz verbreitet.

Im Bereich der Evaluierung und Zertifizierung von IT-Produkten und -systemen findet die Norm ISO/IEC 15408 (Common Criteria) häufig Anwendung.

https://de.wikipedia.org/wiki/Kategorie:IT-Sicherheit

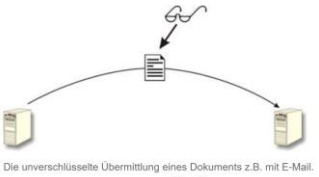


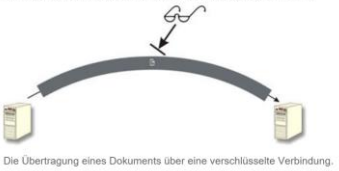

IT-Sicherheit besteht aus verschiedenen Elementen, die je nach Schutzbedarf, bzw. –zielen unterschiedlich mit und von einander abhängig sind. Im Prinzip kann die IT-Sicherheit nur umfassend gewährleistet werden, wenn alle verschiedenen Elemente perfekt auf einander abgestimmt sind.

In der Realität sieht dies jedoch meistens anders aus, da oft aus verschiedensten Gründen (Ressourcen, Änderungen an der Infrastruktur, Zeitdruck, …) unterwandert wird und so das Gesamtbild gefährdet wird.

## Grundwert: **Vertraulichkeit**

- **Vertraulichkeit** ist gewährleistet, wenn nur Personen, die dazu berechtigt sind, von schützenswerten Daten Kenntnis nehmen können.



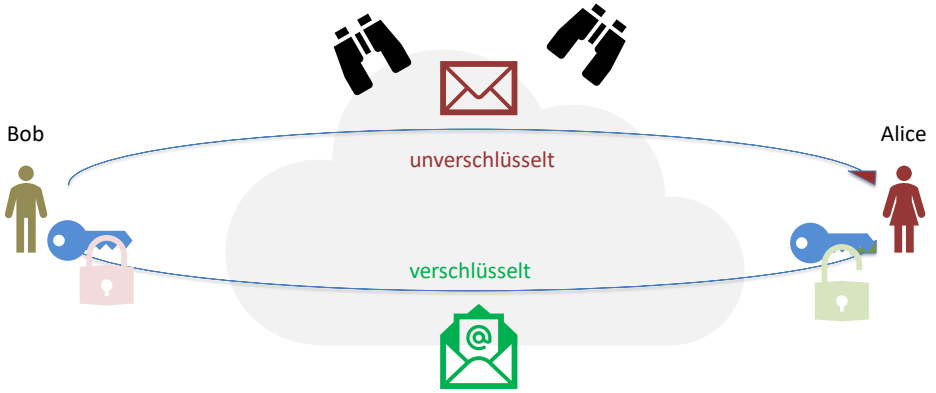




**Forderung nach Vertraulichkeit**
Das Mittel der Wahl vor unberechtigtem Zugriff besteht in der Verschlüsselung der zu schützenden Daten. Dazu stehen eine Vielzahl von Produkten, sowohl kommerzielle als auch kostenlose und frei verfügbare Software, zur Verfügung. Nicht nur gespeicherte Daten (z.B. Dateien auf Festplatten) können verschlüsselt werden, sondern auch Daten, die zu anderen Personen bzw. Computern übertragen werden sollen (z.B. E-Mails).

Darüber hinaus gibt es spezielle Verschlüsselungsprogramme, die auch einen sicheren Übertragungskanal bereitstellen. Zum Beispiel kann beim Einloggen an einem entfernten Rechner der Benutzername und das Passwort mitgelesen werden. Bei Verwendung eines gesicherten Übertragungskanals ist das Mitlesen nicht mehr möglich. Die der Verschlüsselung zu Grunde liegenden Verfahren werden so sicher eingeschätzt, dass ein Knacken des Codes mit den zur Verfügung stehenden technischen Mitteln in keinem realistischen Zeitraum möglich ist. In diesem Fall spricht man von einem sicheren Verschlüsselungsverfahren.

## Ein kurzer Ausflug in die Kryptografie

- … bekannt aus der (E-Mail-)Verschlüsselung.




**E-Mail-Verschlüsselung** wird verwendet, um vertrauliche Informationen so per E-Mail vom Absender zum Empfänger zu schicken, dass niemand ausser Absender und Empfänger Zugang zu diesen Informationen bekommt (Ende-zu-Ende-Verschlüsselung).

Die E-Mail-Verschlüsselung geht oft einher mit der digitalen Signatur und wird in vielen Szenarien tatsächlich mit ihr kombiniert. Das Ziel einer digital signierten E-Mail ist es, Informationen so vom Absender zum Empfänger zu schicken, dass sie niemand unbemerkt auf dem Weg vom Absender zum Empfänger manipulieren kann. Die E-Mail-Signatur befriedigt das Bedürfnis nach Authentizität und Integrität.
Oft wird E-Mail-Verschlüsselung mit TLS-Verschlüsselung in Verbindung gebracht. Bei diesem Verfahren handelt es sich jedoch oft nur um eine Transportverschlüsselung zwischen den E-Mail-Servern. Wenn auch die Anlieferung der E-Mail an den E-Mail-Server und das Abholen der E-Mail vom Postfachserver verschlüsselt erfolgen soll, muss zusätzlich STARTTLS eingesetzt werden. Ausserdem ist die Integrität der E-Mail nicht gewährleistet, da die E-Mail nicht signiert wird.

Siehe: https://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung

## E-Mail-Verschlüsselung


**Prof. Dr.-Ing. Harald Gerlach**, Uni Neu Ulm
**Fakultät**

Informationsmanagement

**Lehrgebiet**
Wirtschaftsinformatik (Informationstechnik)

**Lehrveranstaltungen**
Informationstechnik, Internet- und Officeanwendungen, Einführung in die Wirtschaftsinformatik, Kommunikationstechnik, Datenverarbeitung II (Access), UNIX, PC-Technik, Professionelle Dokumentation

# Klassifizierung von Informationen

- Für die Klassifizierung von Informationen sind folgende Schritte durchzuführen:
  - Ausgangslage
  - Inventur der Daten
  - Bewertung
  - Umsetzung

| Abteilung | Inventar | Vetraulichkeit | Verfügbar | Integrität | Klasse |
|---|---|---|---|---|---|
| Finanz | Rechnungen | 0 | + | ++ | 2 |
| IT | Windows Server Passwörter | ++ | + | ++ | 3 |
| Komm. | Veröffentlichte Medienmitteilungen | - | 0 | + | 1 |

Wichtig bei den gesamten Sicherheits-Massnahmen ist, dass man weiss, was (also welche Informationen) man wie stark schützen muss. Ein geeignetes Hilfsmittel dazu ist die Klassierung der Daten.

Das Hauptproblem ist, dass sich viele Betriebe nicht bewusst sind, was es bedeuten würde, wenn die vorhandenen Daten nicht mehr da wären. Oft hört man den Spruch: «Bei uns ist doch nichts zu holen…»

Für die Klassierung wird zuerst eine Inventur (ähnlich der IT-Grundschutz Struktur-Analyse) gemacht. Danach werden die erhobenen Daten bewertet. Daraus ergibt sich dann die nötige Sicherheitsanforderung.

**Legende:**

| | |
|---|---|
| ++ | Hoch / sehr hoch |
| + | Ja |
| 0 | Neutral |
| - | Nicht nötig |
| -- | kein Bedarf |

**Grundsätzlich gilt: Je höher die Klasse, um so schützenswerter sind die Informationen = je mehr Sicherheitsmassnahmen müssen für diese Daten umgesetzt werden.**

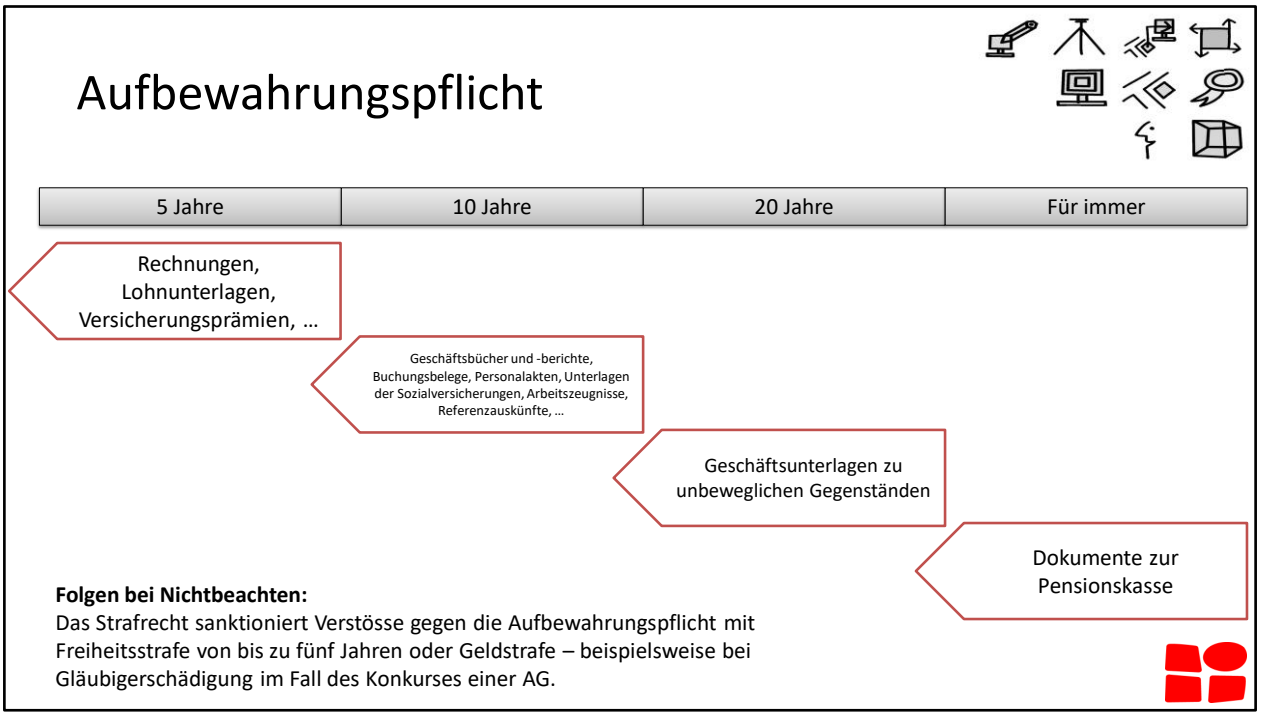
Um die IT-Sicherheit ständig aufrecht zu erhalten, ist es zwingend nötig, dass die Sicherheit immer wieder von neuem geprüft und auch entsprechend angepasst wird, wenn sich Änderungen ergeben.

## Grundwert: **Verfügbarkeit**

- **Verfügbarkeit** bezieht sich auf Daten und Verfahren und bedeutet, dass sie zeitgerecht zur Verfügung stehen.


**Forderung nach Verfügbarkeit**
Je nach konkreter Anforderung der Verfügbarkeit muss der Ausfall von Teil- oder Gesamtsystemen durch geeignete Massnahmen vorgebeugt werden. Resultierend aus der Vielzahl der zu schützenden Systeme gibt es eine mindestens ebenso grosse Vielzahl von technischen und organisatorischen Massnahmen, um die Wahrscheinlichkeit eines Systemsausfalls zu minimieren.

Ein häufig angewandtes Prinzip ist die redundante Auslegung von kritischen Systemen. Zum Beispiel erfolgt die Stromversorgung von Servern über zwei Netzteile, d.h. fällt ein Netzteil aus, kann der Server mit dem verbleibenden Netzteil weiter mit Strom versorgt werden. Besonders kritische Systeme bis hin zu ganzen Rechenzentren sind oft zweifach redundant ausgelegt.




**Die Aufbewahrungsfristen in der Zusammenfassung:**

- **5 Jahre** für Handwerker-, Miet- und Arztrechnungen, aber auch für Lohnunterlagen sowie Versicherungsprämien
- **10 Jahre** für Geschäftsbücher, Geschäftsberichte, Buchungsbelege und unter Umständen den Revisionsbericht, Kontoauszüge, Personalakten, Unterlagen der Sozialversicherungen und Lohndeklarationen sowie Arbeitszeugnisse und Referenzauskünfte
- **20 Jahre** für Geschäftsunterlagen, die in Zusammenhang mit unbeweglichen Gegenständen stehen.
- **Unbegrenzt**e Aufbewahrungspflicht für Dokumente zur Pensionskasse

Gesetzlich sind Privatpersonen nicht dazu verpflichtet, irgendwelche Unterlagen aufzubewahren.

Quelle: http://www.qontis.ch/panorama/personal-finance/aufbewahrungspflicht-in-der-schweiz-die-aktuellen-fristen-815

**Für bestimmte Dokumente gibt es in der Schweiz eine Aufbewahrungspflicht. Bis diese abgelaufen ist, sollte man die Unterlagen nicht vernichten. Denn gerade dann, wenn es zu juristischen Auseinandersetzungen kommt, sollten Rechnungen, Kontoauszüge, Lohnunterlagen und Co. noch bis zur jeweils festlegten Frist zurück gehend vorhanden sein.**

**Aufbewahrungspflicht: Verschiedene Regeln für Private und Unternehmen**
Gesetzlich sind Privatpersonen nicht dazu verpflichtet, irgendwelche Unterlagen aufzubewahren. Die Aufbewahrungsfristen in der Schweiz sollten dennoch unbedingt eingehalten werden, da sie bei allfälligen Rechtsstreitigkeiten, wie bei Auseinandersetzungen mit der Steuerbehörde oder bei Produktmängeln, als Beweismaterial herangezogen werden können. Sie dann parat zu haben kann Vorteile bringen und die Ermittlungen wesentlich beschleunigen.
Selbständige und Unternehmen dagegen sind tatsächlich verpflichtet Aufbewahrungsfristen einzuhalten. Die Aufbewahrungspflicht von Geschäftsunterlagen zu beachten ist zudem ein wichtiger Teil eines ordentlichen

Risikomanagements.
Je nach Dokument, gelten jedoch unterschiedliche Fristen dafür, wie lange man die Unterlagen behalten sollte oder muss.

**Aufbewahrungsfrist für Rechnungen, Kontoauszüge und Co.**

Rechnungen sollten grundsätzlich nicht vor Ablauf der Verjährungsfristen entsorgt werden, da es ansonsten nur schwer möglich ist, Ersatzleistungen bei Schäden innerhalb der Garantiezeit durchzusetzen. Die obligatorische Aufbewahrungspflicht in der Schweiz für Handwerker-, Miet- und Arztrechnungen, aber auch für Lohnunterlagen sowie Versicherungsprämien, beträgt **fünf Jahre**.
Da es verschiedene Verjährungsfristen und Aufbewahrungspflichten in der Schweiz gibt, sollten Kontoauszüge im Idealfall **zehn Jahre** aufbewahrt werden. Das lohnt sich deshalb, weil diese in der Regel herangezogen werden, wenn Zahlungen nachgewiesen werden sollen. Ausserdem sind Kontoauszüge wichtig bei Auseinandersetzungen mit der Steuerbehörde.
Eine **unbegrenzte Aufbewahrungspflicht** in der Schweiz besteht für Dokumente zur Pensionskasse, Rechnungen für spezielle Anschaffungen, die bei einem Schadensfall der Hausratversicherung relevant sein können, sowie für Unterlagen zu Erbschaften und Schenkungen. Auch Belege über den Kontostand zum Zeitpunkt der Heirat sollten unbegrenzt aufbewahrt werden. Nützliche Informationen hierzu finden Sie unter anderem im Internet unter atzuerich.ch
Deshalb legen Sie am besten Ihre Kontoauszüge möglichst lückenlos und chronologisch geordnet ab, damit diese im Fall der Fälle greifbar sind. Das nachträgliche Anfordern von Kontoauszügen bei der Bank bedeutet einen hohen Suchaufwand und ist in der Regel gebührenpflichtig.

