SICHERHEIT IM INTERNET

EIN VORTRAG VOM TERMINAL.21

UM WAS ES HEUTE GEHT:

- Was ist das Internet?
  → Hosts, Browser, Kommunikation
- Verschlüsselung
  → sichere Verbindungen mit dem Browser
- Phishing
  → gefälschte Webseiten, Zertifikate
- Tracking
  → Cookies, Javascript, Fingerprinting, Referrer
- Gegenmaßnahmen

WAS IST DAS INTERNET?

- Internet ist keine große Wolke
  → große Zahl von Computern, ähnlich denen von zu Hause
  → Verbindung zu großen Providern (z.B. Telekom), die große Datenmengen in kurzer Zeit untereinander austauschen können und an ihre Kunden weiterreichen
  → Jeder Computer hat dabei eine eigene Adresse, von der er aus dem Internet heraus erreichbar ist (IP-Adresse)
- Hinter jeder Webseite steckt ein Computer, der diese bspw. als HTML-Datei abgespeichert hat und an den eigenen Computer sendet
- Webbrowser bauen aus dieser Datei eine Webseite, wie wir sie kennen

AUFRUF EINER WEBSEITE

- Webseiten werden über URLs angefordert, dies kann z.B. über Links erfolgen
- Nach anklicken eines Links (oder Eingabe der URL über den Browser) wird zunächst eine Anfrage an einen DNS-Server (Domain Name System) gesendet.
- DNS-Server verwalten riesige Listen mit registrierten Namen von Webseiten und den jeweiligen IP-Adressen der Computer, die diese Webseite betreiben („Hosts“)
- Es wird dann eine IP-Adresse an den Browser gesendet, unter der er den Host, der die Webseite betreibt, erreichen kann

AUFRUF EINER WEBSEITE (II)

- Browser sendet dann über den Internetprovider ein Paket an diese IP-Adresse
- Dieses enthält die eigene IP und den Link zu der angefragten Datei sowie Informationen des Browsers
- Ein Link hat dabei folgendes Aussehen:
  - http://de.wikipedia.org/wiki/Internet
  - https://www.privacy-handbuch.de/handbuch_11.htm
- http/https/ftp/etc. gibt das Protokoll des Datenaustausches an
- Zwischen // und Domainnamen (.de/.com/.org/etc) wird der Name der Webseite referenziert, zu der die IP gehört

AUFRUF EINER WEBSEITE (III)

- Nach erstem „/“ kommt Name der Datei, die abgerufen werden soll
  → Jedes „/“ steht für einen Unterordner, die auf dem Server gespeichert sind
  → Nach letztem „/“ kommt die eigentliche Datei mit Dateiendung (.html/.aspx/.php/etc.)
  → Dateiendung gibt den Typ der Datei an, die vom Browser jeweils anders behandelt werden
  → ist keine Datei angegeben, so wird dort standardmäßig „index.html“ aufgerufen)
- Manchmal werden auch Argumente aufgerufen, anhand denen der Server unterschiedliche Webseiten generiert, dies sieht man an einem „?“
  → Bsp. „https://www.google.de/search?q=dns“
  (mehrere Argumente werden durch „&“ getrennt)

WEBSERVER

- Host der aufgerufenen Webseite generiert dann entweder eine Webseite, oder liefert die angefragte Datei aus
  → Sendet Paket mit entsprechenden Daten an die eigene IP
- Kann prinzipiell keinen Zusammenhang zwischen Anfragen herstellen
  → Server fordert den Webbrowser daher meist auf, bei jeder weiteren Anfrage eine identifizierende Textdatei („Cookie“) anzuhängen, mit der der Server eine Verbindung („Session“) wiedererkennen kann

WEBBROWSER

- Interpretiert Inhalt der HTML-Datei und erstellt die darin beschriebenen („Rendering“)
  → Knöpfe
  → Texte
- Lädt externen Inhalt, wie zum Beispiel
  → Bilder
  → Videos
  → Inhalte von Drittanbietern, wie zum Beispiel Werbung
- Lädt zusätzlich eine Seitenbeschreibungsdatei
  → enthält Informationen zur Anordnung, Größe, Schriftarten, Farbe, etc. von Objekten
  → kann für verschiedene Browser verschiedene Inhalte haben

WEBBROWSER (II)

- Nach Laden der Seite kann der Nutzer mit ihr interagieren
  → Eingabe von Texten, ausführen von Skripten oder navigieren mithilfe von Links
- Anklicken von Objekten löst häufig eine Aktion aus, die mithilfe von Javascript direkt auf dem Computer ausgeführt wird
  → Ein-/Ausklappen von Elementen, springen zu anderen Teilen der Seite o.ä.
  → Skripte dienen aber auch zur Identifizierung des Nutzers, dazu später
- Skripte oder das Anklicken von Links lösen erneute Anfrage beim Server aus
  → Laden der nächsten Seite
  → Hochladen von Nutzereingaben (z.B. LogIn-Daten)
  → Dabei identifiziert sich der Browser häufig mithilfe von Cookies bei der Webseite

GEFAHREN DES INTERNETS

- Es werden unsichere Verbindungen aufgebaut
  → Daten-/Identitätsdiebstahl
- Browser wird gezwungen, viele Verbindungen zu anderen Webseiten aufzubauen
  → Tracking
- Es werden andere URLs geöffnet, als von Nutzer erwartet
  → Phishing
- Verwendete Plug-Ins und Add-Ons oder Browser selbst weisen Sicherheitslücken auf
  → Schadprogramme

VERSCHLÜSSELUNG HILFT

- Ziel: Abhören erschweren, indem abgehörte Informationen unbrauchbar gemacht werden
  → Kosten für Entschlüsselung möglichst hoch halten, damit sich aufwand für ungezielte Angriffe nicht lohnt
- Gezielte Angriffe auf Daten eher selten und bei guten Gewinnaussichten
  → Oft bei Kenntnis des Opfers oder der zu erwarteten Beute
- So viel wie möglich verschlüsseln, um Ausbeute und Gewinnaussichten gering zu halten
  → jede kleine Information könnte missbraucht werden, wenn sie mit anderen kleinen Informationen kombiniert werden
  → Kommunikation wie E-Mails, Chats, Telefonie und Internetverkehr

VERSCHLÜSSELUNGSARTEN

Arten der Verschlüsselung:

- Symmetrisch:
  → Schnelle Ver- und Entschlüsselung mit kurzen Schlüsseln
  → meist Hardwarebeschleunigt durch spezielle Unterstützung der Prozessoren
  → 1 Schlüssel zur Ver- und Entschlüsselung gleichzeitig (sicherer Schlüsselaustausch notwendig)
- Asymmetrisch
  → Langsame Ver- und Entschlüsselung mit langen Schlüsseln
  → 2 verschiedene Schlüssel zur Ver- und Entschlüsselung
  → Schlüssel zum Verschlüsseln öffentlich bekannt, Schlüssel zum Entschlüsseln im Besitz nur einer Person (durch Besitz eines Schlüssels kann nicht auf den anderen geschlossen werden)

UMSETZUNG IM BROWSER

- Browser fragt Zertifikat der Internetseite ab
  → erhält öffentlichen Schlüssel des Servers
  → sendet verschlüsselte Anfrage
  → sendet eigenen Schlüssel
- Server kann die Anfrage entschlüsseln
  → nimmt den Schlüssel des Browsers und verschlüsselt damit die Antwort
- Bisher asymmetrische Verschlüsselung
  → Die Browser senden noch weitere Informationen, womit sie sich auf einen gemeinsamen, symmetrischen Schlüssel einigen
- Eigentliche Kommunikation findet nun mit symmetrischen Schlüssel statt

