Foliensatz Wirtschaftsinformatik

Lehrveranstaltungsinhalte

Termine	Inhalte	Kapitel	Textbuch-Seiten
1. LV-Termin	• Einführung • Informationssysteme in Wirtschaft und Gesellschaft • Geschäftsprozessmanagement	1, 2	1 – 56 57 – 96
2. LV-Termin	• Modellierung betrieblicher Informationssysteme • Unterstützung betrieblicher Leistungsprozesse durch ERP-Systeme	3, 4	97 – 134 135 – 188
3. LV-Termin	• Außenwirksame Informationssysteme und Electronic Commerce • Managementunterstützungs-systeme	5, 6	189 – 266 267 – 316
4. LV-Termin	• **Planung, Entwicklung und Betrieb von Informationssystemen** • **Informationssicherheit und Datenschutz**	**7, 8**	**317 – 368** **369 – 422**
5. LV-Termin	• Datenspeicherung • Rechnersysteme	9, 10	423 – 494 495 – 539

Kapitel 8

Informationssicherheit und Datenschutz

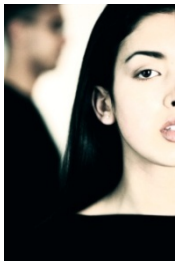
Wiederholungsfrage Kapitel 8

Ein Angreifer liest in der veröffentlichen Firmenzeitschrift des Unternehmens X, dass einer der Manager sich sehr für Corporate-Social-Responsibility (abgekürzt: CSR) einsetzt. Da eine bekannte Website für CSR nicht sonderlich gut abgesichert ist, attackiert der Angreifer diese Website und installiert dort Fallen, um letztendlich in das Firmennetzwerk von X einzudringen.

- Ist dies möglich?
- Wie heißt diese Form des Angriffs?
- Wie kann man als Unternehmen diesen Angriffen entgegenwirken?

Sicherheitstechnische Grundlagen

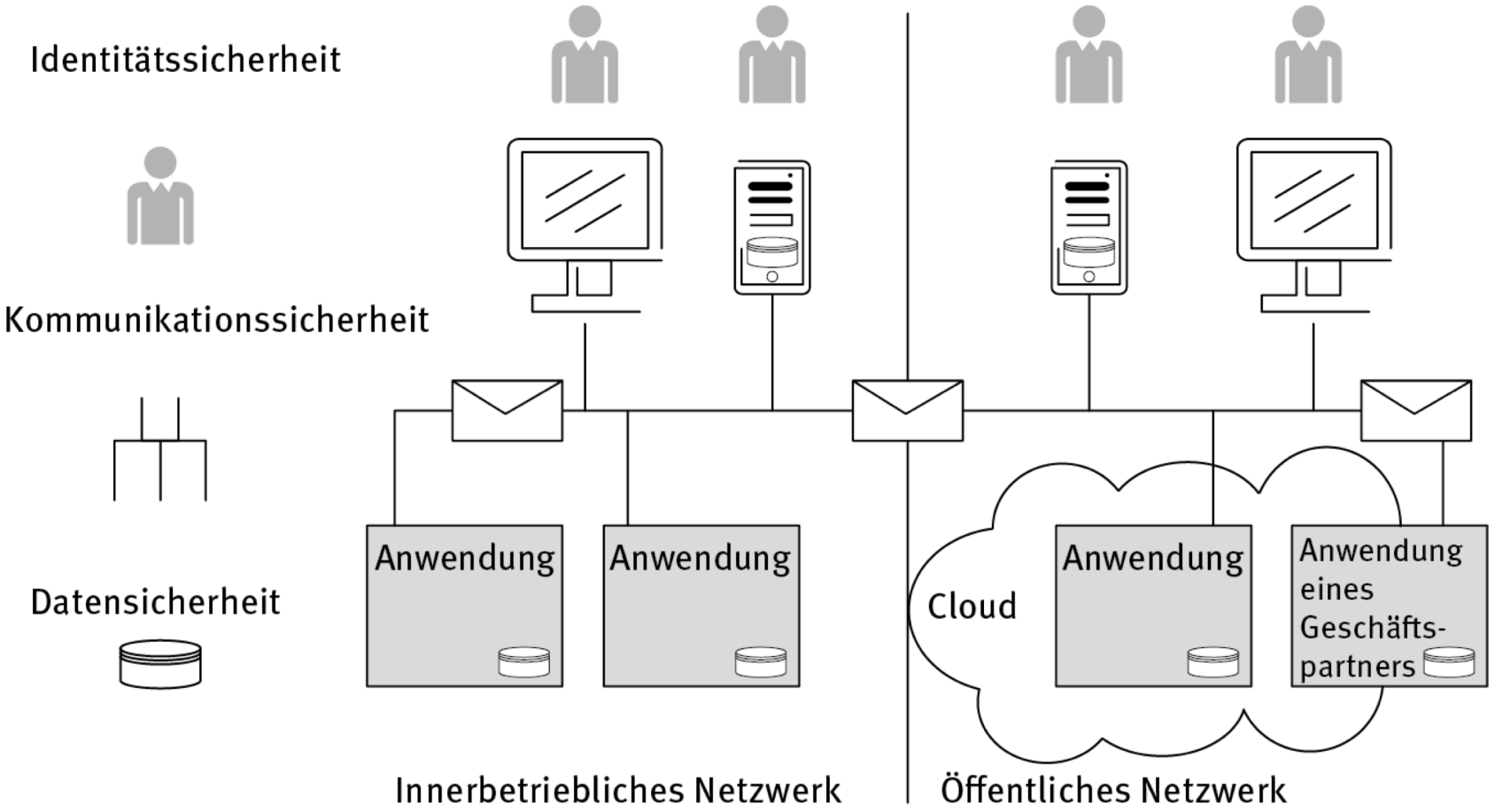
- Datensicherheit (engl.: data security)
  - Verhinderung von
    - Datenverlust
    - Datendiebstahl
    - Datenverfälschung
  - Gewährleistung von
    - Vollständigkeit
    - Korrektheit der Daten



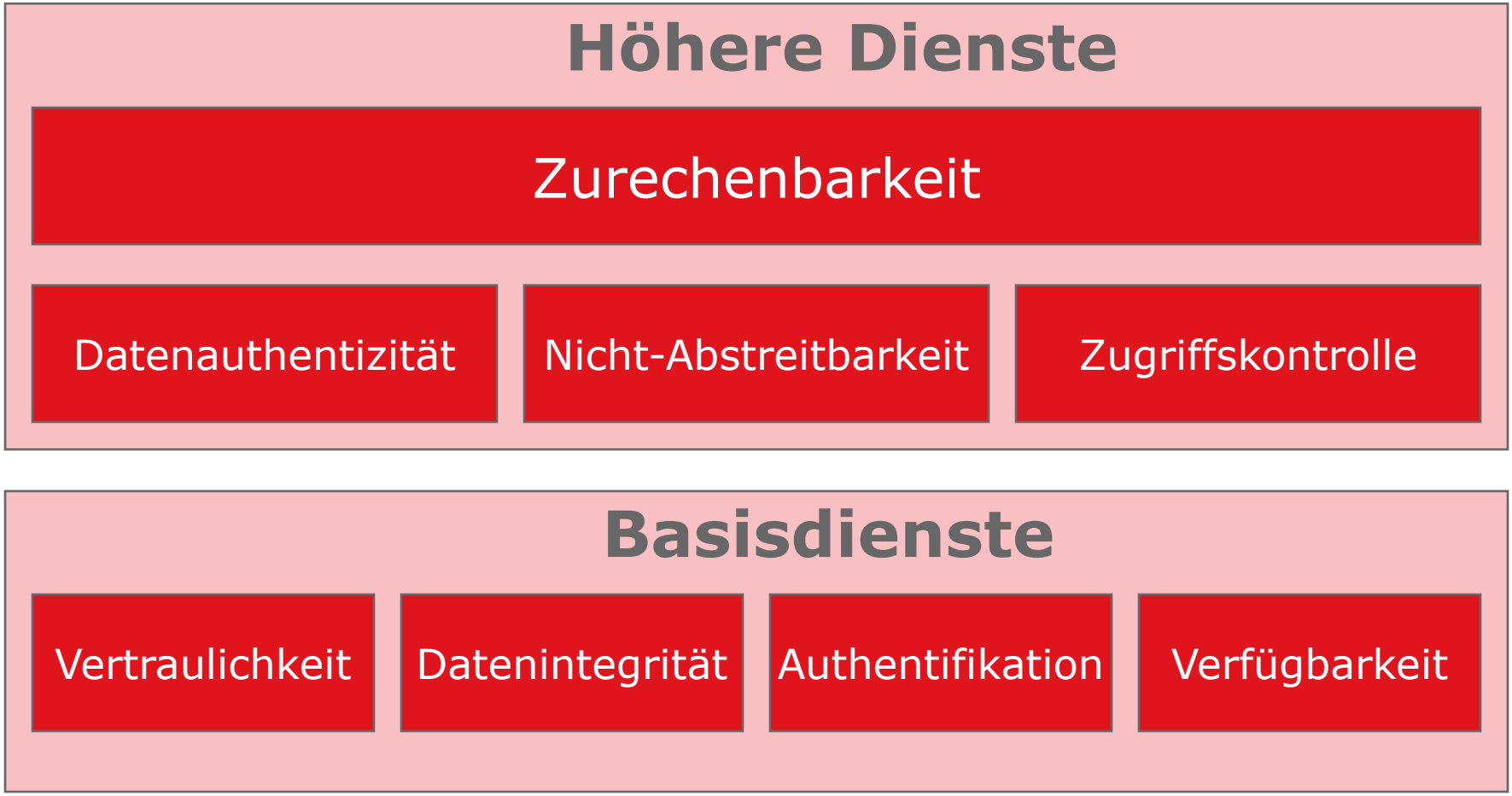
- Datenschutz (engl.: privacy)

  Gesamtheit der gesetzlichen und betrieblichen Maßnahmen zum Schutz der Rechte von Personen vor Verletzung der Vertraulichkeit und der Sicherheit des Informationshaushalts

Aufgaben der Informationssicherheit



Sicherheitsziele und Dienste



Sicherheitsdienste
Basisdienst: Vertraulichkeit

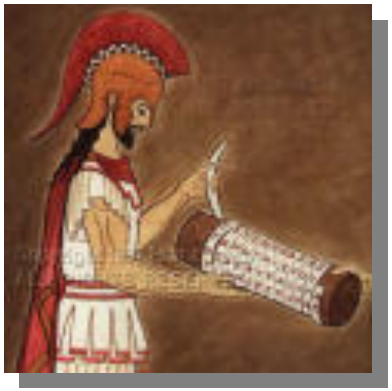
Vertraulichkeit

- Ziel: verhindern, dass geheime Information für unberechtigte Dritte zugänglich wird
- Verfahren: **Verschlüsselung**