**Aufbewahrungspflicht in der Schweiz für Geschäftsunterlagen**

Seit dem 1. Januar 2013 besteht eine Aufbewahrungspflicht in der Schweiz für Geschäftsbücher von Einzelfirmen und Personengesellschaften. Folgende Dokumente müssen Firmen nach dem neuen Rechnungslegungsgesetz daher aufheben: Geschäftsbücher, Geschäftsberichte, Buchungsbelege und unter Umständen den Revisionsbericht. Die Aufbewahrungsfrist für diese Dokumente beträgt **zehn Jahre**. **Zwanzig Jahre** beträgt die Aufbewahrungspflicht dagegen für Geschäftsunterlagen, die in Zusammenhang mit unbeweglichen Gegenständen stehen.
In der Schweiz gibt es ausserdem eine **zehnjährige** Aufbewahrungsfrist für Personalakten, Unterlagen der Sozialversicherungen und Lohndeklarationen. Diese Frist gilt zudem für Arbeitszeugnisse und Referenzauskünfte.

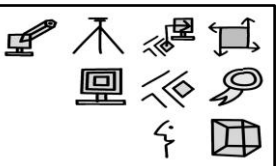
Aus rechtlicher Sicht ist lediglich eine «ordnungsgemässe» Aufbewahrung der Geschäftsunterlagen gemäss den «anerkannten kaufmännischen Grundsätzen» notwendig. Nur für den Jahresabschluss ist ausdrücklich vorgeschrieben, dass Bilanz und Erfolgsrechnung im unterzeichneten Original auf Papier aufzubewahren sind. Bei anderen Geschäftsunterlagen kann die Aufbewahrung auch elektronisch oder auf vergleichbare Weise erfolgen.
Die anerkannten kaufmännischen Grundsätze sehen unter anderem vor, dass die Echtheit, Vollständigkeit und Unverfälschbarkeit sowie der Schutz der aufbewahrten Geschäftsunterlagen gewährleistet werden muss. Die Geschäftsunterlagen müssen jederzeit verfügbar und lesbar sein. Die Aufbewahrung ist praxisgemäss auch im Ausland möglich, sofern Verfügbarkeit und Lesbarkeit jederzeit gewährleistet sind und das schweizerische Datenschutzrecht beachtet wird.
Die Aufbewahrung von Geschäftsunterlagen in Papierform ist vergleichsweise einfach und deshalb empfehlenswert, da bedrucktes Papier als Informationsträger die oben erwähnten Bedingungen erfüllt. Elektronische Geschäftsunterlagen können auf Papier ausgedruckt werden. Bei grösseren Mengen an elektronischen Geschäftsunterlagen hingegen ist die Verwendung von Informationsträgern notwendig, die gemäss den Grundsätzen der ordnungsgemässen Datenverarbeitung entweder unveränderbar sind (beispielsweise nur einmal beschreibbare DVDs) oder bei denen mit technischen Verfahren die Integrität der gespeicherten Informationen gewährleistet ist (beispielsweise Festplatten mit digitalen Signaturen, Zeitstempeln und Protokollen). Ein Schweizer Anbieter entsprechender Systeme ist Archivista.

Siehe auch: https://www.startwerk.ch/2011/08/02/unternehmen-und-ihre-unterlagen-die-vernachlassigte-aufbewahrungspflicht/

# Aufbewahrungspflicht

- Sicherstellung der Aufbewahrungspflicht
  - Mittels Papier
    - Sicheres Archiv mit Klimakontrolle, Zugangskontrolle und regelmässiger Prüfung auf ‘Zerfall’
  - Mittels IT
    - Speicherkonzept inkl. Definition, in welcher Form die Daten langfristig gespeichert werden und lesbar bleiben
    - Geeignete Hard- und Software
    - Geo-Redundante Speicherung auf unterschiedlichen Medien

# Organisatorische Mängel




Organisatorische IT-Sicherheit

**Zu den organisatorischen Massnahmen zählen:**

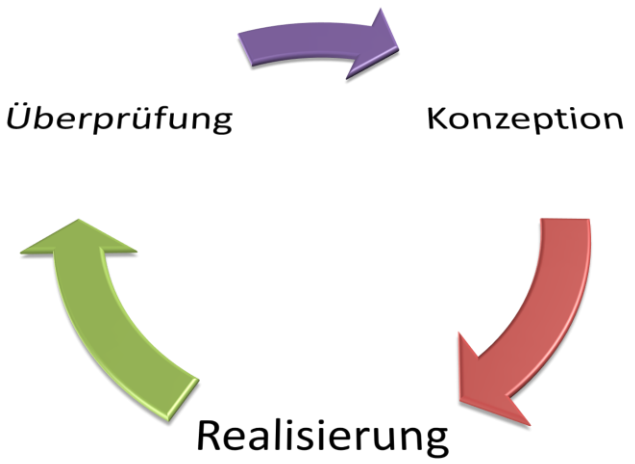
- Unzureichende IT-Sicherheits-Strategie
- Einbezug der Geschäftsleitung beim Thema IT-Sicherheit
- Verantwortlichkeiten bezüglich IT und IT-Sicherheit sicherstellen
- Zuständigkeiten von IT-Dienstleistern im Hinblick auf die IT-Sicherheit klar regeln.
- Regelmässige Schulung von Mitarbeitenden im Umgang mit der IT-Infrastruktur und der IT-Sicherheit
- Regelmässige Überprüfung der Risiken im Bereich Informationssicherheit
- Schutz vor Einbruch/Elementar
- Definition und technische Umsetzung der Passwort-Policy
- Im Zusammenhang mit e-Banking-Applikationen mit der Bank das Thema IT-Sicherheit besprechen (Möglichkeiten von Kollektiv-e-Banking-Verträgen prüfen)
- Schlechte Konfiguration (Alte Betriebssysteme, Keine Update-Politik, Mängel, die Mitarbeitende dazu animieren, Umwege zu suchen um effizient arbeiten zu können, …)
- Mobile Computing nicht genügend durchdacht bzw. leichtfertig eingesetzt
- ‚Bring your own Device' schlecht/ungenügend geregelt.

## Organisatorische Massnahmen

- (IT)-Sicherheit vorleben (Management-Aufgabe!)
- Mitarbeiter informieren und schulen
- Richtlinien erstellen
- ‚Notfälle' üben


Neben den erwähnten Punkten ist ein Security-Verantwortlicher zu bestimmen. Nur, wenn eine Person den Lead übernimmt (und dafür auch die volle Unterstützung des Managements hat) kann IT Security zum Erfolg werden.

# Organisatorische Massnahmen: IT Sicherheit umsetzen




Informationssicherheit ist als dauerhafter Regelkreis, bestehend aus **Konzeption**, **Realisierung** und **Überprüfung** von geeigneten Sicherheitsmassnahmen zu verstehen.

**Konzeption**

- Um die geeigneten Massnahmen für die optimale Sicherheit der IT umsetzen zu können, müssen die möglichen Risiken zuerst analysiert werden und die dafür geeigneten Massnahmen erhoben werden. Ebenfalls ist die Umsetzung der definierten Massnahmen zu planen. Nicht zu vergessen ist dabei der Miteinbezug der betroffenen Mitarbeitenden sowie das Zusichern der Unterstützung des Managements.

**Realisierung**

- Bei der Umsetzung ist darauf zu achten, dass nur die anlässlich der Konzeption definierten Punkte realisiert werden. Die umgesetzen Punkte sind vollständig umzusetzen und sicherzustellen, dass diese korrekt funktionieren.

**Überprüfung**

- In dieser Phase werden die zuvor umgesetzten Punkte minutiös auf deren Effizient, Qualität und Funktionalität geprüft. Wichtig bei diesem Schritt ist, dass die Umsetzung neutral geprüft wird – im Idealfall von nicht bis anhin im Projekt involvierten Personen. Die erhobenen, allfälligen Mängel sind aufzunehmen und in die Phase Konzeption überführt. Nun beginnt der Prozess von vorne. In der erneuten Konzeption werden einerseits die gefundenen Mängel aber auch neue Punkte aufgenommen und bearbeitet.

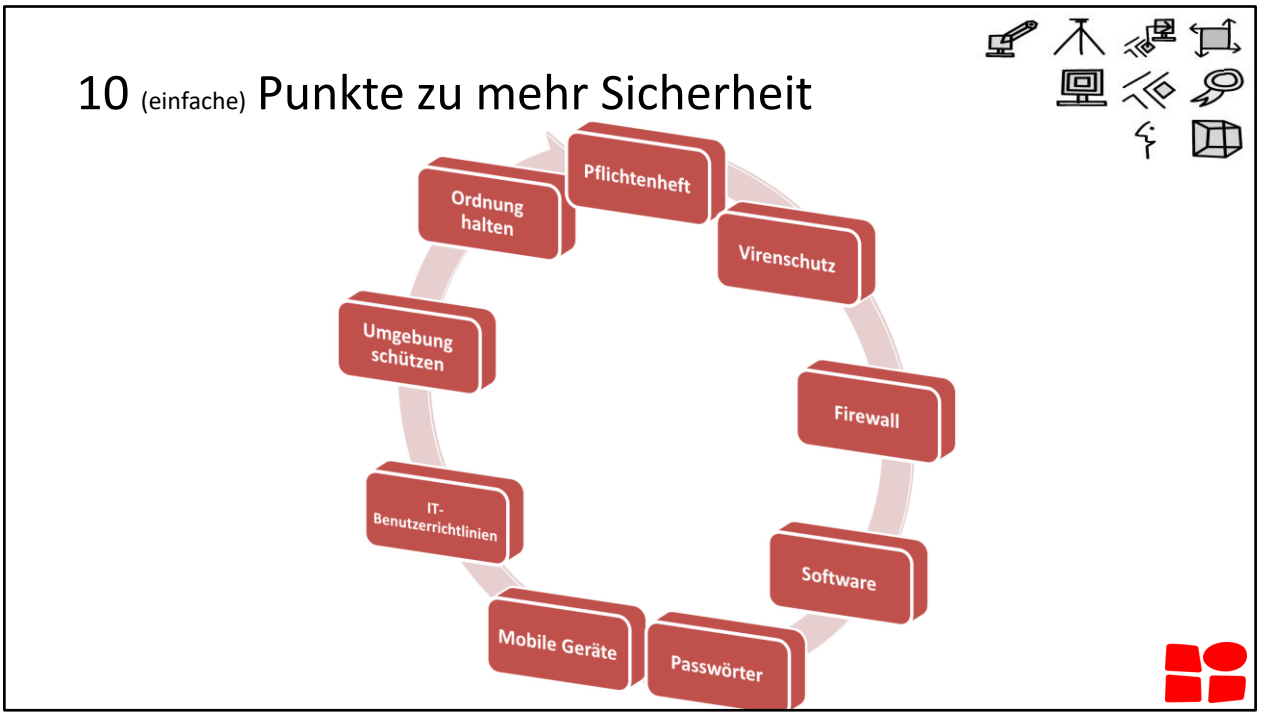
Ist der Prozess der IT Sicherheit einmal gestartet, gibt es theoretisch kein Ende. Denn bei jeder neuen Iteration sollten grundsätzlich neue Punkte auftauchen, welche verbessert werden können. Deshalb ist es entsprechend sinnvoll, dass die einzelnen Iterationen als einzelne Projekte definiert werden, das nötige Budget im Bezug auf Ressourcen und Zeit zur Verfügung gestellt werden.

## IT Sicherheit umsetzen

- Im Bezug auf die Mitarbeiter-Sensibilisierung sind die «10 goldenen Regeln» hilfreich.
- Mit IT-Sicherheits-Richtlinien wird Verbindlichkeit bei den Mitarbeitenden erreicht.

Das erweiterte 10-Punkte-Programm schafft mehr Schutz.
Siehe z.B. *InfoSurance_Broschuere.pdf*

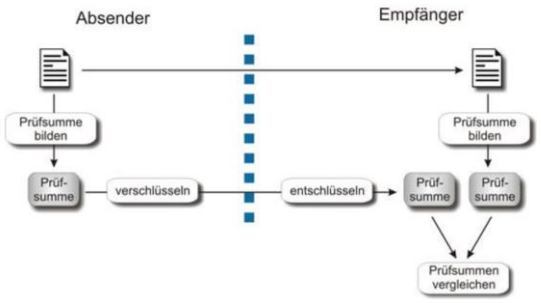
Siehe Beispiel *IT-Sicherheits-Richtilinie.pdf*




- Erstellen Sie ein **Pflichtenheft** für IT-Verantwortliche
- Sichern Sie Ihre Daten regelmässig mit **Backups**
- Halten Sie Ihr **Antivirus-Programm** aktuell
- Schützen Sie Ihren Internetzugang mit einer **Firewall**
- Aktualisieren Sie Ihre **Software** regelmässig
- Verwenden Sie starke **Passwörter**
- Schützen Sie Ihre **mobilen Geräte**
- Machen Sie Ihre **IT-Benutzerrichtlinien** bekannt
- Schützen Sie die **Umgebung** Ihrer IT-Infrastruktur
- **Ordnen** Sie Ihre Dokumente und Datenträger!

# Grundwert: **Integrität**

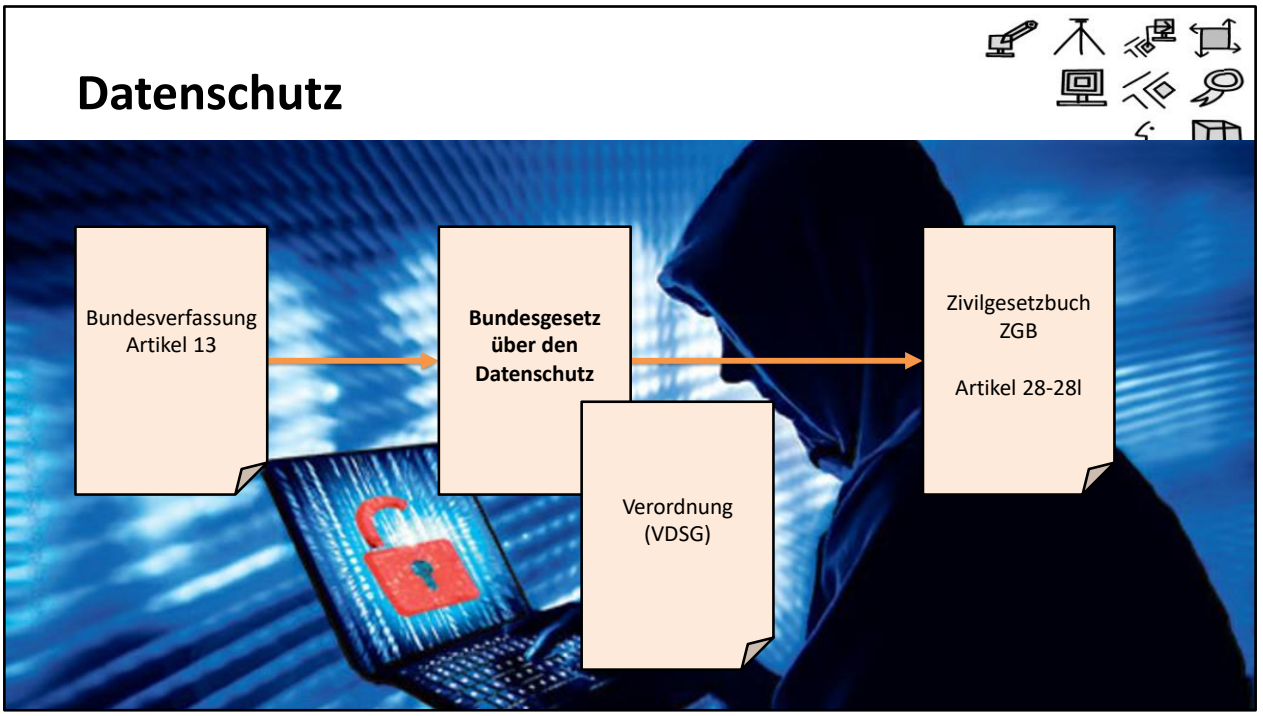
- **Integrität** ist gewährleistet, wenn schützenswerte Daten unversehrt und vollständig bleiben.




Prinzipieller Ablauf eines Verfahrens zur Sicherstellung der Integrität von Dokumenten.

**Forderung nach Integrität**
Die Programme, die zum Schutz der Vertraulichkeit verwendet werden, bieten fast immer auch die notwendigen Werkzeuge, um die Unverfälschtheit von Daten zu gewährleisten.

