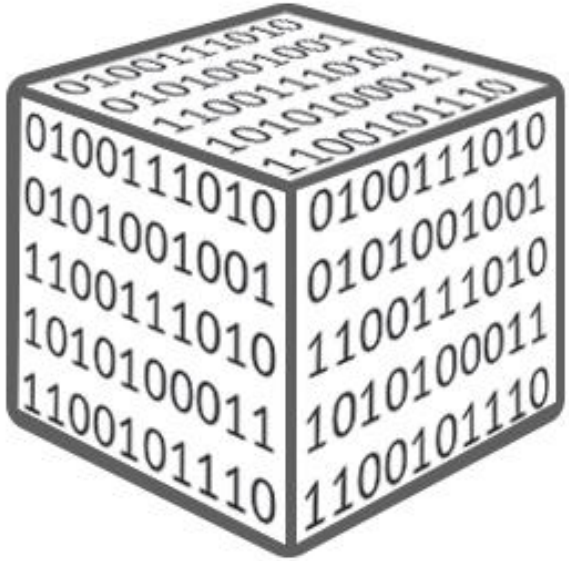
ECDL – IT Security

By www.bbz-edv.org

Kapitel 1 – Grundbegriffe zu Sicherheit

1.1.1 Unterschied zwischen Daten & Informationen

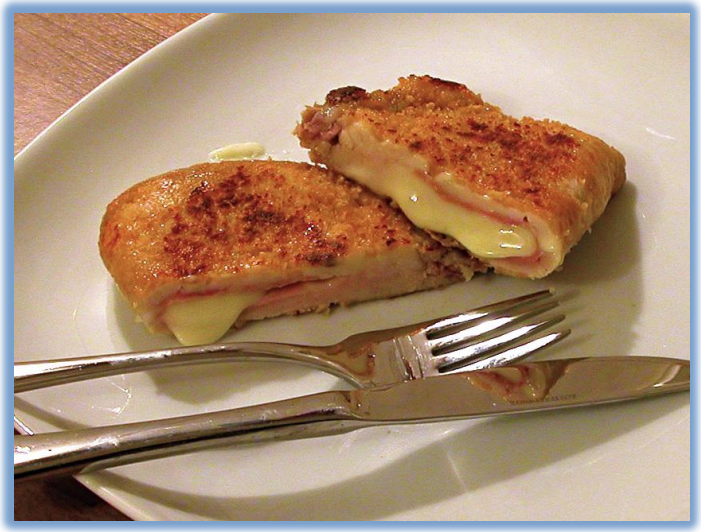
Daten sind Informationen, aber Informationen nicht unbedingt Daten. Damit Informationen zu Daten werden, müssen sie in ein einheitliches System gebracht werden.



Information = Kenntnisse (Details) über Dinge oder Vorgänge.

Daten = Vereinheitlichte/Systematische (vergleichbare) Informationen zur Verarbeitung und Speicherung.

1.1.1 Ein Beispiel



Informationen:

Gabriel ist ein netter Kerl. Er ist eins achtzig groß und isst gerne Cordon Bleu. Seine Freundin ist 1,69m groß und heißt Janine. Janine ist Vegetarierin. Im Moment arbeitet sie als Lehrkraft.

Daten:

Vorname	Größe	Leibspeise	Beruf
Gabriel	1.80m	Cordon Bleu	n/v
Janine	1.69m	n/v	Lehrkraft

1.1.2 Cybercrime - Cyberkriminalität

1.1.2 Cybercrime

Definition:

Der Begriff **Computerkriminalität** umfasst „alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese begangen werden“.

1.1.3 Hacker, Cracker und die Ethik

1.1.3 Hacker & Cracker

Der Hacker:

Hacker sind Personen, die Sicherheitslücken in Netzwerken und Rechensystem auskundschaften und diese nicht ausnutzen, sondern diese den jeweils Betroffenen mitteilen.

Der Cracker:

Das komplette Gegenteil. Sie nutzen die Lücken aus um Chaos und Schaden anzurichten.

1.1.4 Bedrohung für Daten durch höhere Gewalt

Die 4 apokalyptischen Reiter

1.1.4 Krieg

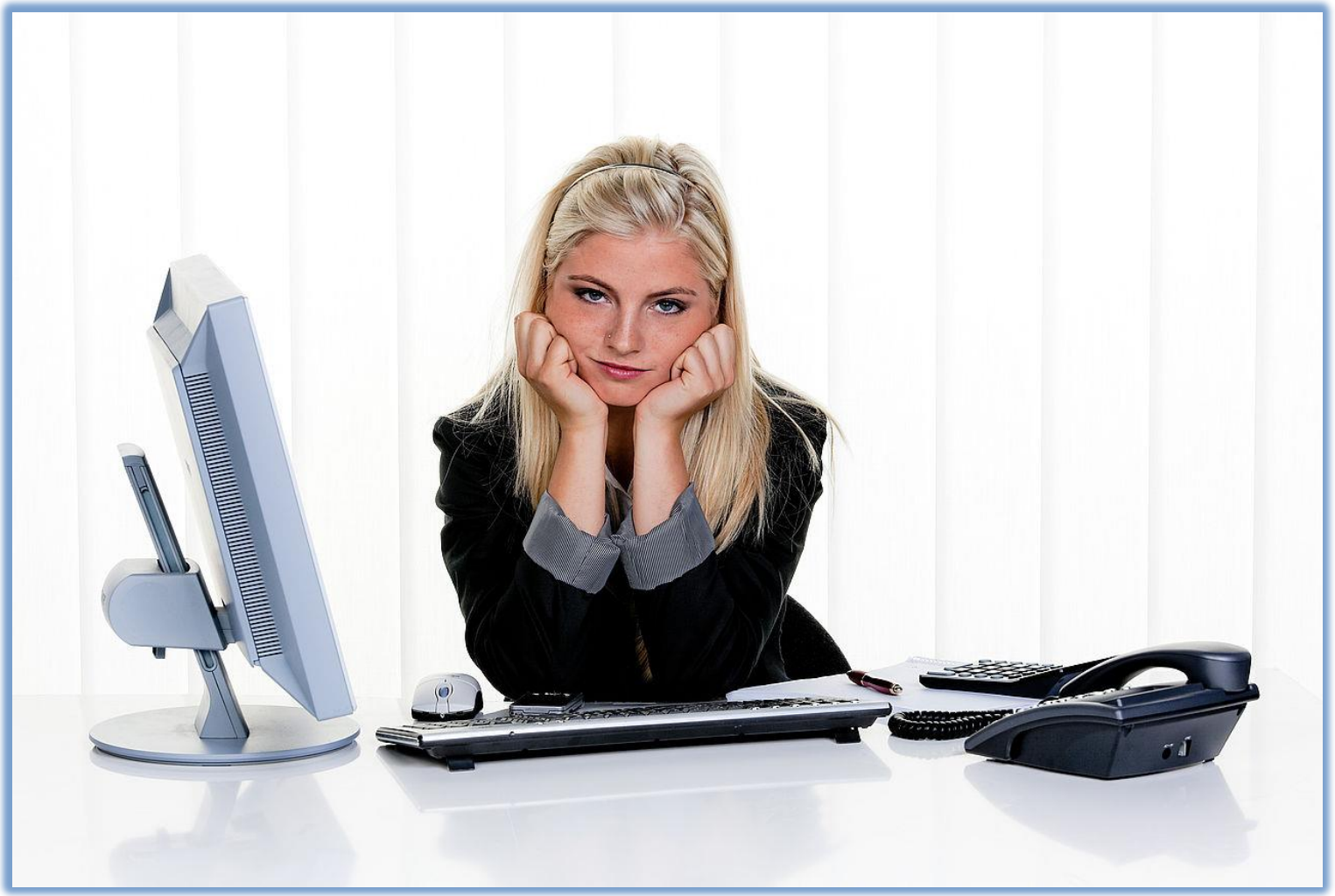
1.1.4 Erdbeben

1.1.4 Hochwasser / Überflutungen

1.1.4 Feuer / Brandkatastrophen

1.1.5 Bedrohung für Daten durch Menschen

1.1.5 Sicherheitslücke Nr. 1 im Betrieb
| Angestellte | Externe Arbeiter | Besucher |



Kapitel 1.2 – Der Wert von Daten & Informationen

1.2.1 – Schutz der Daten (Identitätsdiebstahl / Betrug)

1.2.2 – Schutz von Firmendaten & Kunden

1.2.3 – Daten schützen / Passwörter

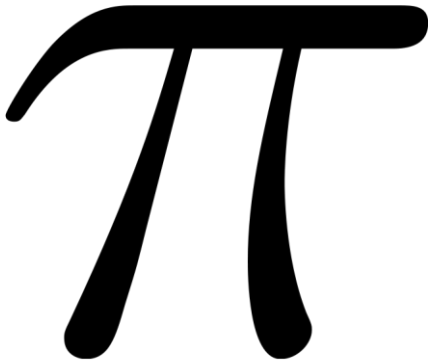
1.2.3 – Sichere Passwörter

Es gelten folgende Kriterien für ein „sicheres“ Passwort:

- Das Passwort muss mindestens aus 8 Zeichen bestehen
- Groß & Kleinschreibung
- Zahlen
- Sonderzeichen

Beispiel:
Wh1teHou5eG0V@Am3r1c@

1.2.3 – Verschlüsselung / Encryption

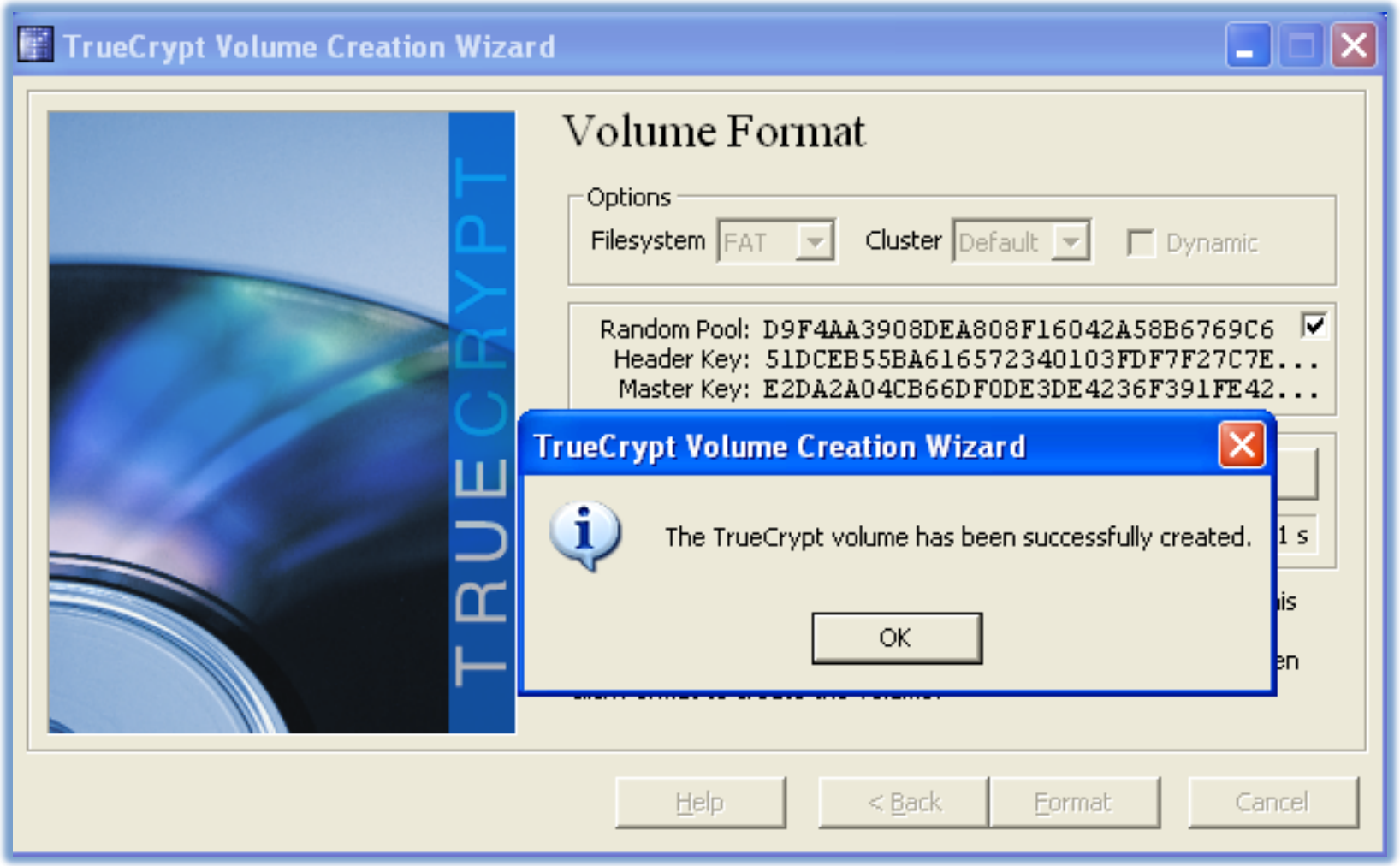


Die Verschlüsselung ist die Umsetzung einer verständlichen Information in eine unverständliche:

Die Umsetzung eines Klartextes in einen Geheimtext. Ziel der Verschlüsselung ist es, die Daten einer mathematischen Transformation (Verschlüsselungsalgorithmus) zu unterwerfen, damit es einem Angreifer, der die Daten in seinem Besitz bekommt, nicht möglich ist, aus den transformierten Daten die „Originaldaten“ zu gewinnen.

1.2.3 – Wie verschlüssele ich?

VeraCrypt



1.2.4 – Vertraulichkeit von Daten

Vertraulichkeit:

Ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein. Weitergabe und Veröffentlichung sind nicht erwünscht. Vertraulichkeit wird durch Rechtsnormen geschützt, sie kann auch durch technische Mittel gefördert oder erzwungen werden.

1.2.4 – Verfügbarkeit von Daten

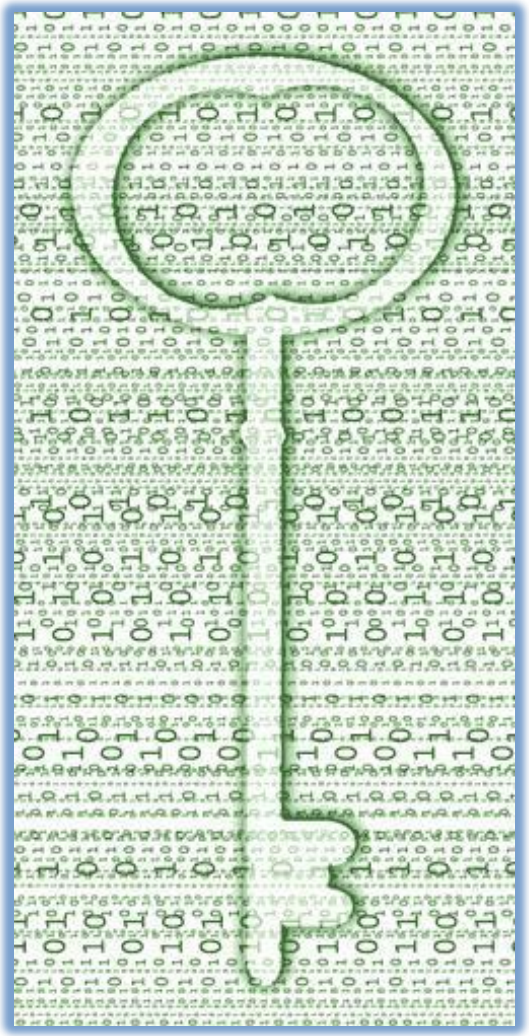
Die **Verfügbarkeit** eines technischen Systems ist die Wahrscheinlichkeit oder das Maß, dass das System bestimmte Anforderungen zu bzw. innerhalb eines vereinbarten Zeitrahmens erfüllt. Sie ist ein Qualitätskriterium und eine Kennzahl eines Systems.

$$\text{Verfügbarkeit} = \frac{\text{Gesamtzeit} - \text{Gesamtausfallzeit}}{\text{Gesamtzeit}}$$

1.2.4 – Integrität von Daten

Integrität ist neben Verfügbarkeit und Vertraulichkeit eines der drei klassischen Ziele der Informationssicherheit. Eine einheitliche Definition des Begriffs Integrität gibt es nicht.

In den Evaluationskriterien für Informationssicherheit der frühen 1990er Jahre (ITSEC) wird Integrität definiert als „Verhinderung unautorisierter Modifikation von Information“. Integrität bezeichnet die „Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.



1.2.4 – Integrität von Daten

Korrekter Inhalt
Diese Integritätsart liegt vor, wenn Sachverhalte der realen Welt korrekt abgebildet werden. Dies soll beispielsweise durch Integritätsbedingungen sichergestellt werden.

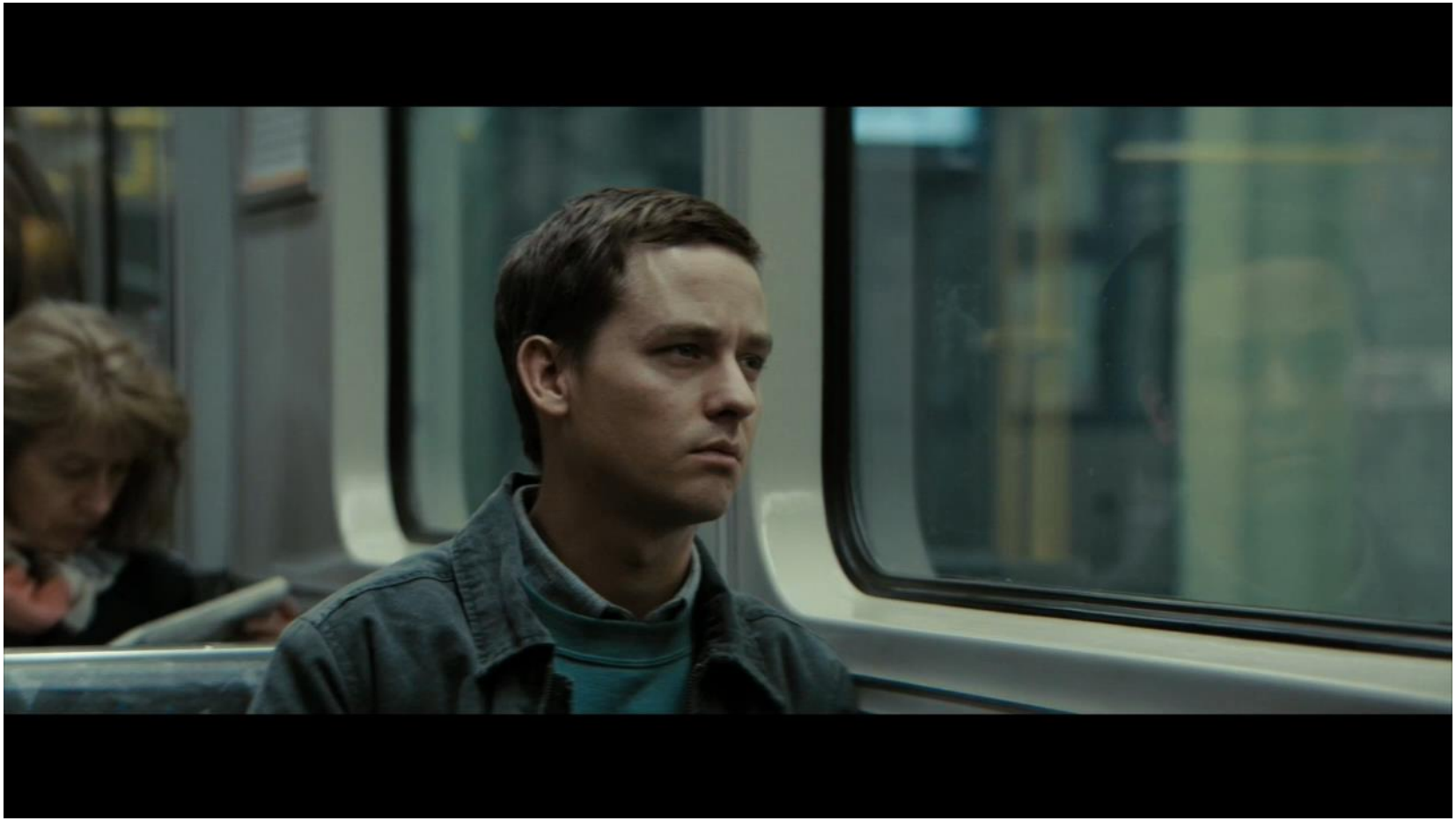
Unmodifizierter Zustand
Diese Integritätsart liegt vor, wenn Nachrichten unverändert zugestellt werden und Programme und Prozesse wie beabsichtigt ablaufen.

Erkennung von Modifikation
Diese Integritätsart liegt vor, wenn unerwünschte Modifikationen, die nicht verhindert werden können, zumindest erkannt werden.

Temporale Korrektheit
Diese Integritätsart liegt vor, wenn Nachrichten ausgetauscht und relevante zeitliche Bedingungen, wie etwa Reihenfolgen oder maximale Verzögerungszeiten, eingehalten werden.

Kapitel 1.3 – Persönliche Sicherheit / Social Engineering

1.3 – Social Engineering – Videoausschnitt „Who am I“



1.3.1 – 1.3.4 Begriffsdefinitionen

SOCIAL ENGINEERING

Informationsbeschaffung direkt beim Computerbenutzer, ohne technische Hilfsmittel.

TELEFONANRUFE / Vishing (VOIP)

Durch Ausspionieren des Umfelds des Opfers oder Vortäuschen falscher Identitäten entlockt man jemandem vertrauliche Informationen Beispiel: Jemand gibt sich am Telefon als Bankbediensteter aus und fragt mich nach meinen Daten / Codes.

1.3.1 – 1.3.4 Begriffsdefinitionen

PHISHING

Passwort-Fischen (password-fishing) durch gefälschte Mails oder SMS wird versucht, Zugang zu Passwörtern zu erlangen PHISHING.

SHOULDER SURFING

Schulter-Surfen" Informationsbeschaffung durch direkte Beobachtung der Eingabe von PINs oder Passwörtern besonders leicht möglich in Internet- Cafés oder an belebten Orten, wenn über Smartphone o.ä. Passwörter eingegeben werden.

1.3.1 – 1.3.4 Begriffsdefinitionen

INFORMATION DIVING

auf dem Rechner gespeicherte Kreditkarten-Nummern etc. können - nach unprofessioneller Entsorgung - problemlos ausgeforscht werden durch Auswertung von Organisationsplänen aus dem Mülleimer wird die Organisations-struktur eines Betriebes ausgeforscht eine ausrangierte Festplatte wird nach persönlichen Daten durchsucht.

1.3.1 – 1.3.4 Information Diving - Videoausschnitt „Who am I“

1.3.1 – 1.3.4 Begriffsdefinitionen

SKIMMING

durch Manipulation von Geldautomaten werden Kundendaten "abgeschöpft" Magnetstreifeninformation einer Bankomatkarte wird durch am Geldautomat angebrachte kleine Lesegeräte ausspioniert Informationsbeschaffung z.B. durch Austausch des Tastenfeldes oder Anbringung kleiner Funkkameras beim Bankomat.