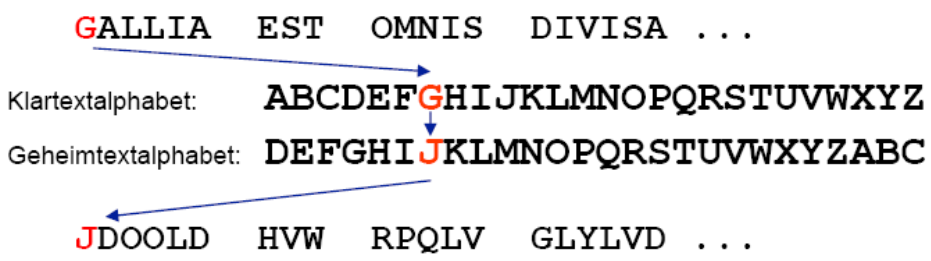
Algorithmus, der aus einem Schlüssel und einem Klartext eine scheinbar sinnlose Zeichenfolge erzeugt, die durch die Anwendung eines zweiten Schlüssels wieder in den Klartext umgewandelt werden kann

Algorithmen: Symmetrische und asymmetrische Verschlüsselung

Herstellung von Vertraulichkeit
Historische Kryptographie



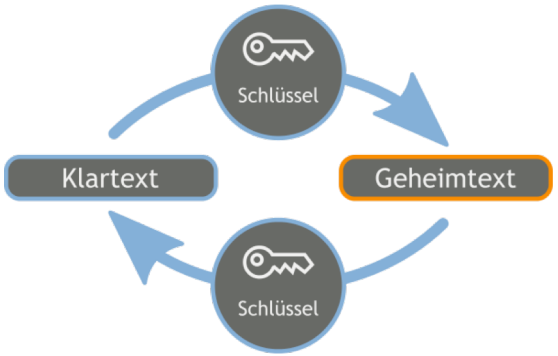
Skytale von Sparta (etwa 500 v. Christus)



Caesar-Verschlüsselung
(Julius Cäsar 100 – 44 v. Chr.)

Enigma Verschlüsselung
(Arthur Scherbius, 1878-1929)

Sicherheitsverfahren **Verschlüsselung**



- Symmetrische Verfahren (Beispiele)
  - Ver- und Entschlüsselung mit dem selben Schlüssel
    - DES (Data Encryption Standard): fixe Schlüssellänge 56 Bit
    - Triple-DES: Fixe Schlüssellänge 168 Bit
    - RC2, RC4 (ursprünglich „trade secrect"): keine fixe Schlüssellänge (diverse Lücken, in SSL nicht mehr erlaubt)
    - IDEA (ETH Zürich): fixe Schlüssellänge 128 Bit

- Asymmetrische Verfahren

  Schlüsselpaare (privater und öffentlicher Schlüssel): unterschiedliche Schlüssel für Ver- und Entschlüsselung
  - **Privater Schlüssel** verlässt nicht den Rechner des Besitzers, **öffentlicher Schlüssel** ist allgemein bekannt
  - Wichtigstes Verfahren: RSA
    Variable Schlüssellänge (2048 Bit sicher bis 2030, danach > 3072 Bit)

Möglicher Angriff gegen **Verschlüsselung**

- Brute-Force-Angriff zur Schlüsselerlangung
  - Durchprobieren von allen möglichen Schlüsselkandidaten
  - Wörterbücher

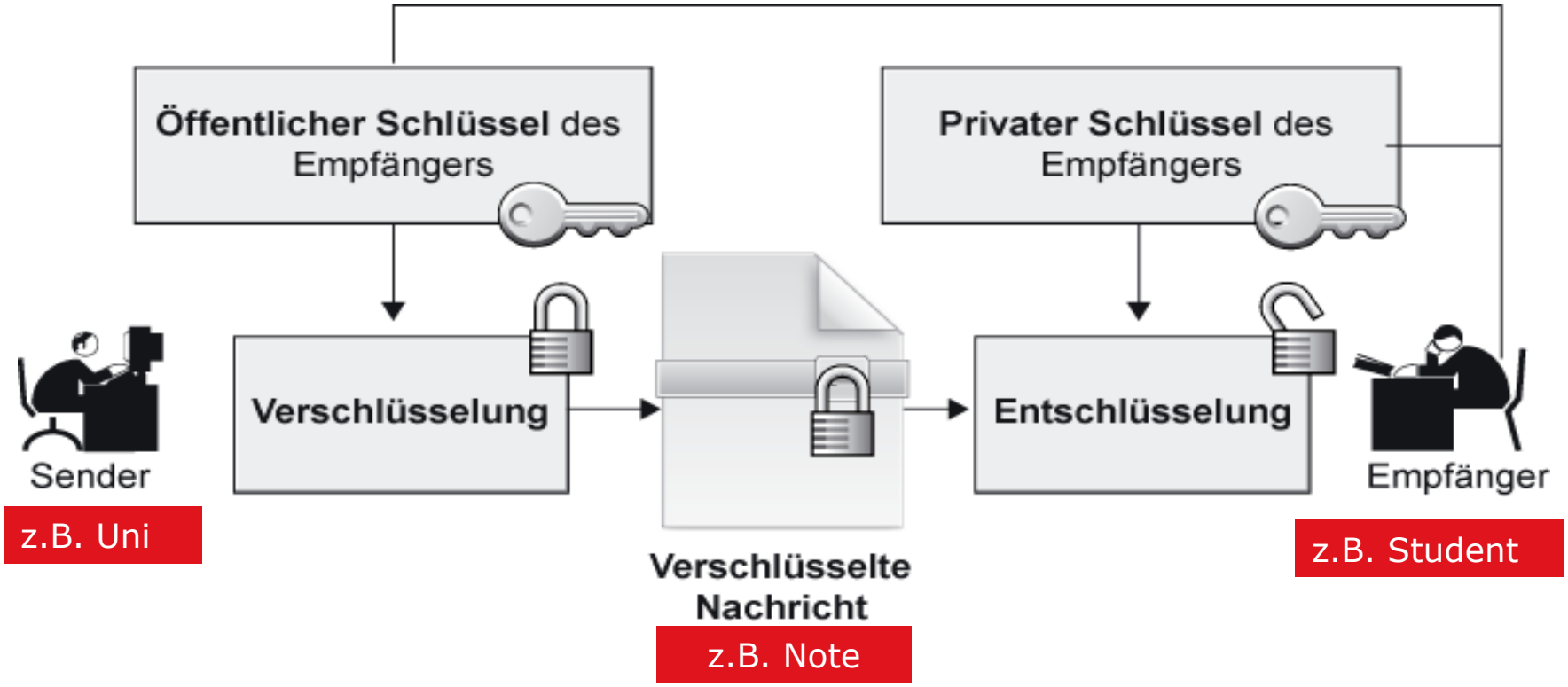
Stellen der Zahl	**Rechenoperationen**	**Rechenzeit (Annahme: eine Operation = 10^{-6} Sekunden)**
50	$1{,}4 \times 10^{10}$	3,9 Stunden
70	$9{,}0 \times 10^{12}$	104 Tage
100	$2{,}3 \times 10^{15}$	74 Jahre
200	$1{,}2 \times 10^{23}$	$3{,}8 \times 10^{9}$ Jahre

- Andere Möglichkeiten
  - Spionage, Unachtsamkeit, ...

Sicherheitsverfahren
Vertraulichkeit durch asymmetrische Verschlüsselungsverfahren

Eine mit einem **öffentlichen** Schüssel verschlüsselte Nachricht kann nur mit zugehörigem **privaten** Schlüssel entschlüsselt werden