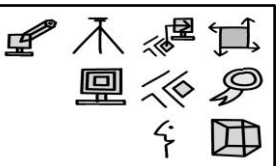
Um ein Dokument vor Verfälschung zu schützen, wird mit Hilfe eines mathematischen Verfahrens eine so genannte Prüfsumme gebildet. Diese Prüfsumme ist nahezu einmalig, d.h. die Wahrscheinlichkeit, dass bei einem anderen Dokument die gleiche Prüfsumme gebildet wird, ist so gering, dass dieser Fall vernachlässigt werden kann. Ausserdem verursacht bereits die kleinste Änderung am Dokument eine vollkommen andere Prüfsumme. Das Dokument wird dann zusammen mit der Prüfsumme an den Adressaten gesendet. Der Adressat bildet aus dem empfangenen Dokument ebenfalls eine Prüfsumme. Wenn beide Prüfsummen übereinstimmen, also die selbst erstellte und die mitgesendete, dann wurde das Dokument nicht verfälscht. Damit auf dem Versandweg das Dokument nicht zusammen mit der Prüfsumme manipuliert wird, wird die Prüfsumme verschlüsselt übertragen.




**Forderung nach Integrität**
Die Programme, die zum Schutz der Vertraulichkeit verwendet werden, bieten fast immer auch die notwendigen Werkzeuge, um die Unverfälschtheit von Daten zu gewährleisten.

Um ein Dokument vor Verfälschung zu schützen, wird mit Hilfe eines mathematischen Verfahrens eine so genannte Prüfsumme gebildet. Diese Prüfsumme ist nahezu einmalig, d.h. die Wahrscheinlichkeit, dass bei einem anderen Dokument die gleiche Prüfsumme gebildet wird, ist so gering, dass dieser Fall vernachlässigt werden kann. Ausserdem verursacht bereits die kleinste Änderung am Dokument eine vollkommen andere Prüfsumme. Das Dokument wird dann zusammen mit der Prüfsumme an den Adressaten gesendet. Der Adressat bildet aus dem empfangenen Dokument ebenfalls eine Prüfsumme. Wenn beide Prüfsummen übereinstimmen, also die selbst erstellte und die mitgesendete, dann wurde das Dokument nicht verfälscht. Damit auf dem Versandweg das Dokument nicht zusammen mit der Prüfsumme manipuliert wird, wird die Prüfsumme verschlüsselt übertragen.

## Aufgaben des Datenschutzes



- **Besonders schützenswerte Personendaten**: Daten über:
  - die **religiösen**, **weltanschaulichen**, **politischen** oder **gewerkschaftlichen Ansichten** oder Tätigkeiten,
  - die **Gesundheit**, die **Intimsphäre** oder die **Rassenzugehörigkeit**,
  - Massnahmen der **sozialen Hilfe**,
  - **administrative oder strafrechtliche Verfolgungen und Sanktionen**

DSG Art. 3

**Welche Daten sind sehr sensibel?**
Es ist schwierig, darüber Aussagen zu machen, da auch auf den ersten Blick unproblematische Daten wie Name, Alter oder E-Mail-Adresse für unredliche Zwecke missbraucht werden können. Zu den Daten, die besonders schützenswert sind, gelten natürlich die, die den Intimbereich des Menschen betreffen, so etwa alle Gesundheitsdaten (vgl. Art. 3 des Bundesgesetzes über den Datenschutz DSG). Aber nochmals: Grundsätzlich können je nach Kontext alle Personendaten als sensibel betrachtet werden.

**Wie sehen die Strafmassnahmen im Fall eines Verstosses gegen das Datenschutzgesetz aus?**
Das Datenschutzgesetz (DSG) sieht Strafbestimmungen (Art. 34, Art. 35 ) vor, allerdings nur bei vorsätzlichen Verletzungen der Auskunfts-, Melde und Mitwirkungspflichten sowie der beruflichen Schweigepflicht, und nur auf Antrag. Allen anderen Klagen wegen Verletzung der Persönlichkeit beurteilt der Zivilrichter gemäss Art. 15 DSG im üblichen zivilrechtlichen Verfahren.
Art. 34 Datenschutzgesetz (DSG)
Art. 35 Datenschutzgesetz (DSG)
Art. 15 Datenschutzgesetz (DSG)

**Schutz der personenbezogen Daten**

Schutz des Einzelnen gegen eine unbegrenzte Erhebung, Speicherung, Weitergabe und Verwendung seiner Daten.
Damit ist gewährleistet, dass jeder selbst über die Preisgabe und Verwendung seiner Daten bestimmen kann.

= informationelle Selbstbestimmung

**Gefährdung des Rechts auf informationelle Selbstbestimmung sind**:

- Unzulässige Erhebung von personenbezogenen Daten
- Speicherung falscher Daten
- Unberechtigter Zugriff
- Verwendung zu anderem Zweck als bei der Erhebung
- Beliebige Vermarktung der Daten

## Daten-Handel

- Die Datenhoheit besitzt, wer die vollständige Herrschaft über den Zugriff, die Verfügbarkeit und die Verwertung seiner Daten innehat.

Der Inhaber der Datenhoheit kann also den Vertraulichkeitsgrad seiner Daten bestimmen, indem *er allein* definiert, wer die Daten (mit-)lesen und bearbeiten darf. Weiter muss er steuern können, wie (sicher) die Daten aufbewahrt werden und wie zuverlässig sie verfügbar sind. Wenn Sie ein eigenes Firmennetzwerk betreiben, können Sie die Datenhoheit gewährleisten— aber es ist eine relativ grosse Herausforderung: Sie brauchen einen Notfallplan, müssen Lösungen für die Resilienz und Redundanz ihrer Systeme implementieren und deren Sicherheit kontrollieren.

Im 'Datenzeitalter' sind Daten die neue Währung. Wer als die Hoheit über 'seine' Daten hat, ist Reich. Somit aber auch angreifbar, bzw. es wird immer jemanden geben, der versucht an die fremden Daten zu gelangen, um diese selbst zu nutzen.

**Wie viel sind unsere Daten im Netz wert – 1/2: Das Spiel mit dem Datenverkauf**
http://berufebilder.de/2015/unsere-daten-netz-wert-12-spiel-datenverkauf/

*Der Wert der persönlichen Daten von Hunderten Millionen Verbrauchern ist enorm. Nach einer Studie der Boston Consulting Group belief er sich in der EU im Jahr 2011 auf 315 Milliarden Euro und wird bis 2020 auf eine Billion Euro steigen. (Liberty Global Policy Series & Boston Consulting Group 2013)*

# Überwachung der Mitarbeitenden

- Es ist gem. Art. 26 Abs 1 Verordnung 3 Arbeitsgesetz verboten, gezielte Überwachungen durchzuführen.
- Erlaubt ist nur eine anonyme Auswertung und bei Verdacht auf Missbrauch eine angekündigte namentliche Auswertung.

Siehe auch: **Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz**
https://www.edoeb.admin.ch/datenschutz/00763/00983/00988/index.html?lang=de

Um Sicherheit im geschäftlichen Umfeld durchzusetzen, greifen Unternehmen oftmals zu zwielichtigen Aktionen. Mitarbeiter werden überwacht – sogar ‚ausspioniert'.

Wichtig zu wissen ist, dass von Gesetztes wegen der Arbeitgeber kein Recht hat, den Mitarbeiter zu belauschen. In begründeten Verdachtsfällen kann, nach vorheriger Information des betroffenen Mitarbeiters, eine Auswertung der verfügbaren Logs vorgenommen werden.

Die bessere Variante ist, dem Mitarbeitenden mit dem Arbeitsvertrag mitzuteilen, dass Überwachungen vorgenommen werden können.

Ein Blick in die EU

… und die mögliche Zukunft in der Schweiz

# GDPR / DSGVO

# EU: General Data Protection Regulation (GDPR / DSGVO)

- Neue Europäische Datenschutz-Grundverordnung
  - Ab 25. Mai 2018

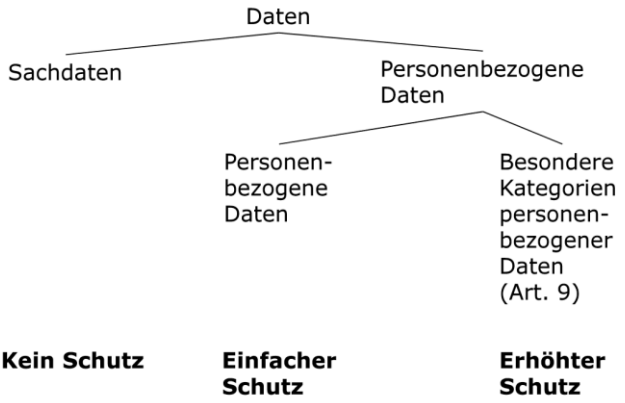
# EU: General Data Protection Regulation (GDPR / DSGVO)

- Sachlicher Anwendungsbereich:
  - Automatisierte Verarbeitung personenbezogener Daten natürlicher Personen
  - Nicht-automatisierte Verarbeitung personenbezogener Daten, sofern die Dateien nach Personen erschlossen sind.
  - NICHT: Bearbeitung durch natürliche Personen im persönlichen Bereich

- Räumlicher Anwendungsbereich:
  - Niederlassungsprinzip: Datenverarbeitungen im Rahmen der Tätigkeit von Niederlassungen in der Europäischen Union
  - Marktorprinzip: Datenverarbeitung in Bezug auf Personen in der EU durch nicht in der EU niedergelassene Verantwortliche, wenn:
    - Diese betroffenen Personen in der EU Waren oder Dienstleistungen anbieten oder
    - das Verhalten von betroffenen Personen in der EU beobachten.

# EU: General Data Protection Regulation (GDPR / DSGVO)

**Arten von Daten gemäss DSGVO**



# EU: General Data Protection Regulation (GDPR / DSGVO)

- Besondere Kategorien personenbezogener Daten mit erhöhtem Schutz (Art. 9 DSGVO)
  - Rassische und ethnische Herkunft
  - Politische Meinungen
  - Religiöse oder weltanschauliche Überzeugungen
  - Gewerktschafszugehörigkeit
  - Gesundheitsdaten
  - Daten zum Sexualleben
  - Sexuelle Orientierung
  - Strafrechtliche Verurteilungen
  - Genetische oder biometrische Daten

- Im Rahmen der Tätigkeit jedes Unternehmen können Daten besonderer Kategorien anfallen, so etwa Gesundheitsdaten (HR-Daten von Mitarbeitenden; Kundendaten, …)

## EU: General Data Protection Regulation (GDPR / DSGVO)

- Die DSGVO bringt für Unternehmen erheblich höhere Risiken als das bisherige europäische und schweizerische Datenschutzrecht:
  - Zivilrechtliche Ansprüche
  - Verbandsklagerecht / Sammelklagerecht
  - Verwaltungsgerichtliche Beschwerdemöglichkeiten
  - Bussgelder (bis zu 4% des globalen Umsatzes des Vorjahres)

# EU: General Data Protection Regulation (GDPR / DSGVO)

- Neue Pflichten für Unternehmen
  - Erweiterte Dokumentations- und Nachweispflicht
  - Informationspflicht bei Datenerhebung vom Betroffenen oder von Drittten (Transparenz)
  - Datenschutz-Folgenabschätzung
  - Erfüllung von Betroffenenrechten
  - Meldepflicht bei Datensicherheitsverletzungen gegenüber den Behörden
  - Privacy by design (Datenschutz durch Technik)
  - Privacy by default (Datenschutzrechtliche Voreinstellungen)
  - Verzeichnis von Verarbeitungstätigkeiten
  - Zusätzliche Verantwortung für Datenschutzverwantwortliche
  - Unter Umständen muss ein Vertreter in der EU ernannt werden

# EU: General Data Protection Regulation (GDPR / DSGVO)

- Betroffenenrecht:
  - Recht auf Auskunft
  - Recht auf Berichtigung
  - Recht auf Löschung
  - Recht auf «Einschränkung der Verarbeitung»
  - Recht auf eine nicht ausschliesslich automatische Entscheidung
- Meldepflicht der Unternehmen
  - Bei Datenschutzverletzung innerhalb von 72 Stunden

# EU: General Data Protection Regulation (GDPR / DSGVO)


https://www.netzwoche.ch/news/2018-11-27/erste-dsgvo-strafe-in-deutschland-verhaengt

Deutsche Datenschutzbehörden haben das erste Unternehmen wegen eines Verstosses gegen die EU-DSGVO zur Kasse gebeten. Das soziale Netzwerk Knuddels.de muss ein Bussgeld von 20'000 Euro bezahlen. Weil das Unternehmen kooperiert, kommt es billig davon.

Der baden-württembergische Datenschutzbeauftragte hat gegen die Chat-Plattform Knuddels.de ein Bussgeld in Höhe von 20’000 Euro verhängt. Das soziale Netzwerk habe Passwörter von Nutzern unverschlüsselt gespeichert. So verstiess das Unternehmen gegen die Pflicht, die Sicherheit von personenbezogenen Daten zu gewährleisten, wie "Spiegel Online" berichtet.
Der zuständige Datenschutzbeauftragte habe Knuddels zugute gehalten, dass es sich nach einem Hackerangriff im vergangenen Sommer an die Behörden wandte und die Nutzer sofort über den Angriff informierte. Bei dem Angriff waren nach Angaben des Unternehmens rund 808'000 E-Mail-Adressen sowie 1'872'000 Pseudonyme und Passwörter von Unbekannten erbeutet und im Internet veröffentlicht worden, wie Spiegel Online weiter schreibt.
Knuddels kooperiere mit den Behörden und komme deswegen glimpflich davon,

schreibt die "Frankfurter Allgemeine Zeitung". Die erste Busse wegen eines Verstosses gegen die EU-DSGVO falle demnach weit niedriger aus als ursprünglich befürchtet.

## Revision des Bundesgesetzes über den Datenschutz (DSG)

- Der Bundesrat will deshalb das DSG den veränderten technologischen und gesellschaftlichen Verhältnissen anpassen und dabei insbesondere die Transparenz von Datenbearbeitungen verbessern und die Selbstbestimmung der betroffenen Personen über ihre Daten stärken.

https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html

Worum geht es? (Läuft seit 2011 …)

Das Bundesgesetz über den Datenschutz (DSG) ist aufgrund der rasanten technologischen Entwicklung nicht mehr zeitgemäss. Der Bundesrat will deshalb das DSG den veränderten technologischen und gesellschaftlichen Verhältnissen anpassen und dabei insbesondere die Transparenz von Datenbearbeitungen verbessern und die Selbstbestimmung der betroffenen Personen über ihre Daten stärken.
Gleichzeitig soll die Totalrevision der Schweiz erlauben, das revidierte Datenschutzübereinkommen SEV 108 des Europarats zu ratifizieren sowie die Richtlinie (EU) 680/2016 über den Datenschutz im Bereich der Strafverfolgung zu übernehmen, wozu sie aufgrund des Schengen-Abkommens verpflichtet ist. Zudem soll die Revision die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Diese Annäherung und die Ratifizierung des revidierten Übereinkommens SEV 108 sind zentral, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig möglich

bleibt.

Gleichzeitig soll die Totalrevision der Schweiz erlauben, das revidierte Datenschutzübereinkommen SEV 108 des Europarats zu ratifizieren sowie die Richtlinie (EU) 680/2016 über den Datenschutz im Bereich der Strafverfolgung zu übernehmen, wozu sie aufgrund des Schengen-Abkommens verpflichtet ist. Zudem soll die Revision die schweizerische Datenschutzgesetzgebung insgesamt den Anforderungen der Verordnung (EU) 2016/679 annähern. Diese Annäherung und die Ratifizierung des revidierten Übereinkommens SEV 108 sind zentral, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig möglich bleibt.

Eine kleine Übung …

# EINE KLEINE RISIKO-ANALYSE …

Zum Thema Risiken in der IT Sicherheit …

Eine kleine Risiko-Analyse …


**Finden Sie die 9 Sicherheits-Lücken?**

Beschreibung der Sicherheitslücken

**1.** _____

**2.** _____

**3.** _____

**4.** _____

**5.** _____

**6.** _____

**7.** _____

8. _____

9. _____

Eine kleine Risiko-Analyse …


**Finden Sie die 9 Lücken?**

**Beschreibung der Sicherheitslücken**

1. Türen und Fenster stehen offen: Rechner und Zubehör könnten aus den Räumen gestohlen werden.
   Infrastrukturelle Massnahme: Schliessystem
   Organisatorische Massnahme: IT-Richtline – EDV darf unbefugten nicht zugänglich gemacht werden.

