Cryptoparty

Einführung in die Verschlüsselung & IT Sicherheit

Thomas Kilian & Philipp Meyer

CIP-RGB der Physik-Fakultät der LMU München

tbd

Inhaltsverzeichnis

Inhaltsverzeichnis

Angriffe auf IT Systeme

Überblick

- Netzwerkangriffe
  - Viren/Trojaner/Würmer
    - Randsomware
  - Browserangriffe
  - Wiretapping/Man-in-the-Middle/Spoofing
  - Denial of Service
- Social Engineering
  - Phishing
- Physische Angriffe
  - Diebstahl
  - USB Sticks ...
  - Keylogger

Viren/Würmer/Trojaner

- schädliche Software
- läuft auf dem eigenen System
- Mischformen sind möglich

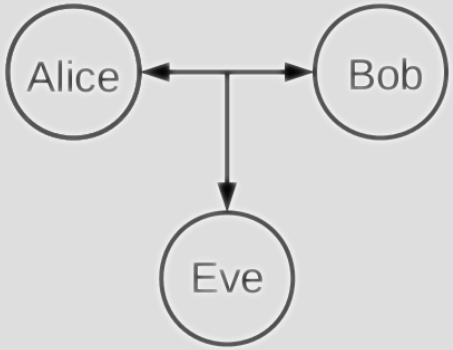
- **Viren**
- **Würmer**
- **Trojanisches Pferd/Trojaner**
- **Randsomware**
- **Botnet**
- **Rootkit**

Browserangriffe

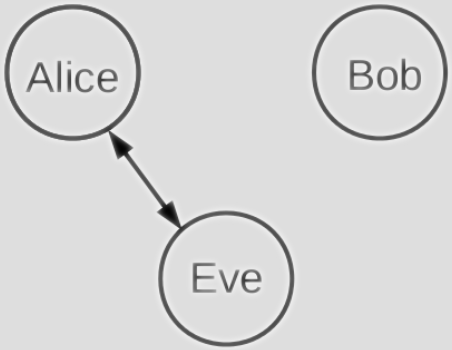
- Lücken in Browsern oder Plugins werden ausgenutzt
  - Plugins: Flash, Java, usw.
- Ziele
  - Ausführen von beliebigen Code durch den Browser
  - Gewinnen von Informationen wie z.B. Bankdaten
- Angriffe erfolgen über kompromittierte oder präparierte Webseiten
- Mit der Komplexität und Funktionen von Browsers steigt auch das Risiko von Fehlern im Code