Nur der Besitzer des **privaten** Schlüssels kann die Nachricht dekodieren

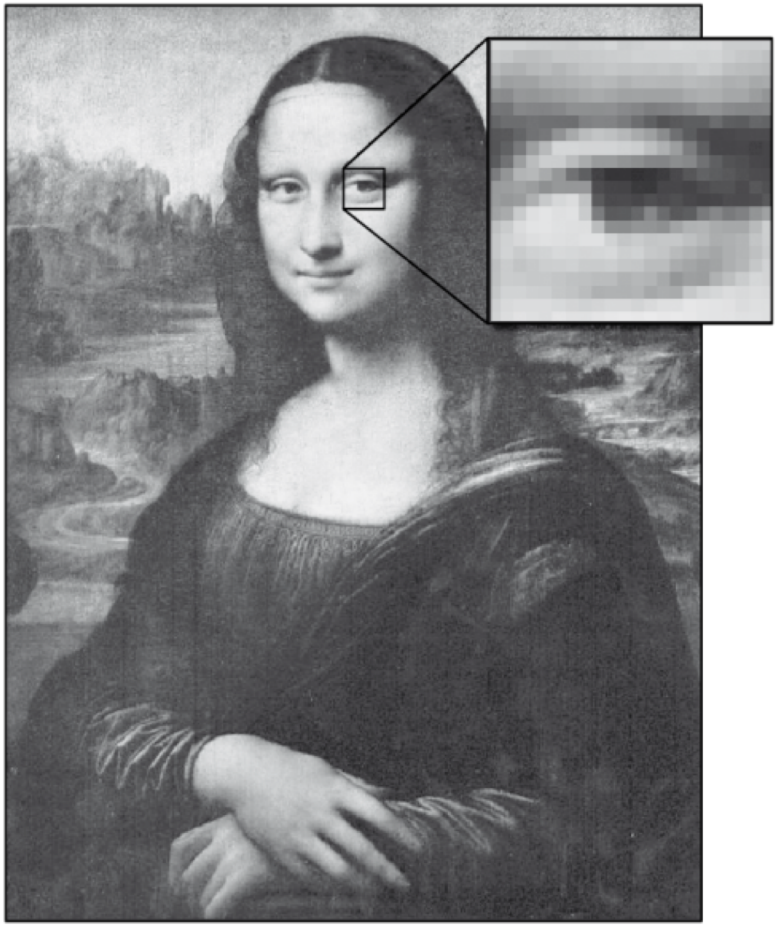


z.B. Uni

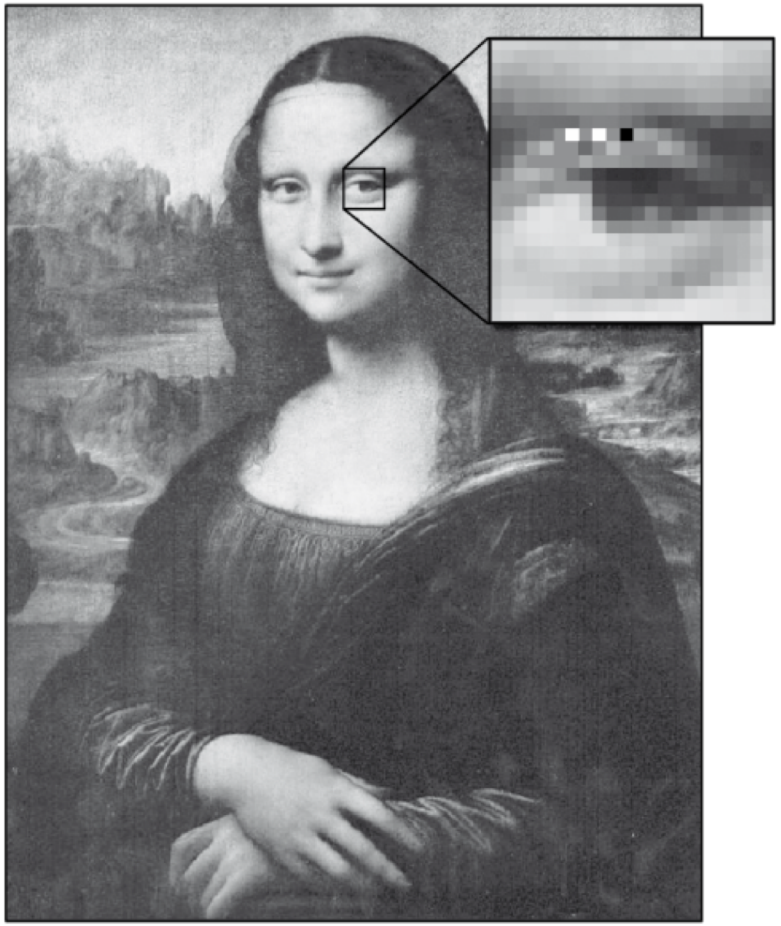
z.B. Student

z.B. Note

Steganografie



Ohne steganografische Information



Mit steganografischer Information

Sicherheitsdienste
Basisdienst: Datenintegrität

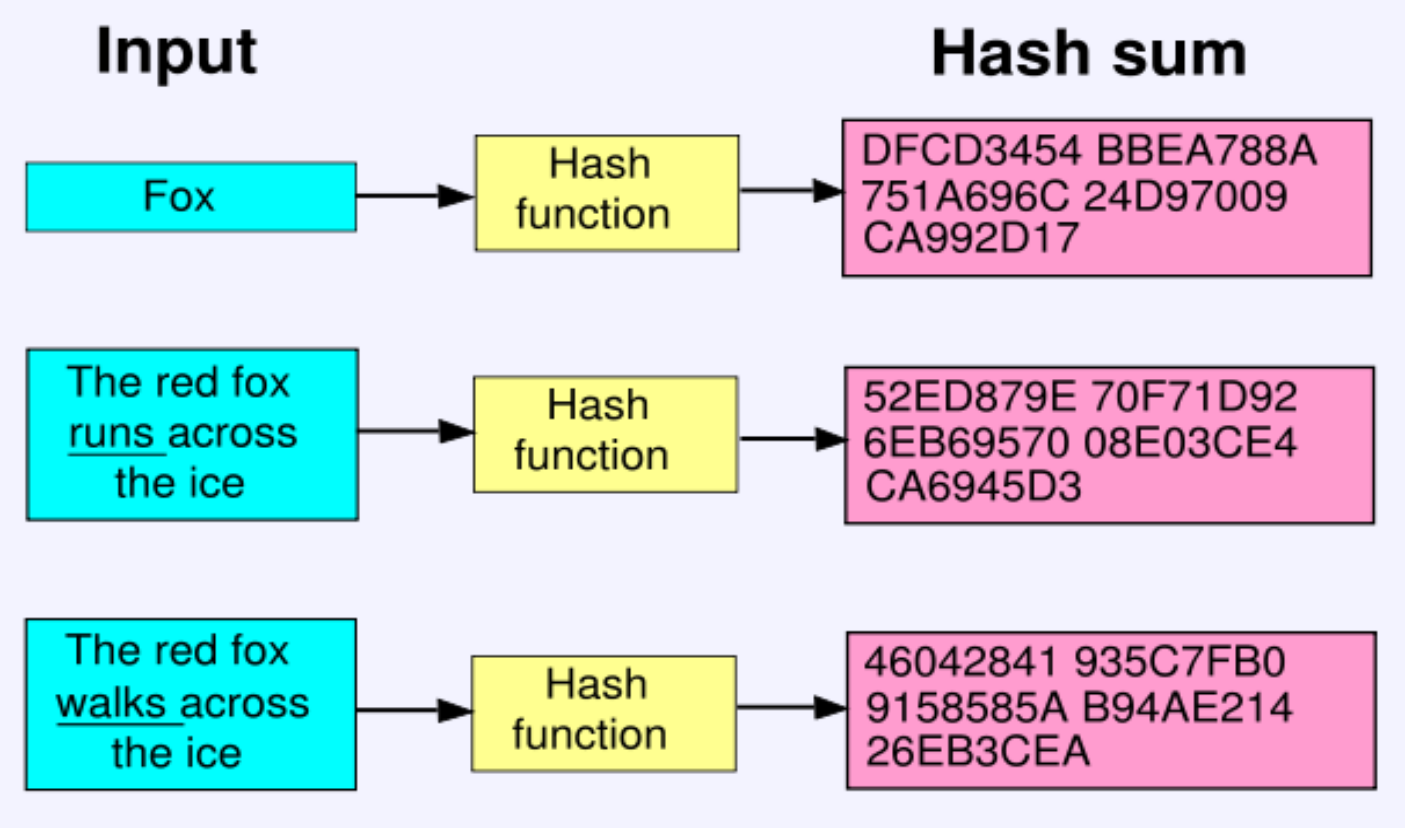
- Datenintegrität (Unverändertheit, kurz: Integrität)
  - Ziel: garantieren, dass Daten in unveränderter Form (im „Originalzustand“) vorliegen
  - Verfahren: Hash-Funktionen

Einweg-Funktion, die aus beliebigen Daten einen **Hash-Wert** in der Länge von meist 128 oder 160 Bit erzeugt, aus dem die Daten **nicht rekonstruiert** werden können. Bei jeder Veränderung der Daten verändert sich auch der Hash-Wert („Elektronischer Fingerabdruck“).

Algorithmen: MD5 (128 Bit† 2010), SHA1 (160 Bit†),
SHA2 (224-512 Bit),
SHA3 (224-512 Bit, Aug 1015)

Verfahren:

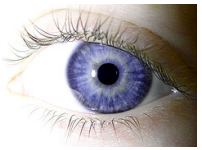
Hash-Funktionen (SHA 1)



Datenmenge des Ergebnisses des Hash-Funktion ist **unabhängig** von der Länge der Eingabe.

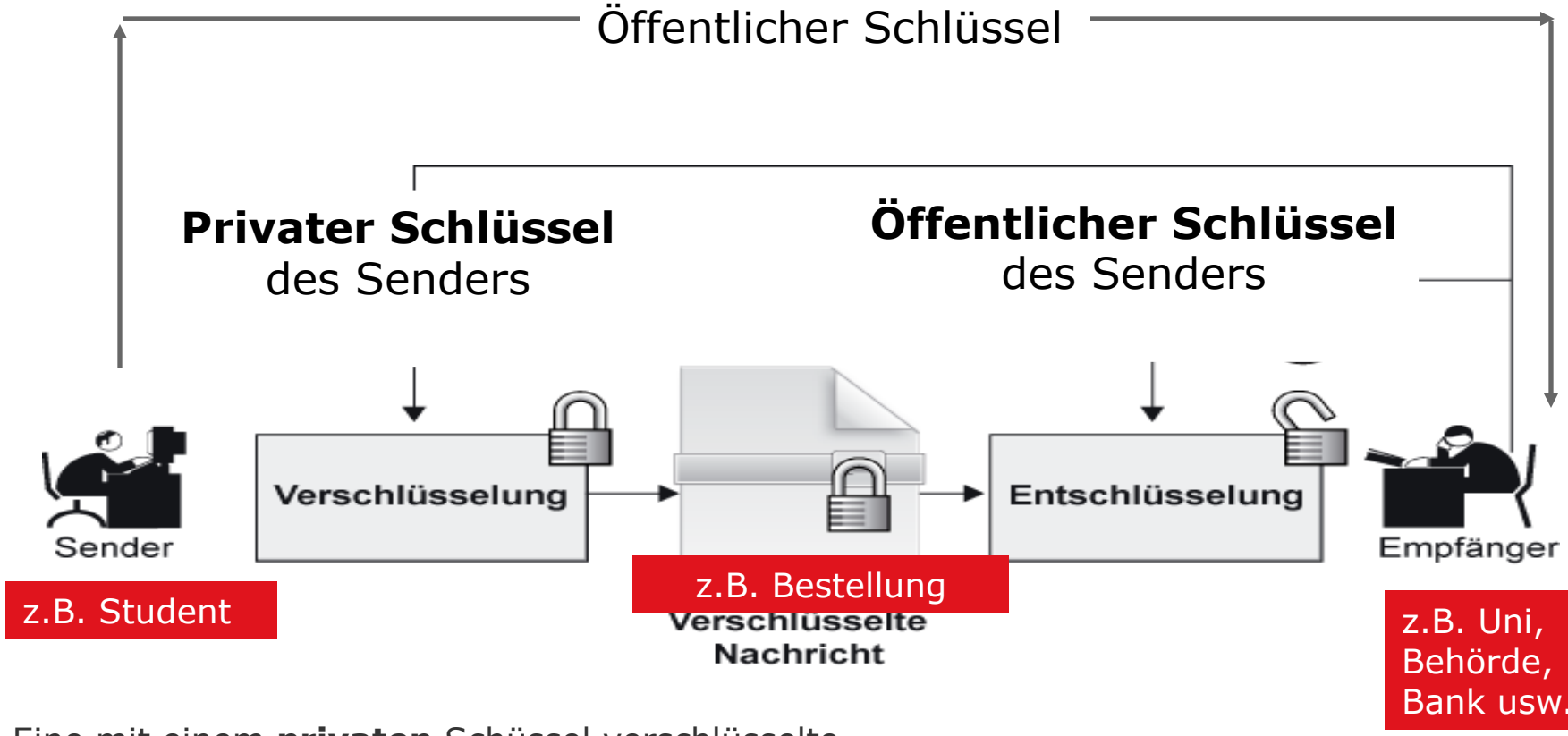
Sicherheitsdienste
Basisdienst: Authentifikation

- Authentifikation
  - Ziel: Prüfung der Identität eines Benutzers
  - Verfahren:
    - Kenntnis eines **Geheimnisses**
      Beispiel: Kennwort (engl.: pass word)
    - Besitz eines **Gegenstandes**, der nicht weiter gegeben werden darf und schwer duplizierbar ist
      Beispiele: Autoschlüssel, Chipkarte, privater Schlüssel
    - **Körperliche Merkmale** (biometrische Verfahren)
      Beispiele: Fingerabdruck, Geometrie der Hand, Netzhaut, Iris, Gesichtsform, Stimme



Sicherheitsverfahren

Authentfikation durch asymmetrische Verschlüsselungsverfahren



Eine mit einem **privaten** Schüssel verschlüsselte Nachricht kann nur mit *zugehörigem* **öffentlichen** Schlüssel entschlüsselt werden