2. Der Bildschirm und damit möglicherweise auch vertrauliche Informationen können von Unbefugten eingesehen werden.
   Organisatorische Massnahme: IT-Richtline – EDV darf unbefugten nicht zugänglich gemacht werden.
   Personelle Massnahme: Schulung der Mitarbeiter

3. Ein Zettel mit Passwörtern ist sichtbar und könnte von Unbefugten missbraucht werden.
   Organisatorische Massnahme: IT-Richtlinie zum Umgang mit Passwörtern.

4. Eine mit ‚Sicherung' beschriftete CD-ROM liegt zugänglich herum.
   Organisatorische Massnahme: IT-Richtline – Datenklassierung
   Personelle Massnahme: Schulung der Mitarbeiter

5. Ausdrucke und Kopien mit vermutlich vertraulichen Daten liegen an Druckern und Kopierern.
   Organisatorische Massnahme: IT-Richtline – Datenklassierung
   Infrastrukturelle Massnahme: Papierschredder anschaffen

6. Rechner mit direkter Verbindung an das Internet können den zentralen Firewallschutz des Netzes aushebeln.
   Technische Massnahme: Port-Security einführen; wenn ein fremdes Gerät angeschlossen wird schliess der Anschluss automatisch
   Organisatorische Massnahme: IT-Richtline – Umgang mit der EDV

7. Durch private Datenträger (im Bild eine CD-ROM) kann Schadsoftware ungeprüft in das Unternehmensnetz gelangen.
   Organisatorische Massnahme: IT-Richtline – Umgang mit der EDV

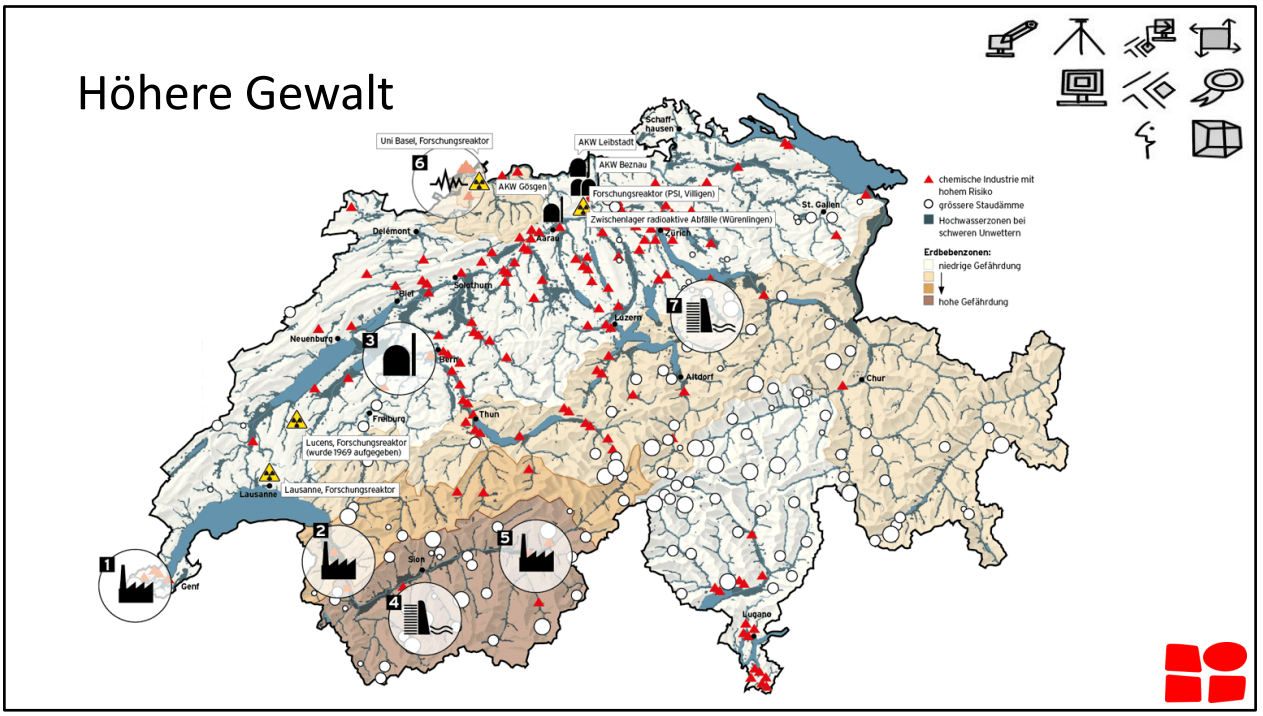
8. Austretende Flüssigkeiten gefährden die Hardware.
   Organisatorische Massnahme: IT-Richtline – Umgang mit der EDV

9. Rauchen bedeutet Brandgefahr
   Infrastrukturelle Massnahme: Feuerschutz

# BEDROHUNGEN UND MASSNAHMEN

Die Bedrohungen in der IT Sicherheit sind sehr vielfältig. Einige der grössten bzw. der am meinsten auftretenden Gefahren schauen wir uns an und machen uns Gedanken zu möglichen Gegenmassnahmen.

Selbstverständlich sind weder die Bedrohungen noch die Massnahmen abschliessend aufgeführt.




Quelle: http://www.beobachter.ch/justiz-behoerde/buerger-verwaltung/artikel/naturgefahren_wo-es-in-der-schweiz-am-gefaehrlichsten-ist/

**1. Tanklager Vernier**: In Vernier GE wird derzeit über die Sicherheit eines riesigen Tanklagers mitten im Siedlungsraum diskutiert. Bei einem Unfall könnten Hunderte Menschen umkommen.

**2. Raffinierie Collombey**: Die Erdölraffinerie liegt im Siedlungsgebiet an der Rhone. Eine Überflutung droht alle 100 Jahre. Oberhalb der Raffinerie befinden sich Staudämme.

**3. AKW Mühleberg**: Das AKW liegt unterhalb einer Staumauer (siehe Seite 36). Bei einem schweren Erdbeben würden voraussichtlich zahlreiche Sicherheitssysteme ausfallen.

**4. Grand Dixence**: Bräche die Staumauer, würde eine Flutwelle das Unterwallis inklusive Sion verwüsten. Die Wahrscheinlichkeit einer Katastrophe ist indes gering (siehe «Staumauern»).

**5. Chemische Industrie Lonza**: Das Industrieareal liegt in einem Erdbebengebiet direkt an der Rhone. Die Firma hat mittlerweile viele ihrer Gebäude erdbebensicher saniert.

**6. Basel**: Mit einer überdurchschnittlichen Erdbebenhäufigkeit, vielen Chemiebetrieben in der Region und der Nähe zu einem Flughafen und drei AKW ist die Zahl der Risiken in Basel gross.

**7. Sihlsee**: Würde der 1937 fertiggestellte Staudamm brechen, würde das Sihltal überflutet, und Teile der Stadt Zürich stünden bis zu acht Meter tief unter Wasser.

**AKW**

Die Schweizer Atomkraftwerke sind nicht so sicher, wie lange angenommen wurde. Eine 2007 veröffentlichte Studie namens «Pegasos» kam zum Schluss, dass die Meiler nicht genügend gegen starke Erdbeben gesichert sind. Das Eidgenössische Nuklearsicherheitsinspektorat (ENSI) ordnete daher an, dass alle AKW neu überprüft und nachgerüstet werden müssen. Diese Arbeiten sind derzeit im Gang.

**Staumauern**

In der Schweiz stehen über 1000 Staumauern, von denen rund 200 über fünf Meter hoch sind. Experten kamen vor einigen Jahren zum Schluss, dass die Mehrzahl dieser Bauten bezüglich Erdbebensicherheit nach veralteten Methoden überprüft wurde. Eine Neuprüfung läuft derzeit und soll bis 2013 abgeschlossen sein. Dass bei einem Erdbeben eine ganze Mauer einstürzt, ist allerdings unwahrscheinlich. Am ehesten möglich wären Risse, durch die grössere Mengen Wasser austreten könnten. Ein Alarmsystem ist nur bei 66 Anlagen installiert.

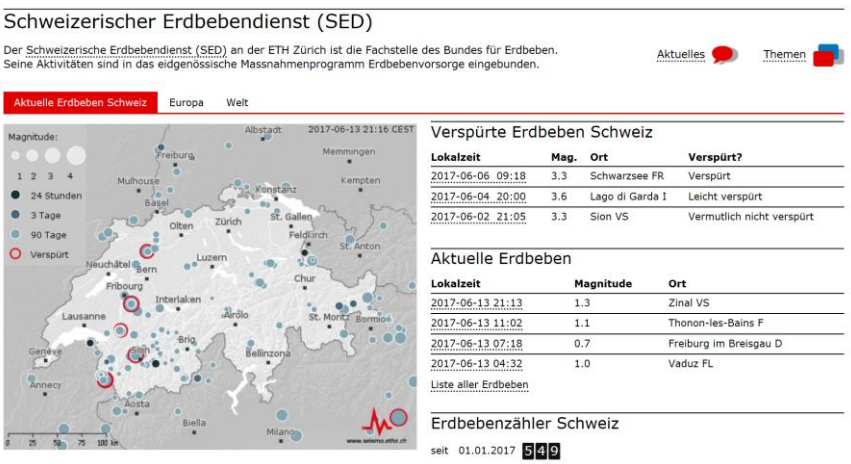
**Chemische Industrie**

Insgesamt 258 chemische Betriebe und Tanklager weisen in der Schweiz ein höheres Unfallpotential auf. Das bedeutet, dass bei einem Unfall mit über zehn Toten und/oder einer schweren Schädigung der Umwelt zu rechnen wäre. Ein solcher Ernstfall trat 1986 mit dem Grossbrand von Schweizerhalle ein. Die Betriebe sind heute verpflichtet, die Risiken zu ermitteln und alle geeigneten Massnahmen zur Vermeidung von Unfällen zu treffen

**Hochwasserzonen**

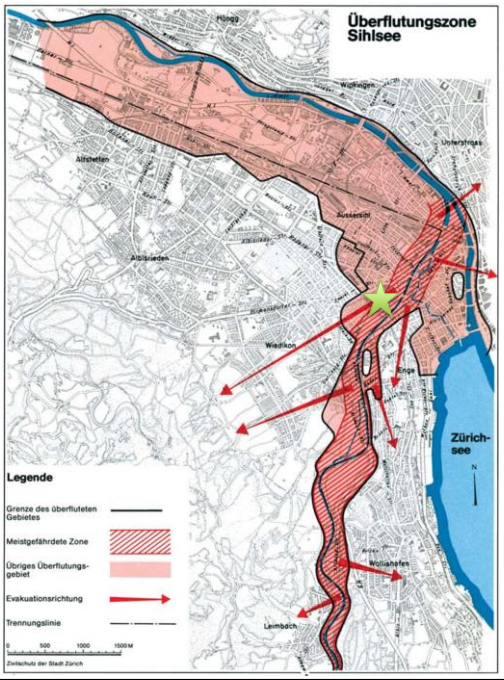
Die massiven Überschwemmungen vom August 2005 haben gezeigt, dass viele Flüsse nach tage- oder wochenlangen Niederschlägen über die Ufer treten. Die Kantone erstellen derzeit detaillierte Gefahrenkarten; viele Kantone lassen sich allerdings erstaunlich viel Zeit damit. Auch mehrere grosse Hochwasserschutzprojekte sind zurzeit im Gang, so an der Rhone, der Thur und der Linth.

# Höhere Gewalt



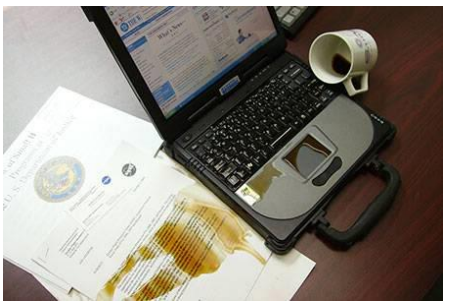

http://www.seismo.ethz.ch/de/home/

# Höhere Gewalt



# Technik

- Auch die beste Technik kann ihren Dienst versagen …



**Die IT-Sicherheit erhöhen lassen sich mit folgenden technischen Massnahmen:**

- Installation von Virenschutzprogrammen auf jedem Computer
- Regelmässige (tägliche) Backups aller Daten
- Erstellen von Logdateien (sogenannte „Logfiles“) zur Nachbearbeitung von IT-Vorfällen
- Arbeiten nach dem Prinzip des „least privilege“Segmentierung von IT-Netzwerken
- Verwendung von Spam-Filter
- Sicherstellen, dass E-Mail Anhänge mit unüblichen oder nicht benötigten Dateiendungen wie *.exe, .cpl, .bat, .com, .scr, .vbs, .vba* abgewiesen werden.
- Installation von Firewalls auf allen Computern
- Eindeutige Authentisierung von Remote-Zugänge (z.B. RAS, VPN)Verschlüsselung von wichtigen Daten bei Nutzung von Clouddiensten und auf mobilen Geräten
- Grundsätzlich ist Vorsicht geboten bei Verwendung von Cloud-Diensten
- Bei Webauftritt sollten Content Management Systeme (CMS) stets auf dem aktuellsten Stand sein.
- Automatisches Einspielen von Sicherheitsupdates (Aktivierung von Automatischen Updates) auf sämtlichen Computern und Servern des Netzwerk (veraltete Software gilt oft als Einfallstor für Schadsoftware).

Siehe auch: Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes
https://www.edoeb.admin.ch/datenschutz/00628/00629/00636/index.html?lang=de

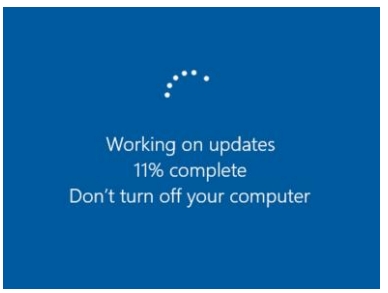
Siehe auch «**IT-Sicherheit: Sicherer kommunizieren»**
https://www.kalaidos-fh.ch/de-CH/Blogs/Posts/2014/08/it-sicherheit-sicherer-kommunizieren-teil-12
https://www.kalaidos-fh.ch/de-CH/Blogs/Posts/2014/09/it-sicherer-kommunizieren-teil-22

# Technik

- Eigene Infrastruktur schützen
  - Vor Diebstahl
  - Vor unberechtigtem Zugriff
  - Vor Schäden (Wasser, Feuer, …)
  - Vor Ausfall

## Technischer Schutz

- Systeme aktuell halten
  - *«Nur ein aktuelles System ist ein sicheres System»*




https://sentinel-it.de/10-gute-gruende-fuer-regelmaessige-windows-updates/

**Warum regelmäßige Windows Updates unerlässlich sind**
Die automatische Aktualisierung der Software ist ein wichtiger Bestandteil von guter, professioneller IT-Sicherheit und schließt wichtige Sicherheitslücken in Ihrem System. Nachfolgend werden im Detail Vorteile aufgezeigt, die regelmäßige Windows-Updates mit sich bringen und somit Ihre IT-Infrastruktur sicherer machen.

**Bekannte Sicherheitslücken werden geschlossen**
Die aktuellen Versionen von Virenschutzprogrammen und anderer Software kümmern sich darum, dass bekannte Sicherheitslücken geschlossen werden. Sobald eine Hintertür im System auffällt, wird ein Update vorbereitet und eingespielt, um genau dieses Loch in der Sicherheit auszubessern. Die Folge: Hacker und Viren haben es weniger leicht, in Ihr System zu kommen.

**Offene Lücken im System bringen Probleme**
Aber warum sollten diese Sicherheitslücken überhaupt so schnell wie möglich gefixt werden? Ganz einfach: Sobald eine Lücke bekannt wird, kann sie schon lange ausgenutzt worden sein. Gerade für Viren ist so ein Hintertürchen geradezu eine

Einladung – und da viele Programme direkt mit dem Internet verbunden sind, finden die Viren Sie fast schon automatisch. Und Viren wiederum bringen eine breite Palette von “Krankheiten” in der IT-Sicherheit mit sich.

**Vorsicht, Datenverlust!**
Wenn Sie einen Virus erwischt haben, der einfach nur Schaden anrichten will, kann das schnell mit Datenverlust einhergehen – entweder, weil Sie Ihr System komplett neu aufsetzen müssen, um den PC-Schädling wieder loszuwerden oder weil der Virus von sich aus Daten in Ihrem Netzwerk angreift. Mit einem Backup können Sie zwar Schlimmeres verhindern, aber dennoch besteht die Gefahr von Datenverlust.