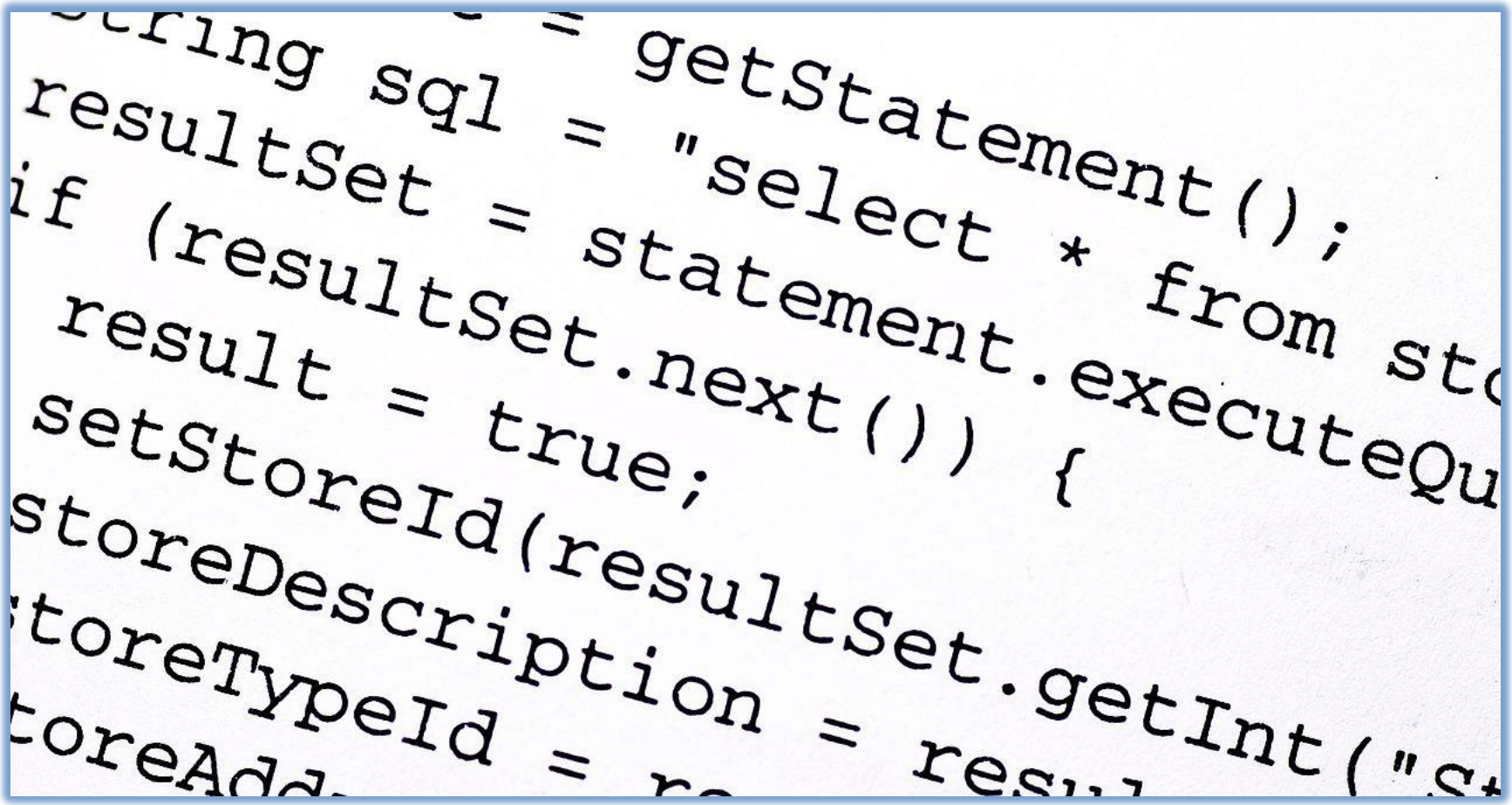
1.3.1 – 1.3.4 Begriffsdefinitionen

PRETEXTING

Der gebräuchlichste Weg, um persönliche Information zu stehlen, ist **Pretexting**. Pretexting ist ein „Kunstbegriff“ und bedeutet, dass unter falschen Vorgaben personenbezogene Daten eingeholt werden, vor allem via Telefon.

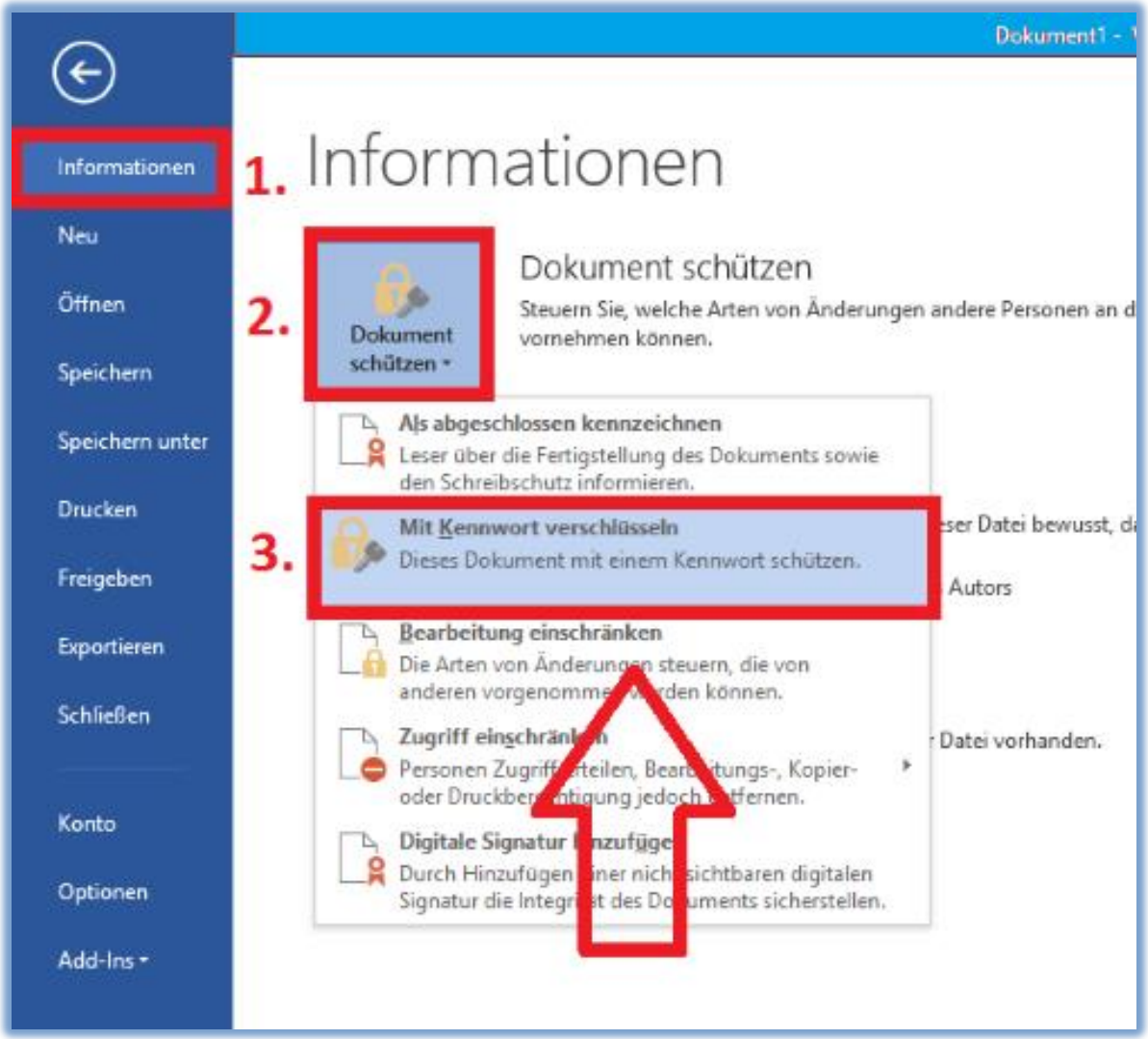
Beispiel: Jemand wird unter falschem Vorwand angerufen. Meist gibt sich der Anrufer als Person aus, die autorisiert ist, diese vertrauliche Information auch zu erhalten.

Kapitel 1.4 – Sicherheit von Daten

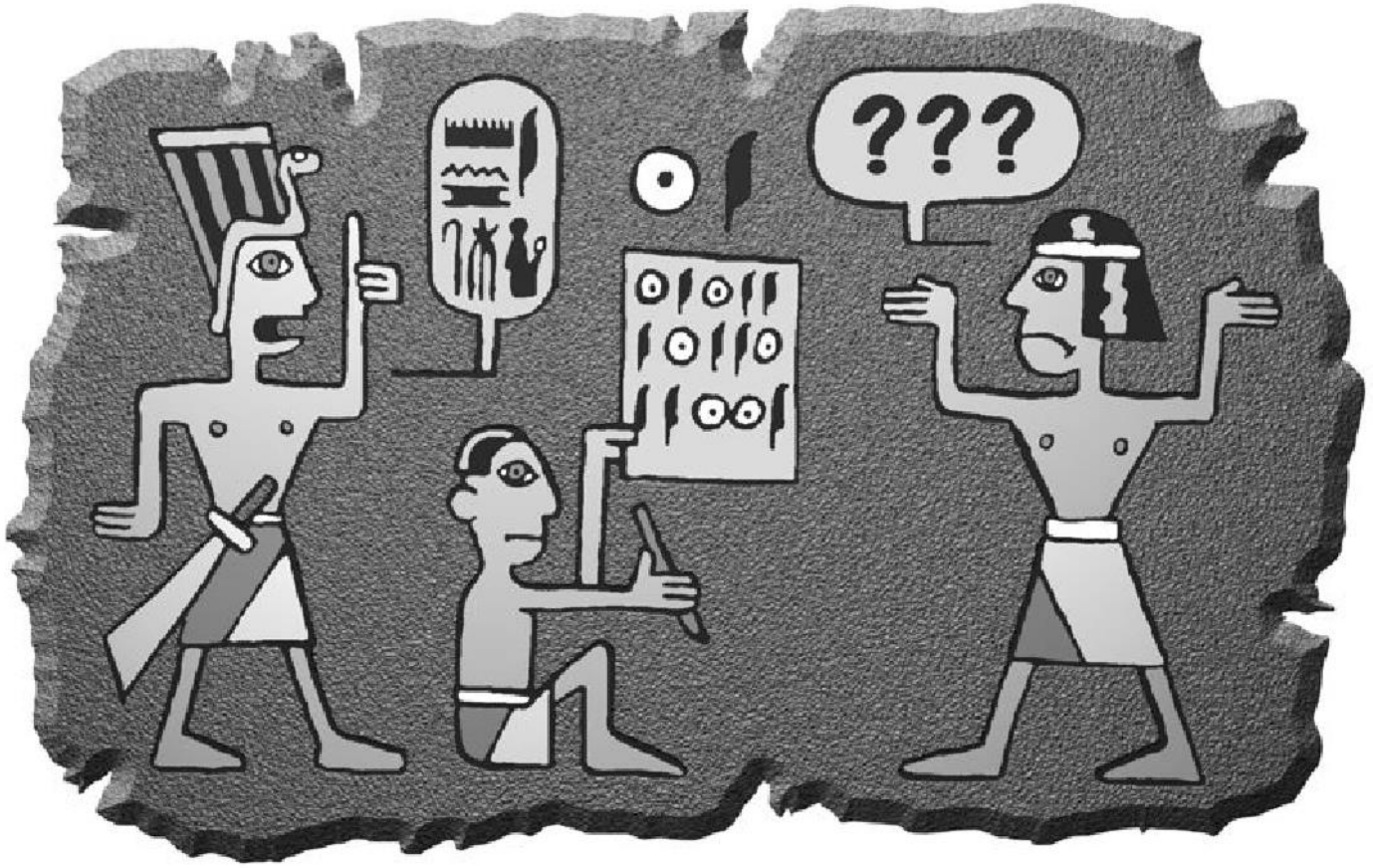


1.4.1 – Makros deaktivieren

1.4.2 – Dateien mit Passwort schützen



1.4.3 – Vorteile und Nachteile von verschlüsselten Daten



Kapitel 2 – Malware & Schutz

2.1 – Den Begriff „Malware“ verstehen

Malware: (Schadprogramme)

Als Schadprogramm auch Evilware oder Malware bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Malware ist damit ein Oberbegriff, der u. a. den Computervirus umfasst.