SICHERE VERBINDUNGEN

- Sichere Verbindung heißt, dass nur der Webseitenbetreiber und das Endgerät die Daten mitlesen können

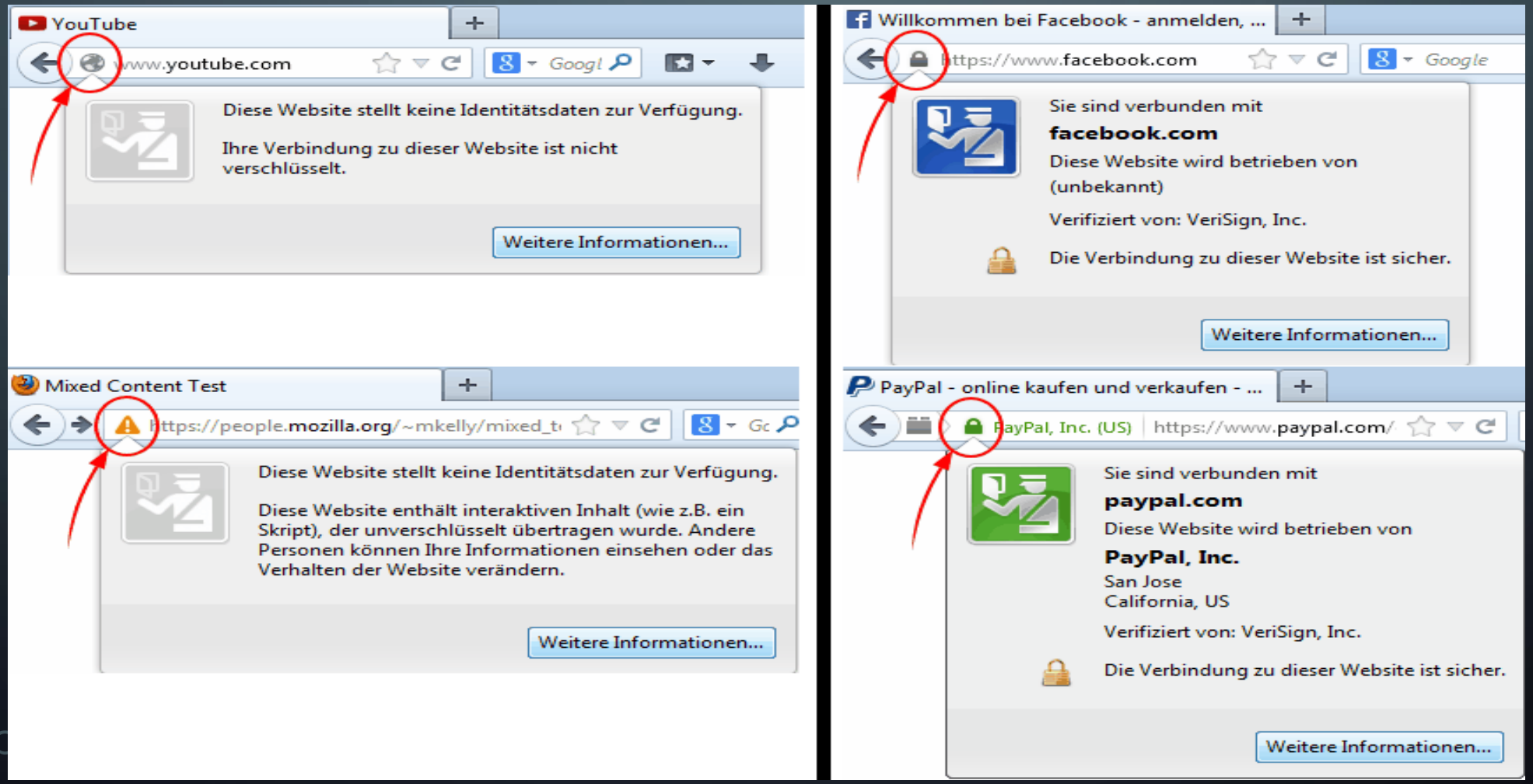
  → Dafür muss das Zertifikat des Servers gültig sein

  Browser führt automatische Plausibilitätskontrolle aus und warnt bei Unstimmigkeiten

  → NIEMALS EINE WARNUNG DES BROWSERS BEZÜGLICH DES ZERTIFIKATES WEGDRÜCKEN UND DANN PERSÖNLICHE DATEN WIE LOGIN O.Ä. PREISGEBEN

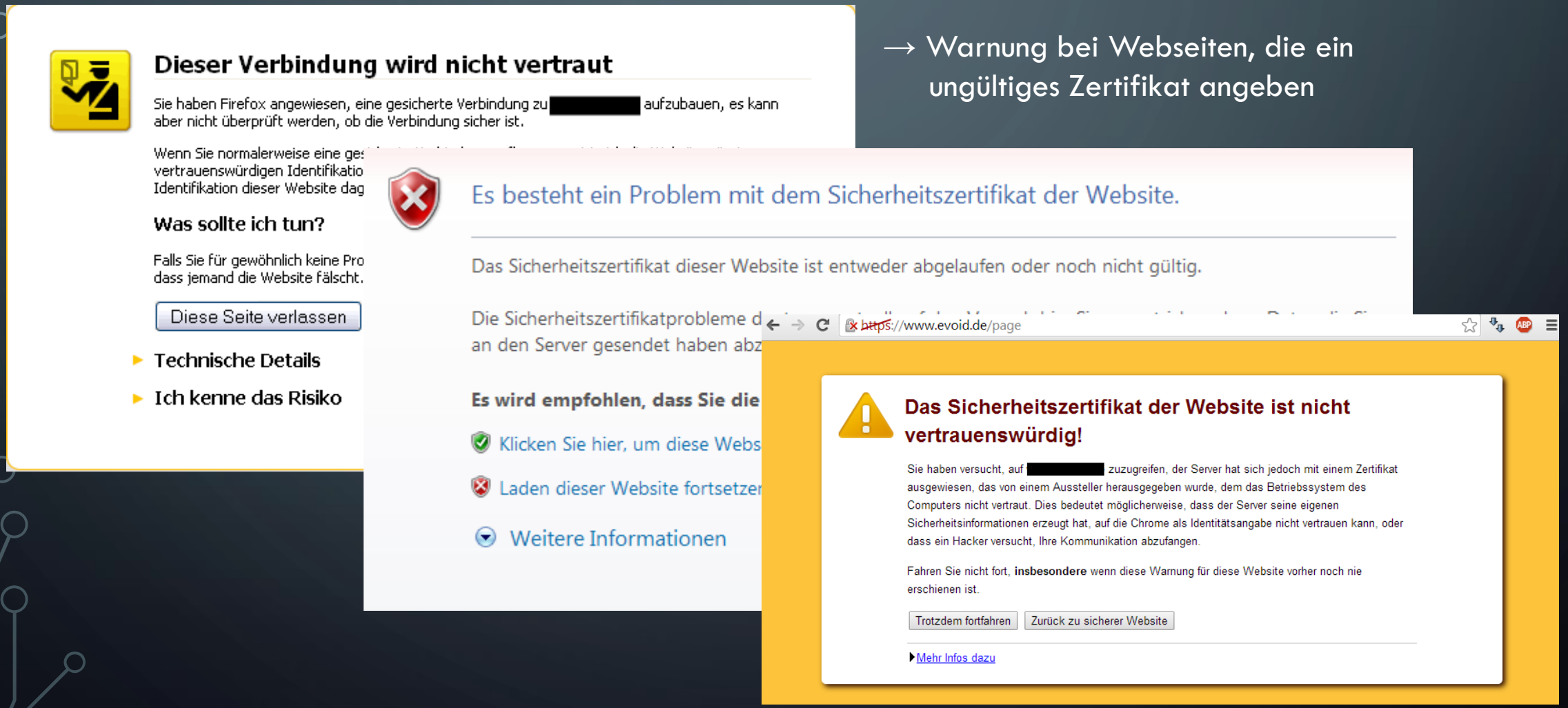
  → Trügerische Sicherheit: Nicht immer sind ALLE Elemente verschlüsselt