**Trojaner spionieren Betriebsgeheimnisse aus**
Nicht jeder Virus ist laut und sofort offensichtlich. Trojaner sind fast noch gefährlicher für die IT-Sicherheit. Denn diese Schadprogramme spionieren Sie still und heimlich aus – und niemand weiß, wo genau die sensiblen Daten dann landen können. Mit regelmäßigen Updates kann das Eindringen der Trojaner verhindert werden und sie können im Notfall schneller aufgespürt werden.

**Jedes Programm zählt!**
Nicht nur das eigentliche Virenschutzprogramm muss regelmäßig geupdatet werden, um sich gegen die neuesten Techniken der Hacker zu wappnen. Auch scheinbar harmlose Programme wie die Textverarbeitungssoftware, das Mailprogramm oder der Grafiktreiber können angegriffen werden, wenn sie eine Sicherheitslücke aufweisen. Auch hier schützen Updates die eigenen Daten – oder wollen Sie, dass jemand Ihre Geschäftsmails mitliest?

**Imageverlust durch Datenklau**
Besonders für Onlineshop-Betreiber eine pikante Situation: Irgendwie sind die Daten aus dem Shopsystem in die Hände von Hackern und Datenkraken geraten – Name, Adresse, Mail oder sogar Bankverbindung der Kunden sind durch ein Sicherheitsloch im Shopsystem geflossen. Das kann nicht nur teuer werden, sondern sorgt nicht gerade für ein gutes Image und vergrault viele Kunden – zu Recht.

**Kleiner Patch, große Wirkung**
Gute Nachrichten: Eine aktuell gehaltene Antivirensoftware und die regelmäßigen Updates des Betriebssystems schließen bereits 90 Prozent aller Sicherheitslücke im System. Wer dann noch auf verschlüsselte E-Mails setzt, kann sich eigentlich schon mit einem guten Gewissen zurücklehnen. Wir gehen noch einen Schritt weiter und schützen auch Ihren Server und Ihre Cloud.

**Sicher in der Cloud**
Sicherheit in der Cloud ist ein aktuelles Thema. Bisher sind nur sehr selten Angriffe auf das lokale Netzwerk via Cloud Services bekannt geworden – schließlich sind das lokale Netzwerk und die Cloud idealerweise voneinander getrennt, beispielsweise durch eine DMZ im Firewall betrieb. Deswegen kann die virtuelle Umgebung für Backups genutzt werden und die IT-Sicherheit ergänzen und stärken. Und auch die

eigenen Daten, die auf einem externen Server liegen, sind meist besser und professioneller geschützt als die Daten im kleinen Unternehmensnetz.

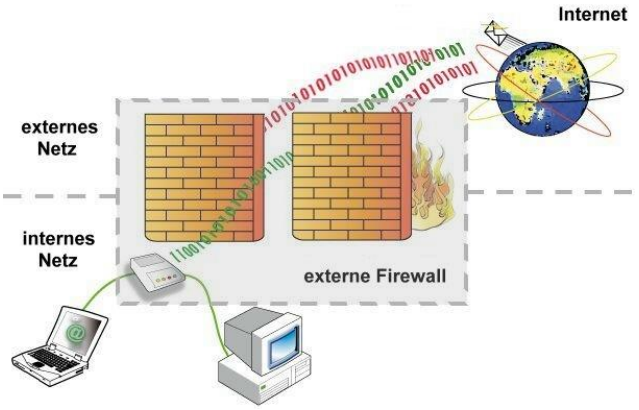
**10 Minuten Update vs. 10 Stunden Betriebsausfall**
Klar, gerade im Workflow können Updates nerven. Pop-Ups stören die Konzentration, nach dem Download soll der PC neu gestartet werden und auch das Installieren dauert seine Zeit. Aber diese 10 Minuten Zwangspause verhindern vielleicht einen mehrstündigen Netzwerkausfall – und schon lohnen sie sich wieder. Wer eine eigene IT-Abteilung hat, der kann überlegen, am Wochenende Updates zu installieren oder die Patches außerhalb der Stoßzeiten im Büro aufzuspielen.

**Die Abwehr steht – das gute Gefühl bei mehr Sicherheit**
Zu guter Letzt ist es einfach ein gutes Gefühl, sich kurz um die IT-Sicherheit gekümmert zu haben. Gerade kleine Betriebe oder KMU können mit wenig Aufwand ein sichereres Gefühl und ECHTE Sicherheit gewinnen. Regelmäßige Updates schützen im Betriebsalltag vor Angriffen und machen Ihr Netzwerk fit für die Zukunft.

**Fazit: Wenig Aufwand, große Wirkung**
Das Patchmanagement im Unternehmen sollte nicht vernachlässigt werden. Ideal ist dabei eine professionelle, zentralisierte Lösung für das Updatemanagement. Denn so laufen alle Fäden in einer Hand zusammen und kleine Sicherheitslücken werden sofort geschlossen. Wer sich dabei in die Hände eines professionellen Dienstleisters begibt, der kann die Sicherheit der Systeme zentral regeln und die Durchführung zu überwachen lassen – ohne sich selbst um das Thema kümmern zu müssen. So haben sie mehr Zeit für Ihr eigentliches Geschäftsfeld.. Wir stehen gerne an Ihrer Seit

# Technischer Schutz

- Internes Netzwerk mit einer Firewall sichern



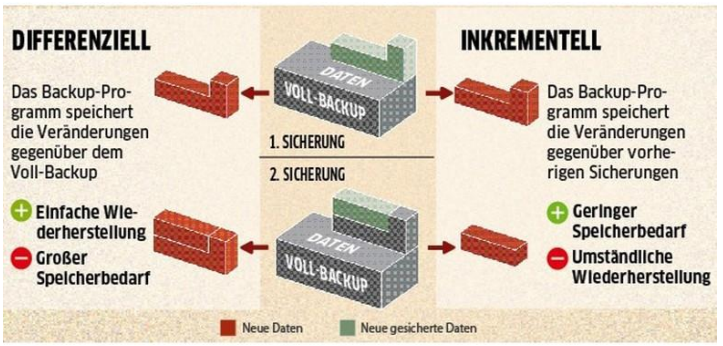

Eine **Firewall** ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Weiter gefasst ist eine Firewall auch ein Teilaspekt eines Sicherheitskonzepts.

Jedes Firewall-Sicherungssystem basiert auf einer Softwarekomponente. Die Firewall-Software dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender oder Ziel und genutzten Diensten. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden.
Abhängig davon, wo die Firewall-Software installiert ist, wird unterschieden zwischen einer Personal Firewall (auch Desktop Firewall) und einer externen Firewall (auch Netzwerk- oder Hardware-Firewall genannt). In Abgrenzung zur Personal Firewall arbeitet die Software einer externen Firewall nicht auf dem zu schützenden System selbst, sondern auf einem separaten Gerät, das Netzwerke oder Netzsegmente miteinander verbindet und dank der Firewall-Software gleichzeitig den Zugriff zwischen den Netzen beschränkt. In diesem Fall kann „Firewall“ auch als Bezeichnung für das Gesamtsystem stehen (ein Gerät mit der beschriebenen Funktion). Bauartbedingt gibt es grosse konzeptionelle Unterschiede zwischen den beiden Arten.
Die Funktion einer Firewall besteht nicht darin, Angriffe zu erkennen. Sie soll ausschliesslich Regeln für die Netzwerkkommunikation umsetzen. Für das Aufspüren von Angriffen sind sogenannte IDS-Module zuständig, die durchaus auf einer Firewall aufsetzen und Bestandteil des Produkts sein können. Sie gehören jedoch nicht zum Firewall-Modul.

Siehe: https://de.wikipedia.org/wiki/Firewall

# Technischer Schutz

- Backup-Art




https://de.wikipedia.org/wiki/Datensicherung

**Umsetzung**
Die Aufbewahrung von Datensicherungen sollte örtlich entfernt von der EDV-Anlage und in einer sicheren Umgebung erfolgen. Das Herstellen der Datensicherung kann zusätzlich auf einem anderen Typ von Medium erfolgen, um typische technische Risiken zu mindern.

- Für Privatpersonen bieten sich externe Festplatten mit FireWire, eSATA oder USB-Anschluss an. Diese lassen sich unkompliziert an das zu sichernde System anschließen und wieder von diesem trennen und ermöglichen so zumindest eine entfernte Aufbewahrung. Auch netzwerkbasierende Festplatten (NAS) und Wechselplatten sind einfach anzuschließen und zu entfernen, wodurch sinnvolle Sicherungen möglich sind.
- Für kleinere Unternehmen eignen sich z. B. Bankschließfächer zur Datenträgeraufbewahrung. Allerdings kann in der Regel nicht zu jeder Zeit darauf zugegriffen werden, da der Zugang zu den Datenträgern nur während der Öffnungszeiten der Bank möglich ist. Eine Alternative dazu stellt die Online-Datensicherung dar: die Datensicherung erfolgt außer Haus, meist in einem Rechenzentrum, und es kann jederzeit darauf zugegriffen werden. In diesem Fall ist aber darauf zu achten, dass der Datentransfer in gesicherter Art und Weise erfolgt; auch der externe Dienstleister sollte die Inhalte nicht lesen können.

- Für größere Unternehmen können sich speziell gesicherte Safes oder Räumlichkeiten (sog. Zellen) zur feuersicheren Unterbringung der Tape-Library lohnen. Auch können die gesicherten Daten auf mehrere Standorte oder Rechenzentren verteilt werden.

**Sicherungsarten**
Je nach Veränderungsintensität der zu sichernden Daten können beim konkreten Sicherungsvorgang bestimmte Sicherungsarten eingesetzt werden. Einzelne Sicherungsvorgänge können in Volldatensicherung, differenzieller und inkrementeller Sicherung unterschieden werden. Differenzielle und inkrementelle Sicherung setzen mindestens eine erfolgte Volldatensicherung voraus. Bei der normalen Datensicherung werden bestimmte Dateien und/oder Verzeichnisse (Ordner) ausgewählt, deren Inhalt gesichert werden soll. Es besteht auch die Möglichkeit, nur bestimmte Dateiformate zu sichern. Daneben lassen sich auch ganze Datenträger oder Partitionen daraus als Abbild sichern. In allen Fällen ist es möglich, auch lediglich Teile aus einem vollständigen Sicherungssatz wiederherzustellen.

Es wird unterschieden in:

**Komplett-/Vollsicherung**
Die Komplett- oder Vollsicherung wird in Programmen auch als „Normale Sicherung“ bezeichnet. Hierbei werden die jeweils zu sichernden Daten (ein komplettes Laufwerk, eine Partition, bestimmte Verzeichnisse und/oder bestimmte Dateien, bestimmte Dateiformate) komplett auf das Sicherungsmedium übertragen und als gesichert markiert.
Als Vorteil gilt, dass die Vollsicherung technisch sehr einfach ist – reines Kopieren der Daten reicht, und eigene Backup-Programme zu schreiben gestaltet sich leicht. Nachteilig ist der sehr hohe Speicherbedarf.

**Speicherabbildsicherung**
Bei der Speicherabbild-Sicherung (englisch image backup) kann der komplette Datenträger (meist die Festplatte, aber auch USB-Massenspeicher, optische Medien oder bei einigen Programmen auch Datenträger im Netzwerk) oder nur eine Partition durch ein 1-zu-1-Abbild gesichert werden. So können beispielsweise nicht nur die Nutzdaten, sondern das gesamte Dateisystem, inklusive Betriebssystem und Benutzereinstellungen, gespeichert werden. Der Vorteil dieser Sicherung besteht darin, dass bei einem Totalausfall des Rechners das Speicherabbild auf den Datenträger zurückgeschrieben und dadurch der Zustand der jeweiligen Datenträger zum Sicherungszeitpunkt vollständig wiederhergestellt werden kann. Bei einer derartigen Wiederherstellung wird entweder das gesamte Dateisystem in seiner Originalstruktur wiederhergestellt (in diesem Fall ist kein Dateisystemtreiber erforderlich, sondern lediglich ein Gerätetreiber für den Datenträgerzugriff), oder ein besonderer Treiber liest regulär das Dateisystem und extrahiert nur die gewünschten Verzeichnisse und Dateien aus der Sicherung, um diese als normale Verzeichnisse und Dateien in das aktuelle Dateisystem zu integrieren bzw. die aktuellen mit den

älteren gesicherten zu überschreiben (siehe auch „Inkrementelle Sicherung“). Seit einigen Jahren sind auch Programme auf dem Markt, die solche Sicherungen ebenfalls inkrementell anlegen können.

**Differenzielle Sicherung**
Bei der sogenannten differenziellen Sicherung werden alle Dateien, die seit der letzten Komplettsicherung geändert wurden oder neu hinzugekommen sind, gespeichert. Es wird also immer wieder auf der letzten Komplettsicherung aufgesetzt, wobei gegenüber einer neuen Vollsicherung Speicherplatz und Zeit gespart werden kann. Wenn eine Datei geändert wurde, wird die jeweilige Version der Datei bei jedem differenziellen Lauf gesichert.
Vorteilig ist der deutlich reduzierte Speicherbedarf, und dass die derzeit aktuelle Datensicherung nur einen Schritt von der letzten Vollsicherung entfernt ist. Die Programmierung der Backup-Software kann relativ simpel sein. Ebenfalls von Vorteil ist, dass nicht mehr benötigte Sicherungsstände unabhängig voneinander gelöscht werden können, während inkrementelle Sicherungen zwangsläufig miteinander verkettet sind. Bei sehr großen Dateien, die sich häufig ändern (virtuelle Maschinen, Datenbanken, Postfach-Dateien mancher E-Mail-Programme) ist die differenzielle Sicherung jedoch nachteilig; die differenzielle Sicherung sichert trotz nur kleiner Änderungen die ganze Datei nochmals.

**Inkrementelle Sicherung**
Bei der inkrementellen Sicherung werden immer nur die Dateien oder Teile von Dateien gespeichert, die seit der letzten inkrementellen Sicherung oder (im Falle der ersten inkrementellen Sicherung) seit der letzten Komplettsicherung geändert wurden oder neu hinzugekommen sind. Es wird also immer auf der letzten inkrementellen Sicherung aufgesetzt. Dieses Verfahren hat den Nachteil, dass bei einer Wiederherstellung die Daten in der Regel aus mehreren Sicherungen wieder zusammengesucht werden müssen. Mittels verschiedener Techniken (Datumsstempel, Prüfsummen) muss gewährleistet sein, dass die vollständige Kette (Vollsicherung – inkrementelle Sicherungen 1, 2, 3 usw. – Originaldaten) fehlerfrei nachvollziehbar ist.

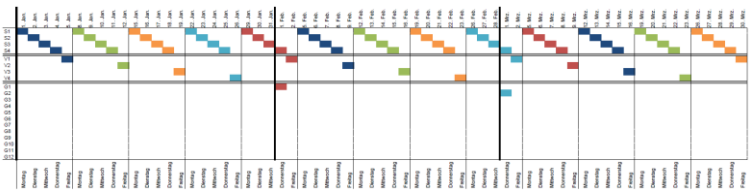
Zu beachten ist, dass die Inkremente auf zwei Weisen gespeichert werden können:
- Üblich sind die forward deltas. Dies entspricht dem oben beschriebenen Fall: Die (ältere) Vollsicherung dient als Fundament und wird nicht verändert, während darauf die Inkremente aufgebaut werden. Der aktuelle Datenbestand kann nur unter Berücksichtigung von Inkrementen wiederhergestellt werden. Beispiele: duplicity.
- Eine inkrementelle Sicherung mit reverse deltas kehrt dieses Prinzip um. Man stelle sich die Kante eines Daches vor, von der Eiszapfen herunterwachsen. Die Vollsicherung verändert sich bei jeder Datensicherung und stellt hier die Dachkante dar. Die anwachsenden Eiszapfen sind die Inkremente. Hat sich eine Datei gegenüber der letzten Vollsicherung verändert, wird die vorherige Dateiversion als Inkrement gespeichert – der Eiszapfen wächst nach unten – während die derzeit aktuelle Version in die Vollsicherung eingefügt wird. Auf die

Vollsicherung kann jederzeit problemlos zugegriffen werden, während eine ältere Version einer Datei nur durch Berücksichtigung der Inkremente wiederhergestellt werden kann. Beispiel: rdiff-backup.