2.1.2 – 2.2.2 – Typen von Schadprogrammen

Rootkit:

Der Begriff Rootkit beschreibt Schadprogramme, die PCs infizieren und dem Angreifer erlauben, verschiedene Programme darauf zu installieren, die ihm dauerhaften Zugriff auf den Computer ermöglichen. Das Schadprogramm wird üblicherweise tief im Betriebssystem versteckt und ist so programmiert, dass es die Entdeckung durch Antivirus-Software und andere Security-Lösungen erschwert. Das Rootkit kann auch verschiedene schädliche Tools enthalten, etwa Keylogger, Programme zum Passwort-Diebstahl, Module zum Diebstahl von Kreditkartennummern und Online-Banking-Informationen.

2.1.2 – 2.2.2 – Der Trojaner

2.1.2 – 2.2.2 – Das Virus

Virus:

Viren sind Schadprogramme die gezielt meine installierte Software auf PC / Smartphone / Tablet usw. angreifen. Sie verändern Systemdateien, Benutzerdateien, löschen wichtige Dateien bis das System unbrauchbar wird.

Ein Virus verteilt sich nicht von alleine, nur durch menschliche Beihilfe ist er erfolgreich!

2.1.2 – 2.2.2 – Der Wurm

Würmer:

Würmer sind Schadprogramme die gezielt meine installierte Software auf PC / Smartphone / Tablet usw. angreifen. Sie verändern Systemdateien, Benutzerdateien, löschen wichtige Dateien bis das System unbrauchbar wird.

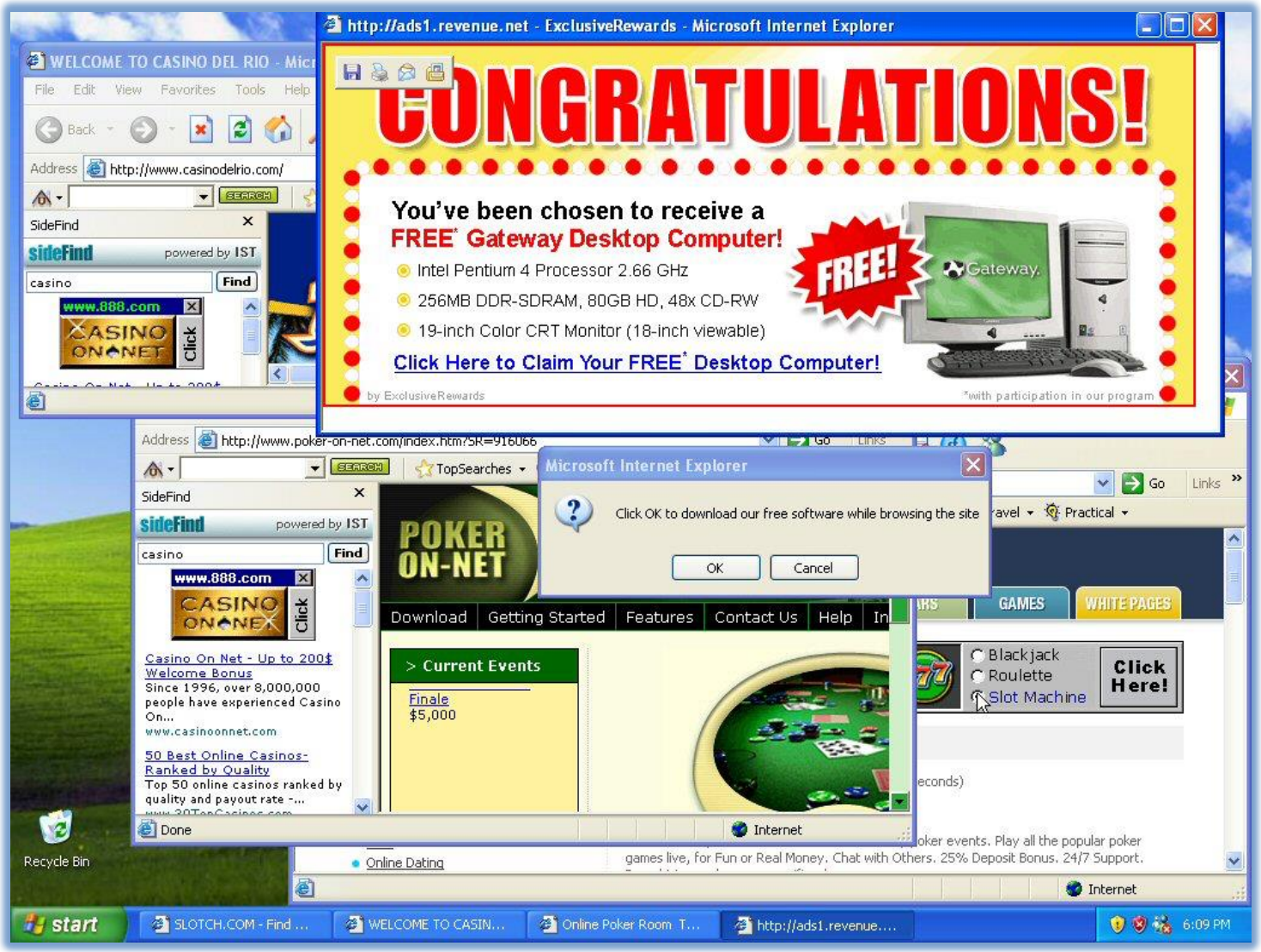
Im Gegensatz zu Viren, verteilen sich Würmer / duplizieren sich selbstständig. Sie verbreiten sich via Mail, Sticks, Web usw.

2.1.2 – 2.2.2 – Adware

Adware:

Als Adware werden Programme bezeichnet, die dazu dienen, Werbung auf Ihrem Computer anzuzeigen, Ihre Suchanfragen auf Werbe-Webseiten umzuleiten und marketing-relevante Daten über Sie zu erfassen – beispielsweise die Art der von Ihnen besuchten Webseiten – , um speziell auf Sie zugeschnittene Werbung anzuzeigen.

2.1.2 – 2.2.2 – Ein Beispiel für Adware



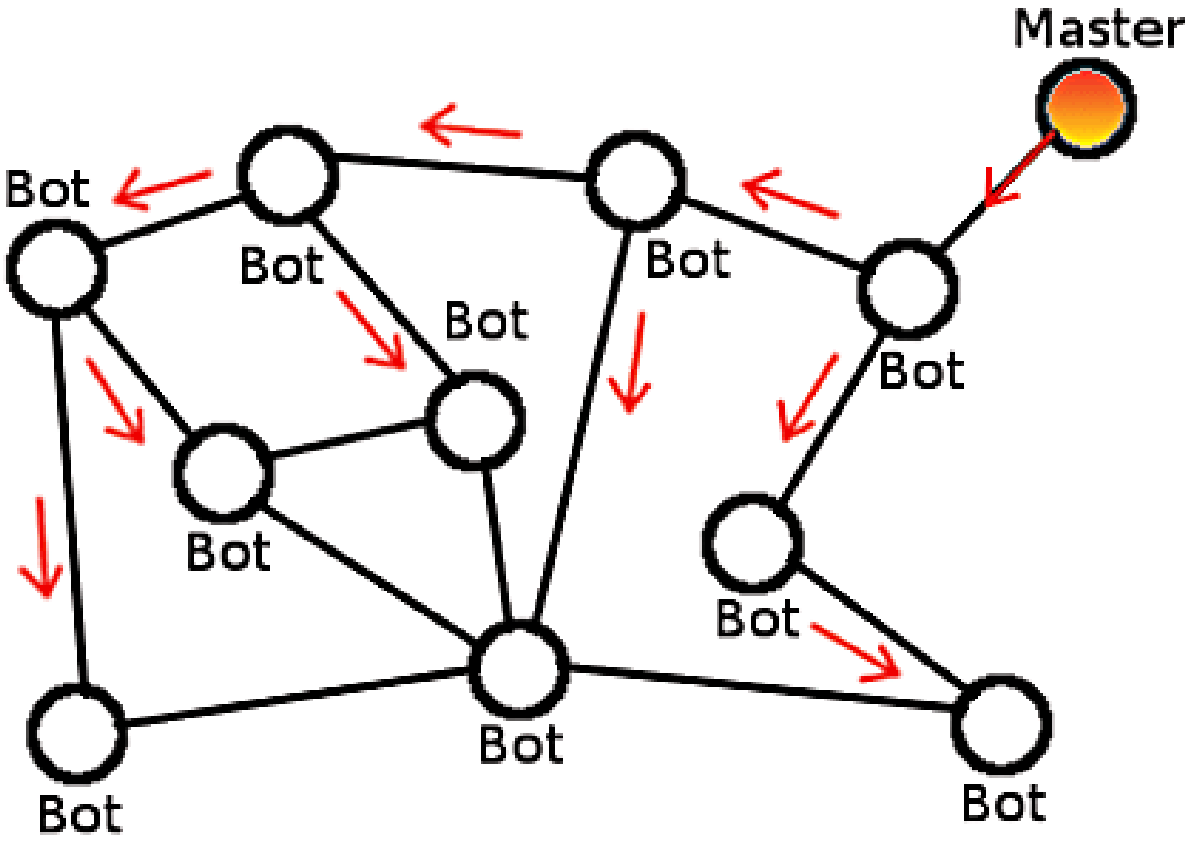
2.1.2 – 2.2.2 – Spyware

Spyware:
(Spionageprogramme)

Spyware sind Schadprogramme die es gezielt auf persönliche Informationen des System-Benutzers absehen.

Sie sammeln Daten wie z.B. besuchte Websites, Passwörter, Kontonummern, Kreditkartennummern usw. Anschließend werden die gesammelten Daten an den Programmierer zugeschickt.