VERSCHLÜSSELUNGEN BEI WEBSEITEN



TRÜGERISCHE SICHERHEIT

→ Warnung bei Webseiten, die ein ungültiges Zertifikat angeben



PHISHING

- Versuch, den Nutzer dazu zu verleiten, persönliche Daten preiszugeben
  → Login-Daten
  → Adresse
  → Kontodaten
  → Kreditkartendaten
- Normalerweise unter Vortäuschung falscher Tatsachen
  → echt aussehende, populäre, nachgebaute Webseiten
  → minimale Rechtschreibfehler in der URL
  → Locken mit Mails und gefälschten Links

BEISPIELE FÜR PHISHING

- 2005 wurde eine Mail im Namen der Postbank gesendet, in der die Nutzer um Herausgabe ihrer TAN Nummern fürs Online-Banking aufgefordert wurden, damit ihr Konto nicht gesperrt wird und ihr Geld nicht verloren geht.
- 2011 wurde mithilfe von Phishing Mails das Personal von RSA Security Zugriff auf MasterKeys der RSA SecureID Tokens erlangt
  → Angreifer verschafften sich danach Zugriff auf interne Daten der Rüstungsfirma „Lockheed Martin“
- 2013 wurden auf die gleiche Weise 110 Millionen Kreditkartendaten bei „Target“ gestohlen

SPEARPHISHING

- Sonderform des Phishings

  → gezieltes Phishing auf spezielle Personen oder Unternehmen

  → speziell auf diese Personen zugeschnittene Argumente

  → häufig werden Personen mit Namen angesprochen und vertrauliche Details erwähnt, um Misstrauen zu zerstreuen

  → mithilfe von Mails, Telefonanrufen oder ähnlichem

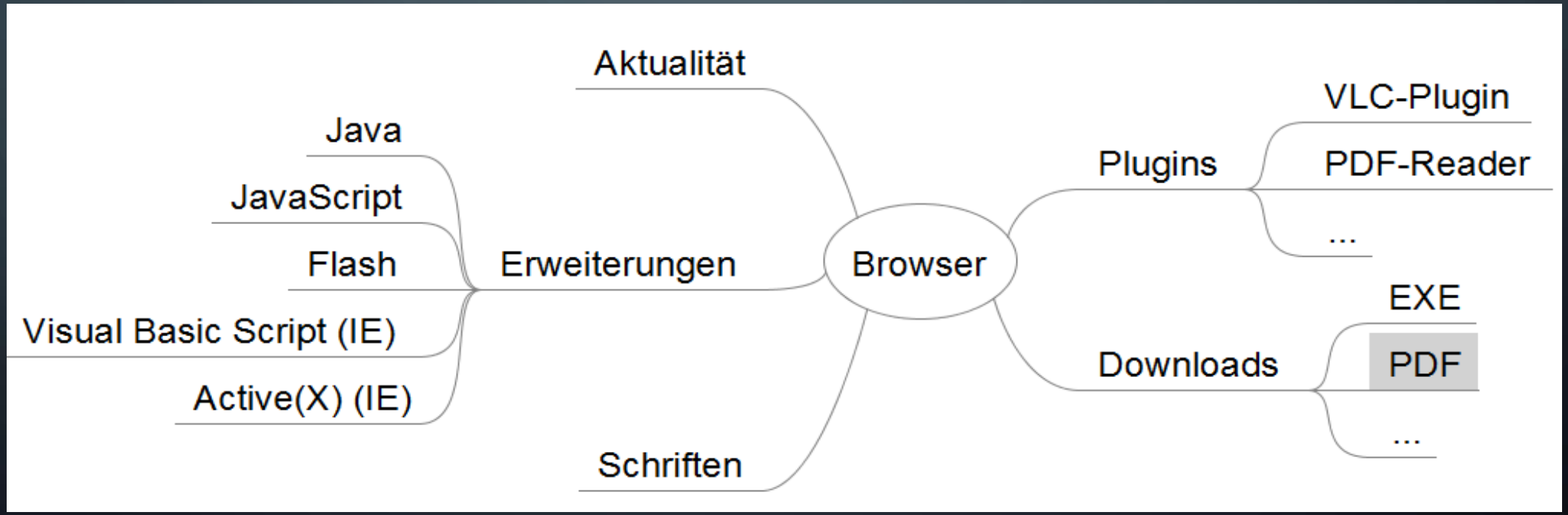
- Siehe Social Engineering

  → Prinzip: „Der Mensch ist die größte Gefahr für Computersysteme“

EINSCHLEUSEN VON SCHADSOFTWARE AUF SYSTEME

- Oftmals im direkten Anschluss an Phishing-Attacken
- Ziele:
  → Etablierung eines verborgenen, aber ständigen Zuganges auf Systeme
  → Verwanzen eines Rechners, um weitere Informationen zu erbeuten, die sich zu Geld machen lassen
  → Verseuchen weiterer Rechner, um Zugang auf privilegiertere Systeme einer Firma zu gelangen
- Meist unter Ausnutzung von Schwachstellen und Sicherheitslücken von Browsern oder anderen Programmen mit Zugriff auf Netzwerke / Internet

BROWSERSCHWACHSTELLEN



TRACKING

- Viele Organisationen haben Interesse an deinem Surfverhalten
  - Analyse der Interaktion mit Webseiten zur „Verbesserung der Dienste“
    → Aufgerufene Webseiten (Browserhistorie)
    → Verweildauer auf den einzelnen Seiten
    → Interaktion mit Webseiten
    → Vorlieben, Interessen, Kaufverhalten der Leute
    → Abschätzen des Clientes der jeweiligen Seite, die Tracker einbindet
  - Gezielte Analyse des Nutzers durch Trackinganbieter zum Verkauf der Daten
    → Auch hier Vorlieben und Interessen
    → zusätzlich bspw. Soziales Umfeld, Familienstand, Vermögensverhälnisse, politische Gesinnung, Religion
    → die „wertvollen“ Informationen, die gezielt bestimmten Personen zugeordnet werden sollen