- Vorteil der inkrementellen Sicherung ist der sehr geringe Speicherbedarf; das Verfahren eignet sich daher für die Datensicherung in Netzwerken oder in der Cloud. Andererseits sind prinzipbedingt alle Inkremente miteinander verkettet, weshalb es nur mit sehr großem Rechenaufwand möglich ist, ein Inkrement zwischen zwei anderen Inkrementen zu entfernen, etwa um Speicherplatz zu sparen oder private Daten zu löschen.

# Technischer Schutz

- Backup-Konzept



Es gibt verschiedene Arten, wie ein regelmässiges Backup geplant und sichergestellt werden kann.

Das BSI hat einen Umsetzungshinweis zum Datensicherungskonzept erarbeitet unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/CON/Umsetzungshinweise_zum_Baustein_CON_3_Datensicherungskonzept.html, welches als gute Grundlage dienen kann.

Grundsätzlich ist aber auf jede Organisation spezifisch zu definieren, wann und was in welcher Form gesichert werden soll. Als Grundformel gilt aber:

- Neu erstellte und geänderte Daten täglich sichern mit einer Verwahrdauer von 30 Tagen.
- Wöchentlich eine Komplett-Sicherung aller Daten. Das Sicherungsmedium an einem zweiten Standort min. 1 Monat aufbewahren (also jede Woche ein neues Medium verwenden)
- Vielfalch wird zudem auch einmal pro Monat und einmal pro Jahr eine zusätzliche Gesamtsicherung erstellt und das Medium an einen dritten Standort gelagert.

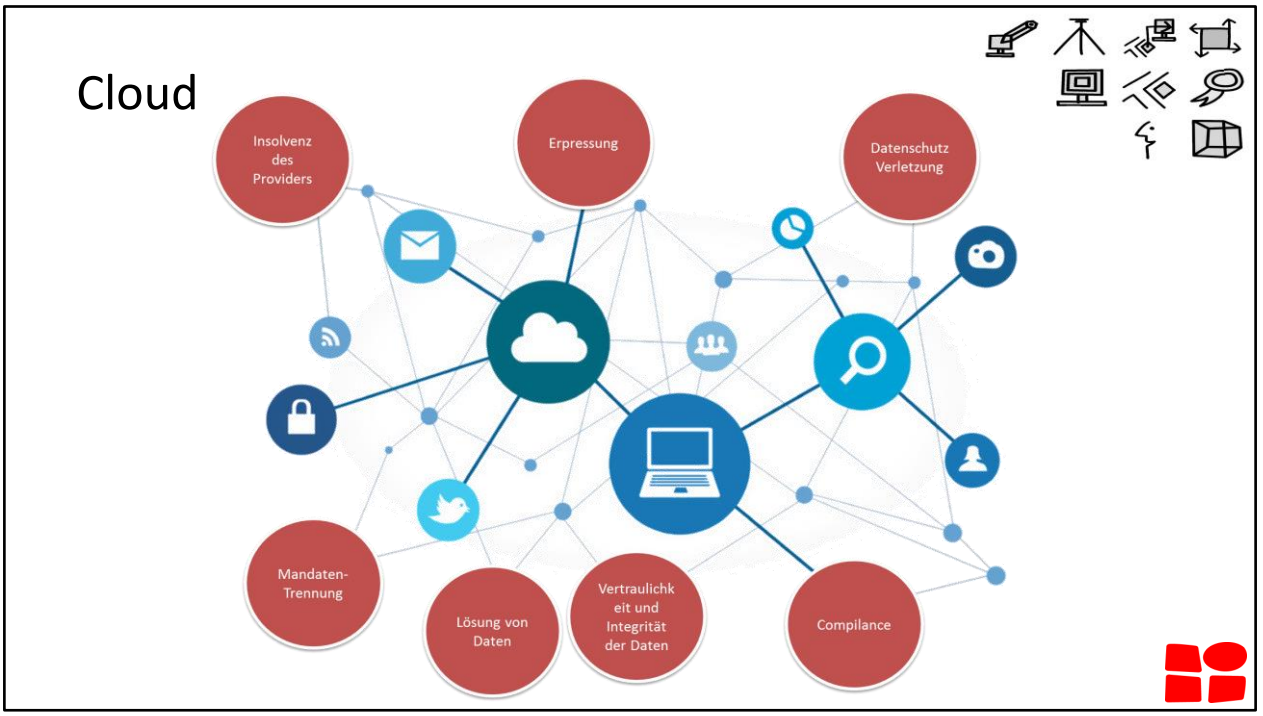
Wichtig zu bedenken sind neben den ‘normalen’ Office-Dateien auch Datenbanken, wo es je nach Art und Verwendungszweck der Datenbank weitergehende, komplexere Sicherungsprozesse braucht, damit die Business-Kontinuität sichergestellt wird.

# Technischer Schutz

- Virenschutz
  - Anforderungen
    - Immer aktuell (wenn möglich automatisch aktualisiert) und nicht durch den Benutzer deaktivierbar
    - Alle sich im Netzwerk befindlichen Geräte (auch Mobile) müssen geschützt sein


avast AVG Bitdefender
KASPERSKY eset F-Secure
McAfee Microsoft Symantec

Es gibt eine sehr grosse Anzahl an Anti-Viren-Software. Im Prinzip spielt es nicht in erster Linie eine Rolle, was für eine Software eingesetzt wird. Es sollte nicht zwingend der günstigste gewählt werden aber sicher auch nicht der teuerste Anbieter.




**Herausforderung Cloud**
Nun werden Daten — auch Firmendaten — zunehmend online produziert, geteilt, gespeichert und bearbeitet. Zum Beispiel mit Cloud-Lösungen oder Online-Versionen von Text- und Kalkulationssoftware. Oder in Tweets, Kurznachrichten, auf Foto- und Grafikservern. Diese Daten lassen sich durch Ihre Firma nicht mehr im Sinne einer absoluten Datenhoheit kontrollieren. Es werden die Angebote von Drittkonzernen genutzt, die, so schreiben die meisten in ihren Nutzungsbedingungen, sozusagen als Bezahlung für die Nutzung ihres Angebotes, einen Teil der Datenhoheit übernehmen.

Indem Sie diese Dienste nutzen, geben Sie Ihre Rechte an den Daten und damit die Datenhoheit zumindest teilweise ab. Ausserdem können Sie auch die Datennachhaltigkeit nicht gewährleisten: Sie können die Daten in der Cloud nicht mehr löschen und auch nicht exportieren bzw. auf einen anderen Betreiber übertragen.

Seit den Enthüllungen Snowdens wissen wir zudem, dass US-Firmen der NSA Zugriff auf alle Kundendaten gewähren müssen — ohne die Kunden zu informieren.

**Der Ort spielt eine Rolle**
Wichtig zu wissen ist ausserdem, dass für die Daten diejenige Gesetzgebung gilt, die für den Ort gilt, an dem die Daten physisch gespeichert sind. Wenn also Ihre Daten zum Beispiel auf einem Server eines Cloud-Anbieters in den USA gespeichert sind, dann gelten für diese Daten ausschliesslich die Gesetze der USA. Und dort sind z. B. die Regelungen zum Urheberrecht fundamental verschieden von den entsprechenden Regelungen in der Schweiz oder in Deutschland. Im amerikanischen Recht liegt beispielsweise das geistige Eigentum einer Idee in der Regel beim Verlag oder Vertrieb und nicht wie in der Schweiz beim Autor. Der Verlag oder Vertrieb ist bei einer Cloud-Lösung sinngemäss der Betreiber der Cloud! In der Schweizer Gesetzgebung (OR) ist vorgeschrieben, dass Firmen ihre Kommunikation vor unbefugtem Zugriff sichern und die Daten 10 Jahre aufbewahren sollen. Können diese Anforderungen mit einer nicht selbst betriebenen Cloud-Lösung wirklich erfüllt werden?

**1. Standort**
Wählen Sie Ihren Provider sorgfältig aus, denken Sie daran, dass die Gesetze des Standorts für den Umgang mit Ihren Daten relevant sind. Deshalb sollten Sie im Idealfall Ihre eigene Cloud in Ihren eigenen Räumen betreiben. Wenn das nicht möglich ist, sollten Sie einen Anbieter suchen, der sich juristisch möglichst in Ihrer Nähe bzw. in einem Land mit einer vergleichbaren Gesetzgebung befindet.
**2. Technologie**
Entscheiden Sie sich für Open Standard-Lösungen. Nur mit solchen können Sie kontrollieren, was mit ihren Daten geschieht. Da nur solche Lösungen transparent sind. Um die Kontrolle über Ihre Daten zu haben, müssen Sie genau nachvollziehen können, was die Lösungen, die Sie nutzen, mit Ihren Daten anstellen.
Achten Sie ausserdem darauf, offene Dateiformate einzusetzen. Nur dadurch können Sie die Exportfähigkeit und den verlustfreien Transport der Daten gewährleisten.
**3. Entwicklung**
Wählen Sie einen Anbieter, der seine Lösungen aktiv weiterentwickelt. Nur ständig weiterbearbeitete Lösungen können auf neue Herausforderungen im Bereich der IT-Sicherheit reagieren
**4. Backup**
Halten Sie immer einen Notfallplan bereit, um Datenverlust zu vermeiden. Das sollte im Idealfall eine lokale Kopie aller Daten in ihren eigenen Räumen sein. Achten Sie insbesondere auch darauf, dass Sie die gesicherten Daten in einem Notfall auch bearbeiten können (offenes Format)!
**5. Nutzungs-bedingungen**
Nicht zu vergessen:
Lesen Sie auf jeden Fall die Nutzungsbedingungen Ihrer Provider!
6. Verantwortungs-voller Umgang
Nebst diesen Tipps der wichtigste ist ein verantwortungsvoller Umgang mit den (Firmen-)Daten. Um die Datenhoheit zu behalten, sollten Sie sich an die folgenden Regeln halten:

> Nutzen Sie zum Erstellen und Bearbeiten von vertraulichen Daten (dazu zählen auch schützenswerte Ideen, geistiges Eigentum) keine öffentlichen Clouddienste!
> Die Datenverfügbarkeit können Sie nur in Ihrer eigenen Netzwerkumgebung kontrollieren. Seien Sie sich bewusst, dass Sie online verwaltete und gespeicherte Daten jederzeit verlieren können und dass Sie Ihre absoluten Rechte daran im Moment des Hochladens verlieren!

Quelle: http://www.computerwoche.de/a/ratgeber-it-sicherheit,2363872

Verletzung der Vertraulichkeit und Integrität der Daten:
Eine Lokalisierung der Daten ist in einer Public oder Hybrid Cloud für den Dateneigentümer nicht mehr einfach möglich. Daher ist der Schutz der Daten auf der Infrastruktur-, Plattform und Applikationsebene häufig nicht mehr mit üblichen Mitteln zu gewährleisten.

Löschung von Daten:
Daten müssen in vielen Fällen (etwa aufgrund gesetzlicher Bestimmungen) gelöscht werden. Auch hier besteht das Risiko einer nur unzureichenden oder unvollständigen Löschung auf allen Plattformen und Datenbanken der Cloud, da die Lokalisierung der Daten nur schwer möglich ist.

Ungenügende Mandantentrennung:
Bei nicht ausreichend abgesicherter Mandantentrennung besteht die Gefahr, dass Dritte unautorisiert Daten einsehen oder manipulieren können.

Verletzung der Compliance:
Da Daten in einer Public Cloud prinzipiell in allen Ländern der Welt in deren spezifischen Rechtsordnungen verarbeitet werden können, ist die Erfüllung aller gesetzlicher Anforderungen eine wesentliche Aufgabe bei der Nutzung von Public Cloud Leistungen.

Verletzung von Datenschutzgesetzen:
Es ist nicht von vornherein klar, in welchen Ländern, Rechenzentren, auf welchen Servern und mit welcher Software die Daten gespeichert und verarbeitet werden.

Insolvenz des Providers:
Die Insolvenz eines Providers bedeutet meist nicht die Insolvenz aller Rechenzentren, die der Provider verwendet hat. Rechenzentren werden zudem bei Insolvenz mit grosser Wahrscheinlichkeit an andere Provider verkauft werden.

Erpressungsversuche:
Die Gefahr von Erpressungsversuchen steigt, da der Personenkreis mit Administrationsaufgaben für Ressourcen der Public Cloud unüberschaubar gross ist. Das eingesetzte Personal verfügt im Allgemeinen über unterschiedliches Ausbildungsniveau und Sicherheitsbewusstsein.


**Lauschende Sprachassistenten sind ein Risiko**

Apple hat einen, Microsoft hat einen, Amazon und Google auch: Digitale Sprachassistenten verbreiten sich immer stärker und sollen Nutzern den Alltag erleichtern. Verbraucherschützer sind davon wenig begeistert. Die lauschenden Assistenten bergen ein Datenschutzrisiko.

Sie bestellt ein Taxi vor die Tür, dreht die Heizung hoch oder trägt Termine in den Kalender ein: "Alexa" ist der Sprachassistent von Amazon. Seit Montag können alle Amazon-Kunden auch in Deutschland den Assistenten in Form des Lautsprechers "Echo" und der kleineren Variante "Dot" kaufen, zuvor war das nur per Einladung möglich.

Echo kann auf Zuruf Aufgaben erledigen, etwa einen Wecker stellen, eine Einkaufsliste ergänzen, in Verbindung mit Amazon Prime Verbrauchsgegenstände bestellen oder Fragen mit Hilfe von Internet-Quellen beantworten.

Daten werden bei Amazon gespeichert

Was als Service am Kunden gedacht ist, birgt jedoch Risiken, warnt die Verbraucherzentrale Nordrhein-Westfalen. Denn alle Sprachbefehle, die ein Nutzer nach der Ansprache "Alexa" an den ständig auf sein Aktivierungskommando lauschenden Lautsprecher richtet, werden auf Amazon-Servern gespeichert und verarbeitet.

Außerdem speichert Amazon nicht nur die Sprachbefehle. Auch zum Beispiel Einkauflisten, Kalendereinträge oder Musikwünsche werden gesichert. Einige Fragen zur Weitergabe von Daten an Dritte seien außerdem unklar formuliert, kritisieren die Verbraucherschützer.

Amazon weist Kritik von sich

Amazon widerspricht diesen Befürchtungen weitgehend: Die Erhebung der Daten sei zur Nutzung und Verbesserung von "Alexa" nötig. Daten sollen nach Angaben eines Unternehmenssprechers auch nur dann weitergegeben werden, wenn dies für einen genutzten Dienst nötig sei: Etwa dann, wenn Nutzer über den Sprachassistenten ein Taxi bestellen und daraufhin das Taxiunternehmen verständigt wird. Daten deutscher Nutzer werden laut Amazon auf Servern in EU-Ländern gespeichert.

Kuriose Einkaufspannen durch Amazon Echo

Der Gebrauch von Echo und Dot kann aber auch andere unerwartete Folgen haben. Ein kurioser Fall aus den USA

zeigt, dass auch unfreiwillige Einkäufe über den Onlinehändler Amazon möglich sind. Ein Kind hatte sich dabei mit dem Sprachassistenten unterhalten und versehentlich ein Puppenhaus sowie zwei Kilogramm Kekse bestellt. Als ein Nachrichtensprecher des lokalen Senders "CW6 San Diego" über den Fall berichtete und im Fernsehen "Alexa ordered me a dollhouse" (zu Deutsch: "Alexa hat mir ein Puppenhaus bestellt") sagte, versuchten auch Heim-Assistenten einiger Zuschauer ein Puppenhaus zu bestellen.
Um solche Fälle zu verhindern, können Einkäufe über den Assistenten ganz gesperrt oder durch einen Zahlencode gesichert werden. Alternativ können die Mikrofone von Echo und Dot durch einen Knopf an der Oberseite des Lautsprechers von Hand ausgeschaltet werden. Statt mit dem üblichen blauen Licht leuchtet das Gerät dann rot.

Von: https://www.t-online.de/digital/computer/id_80374078/amazon-echo-dot-alexa-birgt-ein-risiko-verbraucherzentrale-warnt.html

## Mobile …


Das Thema Sicherheit in Hinblick auf die Nutzung eines Smartphones hat viele Facetten. Da gibt es zum einen die verschiedenen Sicherheitseinstellungen, die am Gerät selbst vorgenommen werden können. Zum anderen kann das Smartphone auch mittels Programmen, Apps, geschützt werden, die aus dem jeweiligen App-Store geladen werden können.