Wiretapping/Man-in-the-Middle/Spoofing

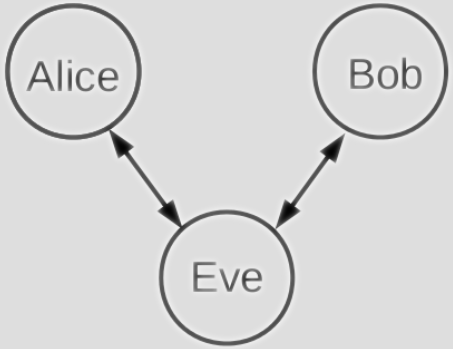
- Abhören



- Spoofing

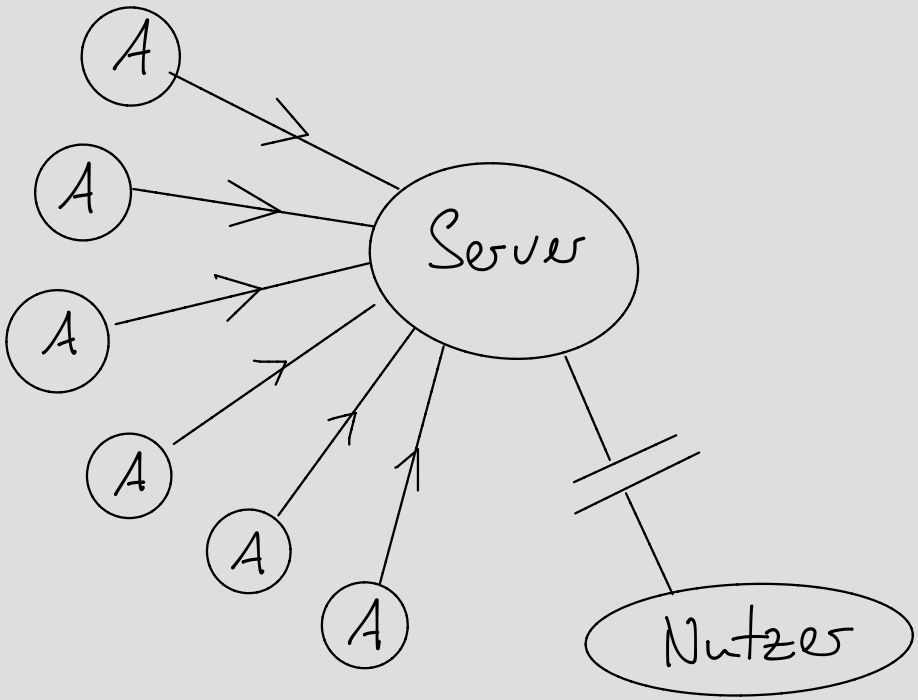


- Man in the Middle



Denial of Service (DoS)

- Ziel: Nicht-Erreichbarkeit des Systems
- Das System wird mit Traffic überlastet und ist dadurch nicht mehr erreichbar
- Die komplette Kapazität des Systems wird vom Angreifer überlastet
- Distributed Denial of Service



Phishing

Social Engineering

- Social Engineering (Überbegriff);
  - Soziale Verwundbarkeiten statt technischen ausnutzen
  - Vor allem durch Vortäuschen von Gegebenheiten
- Phishing
  - Ziel: Herausfinden von Zugangsinformationen, Passwörtern und ähnlichem
  - Wird durch Versand von sehr, sehr vielen Nachrichten, insbesondere E-Mails, erreicht (Spam)
  - E-Mails täuschen in der Regel vor, von einer offiziellen Stelle zu kommen (z.B. Administratoren der Uni) und drohen mit Strafe/Einschränkungen bei Nichtbefolgung oder versprechen Gewinn
  - Aus diesem Grund fragen offizielle Stellen (wie z.B. wir) NIE NIE NIE NIE NIE per E-Mail nach euren Zugangsdaten
  - die meisten Nutzer fallen nicht darauf rein, aber durch die Masse finden sich doch genug, so dass es sich nicht rentiert

Physische Angriffe

- **Zerstörung**
- **Diebstahl**
- **USB Sticks**
  - BadUSB
  - Virenübertragung
- Thunderbold Anschlüsse
- **Keylogger**

Inhaltsverzeichnis

Passwörter

- dient zur Authentifizierung
- kann aus Buchstaben, Zahlen und Sonderzeichen bestehen
  - Buchstaben (groß & klein): 52 Zeichen
  - Buchstaben + Zahlen: 62 Zeichen
  - Buchstaben + Zahlen + Sonderzeichen: 96 Zeichen
- die am häufigsten benutzten Passwörter: password, 123456, 12345678, qwerty
- Auch schlecht sind alle Wörter, die mit dem Nutzer zu tun haben & und Wörter, die in Wörterbüchern vorkommen (egal welche Sprache)

Passwörter

Wie erstellt man sichere Passwörter?

- Wichtige Kriterien: Länge & Komplexität (vgl. Fahrradschloss)
- Für verschiedene Konten verschiedene Passwörter verwenden
- keine Passwörter in Klartext aufschreiben, Passwort-Manager verwenden
- Trick, um Passwörter zu erstellen:
  1. Sich einen einprägsamen Satz suchen:
     z.B. „Luke, May the Force be with you“
  2. Nehme die Anfangsbuchstaben UND Sonderzeichen UND Zahlen (als Ziffern): „L,MtFbwy“
- Passwort Generator

Passwörter - Praktischer Teil

Aufgaben:

1. Erstellen Sie mit dem oben beschriebenen Verfahren ein Passwort.
2. Benutzen Sie `pwgen` in der Konsole zum Generieren eines 16 Zeichen langen Passwortes.
3. Optional: Ändern Sie Ihr LMU-Passwort auf das im 1. Schritt erstellte Passwort.