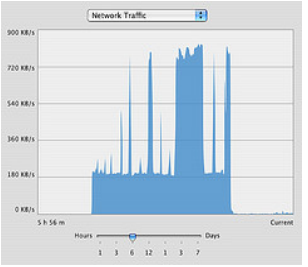
Nur der Besitzer des **privaten** Schlüssels kann die Nachricht geschickt haben

Sicherheitsdienste
Basisdienst: Verfügbarkeit

- Verfügbarkeit
  - Ziel: Gewährleistung, dass Dienste den berechtigten Benutzern stets zur Verfügung stehen
  - Attacken:
    - **Denial-of-Service-Attacke (DoS)**

      Ein Server wird mit „sinnlosen" Anfragen überflutet, sodass er seiner ursprünglichen Aufgabe nicht (oder nicht im vollen Umfang) nachkommen kann (Verweigerung des Dienstes)

    - Spezialfall: Distributed-Denial-of-Service-Attacke (DDoS)
    - Besonders problematisch für E-Commerce-Anwendungen



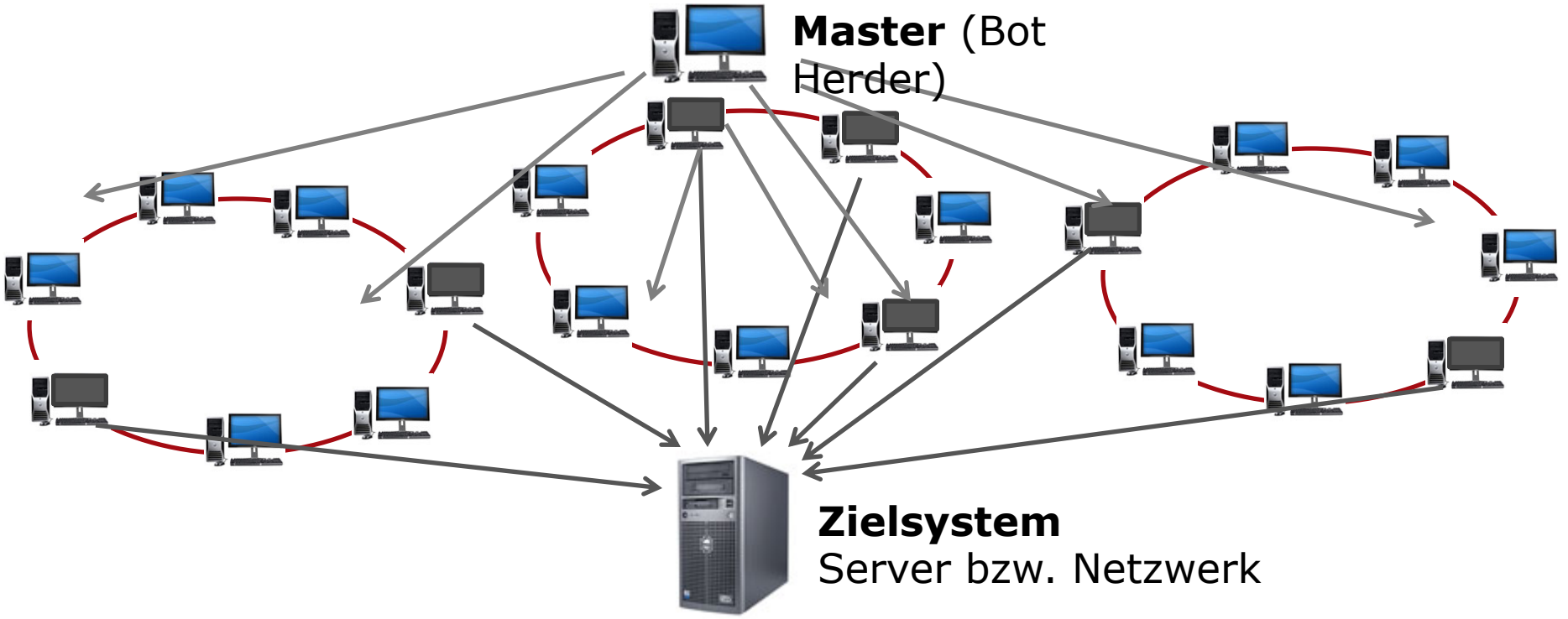
  - Maßnahmen:
    - Erkennen von atypischen Nutzungsmustern
    - Beschränkung der Ressourcenzuweisungen an einzelne Benutzer

DDoS-Attacke

Internet Bot (Abkürzung für engl.: software robot) = Programm, das Aufgaben automatisiert

Botnet: Zahlreiche Rechner werden ferngesteuert, meist ohne Wissen des Benutzers („Zombie Computer")

1. Installation eines Bots (DDoS-Trojanisches Pferd)
2. Signal zur Auslösung des Angriffs



Beispiele von DDOS-Angriffen:

Botnet Mariposa (2010)

- Im Jahr 2010 von spanischen Behörden aufgedeckt
- Das Botnetz umfasste mehr als 12 Millionen Rechner in mehr als 190 Ländern.
- Zu den befallenen Rechnern gehörten Rechner von etwa der Hälfte der 1.000 größten Unternehmen der USA (lt. US Fortune,

Botnet Mirai (2016)

- Besteht aus 800.000+ Mio gekaperten „Smart Devices“, Home-Router, IP-Kameras, TV-Boxes, ...
- **Okt 2016:** Angriff auf Dyn (DNS-Anbieter) hat zur Folge, dass Twitter, Netflix, Paypal, Spotify vorallem in USA einen Tag nicht mehr nutzbar waren
- **Nov 2016:** Gesamte Online-Anbindung des afrikanischen Landes Liberia massiv beeinträchtigt
- **Juli 2018:** zumindest 13 Versionen im Umlauf!

Sicherheitsdienste
Höhere Dienste

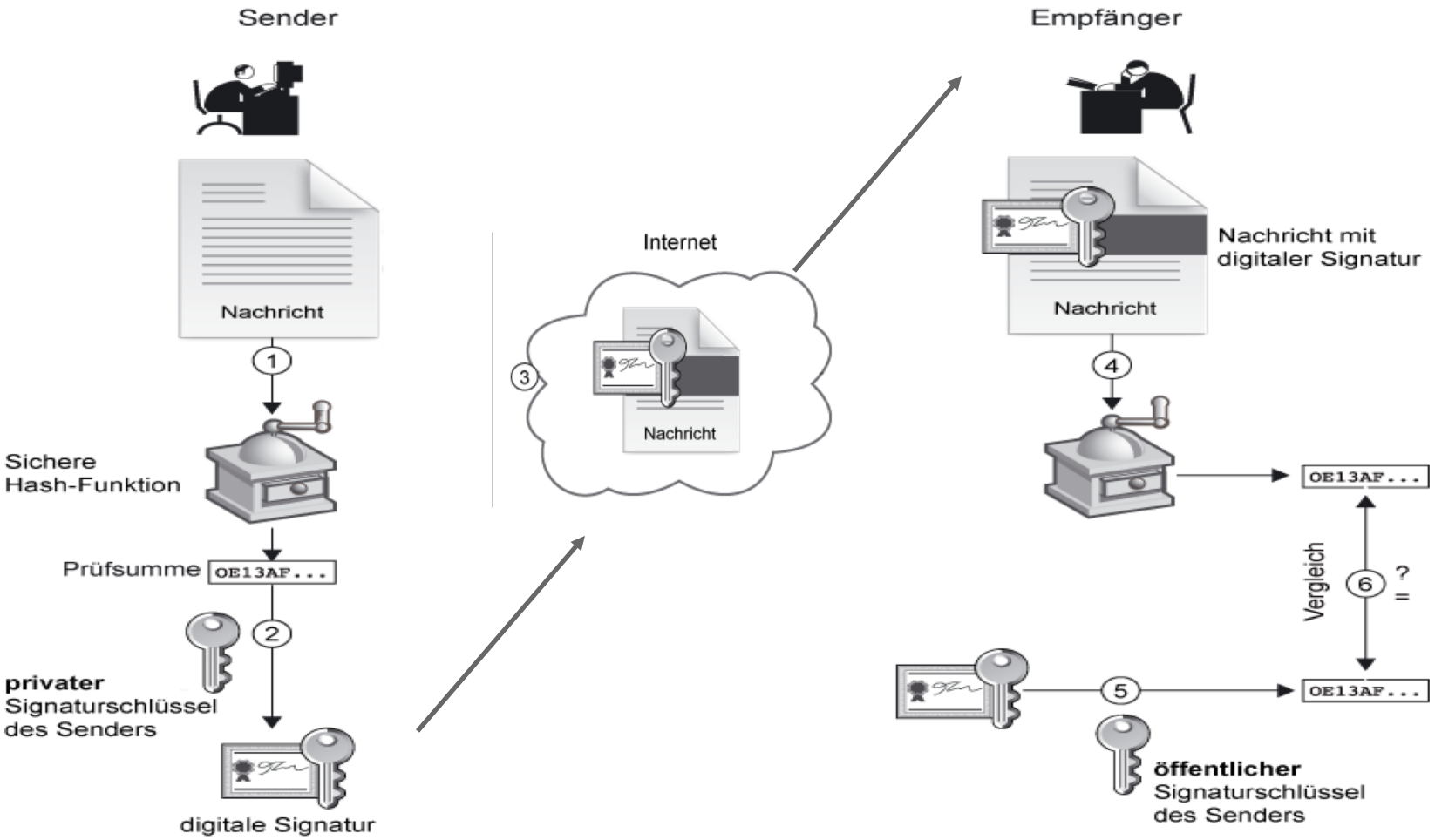
- Datenauthentizität
  - Ziel: nachweisliche Garantie von Integrität und Herkunft von Information
  - Verfahren: Elektronische Unterschrift

- Nicht-Abstreitbarkeit
  - Ziel: Gewährleistung, dass weder Absender noch Empfänger das Versenden (den Empfang) einer Meldung abstreiten kann
  - Verfahren: Kombinierte Verfahren auf Basis von Authentifikation, Integrität und Bestätigungen