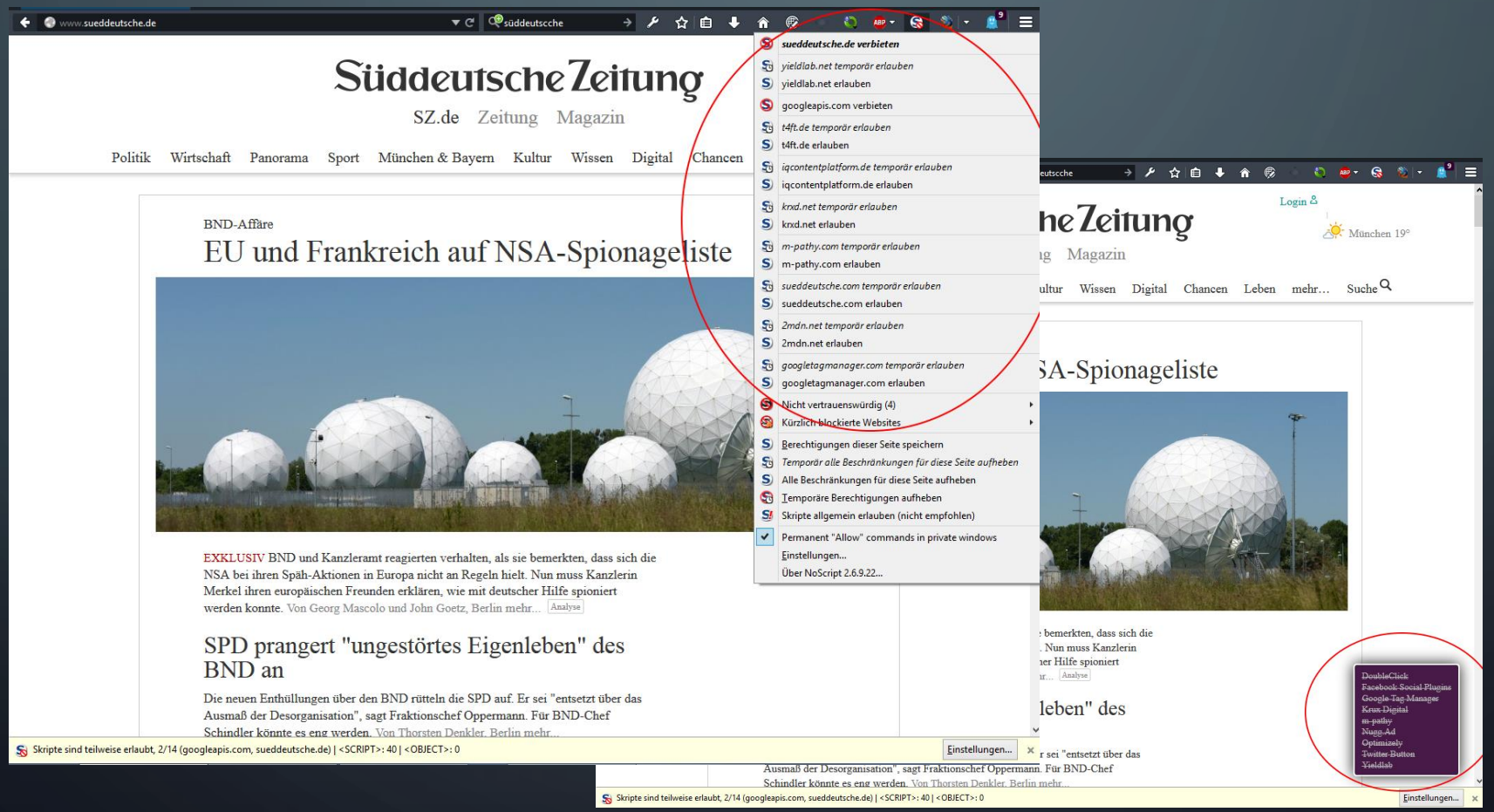
TRACKING (II)

- Webseitenbetreiber möchten Dienste Verbessern und über Werbeplattformen Geld verdienen (z.B. Google AdSense, Google Analytics)
- Diese verlieren jedoch Einfluss auf

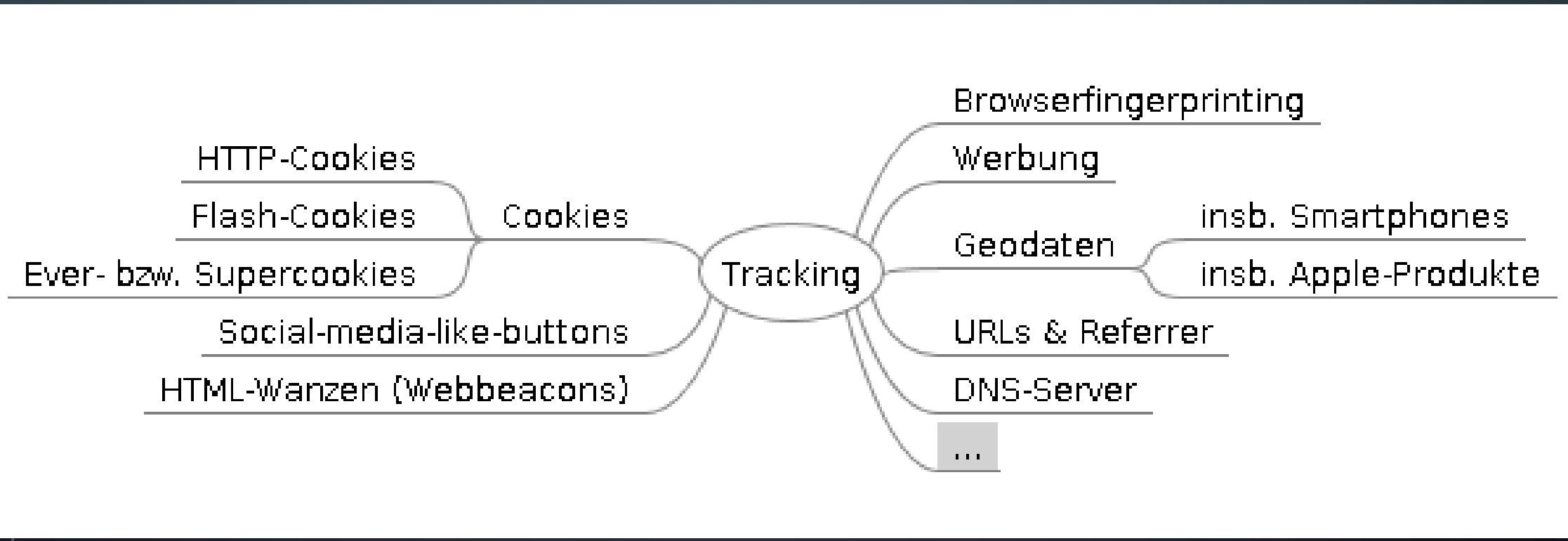
  → Inhalte der Webseite (der Werbung)

  → Daten, die vom Nutzer abgefragt und versendet werden
- Nutzer stimmt unwissentlich auch den Bestimmungen der Partnerunternehmen zu, die er nicht kennt und von deren Existenz er nicht informiert wird, wenn er die Seite nutzt.

VERBORGENE TRACKER AUF WEBSEITEN



WEITER TECHNIKEN DES TRACKINGS



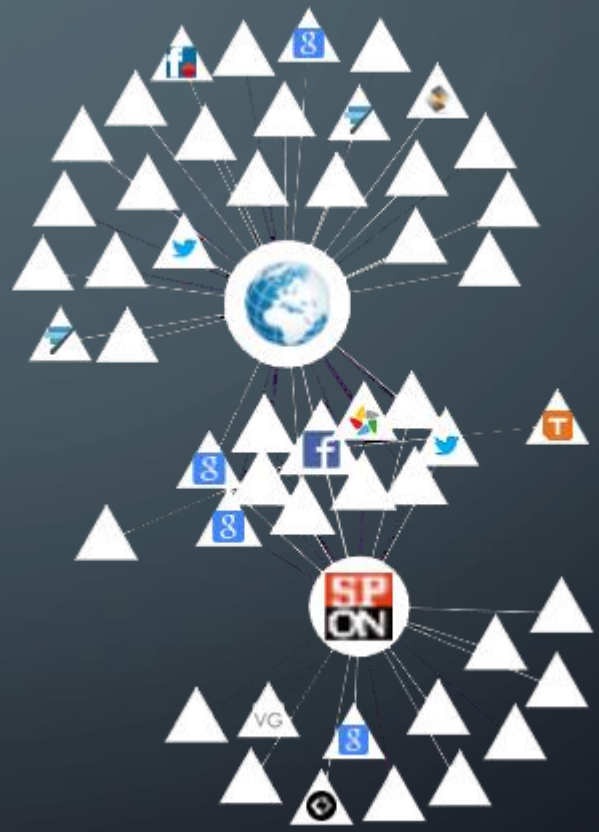
HTTP-COOKIES

- Besuchen der Webseite
- Setzen von Cookie(s)
- Weitersurfen
- Wiederkommen
- Cookie-Abruf
  - → Login-Infos
  - → Tracking