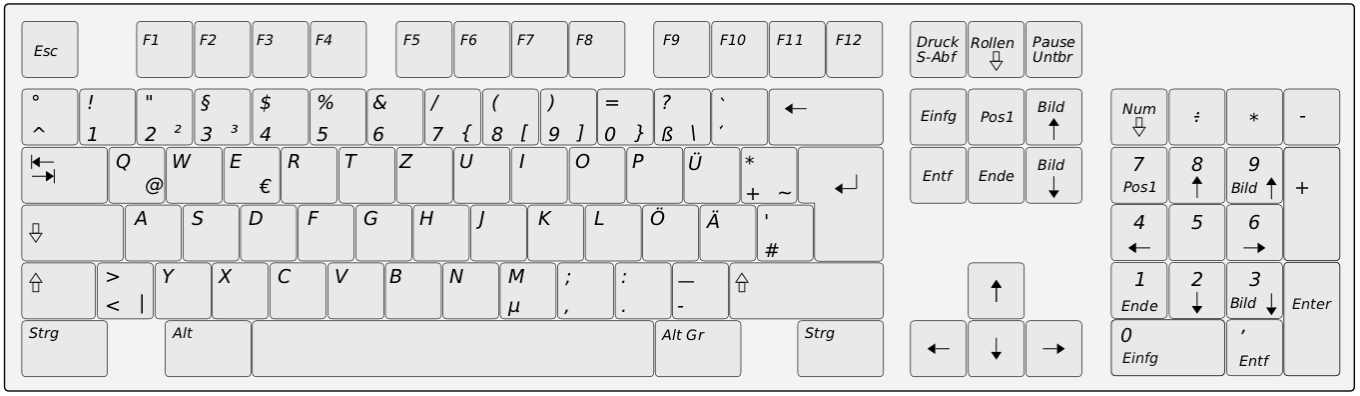
2.1.2 – 2.2.2 – Botnet / Botnetz



2.1.2 – 2.2.2 – Keylogger

Keylogger:

Keylogger sind Spionageprogramme die alles aufzeichnen, was man auf der Tastatur eintippt. Die gesammelten Informationen werden dann dem Programmierer zugeschickt.



2.1.2 – 2.2.2 – Dialer

Dialer:

Sind Schadprogramme die sich in ein anderes Telefonnetz einwählen (ISP) und somit erhöhte Telefonkosten verursachen (Internet-Flatrate setz aus). Dialer führen oft zu Webseiten mit pornografischem Inhalt. Oder auch zu Medien Abos (Smartphone).

Kapitel 2.3 – Schutz

2.3.1 – Sinn und Zweck eines Antivirus

2.3.2 – Wie schütz ich mich richtig?

2.3.2 – Der korrekte Umgang

1. Laufwerke, Ordner und Dateien scannen.

2. Antivirus immer updaten.

3. Nicht vertrauenswürdige Daten sofort scannen oder umgehend löschen.

4. Automatische Scans planen.

2.3.3 – Die Quarantänezone

2.3.4 – Updates und Virensignaturen

Virensignatur:

Virensignaturen werden von Anti-Virus-Programmen zur Identifizierung von Viren genutzt. Sie stellen ein möglichst eindeutiges Erkennungsmerkmal dar.

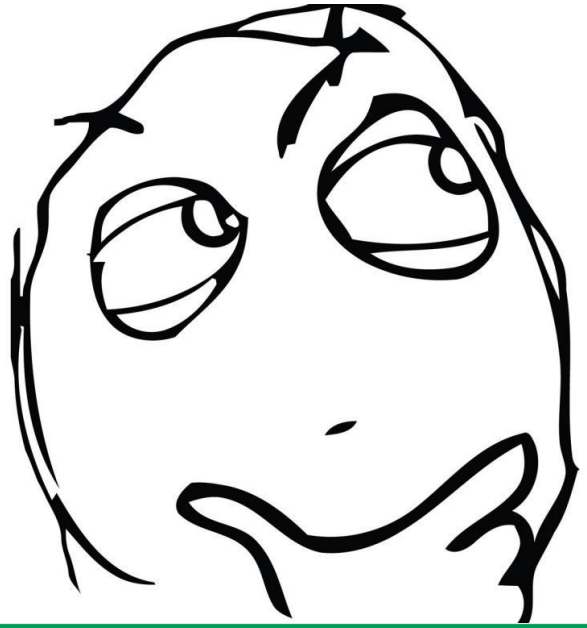
Kapitel 3 – Sicherheit im Netzwerk

3.1.1 – Netzwerktypen

LAN?

WAN?

WLAN?



GAN?

VPN?

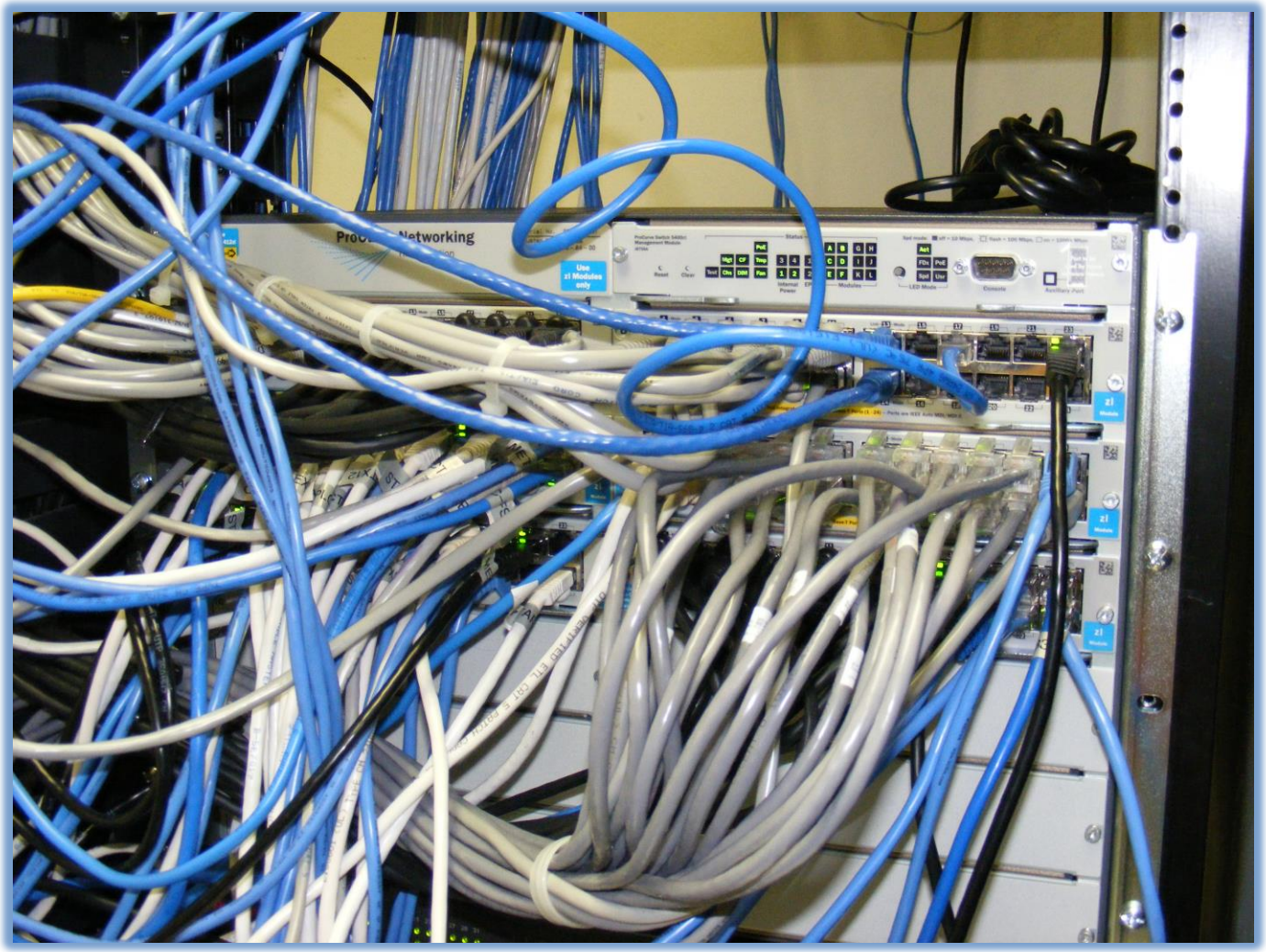
3.1.2 – Aufgaben eines Netzwerkadministrators

3.1.2 – Aufgaben eines Netzwerkadministrators

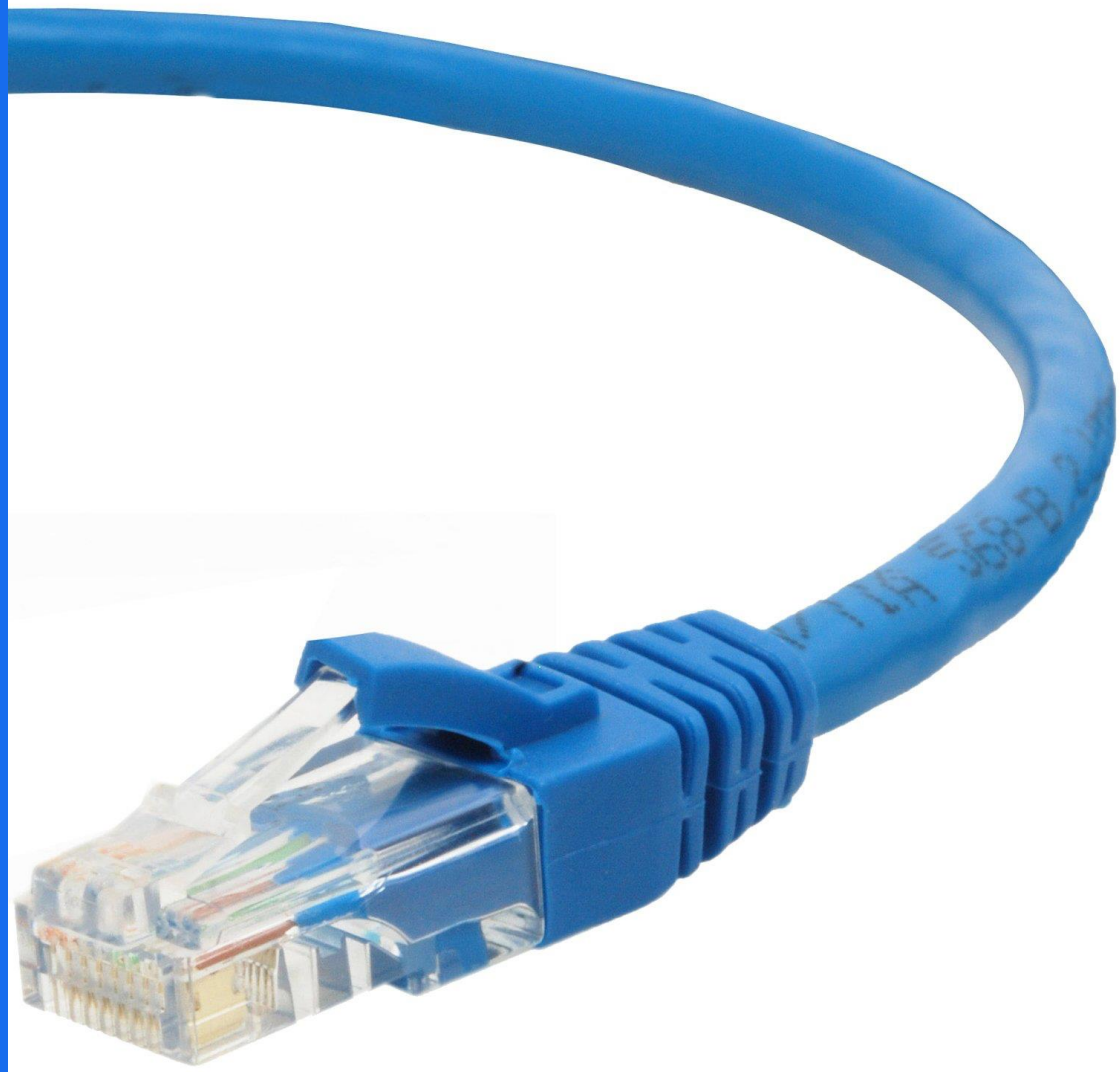
1. Protokollierung der Authentifizierung der User im Netzwerk
2. Das Verwalten von Benutzerrechten
3. Aufrechterhaltung und Absicherung der Infrastruktur
4. Wartungen und Service für User im Netzwerk
5. Installationen und Konfigurationen
6. Dokumentation seiner Arbeit im Netzwerk (schriftlich / Digital)
7. Zuständig für Datenbackups und deren sicheren Aufbewahrung

3.1.3 – Was ist eine Firewall?