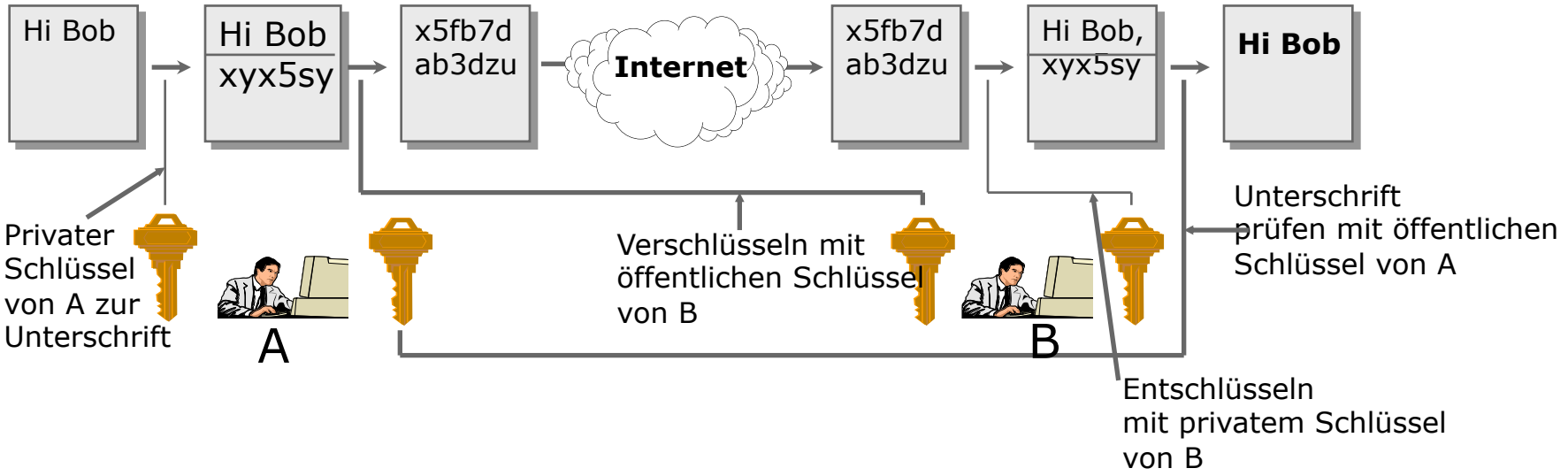
Sicherheitsverfahren **Elektronische Unterschrift (engl.: digital signature)**

- Ein kryptographisch erzeugter Nachweis („Siegel"), dass ein eindeutig identifizierter Benutzer eine digitales Dokument unterzeichnet hat
- Ziele:
  - **Integrität:** Ist ein vorliegendes Dokument in der gleichen Form unterschrieben worden oder wurde es noch später verändert?
  - **Authentifikation:** Ist das Dokument nachweislich von einer bestimmten Person unterschrieben worden?
- Lösung:
  - Verschlüsselung des **Hash-Codes** mit **privatem Schlüssel** des Unterzeichners

Elektronische Unterschrift



Sicherheitsverfahren
Elektronische Unterschrift



- Alle Probleme gelöst?
- Wie kommt ein **Absender** in einem öffentlichen Netz auf zuverlässige Weise **an den öffentlichen Schlüssel des Empfängers**?

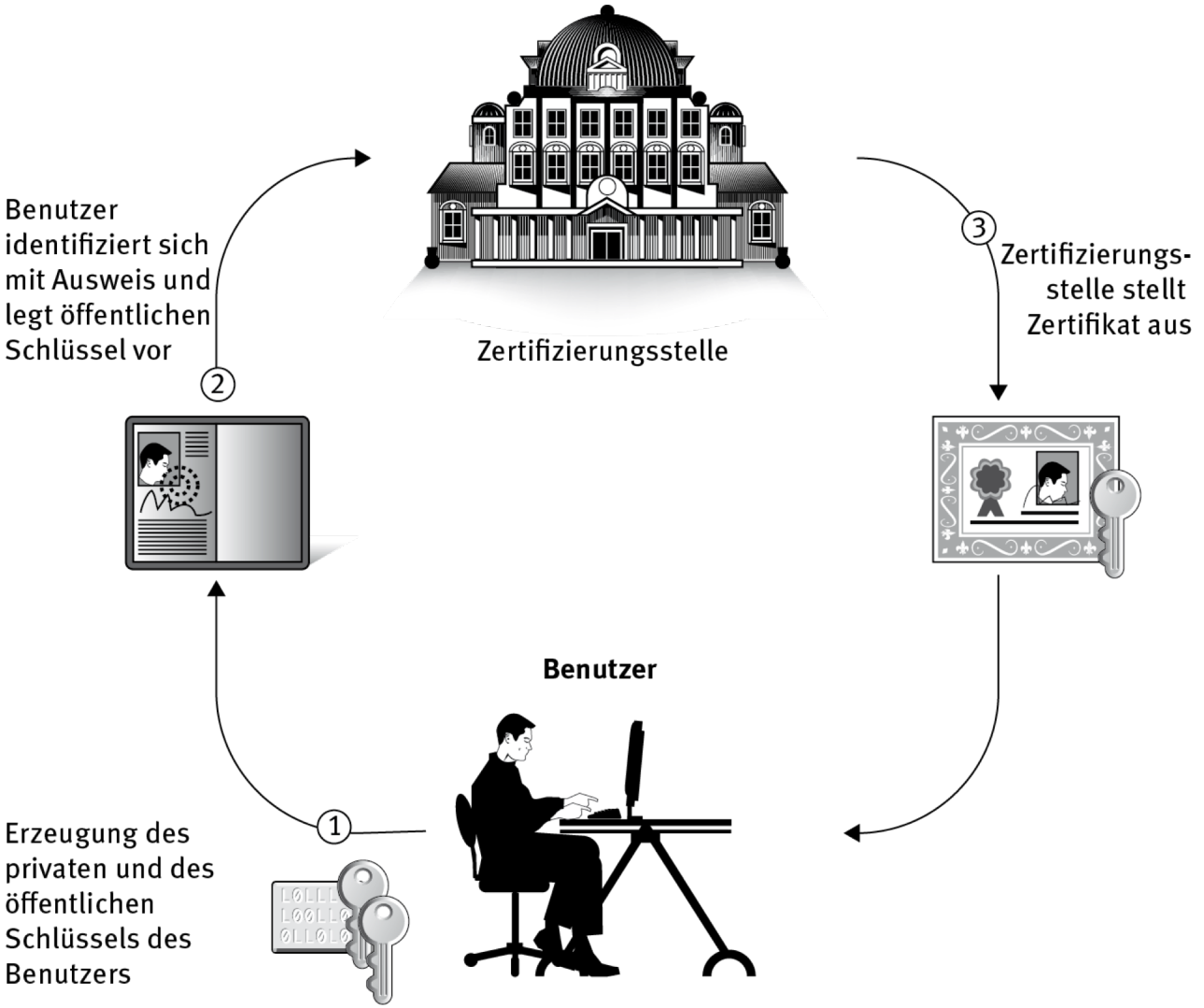
Sicherheitsverfahren
Elektronisches Zertifikat

- Vertrauenswürdige, unabhängige Instanz (Zertifizierungsstelle) bestätigt durch ihre Unterschrift, dass ein öffentlicher Schlüssel zu einer Person gehört

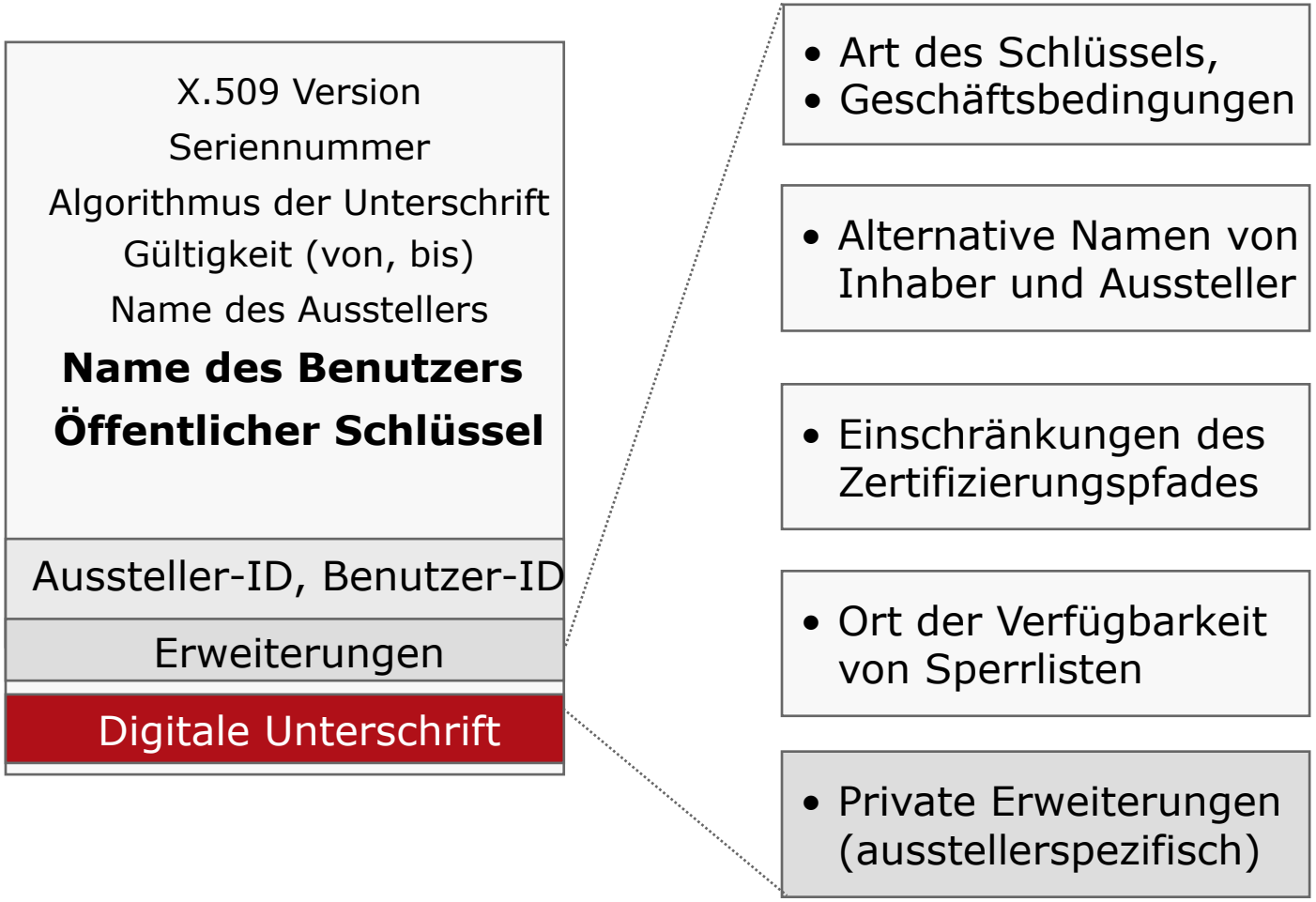
- Wesentliche Bestandteile
  - Seriennummer
  - Persönliche Daten (Name, Firmenzugehörigkeit)
  - Öffentliche Schlüssel einer Person oder Organisation
  - Unterschrift der Zertifizierungsstelle

- Beschränkte *Gültigkeitsdauer*
- Üblich: Identitäts-Zertifikate nach dem Standard X.509 Version 3

