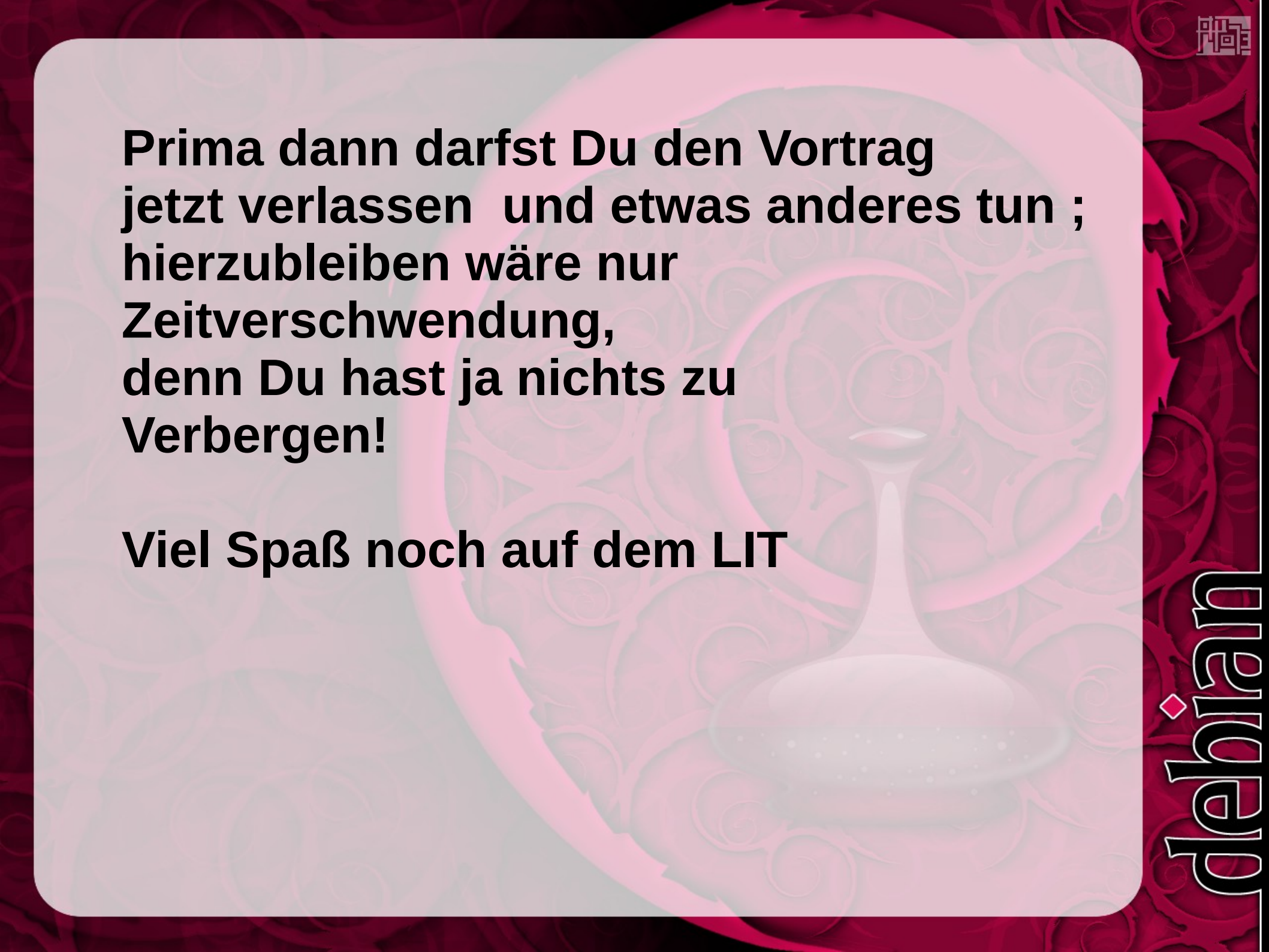


“Ich habe doch nichts zu
verbergen!”

By Uli Kleemann
uek@ukleeman-bw.de

Linux Info Tag
06. 04. 2019
Augsburg





**Prima dann darfst Du den Vortrag
jetzt verlassen und etwas anderes tun ;
hierzubleiben wäre nur
Zeitverschwendung,
denn Du hast ja nichts zu
Verbergen!**

Viel Spaß noch auf dem LIT

Das kostet doch nichts

- Email
- Chat
- Messenger
- Soziale Netzwerke
- Google Dienste (Navigation)
- Suchmaschinen

Ich fürchte für dich ist der Vortrag auch
nicht das Richtige.
Vielleicht suchst du
Dir lieber einen anderen Talk,
der dich mehr interessiert.