Kapitel 3.2 – Netzwerkverbindungen



3.2.1 – Kabelverbindungen / ETHERNET (LAN)

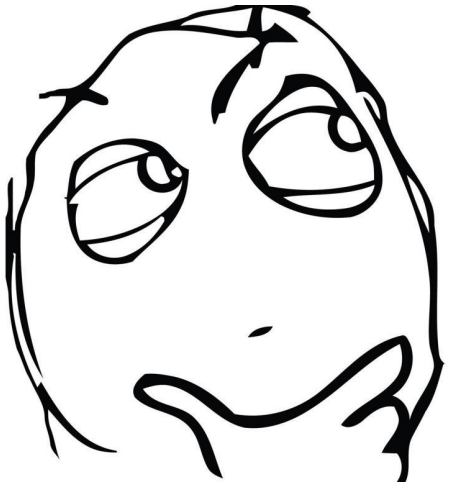


3.2.1 – Schnurlos / WLAN - WiFi

3.2.2 – Datensicherheit im Netzwerk

MALWARE?

PRIVACY?



UNBERECHTIGTER ZUGRIFF AUF DATEN?

Kapitel 3.3 – Sicherheit im Drahtlosen Netz

3.3.1 – 3.3.2 – WLAN-Zugriff absichern

Um mein WLAN vor ungebetenen Gästen zu schützen, muss ich es mit einem Passwort und einem Verschlüsselungsprotokoll schützen!

<u>WEP: (UNSICHER)</u>

Wired Equivalent Privacy

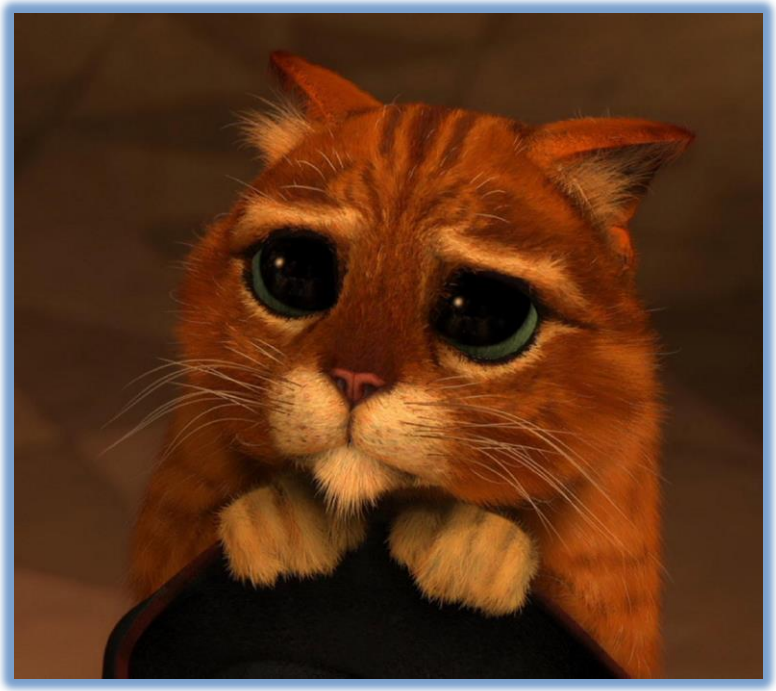
<u>WPA / WPA2: („SICHER“)</u>

Wi-Fi Protected Access

3.3.1 – 3.3.2 – WLAN-Zugriff absichern

MAC – Media Access Control

3.3.3 – Ungeschütztes WLAN



Seien Sie sich bewusst, dass ein ungeschütztes drahtloses Netzwerk es Eindringlingen ermöglicht in Ihr Netzwerk problemlos einzusteigen und Sie Ihnen somit Zugriff auf Daten ermöglichen!

3.3.3 – Verbindung zu einem „offenen-Wlan“

Offene Wlans finden wir sehr häufig, sei es in Museen, Bars, Restaurants, Parks oder öffentlichen Plätzen. Seien Sie sich der Gefahren bewusst, auch ein offenes WLAN kann Gefahren mit sich bringen, Sie wissen nicht mehr mitliest oder ihre Daten abfängt.

3.3.4 – Verbindung zu einem nicht geschützten WLAN

Kann ich mich mit einem nicht geschützten WLAN überhaupt verbinden?

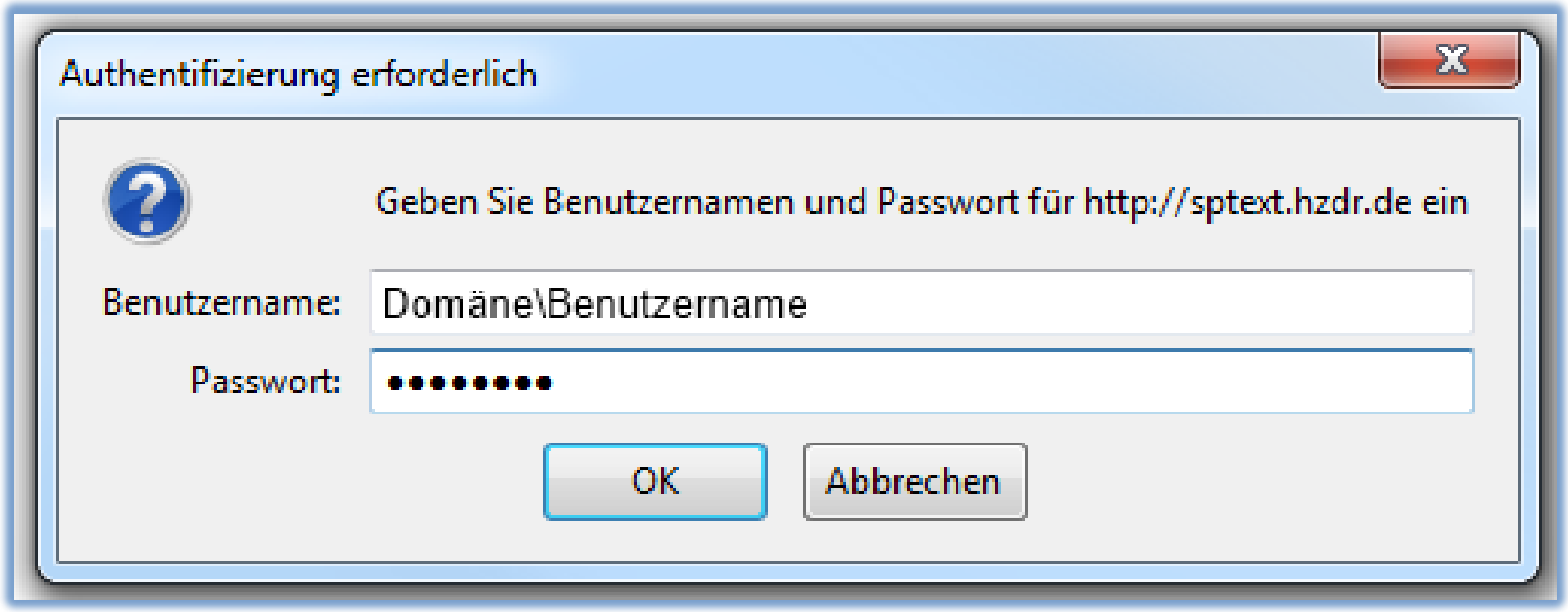
JA!

Wie erkenne ich ein nicht geschütztes WLAN?

Bei der Herstellung der Verbindung zum WLAN-AccessPoint wird kein Passwort zur Eingabe benötigt.

Kapitel 3.4 – Zugriffskontrolle

3.4.1 – Der Netzwerkzugang



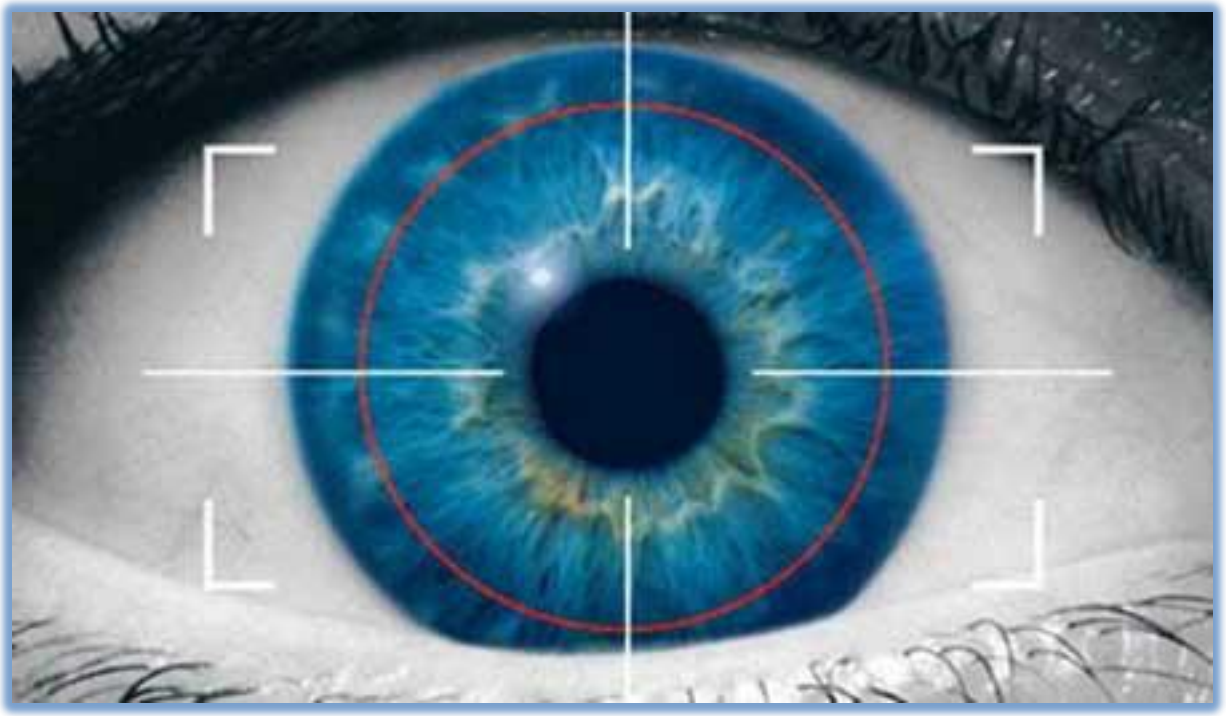
Warum ist es wichtig sich im Netzwerk zu authentifizieren?

3.4.2 – Sichere Passwörter (Wiederholung)

3.4.3 – Biometrische Verfahren zur Zugangskontrolle

Authentifizierung via Fingerabdruck / Fingerabdruckscanner

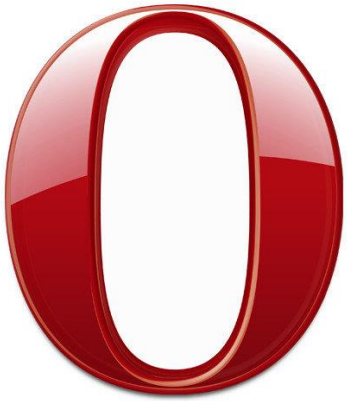
3.4.3 – Biometrische Verfahren zur Zugangskontrolle



Authentifizierung via Netzhaut / Augenscanner

Kapitel 4 – Sichere Webnutzung

4.1 – Der Browser



4.1.1 – Gewisse Dienste nur auf „sicheren Websites“ abwickeln

4.1.2 – 4.1.4 – Wie erkenne ich ob ich mich auf einer „sicheren Website“ befinde?