Sicherheitsverfahren
Elektronisches Zertifikat

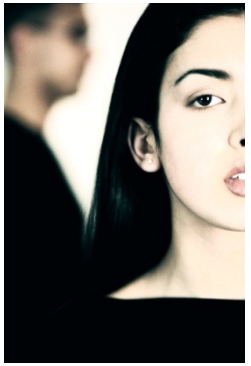


Sicherheitsverfahren
Aufbau von Zertifikaten nach ITU-T X.509



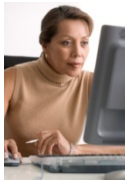
Sicherheitsdienste
Höhere Dienste

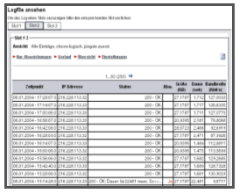
- Schutz der Privatsphäre (Datenschutz)
  - Ziel: Benutzer sollen in der Lage sein zu bestimmen, was mit ihren, das heißt, personenbezogenen Daten geschehen darf
  - Maßnahmen:
    - Juristischer Rahmen (Datenschutzgesetzgebung)
    - Verfahren zur Sicherstellung der Anonymität der Benutzer bzw. der Vertraulichkeit bei der Datenverwaltung



Sicherheitsdienste
Höhere Dienste

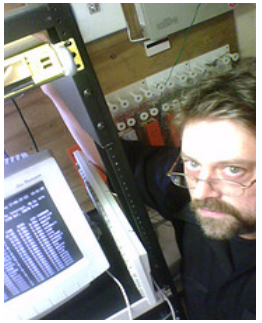
- Zugriffskontrolle
  - Ziel: Benutzer dürfen ausschließlich jene Operationen (meist: Lesen/Schreiben/Ausführen von Dateien/Programmen) verwenden, zu denen sie berechtigt (autorisiert) sind
  - Verfahren:
    - basieren auf korrekter Authentifikation von Benutzern
    - Beispiel: Rollenbasierte Zugriffskontrolle
- Zurechenbarkeit
  - Ziel: Protokollierung, welche Benutzer welche Systemressourcen in Anspruch genommen haben
  - Verfahren:
    - bauen auf Zugriffskontrolle und Nicht-Abstreitbarkeit auf
    - Wichtig beispielsweise für E-Services





Sicherheitsmanagement

- Schutz von IT-Komponenten vor Missbrauch
- Zugriffsberechtigungen für
  - Software
  - Physischer Zugang zu Rechnern, Räumlichkeiten

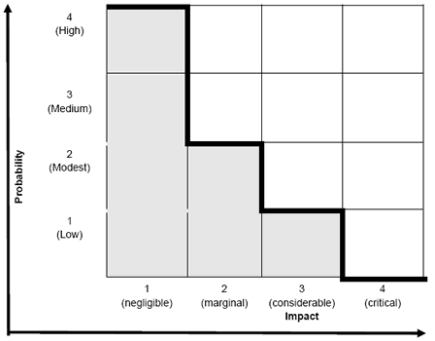


- Umgang mit
  - gezielten Angriffen
  - menschlichen Fehlern
    (beispielsweise: social engineering)

- Risikomanagement

Risikomanagement

- Früherkennung und/oder Verminderung von Risiken des IS-Betriebs, d.h. von Ereignissen, welche den Betrieb des IS gefährden
- Phasen des Risikomanagements
  - Identifikation
  - Risikoanalyse
  - Planung von Gegenmaßnahmen
- Risikoquellen
  - **Menschliche Fehler** (Bedienungsirrtümer, Nachlässigkeit usw.)
  - **Unbefugter Zugang/Zugriff** (Diebstahl und Zerstörung von Hardware usw.)
  - **Schad- und Sabotageprogramme**



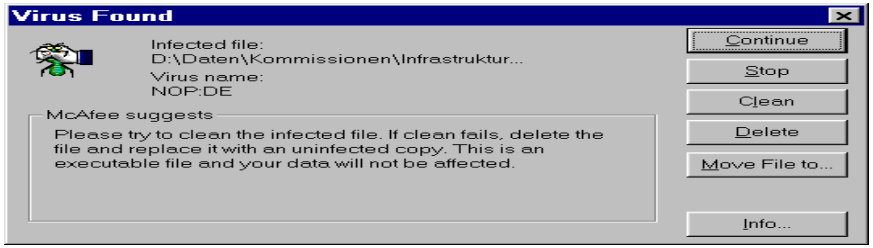
Risiko-Grafik
Quelle: QAA

Risikomanagement

Risikoanalyse durch automatisierte Tests und Echtzeitüberwachung der Zugriffs- und Berechtigungssteuerung

Risikomanagement

- Schad- und Sabotageprogramme
  - Virusprogramme
  - Wurmprogramme
  - Trojanische Pferde



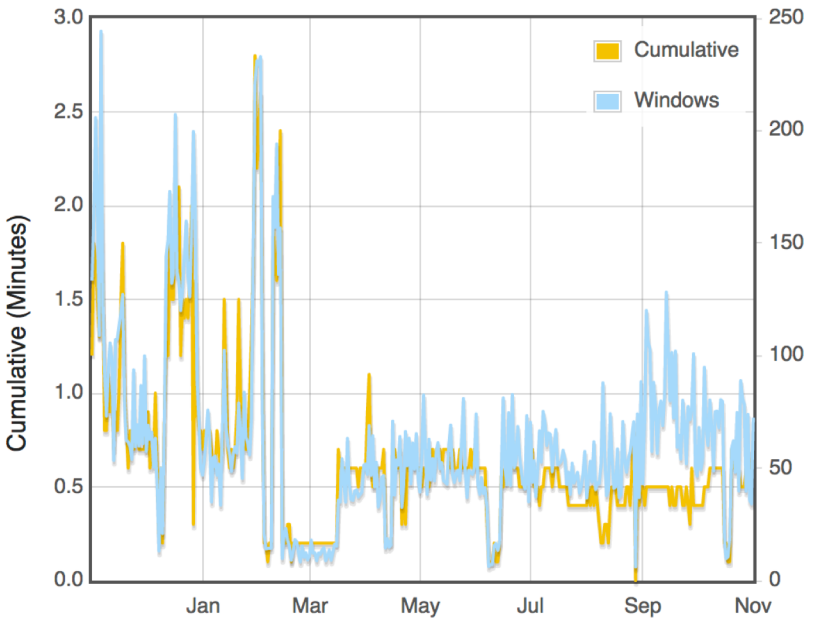
- Schutzmaßnahmen
  - Softwarebasiert: Virenerkennungssoftware, Verschlüsselung, Prüfsummen, Zugriffskontrolle
  - Organisatorisch: Sicherungskopien, Rechtemanagement usw.

Schadprogramme

- Laufende Studie des SANS-Instituts (“Survival Time Graph“):

  Durchschnittliche Zeit zwischen dem Anschluss eines (unzureichend geschützten) Rechners an das Internet zum ersten erfolgreichen Angriff:

  Meist unter 3 Minuten,
  Tendenz eher abnehmend!!
  (Dez 2017 –Nov 2018)

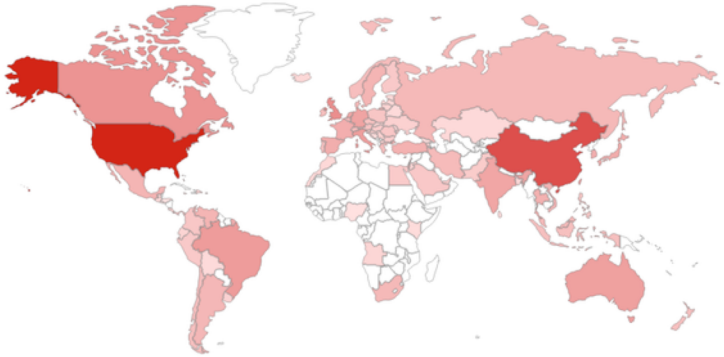


Nutzung ungewarteter Webdienste

- **Angriffswerkzeug Metasploit hackt IIS 6.0**:

  Etwa ein Prozent der weltweiten Webserver laufen mit einer verwundbaren Version von Microsofts Internet Information Services 6.0. Sie sind jetzt noch gefährdeter als bisher, denn es gibt ein Angriffs-Modul für das Exploit-Framework Metasploit.

  Der WebDAV-Dienst des Microsoft Internet Information Services (IIS) 6.0 enthält eine Sicherheits-lücke ...

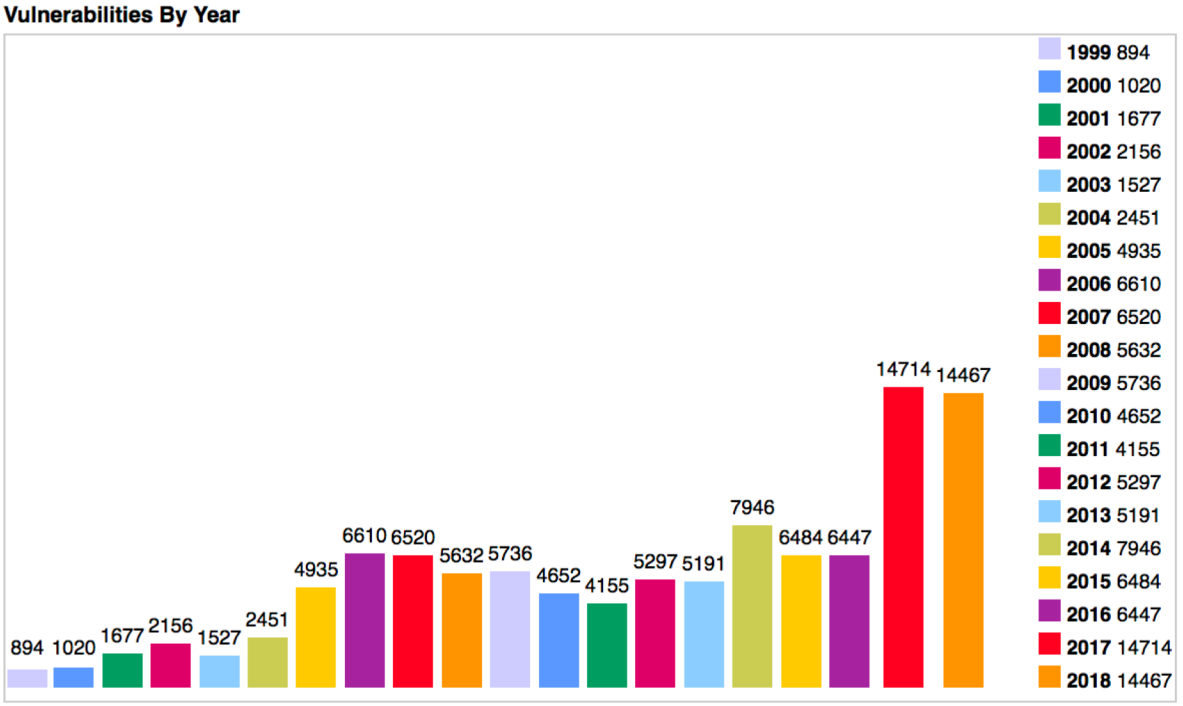
  

  Heise, April 2017

- Nutzungszahlen von IIS6: Derzeit mehr als 4Mio sites online!