Hilfe zu `pwgen`: `pwgen -N` Anzahl `-y` Länge

Firewall

- Kontrolliert den Zu- und Ausgang von Netzwerkaktivitäten von einem Computer
- Filtert und versperrt den Zugang nach bestimmten Regeln (Security Policy)
- sollte immer dann eingesetzt werden, wenn man mit anderen nicht vertrauenswürdigen Systemen im gleichen Netzwerk ist, z.B. Wifi-Hotspots wie eduroam oder Internet
- Software: (Personal Firewalls)
  - Windows: integrierte Firewall
  - Mac OS X: integrierte Firewall, nicht automatisch aktiv
  - Linux: (iptables)

Eine Minute Pause, damit einige panisch ihre Firewalls einschalten können...

Software Updates

- Alle Updates für das Betriebssystem und die installierte Software schnell installieren
- Lücken, die durch die Patches geschlossen wurden, werden innerhalb von Stunden durch Malware ausgenutzt

Schutz vor Phishing

- Nachfragen bei der Person, ob es wirklich von ihr kam (z.B. Bank)
- Tausche Dateien via Websites oder Tauschdiensten (z.B. Dropbox, Google Drive)
- Öffne keine verdächtigen Dokumente, z.B. von unbekannten Personen, oder nur in seperaten Umgebungen (z.B. Virtualbox & Tails)
- Sei vorsichtig, was Anweisungen in E-Mails angeht, z.B. von System-Administratoren und befolge sie nur, wenn du absolut sicher bist, dass sie von der angegebenen Quelle kommen
- Benutze E-Mail Authentifizierung, wie z.B. GPG