Visualisierung: lightbeam

3 Seiten besucht →

87 Cookies von Drittanbietern



ANDERE COOKIES

- Super- oder Evercookies:
  → Werden nicht angezeigt
  → Werden aber mit dem Löschen der anderen Cookies auch gelöscht (Firefox)

- Flash-Cookies
  → Werden nicht angezeigt
  → Browserunabhängig
  → Ohne Verfallsdatum
  → Wurden benutzt um HTTP-Cookies wiederherzustellen :<

SPEICHERORTE DER FLASH-COOKIES

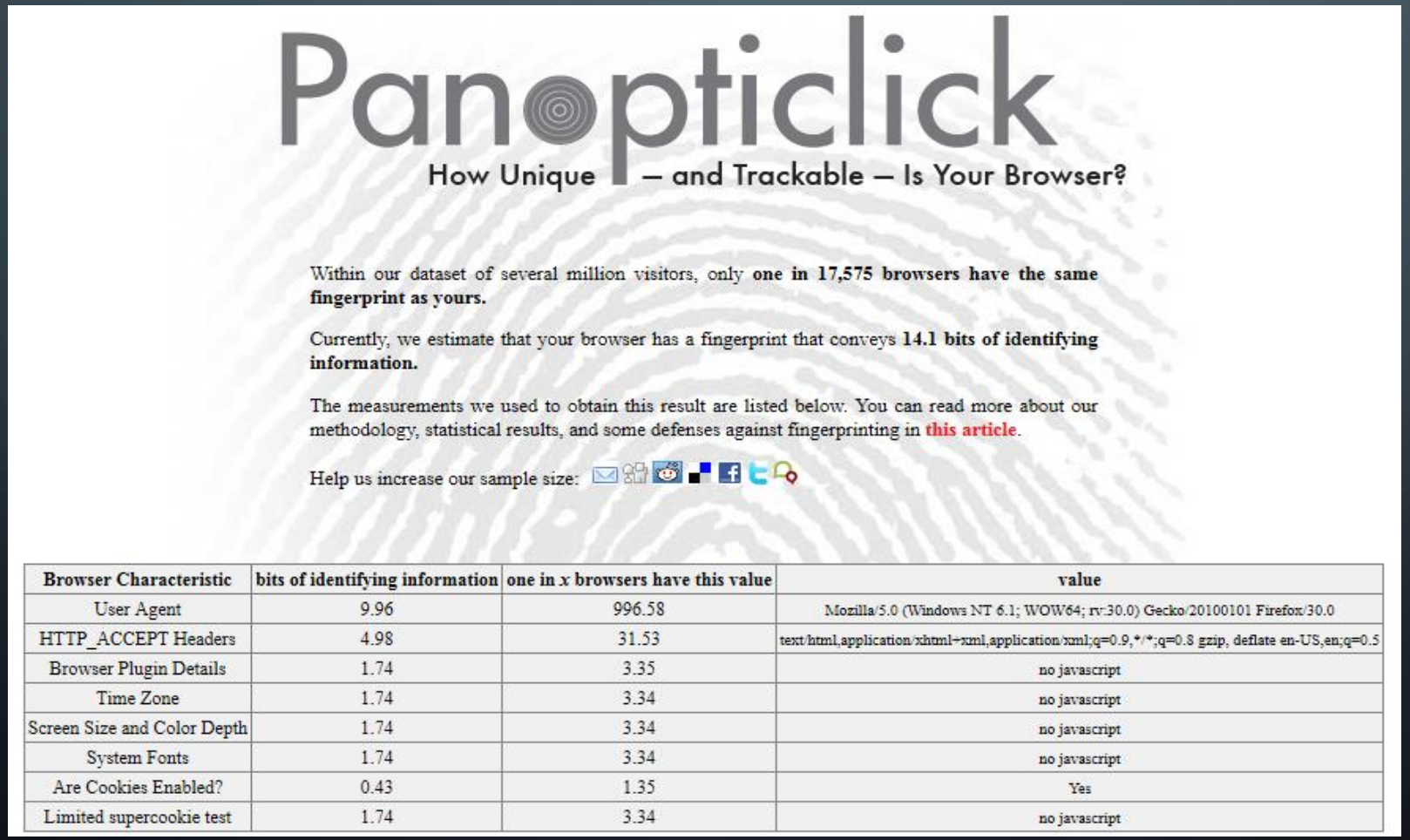
Standard-Speicherorte		
Betriebssystem	**Speicherort**	**Anmerkung**
Windows	• %AppData%\Macromedia\Flash Player\#SharedObjects • %APPDATA%\Macromedia\Flash Player\macromedia.com \support\flashplayer\sys • %APPDATA%\[AIR Paket ID]\Local Store\#SharedObjects\	• *%AppData%* steht für das Benutzerverzeichnis • Adobe-AIR-Anwendungen speichern separat in eigenen Ordner
Mac OS X	• ~/Library/Preferences/Macromedia/Flash Player/#SharedObjects • ~/Library/Preferences/[AIR Paket ID] • ~/Library/Preferences/Macromedia/Flash Player/macromedia.com/support/flashplayer/sys	• ~ steht für das Benutzerverzeichnis • Adobe-AIR-Anwendungen speichern separat in eigenen Ordner
Linux	• ~/.macromedia/Macromedia/Flash Player • ~/.macromedia/Flash_Player/#SharedObjects • ~/.gnash/SharedObjects (bei der Nutzung von Gnash)	• ~ steht für das Benutzerverzeichnis

NOCH MEHR TRACKING

- Browserfingerprinting
  → mithilfe von Javascript
  → Abfrage installierter Programme
  Mail-Programm, sowie alle anderen Programme, die durch bestimmte Links geöffnet werden können
  → Schriftarten des Betriebssystems oder Browsers (variieren teilweise stark)
  → Bildschirmauflösung und Farbtiefe
  → Browser-Plugins
  → Systemzeit
  → Browserkennung bzw. unterstütze Webformate

Dies ergibt einen „Fingerabdruck“ des Browsers und ermöglicht häufig eine Wiedererkennung des Browsers über alle Webseiten hinweg.

BROWSERFINGERPRINTING



Panopticlick

How Unique — and Trackable — Is Your Browser?

Within our dataset of several million visitors, only **one in 17,575 browsers have the same fingerprint as yours.**

Currently, we estimate that your browser has a fingerprint that conveys **14.1 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in this article.

Help us increase our sample size:

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	9.96	996.58	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
HTTP_ACCEPT Headers	4.98	31.53	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 gzip, deflate en-US,en;q=0.5
Browser Plugin Details	1.74	3.35	no javascript
Time Zone	1.74	3.34	no javascript
Screen Size and Color Depth	1.74	3.34	no javascript
System Fonts	1.74	3.34	no javascript
Are Cookies Enabled?	0.43	1.35	Yes
Limited supercookie test	1.74	3.34	no javascript

Panopticlick

How Unique — and Trackable — Is Your Browser?

Your browser fingerprint **appears to be unique** among the 4,235,506 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 22.01 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in this article.