Quelle: http://www.klicksafe.de/themen/kommunizieren/smartphones/sicherheit-wie-schuetze-ich-das-smartphone/

# Mensch

- Die Unachtsamkeit der eigenen Mitarbeiter ist laut Schweizer IT-Abteilungsleitern das grösste Sicherheitsrisiko für die eigene Firma

**Oft ist das unvorsichtige Verhalten von Mitarbeitern das grösste IT-Risiko für Unternehmen.**

Wichtige Datenschätze einer Firma sind nicht nur durch externe Attacken gefährdet. Oft ist es das unvorsichtige Verhalten von Mitarbeitern, das Firmen für Datendiebstahl, Datenverlust oder andere Probleme anfällig macht. Viele Massnahmen gegen diese Bedrohung sind bekannt. So gehört es zum Standard, dass Passwörter regelmässig gewechselt werden, dass Mitarbeiter zum Thema - Datensicherheit geschult werden und dass sensible Daten verschlüsselt werden.
Dieses Standardprogramm ist aber in vielen Fällen nicht mehr wirksam. Denn Mitarbeiter nutzen zunehmend Cloud-Dienste im Büro, die sie nicht mit der eigenen IT-Abteilung abgesprochen haben. Auch private Geräte breiten sich im Büro aus. Die klassischen Sicherheitsmassnahmen der Firmen werden durch dieses Verhalten untergraben.

Quelle: http://www.handelszeitung.ch/management/mitarbeiter-sind-das-groesste-it-risiko-fuer-firmen-259883

# Passwörter

- **Unsicheres Passwort = KEIN Passwort**
- Problem Mensch
  - Passwort nicht aufschreiben
  - Passwort nicht weitergeben
  - Passwort regelmässig wechseln

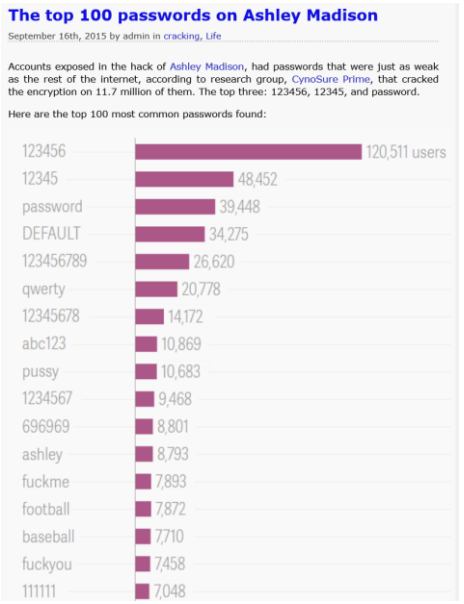
- Das sichere Passwort: v2Jfd€u6%

Passwort-Reminder:

**v**or **2** **J**ahren **f**iel **d**er *Euro* **u**m **6** *Prozent*

# Passwörter

- **Die 25 häufigsten Kennwörter:**
  1. password
  2. 123456
  3. 12345678
  4. 1234
  5. qwerty
  6. 12345
  7. dragon
  8. pussy
  9. baseball
  10. football
  11. letmein
  12. monkey
  13. 696969
  14. abc123
  15. mustang
  16. michael
  17. shadow
  18. master
  19. jennifer
  20. 111111
  21. 2000
  22. jordan
  23. superman
  24. harley
  25. 1234567



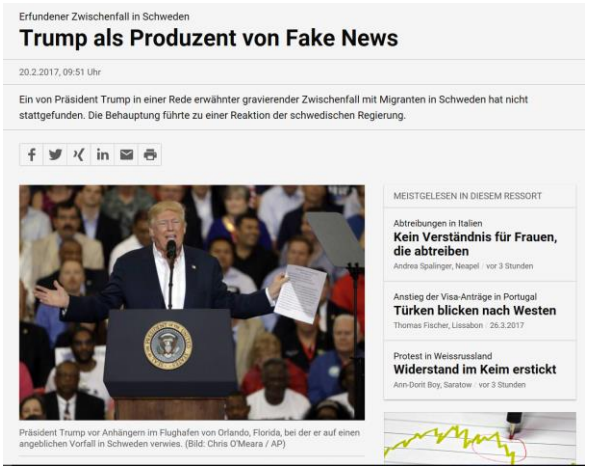
# Passwörter

- Sicherheitsfaktor komplexes Passwort

| Verwendete Zeichen | Anzahl Zeichen | Mögliche Passwörter | Entschlüsselt in |
|---|---|---|---|
| Nur Zahlen | 8 | 100000000 | 0.047 Sek. |
| Nur Zahlen | 15 | 1000000000000000 | 5.52 Tage |
| Kleinbuchstaben | 8 | 208827064576 | 1.66 Minuten |
| Kleinbuchstaben | 15 | 1.677259342285726e+21 | 25372.31 Tage |
| Gross/Kleinbuchstaben | 8 | 53459728531456 | 7.08 Stunden |
| Gross/Kleinbuchstaben | 15 | 5.496043412801867e+25 | 831399806.97 |

- Brute-Force-Attacken sind Versuche eines Computer-Programms, das Passwort eines anderen Programms zu knacken, indem alle möglichen Kombinationen von Buchstaben und Zahlen ausprobiert werden. Daher ist ersichtlich, dass die Länge eines Passworts massgeblich für die Sicherheit von Daten wichtig ist.

# Fake News




**Fake News: Wie sie wirken und wie man sie entlarvt**
Flüchtlinge urinieren gegen eine Kirche, Hillary Clinton leitet einen Kinderporno-Ring und es gehen Koran-CDs mit Gift um. Das sind Fake News - also Lügenmärchen, die gezielt verbreitet werden. Sie beeinflussen das gesellschaftliche Klima und können sich auf Wahlen auswirken. Auch für die kommende Bundestagswahl wird mit Fake News und Social Bots gerechnet.

http://www.ard.de/home/ard/Fakten_statt_Fake_News/3690810/index.html

Paul Horner, der bekannteste Fake News Macher der Welt
http://ch.galileo.tv/video/der-bekannteste-fake-news-macher-der-welt

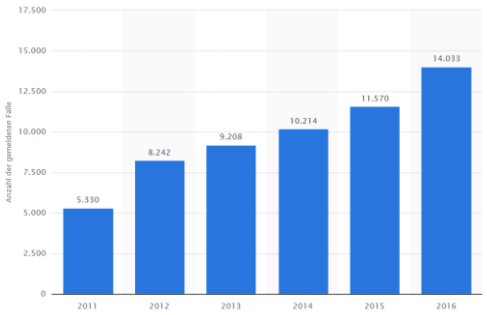
http://www.uncutnews.ch
http://alles-schallundrauch.blogspot.ch/

# Fake News


**Russische Hacker stehen laut FBI hinter Katar-Krise**
Russische Hacker haben offenbar eine Fake-News-Geschichte bei der staatlichen Nachrichtenagentur Katars platziert, die Saudi-Arabien und andere Staaten zum Abbruch der diplomatischen Beziehungen mit Katar veranlasst habe.

# Cybercrime und Spionage

**Anzahl der gemeldeten Fälle von Cyberkriminalität in der Schweiz von 2011 bis 2016** PREMIUM




**INFORMATIONEN ZUR STATISTIK**

Die Statistik zeigt die Anzahl der gemeldeten Fälle* von Cyberkriminalität in der Schweiz von 2011 bis 2016. Im Jahr 2011 wurden in der Schweiz 5.330 Verdachtsfälle von Cyberkriminalität an die zuständigen Behörden gemeldet.


**Statistiken zum Jahresbericht fedpol 2016; Kriminalpolizeiliche Aufgaben**
https://www.ejpd.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/jabe/jabe-2016-stat-d.pdf

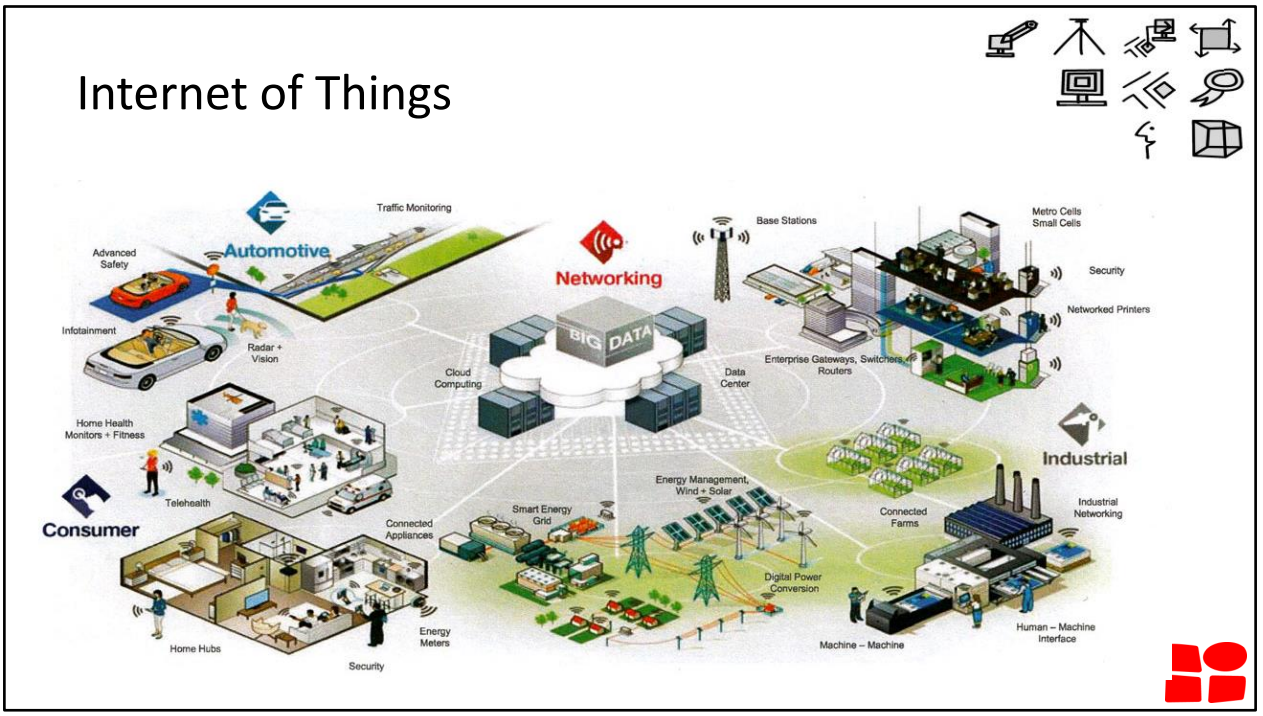
**Anzahl der gemeldeten Fälle von Cyberkriminalität in der Schweiz von 2011 bis 2016**
https://de.statista.com/statistik/daten/studie/294565/umfrage/gemeldete-faelle-von-internetkriminalitaet-in-der-schweiz/

## Social Engineering

- Die Betrüger manipulieren ihre Opfer im (direkten) zwischenmenschlichen Kontakt.
- 90 % Erfolgsquote
- Beispiele:
  - September 2016: «Vor kurzem wurde in Kalkutta ein Callcenter ausgehoben, in dem 250 vermeintliche Microsoft-Mitarbeiter Anrufe in alle Welt tätigten, um sich Zugang zu den PC nichts ahnender Opfer zu verschaffen.»
  - 'Enkel-Trick' …

**Definition Social Engineering**
Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.
Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Häufig dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking.

**Für solche Angriffe braucht es null IT-Kenntnisse**
http://www.tagesanzeiger.ch/digital/internet/Fuer-solche-Angriffe-braucht-es-null-ITKenntnisse/story/12030494




- Der Kühlschrank, der selbstständig Milch nachbestellt, bevor diese aus ist.
- Das Auto, das selbst zur Arbeit fährt.
- Die Smartwatch, die der Krankenkasse meldet, wenn wir uns nicht genug bewegen.
- Der Parkplatz, der das geparkte Auto kennt und aufgrund der Belegungsdauer automatisch die Gebühren von der Handyrechnung abbucht.

Zukunftsmusik? Nein – was vor wenigen Jahren noch als Science Fiction abgetan wurde, hat uns schon lange eingeholt. Viele der Innovationen erleichtern vordergründig unser aller Alltag erheblich. Denn wer träumt nicht davon, in der eigenen Garage ins eigene Auto einzusteigen und während der Fahrt noch die Zeitung in Ruhe zu lesen und dabei Kaffee und Gipfeli zu geniessen, um dann erholt im Büro den Arbeitstag starten zu können.

Die Schattenseite dieser Entwicklung ist, dass wir immer (noch) mehr digitale Spuren hinterlassen. Auch wenn wir in vielen Bereich schon längst, teilweise ohne uns dessen wirklich bewusst zu sein, zum gläsernen Menschen geworden sind, werden mit all den Neuerungen Tür und Tor geöffnet, um auch das letzte bisschen Privatsphäre zu verlieren. Wir werden dadurch immer angreifbarer – mit der Vorstellung, dass unser Smart-Home plötzlich gegen uns verwendet werden kann, nimmt der Cyberwar plötzlich Einzug in unser Wohnzimmer. Wenn wir uns der Gefahren nicht bewusst sind und die entsprechenden Vorkehrungen treffen (bzw. die Systeme dies auch wirklich zulassen), dann finden wir uns im schlimmsten Fall plötzlich in einem bisher nur aus Hollywood-Filmen bekannten Szenario wieder, in welchem wir von einem Hacker erpresst werden, in dem er uns einfach nicht mehr aus dem Haus lässt, uns das Wasser abstellt oder mitten in der Nacht mit lauter Musik und flackerndem Licht foltert.

Mit der rasanten Zunahme von ‘smarten’ Alltagsgegenständen wird das Thema (IT-)Sicherheit zum Thema für jedermann. Es wird künftig nur noch ganz wenige Bereiche des täglichen Lebens geben, welche ohne IT auskommen und so ist es im Interesse jedes einzelnen, sich den Gefahren bewusst zu sein und sich entsprechend zu verhalten.

## Sicherheit zu Hause und unterwegs

- Risiken
  - Internet-Anschluss
  - PC
  - Handy
  - TV
  - Telefon
  - Auto
  - Ferien, z.B. beim Fliegen …

Grundsätzlich gelten für die private Nutzung von Kommunikationsmitteln die gleichen Überlegungen wie sie auch geschäftlich vorgegeben sind (bzw. sein sollten). Auch die privaten Daten (als Beispiel die Kontoinformationen, Reiseunterlagen, …) können in falschen Händen missbraucht werden.

Aber auch bei der Nutzung von Auto, Bus oder Zug verlassen wir uns immer stärker auf die modernen Technologien und da diese immer ‘nomaler’ in unserem Alltag Ihren Platz einnehmen, gehen wir immer selbstverständlicher damit um und machen uns meist wenig Gedanken, dass wir der Technik vielfach völlig ausgeliefert sind – das beste Beispiel ist hier die Nutzung des Fliegers in den nächsten Urlaub.

# Sicherheit zu Hause und unterwegs

- z.B. beim Fliegen: **Können Hacker ein Flugzeug übernehmen?**

**IT-Sicherheit: Können Hacker ein Flugzeug übernehmen?**
20.04.2017 | 3 Min. | Quelle: BR
Es ist das Albtraumszenario jedes Kapitäns: Der Pilot bewegt den Steuerknüppel, aber die Maschine reagiert nicht. Terroristen haben sich in den Bordcomputer gehackt und die Kontrolle übernommen. Wie angreifbar sind Flugzeuge? Ein Thema auf dem Verkehrspilotentag der Pilotengewerkschaft Cockpit.