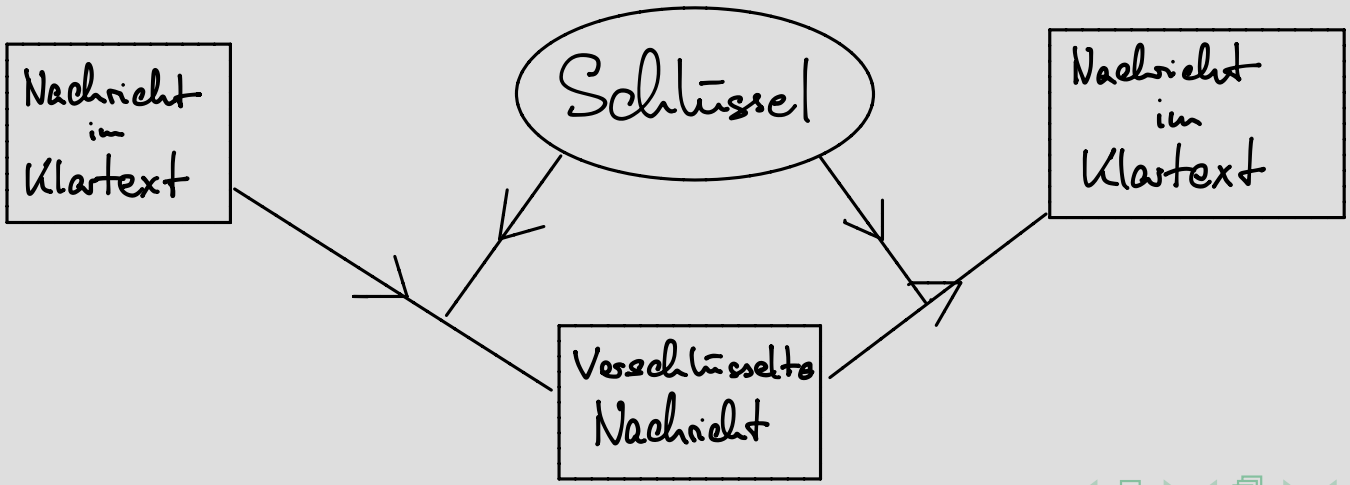
Cryptoparty

- Ziel: sichere Übertragung & Aufbewahrung von Informationen
- besteht heute aus zwei verschiedenen Arten:
  - Symmetrische Verschlüsselung
  - Asymmetrische Verschlüsselung
- werden häufig auch kombiniert

Kryptographie

Symmetrische Verschlüsselung

- Für Ver- und Entschlüsselung wird der gleiche Schlüssel verwendet
- Beispiel Türschloss: der gleiche Schlüssel kann die Tür ab- und aufschließen
- **Vorteil:** hohe Geschwindgkeit
- **Nachteil:** der geheime Schlüssel muss auch zum Enpfänger übertragen werden & Sicherheit hängt von der Geheimhaltung des Schlüssels ab