Viel Spass noch auf dem LIT

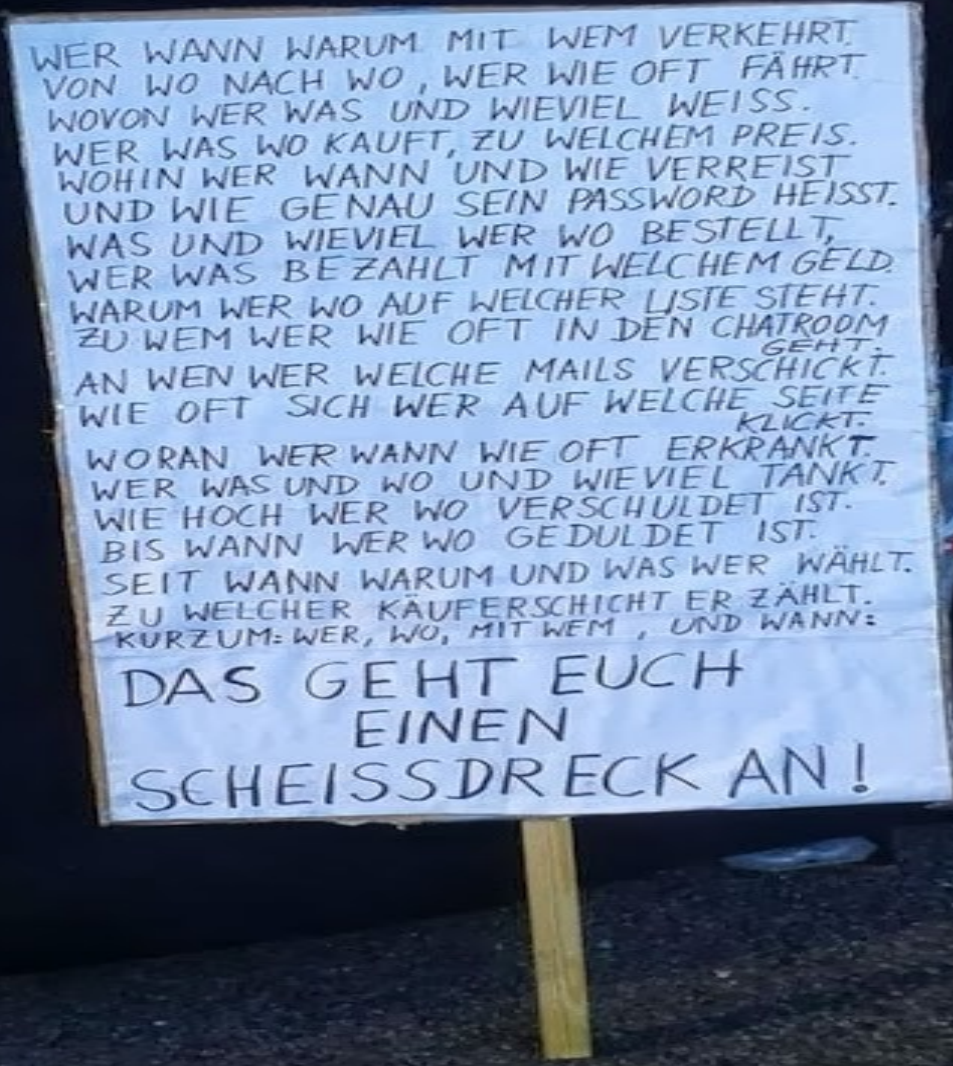
3 Internetwahrheiten

1. Das Web ist ein offenes Netz d.h. jeder kann alle Informationen über seine Funktionalität in Erfahrung bringen, Sicherheit spielte bei der Implementierung keine Rolle, jeder kann mitlesen !!!

2. “There is no free lunch!” Es gibt nichts für nichts auch nicht im web!!!!

3. IN THE INTERNET NOBODY KNOWS THAT YOU ARE A DOG!!!!

Noch'n Gedicht



WER WANN WARUM MIT WEM VERKEHRT.
VON WO NACH WO, WER WIE OFT FÄHRT.
WOVON WER WAS UND WIEVIEL WEISS.
WER WAS WO KAUFTE, ZU WELCHEM PREIS.
WOHIN WER WANN UND WIE VERREIST.
UND WIE GENAU SEIN PASSWORD HEISST.
WAS UND WIEVIEL WER WO BESTELLT,
WER WAS BEZAHLT MIT WELCHEM GELD.
WARUM WER WO AUF WELCHER LISTE STEHT.
ZU WEM WER WIE OFT IN DEN CHATROOM
AN WEN WER WELCHE MAILS VERSCHICKT.
WIE OFT SICH WER AUF WELCHE SEITE
WORAN WER WANN WIE OFT ERKRANKT.
WER WAS UND WO UND WIEVIEL TANKT.
WIE HOCH WER WO VERSCHULDET IST.
BIS WANN WER WO GEDULDET IST.
SEIT WANN WARUM UND WAS WER WÄHLT.
ZU WELCHER KÄUFERSCHICHT ER ZÄHLT.
KURZUM: WER, WO, MIT WEM, UND WANN:

DAS GEHT EUCH
EINEN
SCHEISSDRECK AN!