Sicherheitslücken (2017)

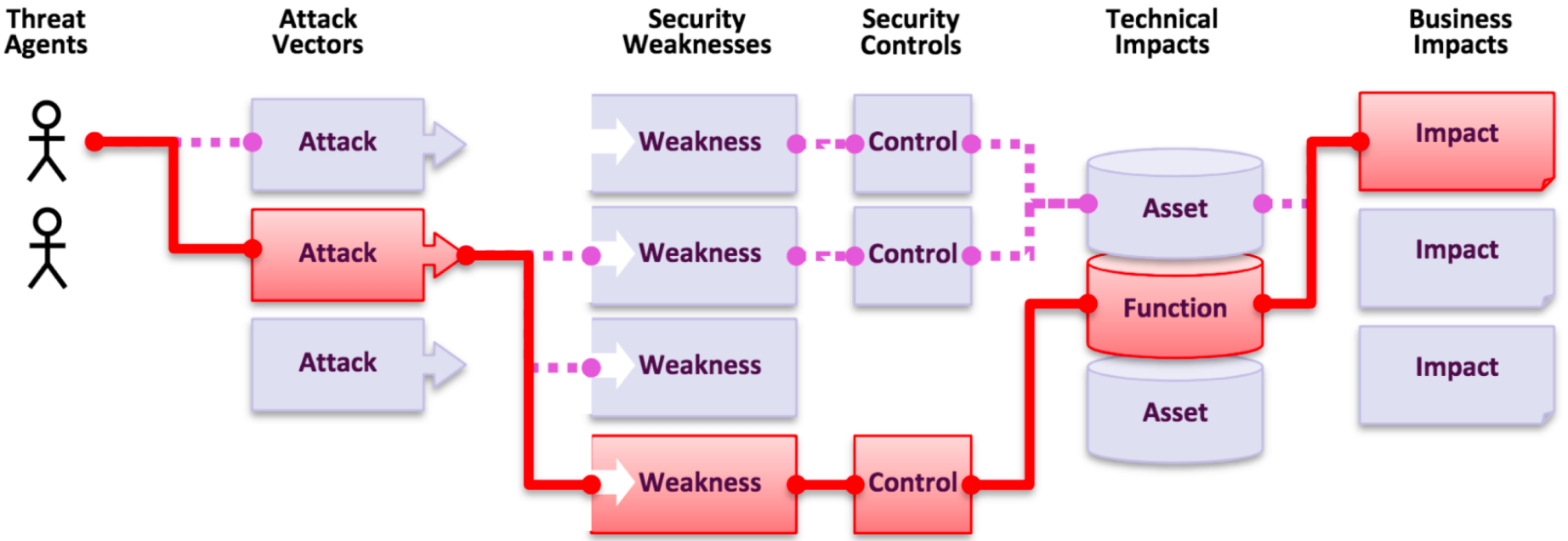
- Common Vulnerabilities and Exposures (CVE) von MITRE (non-profit Organisation für öffentliche Sicherheit)



Quelle: http://www.cvedetails.com/browse-by-date.php

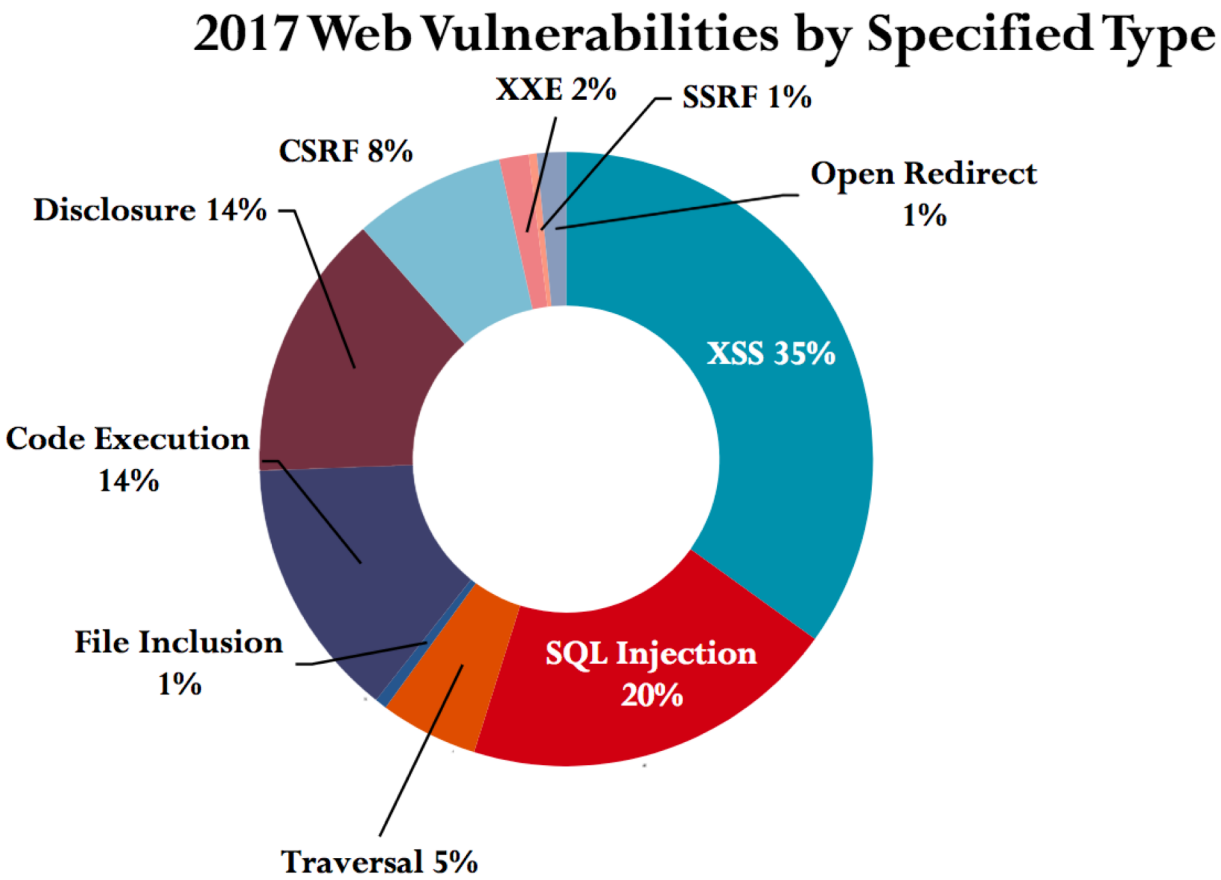
-> 2017 Rekordjahr an Sicherheitslücken

Von der Sicherheitslücke zum Schaden im Unternehmen



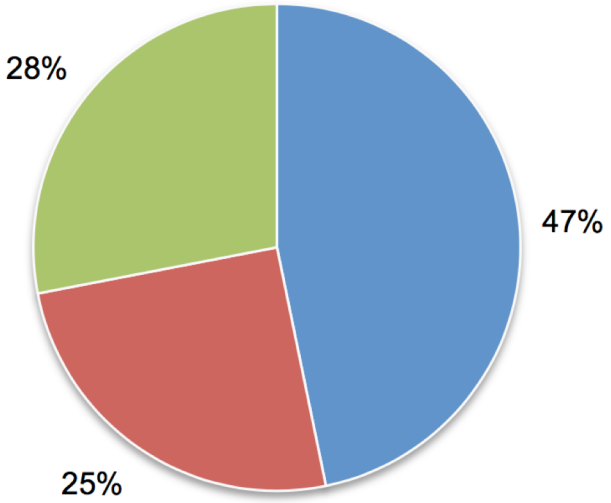
Quelle: https://github.com/OWASP/Top10/blob/master/2017/OWASP%20Top%2010%202017%20RC2%20Final.pdf

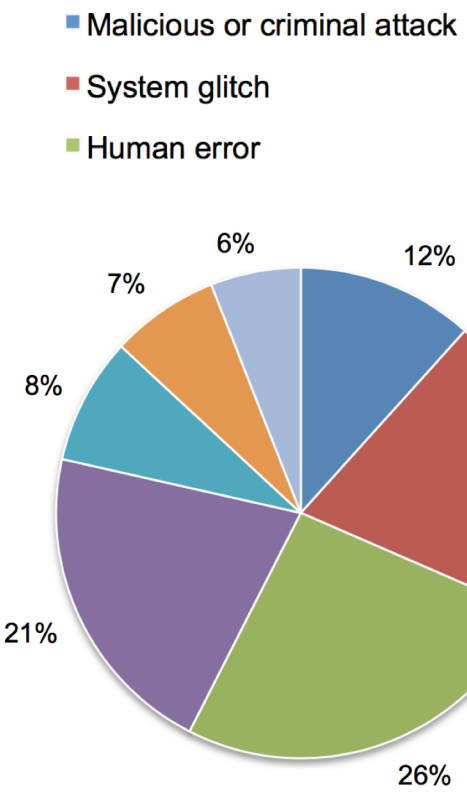
Web-Sicherheitslücken



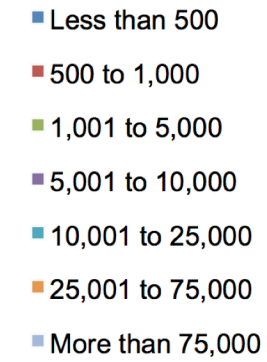
https://pages.riskbasedsecurity.com/hubfs/Reports/

Ursachen von Einbrüchen (2017)





Größe der attackierten Unternehmen



Ponemon Institute: 2017 Cost of Data Breach Study

Identitätsdiebstahl (Phishing)

Achtung! Diese Mitteilung wird von der Sicherheitsabteilung geschickt.

Sehr geehrte Kundin,
sehr geehrter Kunde,

denn Banksicherheitssystem hat einen Ausfall, viele Zutritte zu den Konten wurden verloren. Man muss sich nach der Vorschrift richten, um man Online-Banking erneuern zu kann. Man muss unter klicken und seine Angaben hineinführen, um eine Zutritt zum Konto frei zu geben. Oder Online-Banking wird nicht aktiv.

weiter zum Online-Banking

Wir vorbringen Entschuldigungen dafür. Jetzt Sicherheitsabteilung macht alles, um alle Auswirkungen zu beseitigen. Klicken bitte hier.