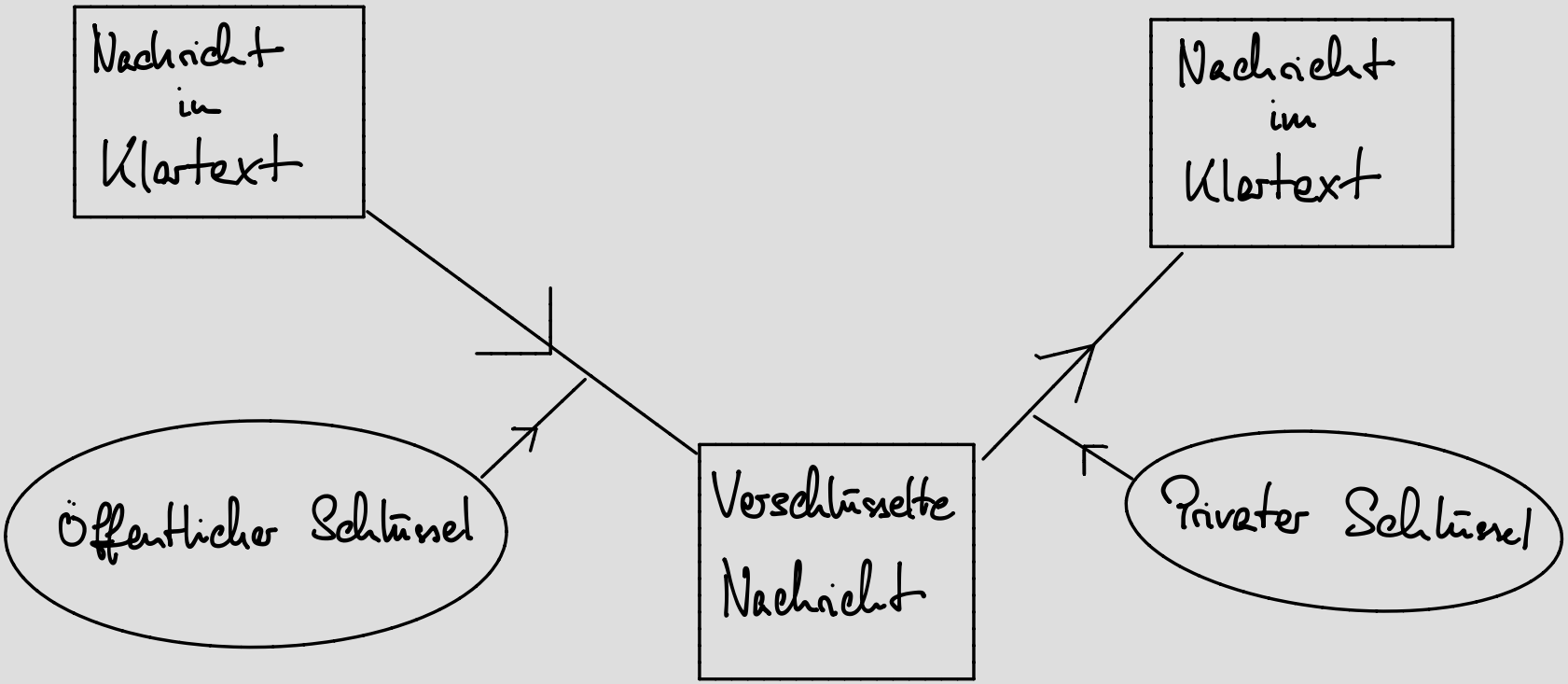
Kryptographie

Asymmetrische Verschlüsselung

- Benutzt zwei verschiedene Schlüssel zum ver- und entschlüsseln
  - Schlüssel zur Verschlüsselung wird öffentlicher Schlüssel genannt (public key)
  - Schlüssel zur Entschlüsselung wird privater Schlüssel genannt (private key)
- Beispiel Hängeschloss: Jeder kann mit dem Schloss (public key) abschließen, aber nur der Besitzer des Schlüssels zum Schloss (private key) kann aufschließen
- Öffentliche Schlüssel können frei geteilt und auf z.B. auf Servern veröffentlicht werden (z.B. pgp.mit.edu)

Kryptographie

Asymmetrische Verschlüsselung



Kryptographie

Datei- & Festplattenverschlüsselung

- symmetrische Verschlüsselung
- Dateiverschlüsselung: Verschlüsselung einzelner Dateien oder in sog. Containern
- Festplattenverschlüsselung: Verschlüsselung des gesamten Dateisystems, bei Hardwareverschlüsselung inkl. Boot Sektor
- Gängige Software für die einzelnen Betriebsysteme sind:
  - Dateiverschlüsselung:
    - GPG
    - VeraCrypt
  - Festplattenverschlüsselung:
    - **Windows:** BitLocker
    - **Mac OS X:** Filevault
    - **Linux:** LUKS
    - **Android:** integrierte Softwareverschlüsselung
    - **iOS:** integrierte Hardwareverschlüsselung

Kryptographie

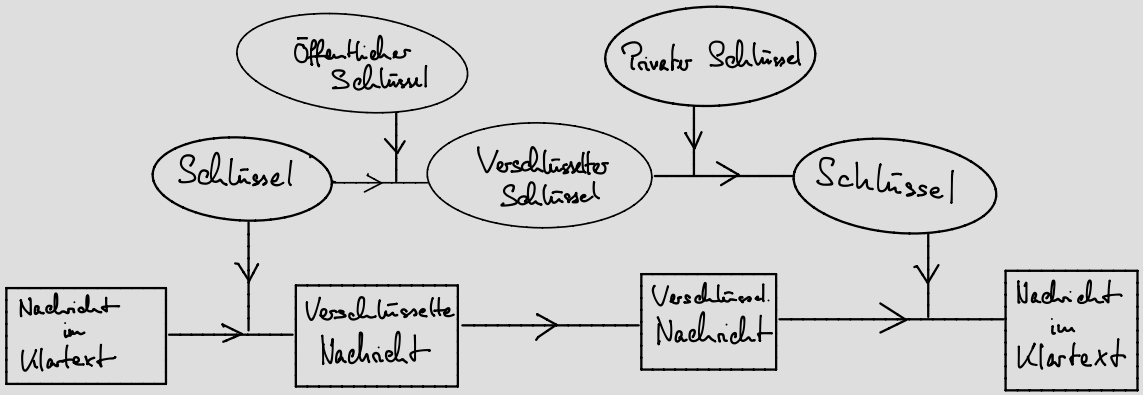
SSL/Zertifikate

- SSL
  - SSL Protokoll ermöglicht Client-Server Anwendungen (z.B. HTTPS) die verschlüsselte ohne Abhören & Manipulation
  - Jedes Anwendung kann mit oder ohne SSL verwendet werden (z.B. HTTP & HTTPS)
  - Wird für praktisch alle Client-Server Kommunikation im Internet verwendet.
- Zertifikate
  - Authentizität und Integrität von Personen und Objekten kann durch Kryptographie geprüft werden
  - Am meisten verbreitet sind Public-Key-Zertifikate
  - Signatur wird aus privatem Schlüssel generiert und mit öffentlichem Schlüssel überprüft