Quelle: http://www.ardmediathek.de/tv/Mittagsmagazin/IT-Sicherheit-K%C3%B6nnen-Hacker-ein-Flugzeu/Das-Erste/Video?bcastId=314636&documentId=42226832

# STANDARDS / ZERTIFIZIERUNGEN

# ISO 27001

- Organisationen, die ISO 27001 erfolgreich eingeführt haben, profitieren von:
  - Optimaler Mitteleinsatz zum Schutz der Informationen
  - Geschäftsrisiken und Schutzbedarf sind identifiziert
  - Reduzierung des Haftungsrisikos für GL und VR
  - Beherrschung der Top-Risiken
  - Garantierte Verfügbarkeit und Integrität der Informationen
  - Vertrauensbildung bei Kunden und Geschäftspartner
  - Nachhaltiger Schutz des Unternehmenswertes ‚Information'
  - Sicherheitsbewusstsein bei allen Mitarbeitenden

https://www.iso.org/isoiec-27001-information-security.html

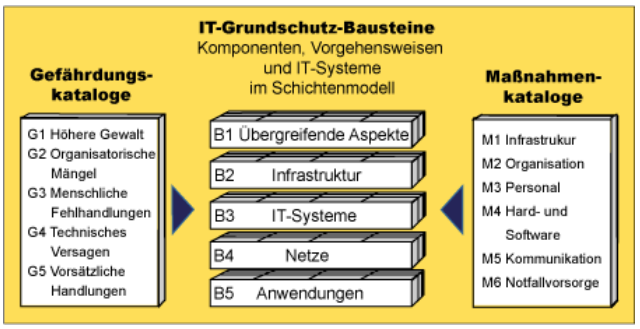
https://www.swissts.ch/de/zertifizierung-von-unternehmen/produkte/iso-27001/wissenswertes/

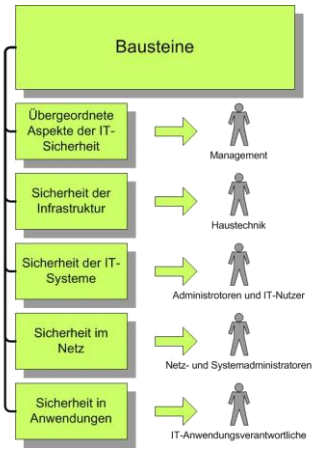
Die internationale Norm **ISO/IEC 27001** Information technology – Security techniques – Information security management systems – Requirements spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation. Darüber hinaus beinhaltet die Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Hierbei werden sämtliche Arten von Organisationen (z. B. Handelsunternehmen, staatliche Organisationen, Non-Profitorganisationen) berücksichtigt. Die Norm wurde auch als DIN-Norm veröffentlicht und ist Teil der ISO/IEC 2700x-Familie.
Die Norm spezifiziert Anforderungen für die Implementierung von geeigneten Sicherheitsmechanismen, welche an die Gegebenheiten der einzelnen Organisationen adaptiert werden sollen. Der deutsche Anteil an diesem internationalen Normungsprojekt wird vom DIN NIA-01-27 IT-Sicherheitsverfahren betreut.
Die ISO/IEC 27001:2005 wurde entworfen, um die Auswahl geeigneter Sicherheitsmechanismen zum Schutz sämtlicher Werte (Assets) in den Wertschöpfungsketten (siehe Scope der ISO/IEC 27001, ...organization's overall business risk) sicherzustellen.

https://de.wikipedia.org/wiki/ISO/IEC_27001

# IT Grundschutz

die Basis für Informationssicherheit




IT-Grundschutz - die Basis für Informationssicherheit - Der vom BSI entwickelte IT-Grundschutz ermöglicht es, notwendige Sicherheitsmassnahmen zu identifizieren und umzusetzen. Viele Arbeitsprozesse werden elektronisch gesteuert und grosse Mengen von Informationen sind digital gespeichert, werden verarbeitet und in Netzen übermittelt. Damit sind die Institutionen in Wirtschaft und Verwaltung und jeder Bürger von dem einwandfreien Funktionieren der eingesetzten IT abhängig.

https://de.wikipedia.org/wiki/IT-Grundschutz-Kataloge

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

# SN 612 010

Vermessung – Informatiksicherheit – Sicherheit und Schutz von Geodaten

- Schweizerische Norm im Bezug auf die
  **Sicherheit und den Schutz von Geodaten**

INB Schweizer Norm SN 612010

Vermessung – Informatiksicherheit – Sicherheit und Schutz von Geodaten

Mensuration – Sécurité informatique – Sécurité et protection des géodonnées

Siehe: *Download Educanet*

«Die Bearbeitung und Bereitstellung von Geodaten in Verwaltung und Privatwirtschaft erfolgt weigehend durch dein Einsatz von Informationstechnologie (IT). Die Durchdringung der Verarbeitungs- und Verwaltungsprozesse mit IT-Mitteln ist weit fortgeschritten; entsprechend hoch ist die Abhängigkeit von deren zuverlässigen und sicheren einsatz. Die ständige auseinandersetzung mit der Sicherheit der IT-Infrastruktur ist von fundamentaler Bedeutung und ist als permanenter Prozess zu initiieren und aufrecht zu erhalten.»

Die SN612010 : 2000 legt fest, wie Geodaten gegen Verlust, Verfälschung und nicht autorisierten Zugriff gesichert werden. Sie behandelt die betriebliche Informatiksicherheit , um Datensicherheit und Schutz der Daten zu erreichen.

Zugabe

# URHEBERRECHT

**Das Thema Urheberrecht hat nur am Rande einen direkten Zusammenhang mit der IT Sicherheit. Problematisch ist es aber dennoch, weil überall Themen aus den einzelnen Bereichen aufeinandertreffen und gewisse Verstösse im Urheberrecht auf die IT Sicherheit Einfluss haben können.**

**Datenschutzgesetzt zum Download:**
https://www.admin.ch/opc/de/classified-compilation/19920153/201401010000/235.1.pdf

**Revisionen des Bundesgesetzes über den Datenschutz (DSG)**
**2. Revision**
Der Bundesrat will den Datenschutz stärken und an die veränderten technologischen und gesellschaftlichen Verhältnisse anpassen. Er hat an seiner Sitzung vom 21. Dezember 2016 den Vorentwurf zu einer Totalrevision des Datenschutzgesetzes (DSG) in die Vernehmlassung geschickt.

https://www.bj.admin.ch/bj/de/home/aktuell/news/2016/ref_2016-12-21.html
https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf

# Urheberrecht

| Wer wird geschützt? | | Urheber | Interpreten | Ton- und Tonbild-trägerhersteller | Sendeunternehmen |
|---|---|---|---|---|---|
| Was wird geschützt? | | Werk (inkl. Software) | Darbietung | Aufnahme | Sendung |
| Wie lange? | | 70 Jahre (Software: 50 Jahre) Nach dem Tod des Urhebers bzw. seit Erbringung der Leistung | 50 Jahre | 50 Jahre | 50 Jahre |
| Welche Rechte bestehen? | Aufführungs-, Vortrags- und Vorführungsrecht | • | | | |
| | Aufnahmerecht | • | • | | • |
| | Vervielfältigungsrecht | • | • | • | • |
| | Verbreitungsrecht | • | • | • | • |
| | Recht zur Wahr-nehmbarmachung | • | • | | • |
| | Senderecht | • | • | | |
| | Weitersenderecht | • | • | | • |

Bundesgesetz über das Urheberrecht und verwandte Schutzrechte
https://www.admin.ch/opc/de/classified-compilation/19920251/

Im Urheberrechtsgesetz sind zudem die **verwandten Schutzrechte** geregelt. Sie umfassen
- die Rechte der ausübenden Künstler (Musiker, Schauspieler) an ihren Darbietungen,
- die Rechte der Hersteller von Ton- und Tonbildträgern an ihren Produkten (CD, DVD usw.),
- die Rechte der Sendeunternehmen an ihren Radio- und Fernsehsendungen.

# Urheberrecht

Filme, Serien, Musik, E-Books und Hörbücher.

Spiele für PC, Handy und Konsole oder Computerprogramme

**Warum ist das Herunterladen in der Schweiz im Gegensatz zu vielen anderen Ländern erlaubt?** In der Schweiz wird auf Datenträger bereits beim Kauf eine pauschale Urheberrechtsabgabe von rund 2 bis 6 Rappen pro Gigabyte Speicherplatz erhoben. Der Gesetzgeber zieht damit schon im Vornherein eine Entschädigung für allfällige Urheberrechtsverletzungen mit ein. Die Abgabe erhalten Verwertungsgesellschaften wie beispielsweise die Suisa, welche die Interessen der Künstler vertritt. Der Schlüssel, nach dem Suisa die Abgabe berechnet, ist nicht öffentlich einsehbar.

«Illegaler Download» aus dem Internet
https://www.suissimage.ch/index.php?id=faq_privatgebrauch#faq_8e296a067a37563370ded05f5a3bf3ec

URG: https://www.admin.ch/opc/de/classified-compilation/19920251/index.html

**Zitatrecht**
Das Urheberrecht in der Schweiz sieht Zitate ausdrücklich vor (Art. 25 URG). Für das Zitieren – beispielsweise durch Blogger aus anderen Weblogs – ist weder eine «Wiederverwendungserlaubnis» noch eine sonstige Genehmigung notwendig.
Urheberrechtlich geschützte Inhalte beziehungsweise Werke dürfen in der Schweiz frei zitiert werden um eigene Aussagen zu erläutern, zu veranschaulichen oder mit Hinweisen zu versehen. Zitate sind

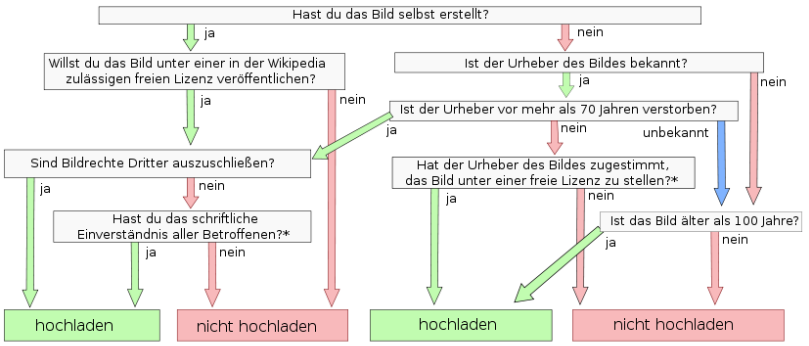
nach herrschender Lehre für alle Kategorien von Werken möglich, das heisst nach herrschender Lehre können auch Bildzitate verwendet werden und das Zitatrecht beschränkt sich nicht ausschliesslich auf Texte.
Rechtskonformes Zitieren setzt voraus, dass ein inhaltlicher Zusammenhang zwischen denn eigenen Inhalten und den verwendeten Zitaten besteht. Der Zitatumfang bemisst sich nach dem Zitatzweck und muss den eigenen Inhalten immer untergeordnet bleiben. Zitate müssen als solche erkennbar sein und sowohl die Urheberschaft als auch die Quelle müssen jeweils genannt werden.
Urheberrechtlich gesehen nicht notwendig ist hingegen eine Verlinkung von Urheberschaft und Quelle, doch ist eine solche Verlinkung bei digitalen Inhalten benutzerfreundlich, denn sie ermöglicht einen einfachen und schnellen Quellenzugriff.

**Bildverwendung im internet**
https://steigerlegal.ch/wp-content/uploads/2013/01/blogwerk_whitepaper_bildverwendung-im-internet_201204.pdf

Der Entwurf des neuen Urheberrechtsgesetzes, den Bundesrätin Simonetta Sommaruga nun präsentierte, legt den Fokus vor allem auf folgende zwei Punkte:
Die sogenannte «Stay-Down-Regel» soll die Piraterie im Internet eindämmen. Hosting-Provider werden dazu verpflichtet, illegale Angebote nicht nur einmal von ihren Servern zu entfernen, sondern auch dafür zu sorgen, dass die urheberrechtlich geschützten Werke nicht erneut hochgeladen werden.
Den Eigentümern von Urheberrechten soll es möglich sein, IP-Adressen, unter denen urheberrechtlich geschützte Werke illegal zum Download angeboten werden, zu speichern und weiterzuleiten. Diese Praxis war bisher verboten.
Beide Massnahmen sind auf illegale Angebote in der Schweiz beschränkt. Sie haben damit auf Betreiber von ausländischen Seiten wie *thepiratebay.org* oder *kinox.to* keinen Einfluss.

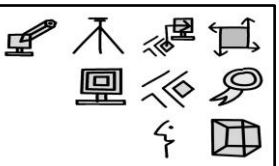
# Urheberrecht

- Immer Quellenangaben verwenden
- Im Idealfall beim Urheber das Einverständnis einholen




https://de.wikipedia.org/wiki/Wikipedia:Bildrechte

## Modernisierung des Urheberrechts



- Das Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (URG) regelt den Schutz der Urheber und Urheberinnen von Werken der Literatur und Kunst, den Schutz der ausübenden Künstler und Künstlerinnen, der Hersteller und Herstellerinnen von Ton- und Tonbildträgern sowie der Sendeunternehmen und die Bundesaufsicht über die Verwertungsgesellschaften (Art. 1 URG).
- Das Parlament hatte das schweizerische Urheberrecht zuletzt 2008 revidiert und dabei erste Anpassungen an das digitale Umfeld vorgenommen

https://www.ejpd.admin.ch/ejpd/de/home/aktuell/themen/urg.html

Worum geht es?
Das Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (URG) regelt den Schutz der Urheber und Urheberinnen von Werken der Literatur und Kunst, den Schutz der ausübenden Künstler und Künstlerinnen, der Hersteller und Herstellerinnen von Ton- und Tonbildträgern sowie der Sendeunternehmen und die Bundesaufsicht über die Verwertungsgesellschaften (Art. 1 URG). Das Parlament hatte das schweizerische Urheberrecht zuletzt 2008 revidiert und dabei erste Anpassungen an das digitale Umfeld vorgenommen. Die Überprüfung durch die 2012 einberufene Arbeitsgruppe zum Urheberrecht (AGUR12) hat ergeben, dass durch den fortschreitenden digitalen Wandel und die technologische Entwicklung in gewissen Bereichen Nachbesserungsbedarf besteht. Insbesondere ist es den Rechteinhabern im geltenden Recht nicht gelungen, die Urheberrechtspiraterie zurückzudrängen. Die vom Bundesrat am 11. Dezember 2015 in die Vernehmlassung geschickte Vorlage zur Änderung des Urheberrechtsgesetzes zielt daher in erster Linie auf eine verbesserte Pirateriebekämpfung. Zudem wird eine effizientere kollektive Verwertung von Urheberrechten angestrebt. Weiter sieht die Vorlage die Gutheissung der Verträge der Weltorganisation für geistiges Eigentum (WIPO) von Peking für einen besseren Schutz der Schauspieler und von

Marrakesch für einen besseren Zugang von Menschen mit Sehbehinderungen zu Werken vor. Im Rahmen der Vernehmlassung gingen 1224 Stellungnahmen mit zum Teil stark auseinandergehenden Stossrichtungen ein.

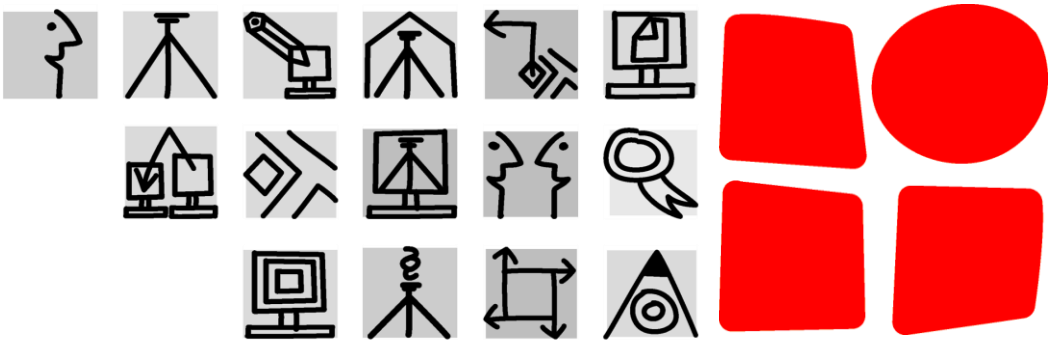
**Die Pirateriebekämpfung ist daher ein zentrales Anliegen der Revision des Urheberrechtsgesetzes.**

## Downloads

Alle Unterlagen zum Kurs gibt’s unter

**geomatik.eugster.net**

Wenn jemand abwesend ist: Für die Gruppenzuteilung beachten, damit alle Gruppen ausgeglichen viele Teilnehmer haben!



**Sekretariat Bildungszentrum Geomatik Schweiz**

www.biz-geo.ch

E-Mail: andre@biz-geo.ch
Tel: +41 (78) 674 13 77