Mit freundlichen Grüßen,
Sicherheitsabteilung,
Deutsche Postbank AG

Zugriffskontrolle

- Zugriffskontrollmodelle in Softwaresystemen
  - Wahlfreie oder diskrete Zugriffskontrolle
  - Zentralistisch verpflichtende Zugriffskontrolle
  - Rollenbasierte Zugriffskontrolle

Zugriffskontrollmodelle

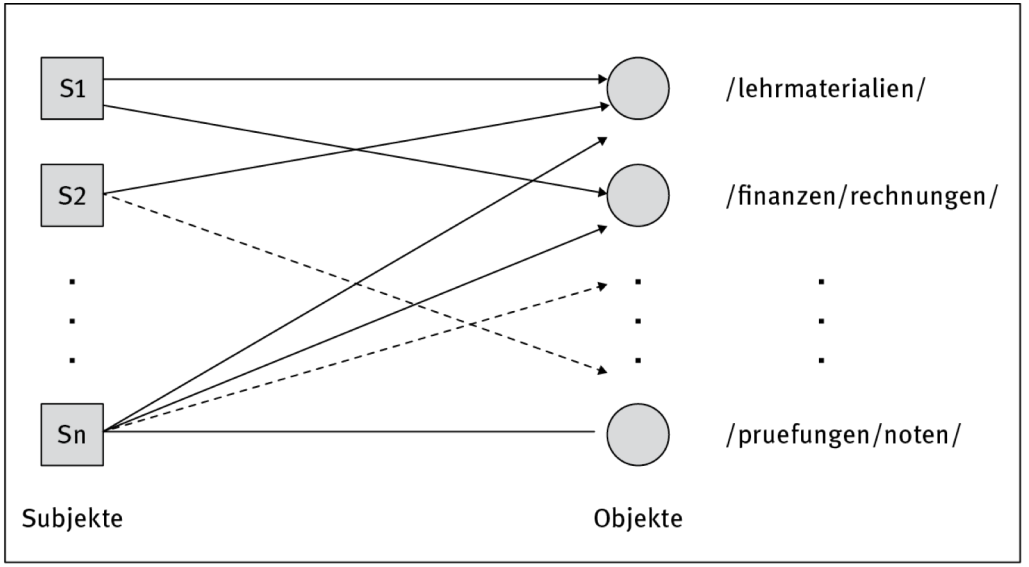
A) Wahlfreies Modell

B) Rollenbasiertes Modell

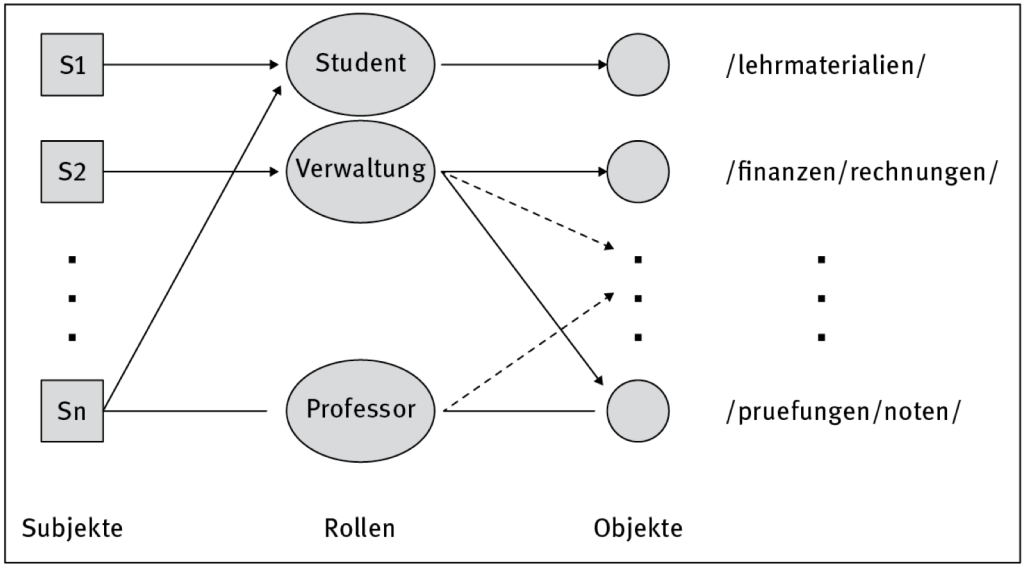
Wichtiger Unterschied:
Aufwand zur Wartung der Berechtigungen:

Was passiert, wenn Mitarbeiter ausscheidet, oder andere Aufgaben übernimmt, ...?

a)



b)



Datenschutz

- Problem- und Gefahrenfelder
  - E-Mail-, Handy- und Video-Überwachung
  - Zutrittskontrollsysteme als Arbeitszeitüberwachung
  - „Transparente Konsumenten" durch Cookies, Personalisierung und Funketiketten (RFID)
  - Beispiel: Echelon

- Rechtliche Schutzmaßnahmen
  - Europäische Datenschutzgesetzgebung (EG-Datenschutzrichtlinie 1995, Bundes- und teils auch Länderdatenschutzgesetze)
  - *Datenschutzgrundverordnung (DS-GVO, 2014 verabschiedet)*
  - Verankerung von Grundsätzen zum Schutz der Privatsphäre (Publizität, Datengeheimnis, …)
- Technische Schutzmaßnahmen

Vorratsdatenspeicherung, Online-Durchsuchung?

- Bekämpfung von Terrorismus und organisierter Kriminalität

http://www.myfaible.de/dacity/Direktlink/DA-TUD-h-da/Verschiedenes/2007-11-13-07-21-09-OnlineDurchsuchungen-im-Visier-Der-Bundestrojaner-ist-teuer-und-kann/

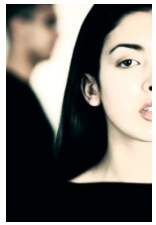
Grundsätze zur Sicherstellung des Schutzes der Privatsphäre (DSG, BDSG)

- Relevanz (nur für den Betriebszweck wesentliche Daten)
- Publizität (Auskunftsrecht des Betroffenen)
- Richtigkeit (Richtigstellung, Löschung falscher Daten)
- Weitergabebeschränkung
- Trennung der Funktionen (Auftraggeber, Durchführung)
- Verpflichtung zu Datensicherheitsmaßnahmen
- Geheimhaltungspflicht
- Kontrollorgane (Datenschutzbeauftragte und -rat)
- Kontrolle internationaler Datenverkehr

Technisch-organisatorische Maßnahmen bei der Verarbeitung personenbezogenen Daten

- Zugangskontrolle
- Abgangskontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übermittlungskontrolle
- Eingabekontrolle
- Auftragskontrolle
- Transportkontrolle
- Organisationskontrolle

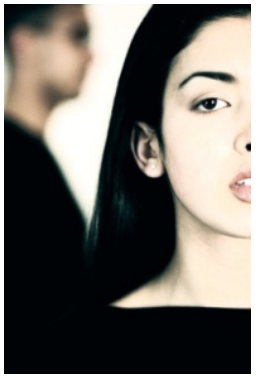
Schutz der Privatsphäre vs. Personalisierung von Informationsangeboten



- Informationssammlung über demografische, psychografische und soziografische Merkmale und das Kaufverhalten
- Maßgeschneiderte
  - Sortimente und Produktempfehlungen
  - Kundendienstleistungen
  - Preise und Rabatte
  - Liefer- und Zahlungsbedingungen, Zustellung
  - Werbebotschaften

Kunden-DB Maßnahmen-DB

Beispiel zum Datenschutz: E-Commerce Zulässigkeit von Persönlichkeitsprofilen



- Nach dem Datenschutzgesetz dürfen personenbezogene Daten nur erhoben, verarbeitet und genutzt werden
  - soweit eine Rechtsvorschrift es erlaubt oder
  - der Betroffene vorher eingewilligt hat

- Die Einwilligung muss
  - freiwillig sein
  - auf einer Information über den vorgesehenen Zweck der Datenverwendung, die Folgen der Verweigerung der Einwilligung und die Widerrufsmöglichkeit beruhen
  - hinsichtlich Umfang und Zweck bestimmt sein
  - eine bestimmte Form einhalten
    - in der Regel Schriftform oder
    - elektronische Form mit qualifizierter elektronischer Signatur

Beispiel zum Datenschutz: Social Communities

"Sie übertragen Facebook hiermit eine unabänderliche, unbefristete, nicht exklusive, übertragbare, hiermit vollständig bezahlte, weltweit gültige Lizenz (mit dem Recht sie weiter zu lizenzieren), alle Nutzer-Inhalte zu verwenden, kopieren, veröffentlichen, speichern, öffentlich aufzuführen, neu zu formatieren, verändern, übersetzen … und zu verbreiten, die Sie bei Facebook einstellen (…)."

Nutzungsbedingungs-Vorschlag von Facebook, 17.02.2009

XING studiVZ

Quelle: http://www.spiegel.de/netzwelt/web/0,1518,608116,00.html

facebook

LinkedIn

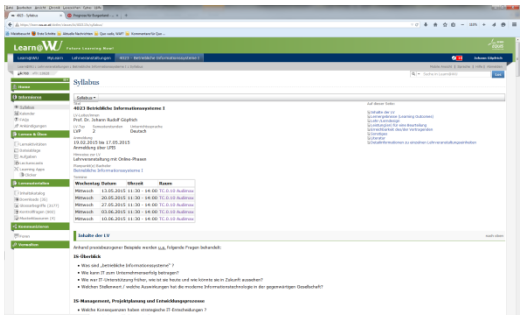
Anwendungsfragen Kapitel 8

- In einem Unternehmen wird ein Mitarbeiter des Rechnungswesens von einer Person angerufen, die sich fälschlicherweise als Mitarbeiter einer Unternehmensberatung ausgibt, die gerade ein Audit durchführt. Der Anrufer bittet um dringende, unbürokratische Übermittlung des Administratorkennworts des SAP-Systems, um schnell noch die Folien vor der anstehenden Präsentation zu aktualisieren. Um welche Form des Angriffs handelt es sich hierbei?
- Sie haben auf ihrem Privatcomputer ein aktuelles Programm zur Erkennung von Schadsoftware installiert, das beim Aufruf keine Warnungen ausgibt. Können Sie sicher sein, dass Ihr Rechner frei von Schadsoftware ist?

Diskussionsfragen zu Kapitel 8

- Diskutieren Sie die Vor- und Nachteile bei der Nutzung öffentlicher Infrastrukturen (in der Cloud) für die Speicherung von Firmendokumenten.
- Nehmen wir an, Vertraulichkeit kann bei der Datenübertragung technisch mittels Kryptografie absolut gewährleistet werden.
  - Wäre dieses Ausmaß an Privatsphäre nicht ein Freibrief für Steuerhinterziehung und für sichere Kommunikation des organisierten Verbrechens?
  - Würde es Sinn machen, Verschlüsselung generell zu verbieten?

Diskussionsfragen zu Kapitel 8



Learn@WU:

- Was wären mögliche Folgen eines Identitätsdiebstahls je nach Interessengruppe?
- Skizzieren Sie einen möglichen Phishing-Angriff auf das E-Learning-System.
- Welche Eigenschaft des Systems würde durch eine DoS-Attacke gefährdet? Was wären die Konsequenzen für die Benutzer der unterschiedlichen Interessengruppen, beispielsweise in der Zeit der Prüfungsvorbereitung?
- Diskutieren Sie die Vor- und Nachteile der vorgestellten Zugriffskontrollmodelle, wenn beispielsweise unterschiedliche Berechtigungen je nach Zugehörigkeit zu Studienrichtungen und Lehrveranstaltungen (neben individuellen Berechtigungen) realisiert werden sollen.
- Nehmen wir an, für das E-Learning-System soll ein Zugang über biometrische Verfahren (im konkreten Fall: Fingerabdruckleser) eingerichtet werden. Welche Schritte wären hierfür notwendig? Was wären die Vor- und Nachteile dieses Systems gegenüber einer Anmeldung mit Benutzerkennung und Kennwort?