Kryptographie

GPG - GNU Privacy Guard

- Verschlüsselung auf Basis von asymmetrischen Algorithmen (Public Key) & symmetrischen Verfahren
- PGP Verschlüsselt mit einer symmetrischen Verschlüsselung und verschlüsselt nur den symmetrischen Schlüssel (session key) asymmetrisch.
- Dadurch wird es möglich, eine Nachricht an mehrere Empfänger gleichzeitig zu schicken
- Kann auch zum Signieren verwendet werden



Kryptographie - Praktische Phase

Aufgaben:

Anleitungen siehe Handout

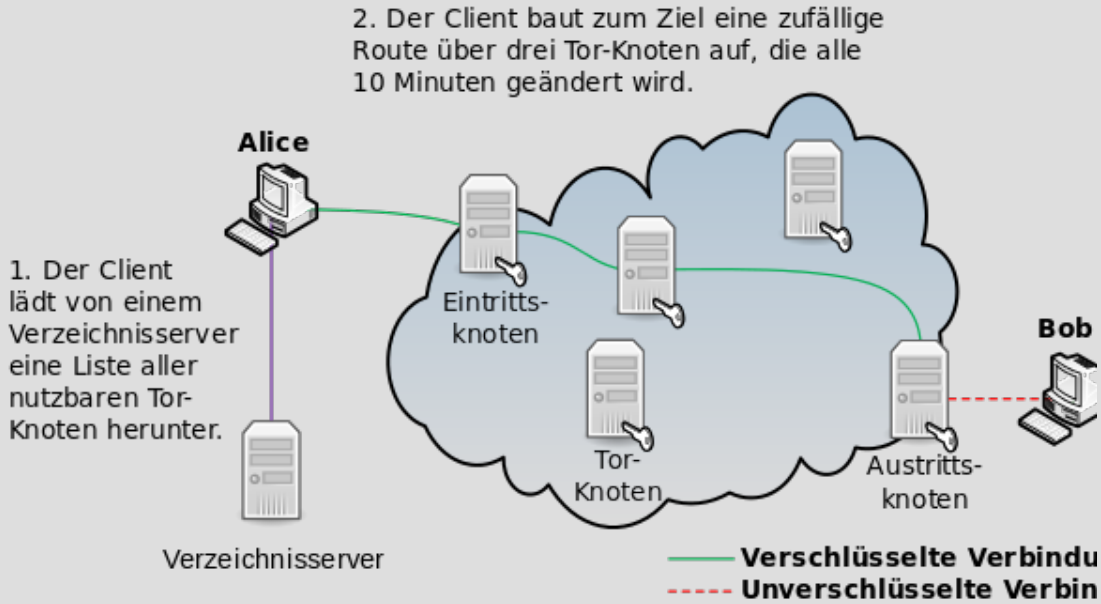
1. Optional: Richten Sie in Thunderbird Ihren Physik E-Mailaccount ein.
2. Installieren Sie Enigmail in Thunderbird.
3. Benutzen Sie den *Setup Wizard* und erstellen Sie ein Schlüsselpaar.
4. Laden Sie Ihren öffentlichen Schlüssel auf einen Schlüsselserver hoch. (*Keyserver* und *Upload public key*
5. Tauschen Sie mit einem Sitznachbarn ihre Schlüssel. (via E-Mail, USB, ...)
6. Verifiziern Sie durch abgleichen den Fingerabdruckes, dass der Schlüssel korrekt ist.
7. Bestätigen Sie in Enigmail, dass Sie dem Schlüssel vertrauen.
8. Senden Sie Ihrem Sitznachbarn eine verschlüsselte & signierte E-Mail.
9. Verschlüsseln Sie eine Datei mit GPG.