Help us increase our sample size:

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	9.37	659.43	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
HTTP_ACCEPT Headers	9.81	895.65	text/html, */* gzip, deflate de-DE
Browser Plugin Details	13.54	11897.49	Plugin 0: Shockwave Flash; Shockwave Flash 13.0 r0; Flash32_13_0_0_214.ocx; (Shockwave Flash; application/x-shockwave-flash; swf) (Shockwave Flash; application/futuresplash; spl). Plugin 1: Silverlight Plug-In; 5.1.30214.0; npctrl.dll; (Silverlight Plug-In; application/x-silverlight;) (Silverlight Plug-In; application/x-silverlight-2;).
Time Zone	2.72	6.61	-120
Screen Size and Color Depth	8.74	427.05	1536x864x24
System Fonts	22.01+	4235506	Adobe Caslon Pro Bold, Adobe Caslon Pro, Adobe Fangsong Std R, Adobe Fan Heiti Std B, Adobe Gothic Std B, Adobe Heiti Std R, Adobe Kaiti Std R, Adobe Naskh Medium, Adobe Garamond Pro Bold, Adobe Garamond Pro, Birch Std, Blackoak Std, Brush Script Std, Chaparral Pro, Chaparral Pro Light, Charlemagne Std, Cooper Std Black, Giddyup Std, Hobo Std, Kozuka Gothic Pro B, Kozuka Gothic Pro EL, Kozuka Gothic Pro H, Kozuka Gothic Pro L, Kozuka Gothic Pro M, Kozuka Gothic Pro R, Kozuka Mincho Pro B, Kozuka Mincho Pro EL, Kozuka Mincho Pro H, Kozuka Mincho Pro L, Kozuka Mincho Pro M, Kozuka Mincho Pro R, Lithos Pro Regular, Mesquite Std, Minion Pro Cond, Minion Pro Med, Minion Pro SmBd, Myriad Arabic, Nueva Std, Nueva Std Cond, OCR A Std, Orator Std, Poplar Std, Prestige Elite Std, Rosewood Std Regular, Stencil Std, Tekton Pro, Tekton Pro Cond, Tekton Pro Ext, Trajan Pro, Adobe Arabic, Adobe Devanagari, Adobe Hebrew, Adobe Ming Std L, Adobe Myungjo Std M, Adobe Song Std L, Kozuka Gothic Pr6N B, Kozuka Gothic Pr6N EL, Kozuka Gothic Pr6N H, Kozuka Gothic Pr6N L, Kozuka Gothic Pr6N M, Kozuka Gothic Pr6N R, Kozuka Mincho Pr6N B, Kozuka Mincho Pr6N EL, Kozuka Mincho Pr6N H, Kozuka Mincho Pr6N L, Kozuka Mincho Pr6N M, Kozuka Mincho Pr6N R, Letter Gothic Std, Minion Pro, Myriad Hebrew, Myriad Pro, Myriad Pro Cond, Myriad Pro Light, TeamViewer9, Marlett, Arial, Arabic Transparent, Arial Baltic, Arial CE, Arial CYR, Arial Greek, Arial TUR, Batang, BatangChe, Gungsuh, GungsuhChe, Courier New, Courier New Baltic, Courier New CE, Courier New CYR, Courier New Greek, Courier New TUR, DaunPenh, DokChampa, Estrangelo Edessa, Euphemia, Gautami, Vani, Gulim, GulimChe, Dotum, DotumChe, Impact, Iskoola Pota, Kalinga, Kartika, Khmer UI, Lao UI, Latha, Lucida Console, Malgun Gothic, Mangal, Meiryo, Meiryo UI, Microsoft Himalaya, Microsoft JhengHei, Microsoft YaHei, MingLiU, PMingLiU, MingLiU_HKSCS, MingLiU-ExtB, PMingLiU-ExtB, MingLiU_HKSCS-ExtB, Mongolian Baiti, MS Gothic, MS PGothic, MS UI Gothic, MS Mincho, MS PMincho, MV Boli, Microsoft New Tai Lue, Nyala, Microsoft PhagsPa, Plantagenet Cherokee, Raavi, Segoe Script, Segoe UI, Segoe UI Semibold, Segoe UI Light, Segoe UI Symbol, Shruti, SimSun, NSimSun, SimSun-ExtB, Sylfaen, Microsoft Tai Le, Times New Roman, Times New Roman Baltic, Times New Roman CE, Times New Roman CYR, Times New Roman Greek, Times New Roman TUR, Tunga, Vrinda, Shonar Bangla, Microsoft Yi Baiti, Tahoma, Microsoft Sans Serif, Angsana New, AparajIta, Cordia New, Ebrima, Gisha, Kokila, Leelawadee, Microsoft Uighur, MoolBoran, Symbol, Utsaah, Vijaya, Wingdings, Andalus, Arabic Typesetting, Simplified Arabic, Simplified Arabic Fixed, Sakkal Majalla, Traditional Arabic, Aharoni, David, FrankRuehl, Levenim MT, Miriam, Miriam Fixed, Narkisim, Rod, FangSong, SimHei, KaiTi, AngsanaUPC, Browallia New, BrowalliaUPC, CordiaUPC, DilleniaUPC, EucrosiaUPC, FreesiaUPC, IrisUPC, JasmineUPC, KodchiangUPC, LilyUPC, DFKai-SB, Lucida Sans Unicode, Arial Black, Calibri, Cambria, Cambria Math, Candara, Comic Sans MS, Consolas, Constantia, Corbel, Franklin Gothic Medium, Gabriola, Georgia, Palatino Linotype, Segoe Print, Trebuchet MS, Verdana, Webdings, MT Extra, Haettenschweiler, MS Outlook, Book Antiqua, Century Gothic, Bookshelf Symbol 7, MS Reference Sans Serif, MS Reference Specialty, Garamond, Monotype Corsiva, Agency FB, Arial Rounded MT Bold, Blackadder ITC, Bodoni MT, Bodoni MT Black, Bodoni MT Condensed, Bookman Old Style, Bradley Hand ITC, Calisto MT, Castellar, Century Schoolbook, Copperplate Gothic Bold, Copperplate Gothic Light, Curlz MT, Edwardian Script ITC, Elephant, Engravers MT, Eras Bold ITC, Eras Demi ITC, Eras Light ITC, Eras Medium ITC, Felix Titling, Forte, Franklin Gothic Book, Franklin Gothic Demi, Franklin Gothic Demi Cond, Franklin Gothic Heavy, Franklin Gothic Medium Cond, French Script MT, Gigi, Gill Sans MT, Gill Sans MT Condensed, Gill Sans Ultra Bold, Gill Sans Ultra Bold Condensed, Gill Sans MT Ext Condensed Bold, Gloucester MT Extra Condensed, Goudy Old Style, Goudy Stout, Imprint MT Shadow, Lucida Sans, Lucida Sans Typewriter, Malandra GD, OCR A Extended, Palace Script MT, Papyrus, Perpetua, Perpetua Titling MT, Pristina, Rage Italic, Rockwell, Rockwell Condensed, Rockwell Extra Bold, Script MT Bold, Tw Cen MT, Tw Cen MT Condensed, Tw Cen MT Condensed Extra Bold, Algerian, Baskerville Old Face, Bauhaus 93, Bell MT, Berlin Sans FB, Berlin Sans FB Demi, Bernard MT Condensed, Bodoni MT Poster Compressed, Britannic Bold, Broadway, Brush Script MT, Californian FB, Centaur, Chiller, Colonna MT, Cooper Black, Footlight MT Light, Freestyle Script, Harlow Solid Italic, Harrington, High Tower Text, Jokerman, Juice ITC, Kristen ITC, Kunstler Script, Lucida Bright, Lucida Calligraphy, Lucida Fax, Lucida Handwriting, Magneto, Matura MT Script Capitals, Mistral, Modern No. 20, Niagara Engraved, Niagara Solid, Old English Text MT, Onyx, Parchment, Playbill, Poor Richard, Ravie, Informal Roman, Showcard Gothic, Snap ITC, Stencil, Tempus Sans ITC, Viner Hand ITC, Vivaldi, Vladimir Script, Wide Latin, Century, Wingdings 2, Wingdings 3, Arial Unicode MS, Eurostile, Matisse ITC, MS Reference 1, MS Reference 2, Arial Narrow, GiovanniITCTT, Lucida Blackletter, Xirod, Liberation Sans Narrow, DejaVu Serif Condensed, Calibri Light, DejaVu Sans Condensed, OpenSymbol, Arimo, Gentium Basic, Gentium Book Basic, DejaVu Sans, DejaVu Sans Mono, DejaVu Serif, DejaVu Sans Light (via Flash)
Are Cookies Enabled?	0.43	1.35	Yes
Limited supercookie test	0.92	1.89	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No