1. URL / PROTOKOLL
2. SYMBOLIK
3. SICHERHEITSZERTIFIKAT
4. GÜLTIGKEITSDAUER
5. HERAUSGEBER D. ZERTIFIKATS

4.1.3 – Pharming

Pharming ist eine Betrugsmethode, die durch das Internet verbreitet wird.
Sie basiert auf einer Manipulation von Webbrowsern, um den Benutzer auf gefälschte Webseiten umzuleiten.
Es ist eine Weiterentwicklung des klassischen Phishings.

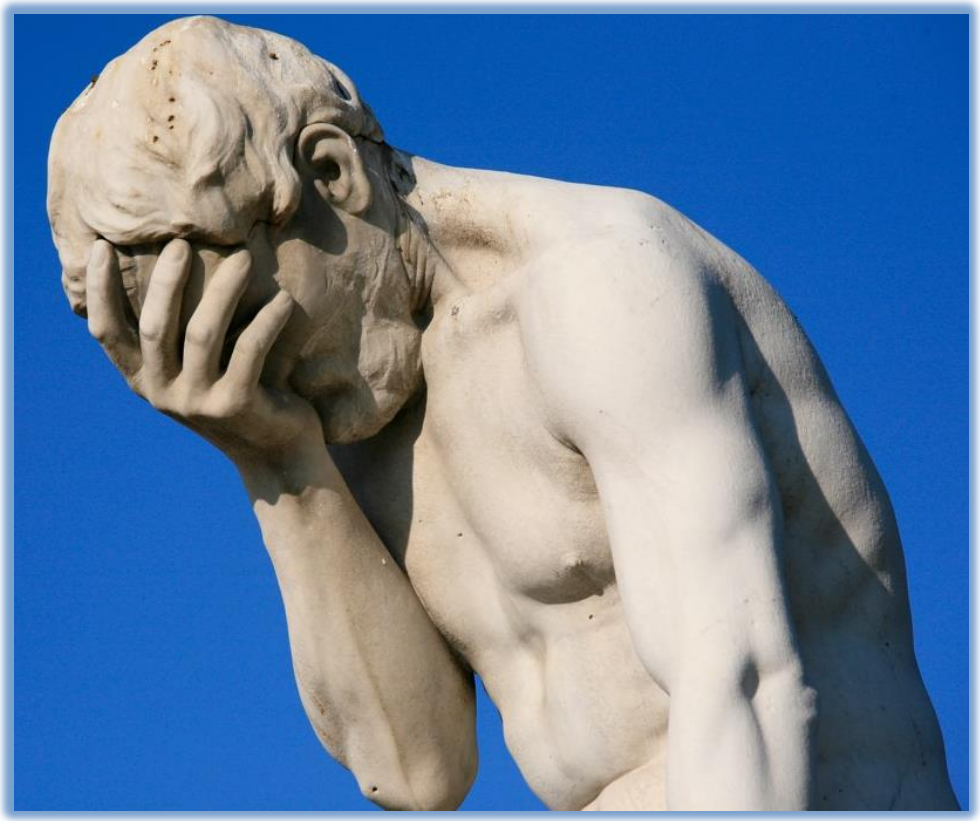
4.1.5 – Einmal-Kennwort

Ein **Einmalkennwort** oder **Einmalpasswort** ist ein Kennwort zur Authentifizierung oder auch Autorisierung. Jedes Einmalkennwort ist nur für eine einmalige Verwendung gültig und kann kein zweites Mal benutzt werden. Entsprechend erfordert jede Authentifizierung oder Autorisierung ein neues Einmalkennwort.

4.1.5 – Browserfunktionen deaktivieren

Folgende Browserfunktionen, müssen / sollen deaktiviert werden:

- Autovervollständigung
- Passwort speichern

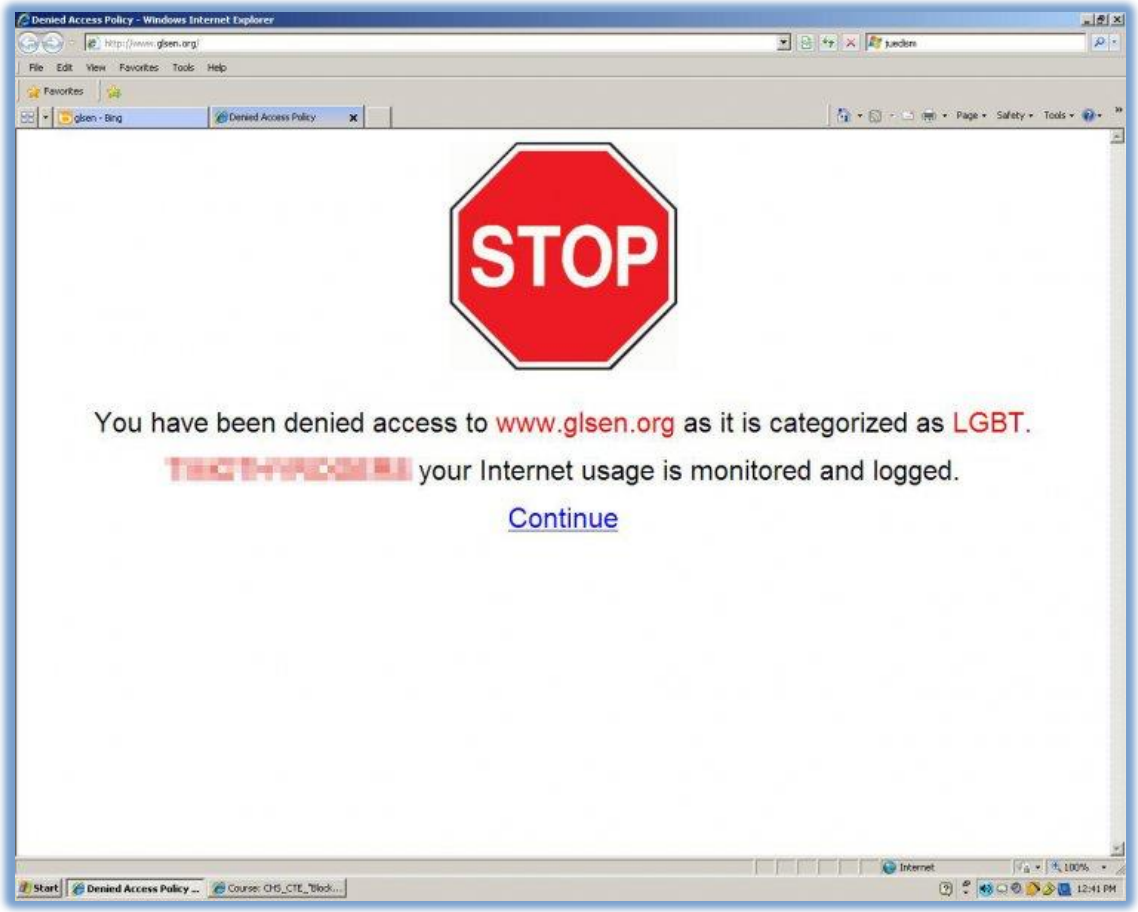


4.1.7 – 4.1.8 – Was sind Cookies? Zulassen, ja oder nein?

4.1.9 – Warum sollte ich meine Browserdaten löschen?

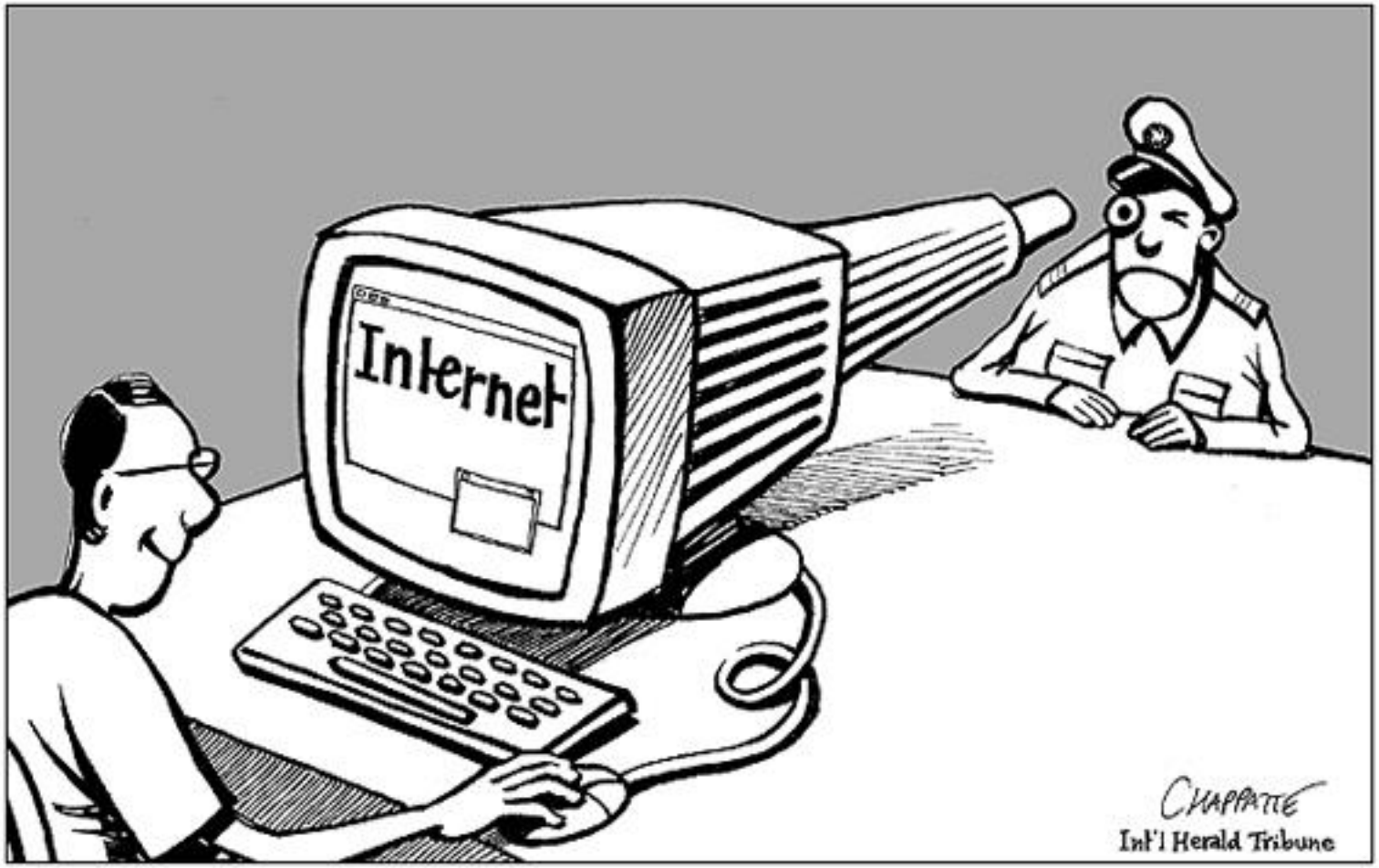
- Verlauf
- Temporäre Internetdateien
- Cookies
- Passwörter
- Formulardaten