Kryptographie

Tor

- Tor steht ursprünglich für „The Onion Router“(s.u.)
- wird von ca. 36 Millionen Menschen genutzt (Stand 2011)
- Netzwerk zur Anonymisierung von Verbindungsdaten

- Basiert auf der Idee des Onion-Routings



Von Saman Vosoghi - Selbst erstellt, Bild-frei, https://de.wikipedia.org/w/index.php?curid=7906487

Kryptographie

Tor

- hidden services
  - wird wird vor allem benutzt, um anonym Server zu betreiben, die nur dem Tor-Netz erreichbar sind Beispieladresse: http://oldd6th4cr5spio4.onion/
- Tor bridges
  - Zur Umgehung von Zensur des Tor Netzwerkes
- Tor Browser
  - Client um auf das Tor Netzwerk zuzugreifen
  - basiert auf Firefox
- Orbot & Orfox
  - Client für Android

TOR - Praktische Phase

Aufgaben:

1. Installieren Sie Tor Browser in Ihrem Home Verzeichnis. (Download: www.torproject.org)
2. Starten Sie Tor Browser und verbinden Sie sich mit dem Internet.

gegen Physische Schäden & Angriffe

Backups

- So viele wie möglich
- An möglichst verschiedenen Orten
- Backups überprüfen
- Software:
  - Windows: Verschiedene
  - Mac OS X: TimeMachine
  - Linux: Verschiedene
  - iOS: iTunes
  - Android: z.B. Hersteller Lösungen
- Alternativen: Unison, BitTorrent Sync

Inhaltsverzeichnis

Datenschutz

- Datenschutz bedeutet der Schutz vor missbräuchlicher Datenverarbeitung
- Rechtliche Grundlage: Informationelle Selbstbestimmung
- Dieses Recht verschwindet im Laufe der Ausbreitung des Internets immer weiter
- durch Internet-Konzerne & staatliche Überwachung

Arten von missbräuchlicher Datenverarbeitung

Eine nicht-vollständige Auflistung;

- Auf Webseiten:
  - Cookies
  - Flash-Cookies
  - Tracker wie Zählpixel
  - personalisierte Werbung
  - Suchmaschinen
- Beim Kommunizieren:
  - Kommunikationsprofile
  - inhaltliche Analyse
  - HTML Mails mit Bildern
- Mobile:
  - Bewegungsprofile
  - Smartphone = Wanze
- Sonstige Dienste:
  - Clouds
  - EC-Transaktionen

Gegenwehr

- Überwachung im Browser
  - Tracker blocken mit Addons wie Ghostery
  - In Browsereinstellungen Cookies deaktivieren oder am Ender der Session löschen
  - anonyme Suchmaschinen nutzen wie z.B. startpage.com
  - Dienste wie Tor nutzen
  - VPN Anbieter
- Kommunikation
  - Verschlüsselung der Nachrichten
  - Wechsel der App für Textnachrichten z.B. auf Signal
  - E-Mailprogramm verbieten Bilder sofort mitzuladen
- Mobile
  - Handys für „wichtige Treffen“ausschalten, Akku rausnehmen und in einen Kühlschrank o.ä. tun
  - Einfache Handys verwenden, weil dort weniger Daten anfallen

Gegenwehr - Praktische Phase

Aufgaben:

1. Installieren Sie die Erweiterung *Ghostery* oder *PrivacyBadger* in Ihrem Browser.
2. Besuchen Sie eine beliebige Seite und schauen Sie sich an, wie viele Tracker auf der Seite sind.
3. Installieren Sie die Erweiterung *HTTPS Everywhere*

Danke für Ihre Aufmerksamkeit