GEGENMAßNAHMEN

- Aktuelle Open Source Browser nutzen
- Wenn, dann aktuelle Erweiterungen nutzen und sinnvollen Gebrauch machen
  → JS mit NoScript kontrollieren
- Wenn, dann aktuelle Plugins nutzen und sinnvollen Gebrauch machen
  → vor dem Ausführen nachfragen lassen
- Browser ab und zu auf Schwachstellen überprüfen
  → Add-ons und Plugins prüfen
  → Virenscan durchführen (können auch Browser infizieren)

Schwachstellenabfrage

Hasso-Plattner-Institut

All Search Self-Diagnosis Log In Language Vulnerability Database by Hasso-Plattner-Institut

Self-Diagnosis:

Firefox 30.0 on Windows 7 was detected on your machine

No vulnerabilities were found for Firefox 30.0 on Windows 7

The following plugins were detected in your browser:

In the case that your version could not be identified perfectly, you will get information about similar vulnerable versions.

Name	Your version	Similar Version	Plugin and its Vulnerabilities
Java	1.7.0.55		No vulnerabilities found for Java 1.7.0.55
Flash	14.0.0.125		No vulnerabilities found for Flash 14.0.0.125
AdobeReader	11.0.7.79		No vulnerabilities found for AdobeReader 11.0.7.79
VLC Player	2.1.0.0	2.1.0	1 Vulnerability for Videolan Vlc_media_player 2.1.0
Silverlight	5.1.30214.0		No vulnerabilities found for Silverlight 5.1.30214.0

Note: Most of the vulnerabilities could be solved with the current version of the browser and updates of every plugin.

… mit Firefox

Hasso-Plattner-Institut

Alle Suche Selbst-Diagnose Anmeldung Sprache Vulnerability Database by Hasso-Plattner-Institut

Selbst-Diagnose:

Explorer 11.0 auf Windows 7 wurde auf Ihrem Computer gefunden

← Vorige 1 2 3 … 8 9 Nächste →

*Das Farbschema basiert auf dem Schweregrad der Schwachstellen bzw. dem vergebenen CVSS_Score

Schwachstellen	Beschreibung	Notwendiger Bereich des Angreifers
CVE-2014-1776	Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows …	Netzwerk
CVE-2014-1765	Multiple use-after-free vulnerabilities in Microsoft Internet Explorer 11 allow remote …	Netzwerk
CVE-2014-1764	Microsoft Internet Explorer 7 through 11 allows remote attackers to …	Netzwerk
CVE-2014-1763	Use-after-free vulnerability in Microsoft Internet Explorer 11 allows remote attackers …	Netzwerk
CVE-2014-2782	Microsoft Internet Explorer 9 through 11 allows remote attackers to …	Netzwerk
CVE-2014-2776	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary …	Netzwerk
CVE-2014-2775	Microsoft Internet Explorer 9 through 11 allows remote attackers to …	Netzwerk
CVE-2014-2772	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary …	Netzwerk
CVE-2014-2771	Microsoft Internet Explorer 10 and 11 allows remote attackers to …	Netzwerk
CVE-2014-2769	Microsoft Internet Explorer 10 and 11 allows remote attackers to …	Netzwerk

← Vorige 1 2 3 … 8 9 Nächste →

Die folgenden Plugins wurden in Ihrem Browser erkannt:

Im Fall, dass Ihre Version nicht einwandfrei identifiziert werden konnte,werden Sie Informationen zu ähnlichen anfälligen Versionen erhalten.

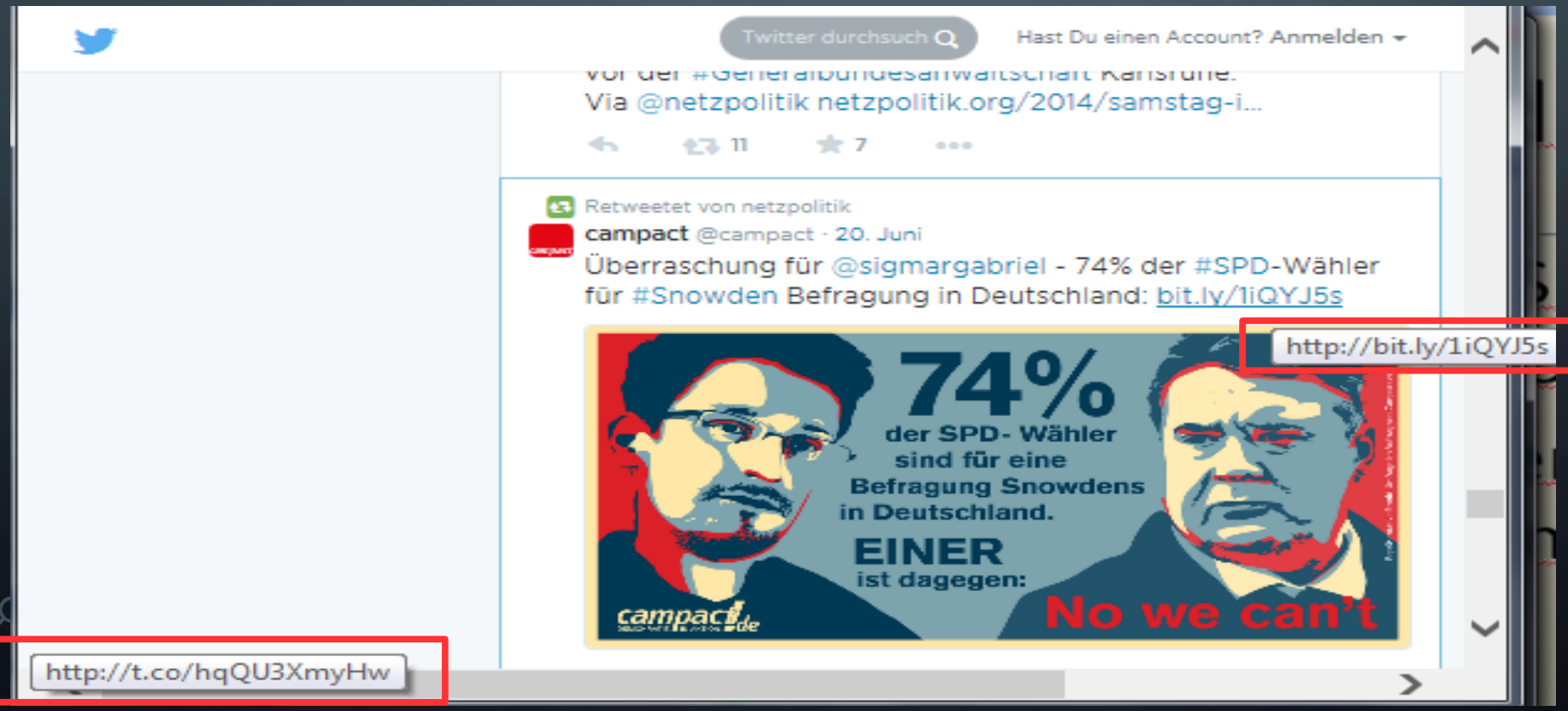
Name	Ihre Version	Ähnliche Version	Plugin und dessen Schwachstellen
Flash	13.0.0.214		6 Schwachstellen für Adobe Flash_player 13.0.0.214
Silverlight	5.1.30214.0		Keine Schwachstellen gefunden für Silverlight 5.1.30214.0

Hinweis: Die meisten Schwachstellen können mit einem Update auf die aktuelle Version des Browsers oder der Plugins behoben werden.