4.1.10 – Inhaltskontrolle – Webfilter & Kinderschutz



Kapitel 4.2 – Soziale Netzwerke

4.2.1 – 4.2.2 – Der Hausverstand



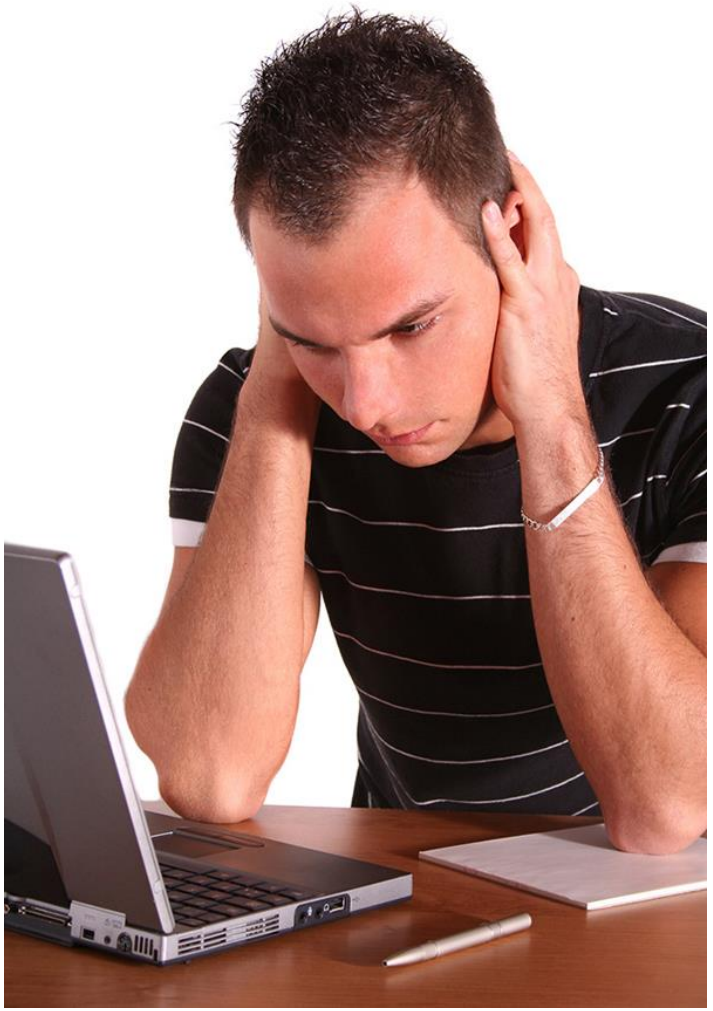
Privacy Einstellungen vornehmen

4.2.1 – 4.2.2 – Der Hausverstand

Keine vertraulichen Infos in Sozial Netzwerken teilen

4.2.3 – Gefahren in Social Networks

Cyber-Mobbing, Cyber- Grooming, irreführende oder gefährliche Information, falsche Identität, arglistige Links oder Nachrichten.



Kapitel 5 – Kommunikation

5.1.1 – Die Funktionsweise von E-Mail und dessen Verschlüsselung

5.1.2 – 5.1.3 – Digitale Signatur in E-Mails

Verschlüsselte Daten, die Dokumenten oder E-Mails beigefügt sind und wie eine eigenhändige Unterschrift die Authentizität des Erstellers bzw. Absenders nachweisen.
Eine digitale Signatur verleiht elektronisch übermittelten Dokumenten je nach Signaturverfahren und Art des signierten Dokuments (bzw. der Nachricht) Rechtsgültigkeit.
Die digitale Signatur macht es unmöglich, das die originale Nachricht von Dritten verändert werden kann.

Signaturwert	KPL89mlL7gHkdJHGN4Da0mxtAydcSVVUtknb183ZnXRwYFfEbPt1ZR1EDcBFxmy1+SWu7/aYedcEsEXWk7nO9A==	
SIGNATURINFORMATIONEN	**Unterzeichner**	Mag. Ulrich Wolfgang Latzenhofer
	Aussteller-Zertifikat	CN=a-sign-premium-mobile-03,OU=a-sign-premium-mobile-03,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	408737
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-atrust-1.0:ecdsa-sha256:sha256:sha256:sha1
Prüfinformation	Signaturpruefung unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß § 4 Abs. 1 Signaturgesetz einem handschriftlich unterschriebenen Dokument grundsätzlich rechtlich gleichgestellt.	
Datum/Zeit-UTC	2013-03-20T09:21:35Z	

5.1.4 – 5.1.6 – Digitale Signatur in E-Mails

ECDL Syllabus

Sich der Möglichkeit bewusst sein, arglistige und unerwünschte E-Mails zu erhalten.

Sich der Gefahr bewusst sein, dass ein Computer mit Malware infiziert werden kann:
Beim öffnen eines Attachments(E-Mail-Anhang)
Makroviren in Officedateien
Beim öffnen eines ausführbaren Datei (.exe)

Den Begriff Phishing verstehen; typische Merkmale von Phishing kennen, wie:

Verwendung der Namen von seriösen Unternehmen und Personen
Links zu gefälschten Websites

Kapitel 5.2 – Instant Messaging

5.2.1 – 5.2.2 – Den Begriff Instant Messaging verstehen & Schwachstellen

5.2.3 – Sicherheit bei IM

Methoden kennen, um beim Gebrauch von IM Vertraulichkeit sicherzustellen, wie:

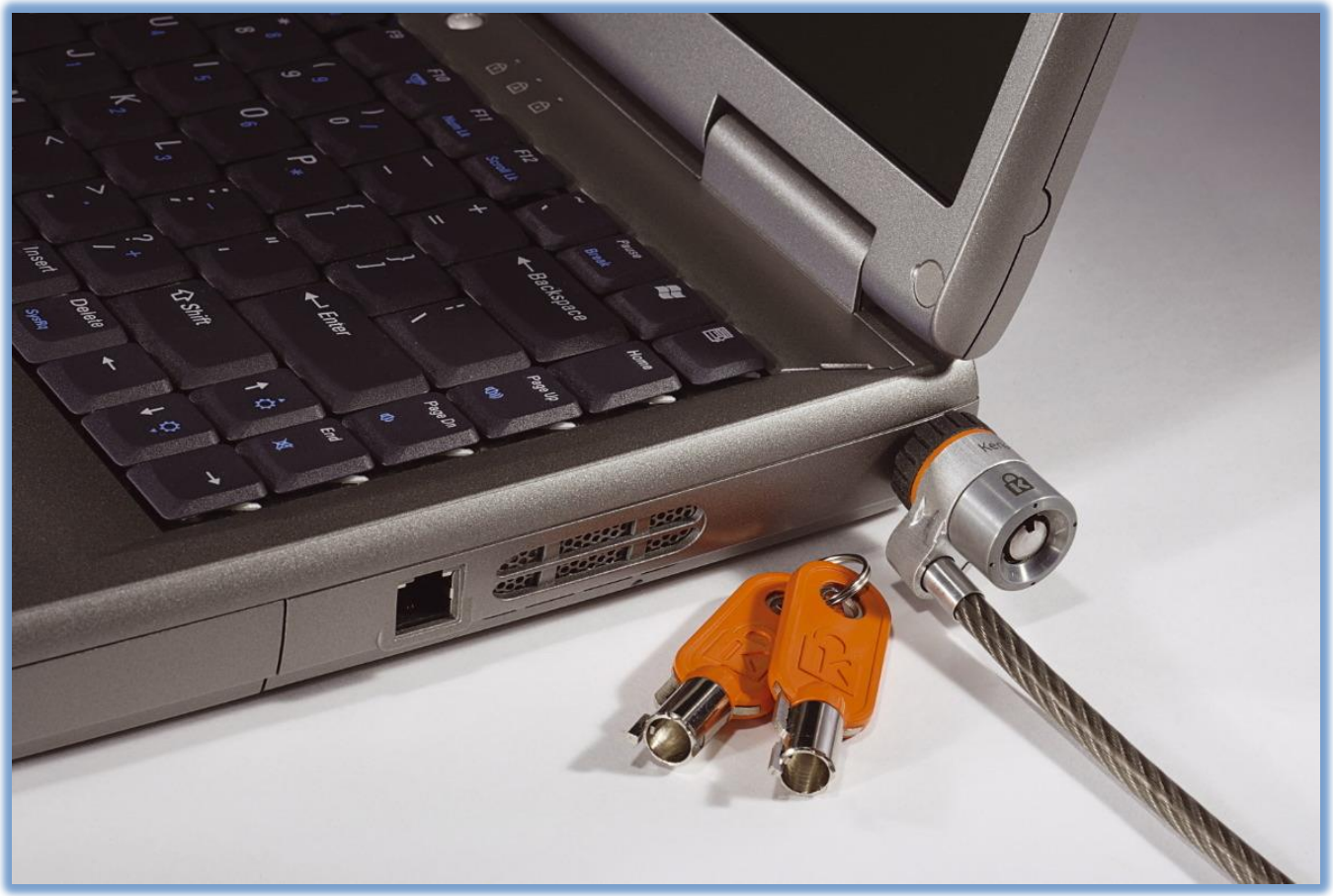
Verschlüsselung
Nicht-Veröffentlichung von wichtigen Informationen
Zugriff auf Daten einschränken

Kapitel 6 – Sicheres Datenmanagement

6.1.1 – Physische Sicherung von Geräten

Inventarisierung

6.1.1 – Physische Sicherung von Geräten



Sicherungskabel (z.B. Kensington Lock)

6.1.1 – Physische Sicherung von Geräten

Zugangskontrolle / Authentifizierung

6.1.2 – Sicherung von Daten (Backups) – Verlust von Daten

6.1.3 – 6.1.4 – Modernes Backup-Konzept

Ein Konzept für Datensicherung:

- Regelmäßigkeit
- Häufigkeit
- Zeitpunkt und Ablaufsplanung
- Verschiedene Speicherorte

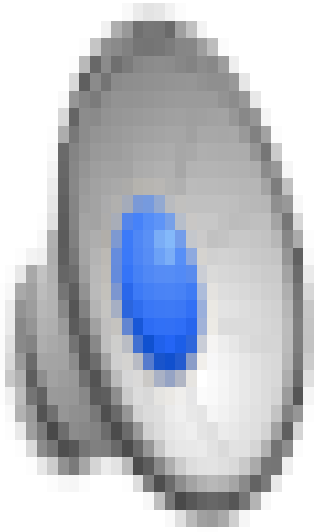
6.1.5 – Daten / Backup wiederherstellen und überprüfen

Kapitel 6.2 – Datenvernichtung

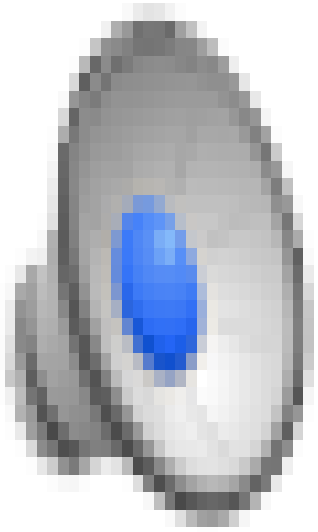
Kapitel 6.2 – Datenvernichtung

Löschen != Vernichten

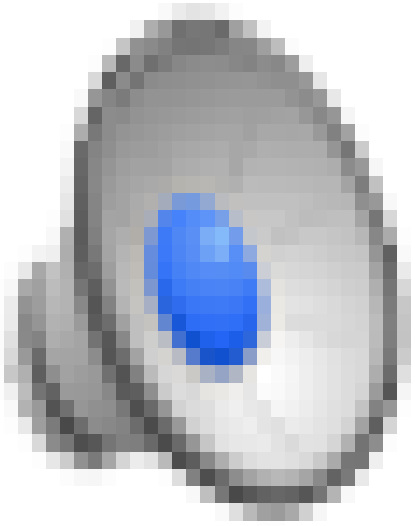
6.2 – Inside of a Hard Drive



6.2 – Festplatten shreddern



6.2 – Festplatten entmagnetisieren



!!! ES IST VOLLBRACHT !!!