… mit Internet Explorer

GEODATEN, URLS, REFERRER

- Geodaten: Smartphones, Apps, Apple-Produkte, Fotos
- Personalisierte URLS in Newslettern oder Weiterleitung über Trackingdienste; Referrer



towerdata
Formerly Rapleaf.com

Products & Pricing | About Us | Blog | Visit TowerData.com | Login

Email Intelligence, a TowerData Service

GET DATA ON YOUR EMAILS
START PERSONALIZING CONTENT FOR YOUR CUSTOMERS

To get started:

1. Enter the number of emails in your list
2. Click on the data fields you are interested in
3. Get an estimate of pricing for a batch append

Or create a free account to upload your file of email addresses and get an exact match report for free

Number of Emails	Fields Selected	Estimated Price
3,500	3 Age and 2 more	$57.40

Upload your file for an exact quote:

Create A Free Account

Which fields would you like to purchase?

	Select All	Estimated Matches	Field Price	Estimated Price
DEMOGRAPHIC DATA	☑ Age	1,715	$0.01	$17.15
	☑ Gender	2,800	$0.01	$28.00
	☑ Zip	1,225	$0.01	$12.25
HOUSEHOLD DATA	☐ Household Income	1,295	$0.01	$12.95
	☐ Marital Status	1,330	$0.01	$13.30
	☐ Presence of Children	1,400	$0.01	$14.00
	☐ Home Owner Status	1,400	$0.01	$14.00
	☐ Home Market Value	1,435	$0.01	$14.35
	☐ Length of Residence	1,400	$0.01	$14.00
	☐ High Net Worth	560	$0.01	$5.60
	☐ Occupation	315	$0.01	$3.15
	☐ Education	1,295	$0.01	$12.95
INTEREST DATA	☐ Arts & Crafts	245	$0.01	$2.45
	☐ Blogging	35	$0.01	$0.35
	☐ Books	525	$0.01	$5.25
	☐ Business	105	$0.01	$1.05
	☐ Health & Wellness	700	$0.01	$7.00
	☐ News & Current Events	210	$0.01	$2.10
PURCHASE DATA	☐ Automotive	210	$0.01	$2.10
	☐ Baby Product Buyer	35	$0.01	$0.35
	☐ Beauty	280	$0.01	$2.80
	☐ Charitable Donor	1,470	$0.01	$14.70
	☐ Cooking	560	$0.01	$5.60
	☐ Discount Shopper	490	$0.01	$4.90
	☐ High-End Brand Buyer	245	$0.01	$2.45
	☐ Home & Garden	490	$0.01	$4.90
	☐ Home Improvement	490	$0.01	$4.90
	☐ Luxury Goods & Jewelry	105	$0.01	$1.05
	☐ Magazine Buyer	770	$0.01	$7.70
	☐ Outdoor & Adventure	245	$0.01	$2.45
	☐ Pets	245	$0.01	$2.45
	☐ Sports	490	$0.01	$4.90
	☐ Technology	420	$0.01	$4.20
	☐ Travel	210	$0.01	$2.10

Frequently Asked Questions

- How is price calculated?
- What's an estimated match?
- What is a field price?
- Where's your data dictionary?
- How do I purchase?
- Do you offer bulk discounts?

More FAQs

PRÄVENTION - VERHALTEN

- Überlegen, ob wirklich jede 2. Seite den Facebook-Login braucht (das führt dazu, dass diese auf sämtliche Daten zugreifen kann)
  → generell ist dieser nie notwendig, nur bequem
- Nachsehen, wohin ein Link zeigt, notfalls die URL direkt eingeben
  → dadurch landet man definitiv da, wo man hinwollte, ohne Umleitungen
  → nur, wenn man sich nicht vertippt hat
- Links möglichst nicht googlen oder über andere Verweise suchen
  → Lesezeichen setzen, um Seiten wiederzufinden
- Privaten Modus des Browsers nutzen, damit Cookies gelöscht werden
- „Eingeloggt bleiben“-Funktion beim Login für z.B. Shopping-Portale nicht nutzen
  → setzen Ever-Cookies oder speichern MAC-Adresse über Javascript

PRÄVENTION – TECHNISCHE MAßNAHMEN

Es gibt eine Vielzahl von Plugins, die das Browsen sicherer machen, hier eine Auswahl der wichtigsten (Firefox):

→ AdBlockPlus blockiert Werbung und verhindert Zugriff auf Fremdwebseiten

→ Ghostery hindert Browser, Verbindungen zu Werbenetzwerken und Trackern aufzubauen

→ NoScript deaktiviert Javascript, sodass Webseiten nur sehr eingeschränkte Methoden zur Identifizierung des Nutzers zur Verfügung stehen

→ Self-Destructing Cookies löscht alle Cookies, sobald die Seite verlassen wurde

→ FireGloves versteckt installierte Addons und Schriftsätze bei der Abfrage durch die Webseite, um das Fingerprinting zu erschweren

→ WebOfTrust kennzeichnet die Vertrauenswürdigkeit von Webseiten aufgrund von Nutzermeinungen

→ HttpsEverywhere zwingt die meisten Webseiten, verschlüsselte Verbindung zu nutzen

PRÄVENTION – TECHNISCHE MAßNAHMEN (II)

Nicht nur Plugins sind wichtig, ebenso wichtig sind die Einstellungen des Browsers:

- Cookie-Verarbeitung:
  → Cookies von Drittanbietern sollten niemals akzeptiert (d.h. gespeichert) werden
- Verschlüsselung:
  → Browser sollte keine alten Verschlüsselungsverfahren akzeptieren (RC4)
- Privatsphäre
  → Browser sollte Seitenverlauf (Browser Historie) und Cookies beim Beenden löschen
  → Telemetry (Senden von Nutzungsstatistiken) sollte deaktiviert werden
- Plugins
  → auf PlugIns wie zum Beispiel Flash, Java sollte verzichtet werden

HINWEIS

Verschlüsselung in der Praxis zeigen wir in unserem anschließendem Workshop

Swap 11: Verschlüsselung im Alltag, Melanchtonianum HS A, 13 – 14 Uhr

- E-Mail
- Alternativen zu gängigen Chatprogrammen
  → Facebook, Skype, etc.
- Browserkonfiguration

VIELEN DANK FÜR EURE AUFMERKSAMKEIT ☺

Hintergrundinfos zu Schwachstellen allgemein

→ http://www.heise.de/security/dienste/Browsercheck-2107.html

- Browser auf bekannte Schwachstellen überprüfen lassen

  → https://hpi-vdb.de/vulndb/sd_first/

- Tracking und Anonymität Hintergrundwissen

  → https://www.privacy-handbuch.de/print.htm

- Browserfingerprinttest

  → https://panopticlick.eff.org/

- http://download.terminal21.de/workshops/swap2015/Sicherheit_im_Internet.pdf