Worum gehts hier eigentlich?



Darum; euere Daten sind bares Geld wert, weshalb sich soviel Mühe gemacht wird heranzukommen.

Versprechen und Vertrauen ?

Sicherheit was bedeutet sicher?

Wovor schützt was?

“Heute hack ich, morgen phish ich
und übermorgen klau ich deine Identität.”



“Ach wie gut daß niemand weiss, wie ich euch im Netz bescheiss”

- Gratis Download
- Gratis Domain
- Gratis Email
- Gewinnspiel

Ich will doch nur alle deine Daten

Der Spion auf deinem Rechner

- IP: 84.141.45.1xx
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36
- Decimal: 1418538350
- Sprache: en-US,en;q=0.9
- Hostname: p548d2d6e.dip0.t-ipconnect.de
- ASN: 3320
- ISP: Deutsche Telekom AG
- Organization: Deutsche Telekom AG
- Operating System: Linux Platform: UNIX
- Internet Browser: Chrome 72.0.3626.109 Beta
- Version: Yes Connection Speed: 6.08 Mbps
- Restrictive Firewall: Yes Local Date/Time: 3/8/2019, 6:43:05 PM Language: English System Language: Not detectable with this browser User Language: en-us Popups Blocked: Yes SSL Support: Yes SSL Enabled: No Style Sheet Support: Yes Supports Tables: Yes Table Cell BG Colors: Supported Table Cell BG Images: Supported CDF Support: No (Channel Definition Format) Color Depth: 16.77 Million Colors (24-bit True Color) Supports GZip: Yes Supports Cookies: Yes Cookies Enabled: Enabled Supports JavaScript: Yes JavaScript Enabled: Yes JavaScript Version: 1.8 JavaScript Build: Not detectable with this browser Supports VBScript: No Supports ActiveX: No ActiveX Enabled: No Supports Java: Yes Java Enabled: No Java Vendor: Java N/A (requires Java plugin, not available) Java Version: Java N/A (requires Java plugin, not available) MS JVM Build: Not detectable with this browser Supports DHTML: Yes Supports Uploads: Yes Supports Frames: Yes Gecko Engine: Yes Screen Dimensions: 1024 x 768 Browser Dimensions: 996 x 637 Supports IFrames: Yes Images Enabled: Yes PNG Support: Yes XML Support: Yes MS XML Parser: Not detectable with this browser Background Sounds: Supported Supports MouseOver: Yes Windows Installer: 0 .NET CLR Installed: No MS Media Player: Not installed Apple QuickTime: Not installed RealPlayer: Not installed Adobe Acrobat: Not installed Adobe SVG Viewer: Not installed Macromedia Flash: Not installed Macromedia Director: Not installed Macromedia Authorware: Not installed Citrix: Not installed iPIX Image Viewer: Not installed Crystal Reports: Not installed Viewpoint: Not installed Autodesk MapGuide: Not installed NetMeeting Build: Not detectable with this browser Using PDA: No WAP Support: No Proxy Connection: No Font Smoothing: No Font Sizing: Yes IE Text Size: Not detectable with this browser Fonts Installed:
- Und das ist noch nicht alles

Add-ons, plugins, Anonymizer & Proxies

Da bin ich doch dann anonym?

- Betreiber HTML/CSS/FTP JavaScript Java
- Anonymouse Gebrochen Gebrochen* Gebrochen
- Cyberghost Web - Gebrochen Gebrochen
- Hide My Ass! - Gebrochen* Gebrochen
- WebProxy.ca - Gebrochen Gebrochen
- KProxy- Gebrochen* Gebrochen
- Guardster - Gebrochen (falls erlaubt)* Gebrochen
- Megaproxy Gebrochen (kostenfrei nicht verfügbar) (kostenfrei nicht verfügbar)
- Proxify - Gebrochen (falls erlaubt) Gebrochen (falls erlaubt)
- Ebumna Gebrochen Gebrochen* Gebrochen

Gebrochen : Ihre eigene IP-Adresse wird aufgedeckt. Beachten Sie, dass auch Ihre privaten Browser-Daten aufgedeckt werden...

- * : Der so markierte Dienst erreicht nicht einmal die Testseite wenn JavaScript aktiviert ist. Er parst so schlecht, dass der Browser in manchen Fällen den Dienst einfach stillschweigend verlässt.

Dein Fingerabdruck im Netz

ich weiss was du denkst, was dich interessiert und was du am 17.01.2018 getan hast

Webseitenbetreiber können euch im Internet eindeutig anhand eures Browser-Fingerprints erkennen und verfolgen, um euch etwa individualisierte Werbung anzuzeigen oder euer Surf-Verhalten zu analysieren

Passives Fingerprinting: Informationen, die vom Computer automatisch an den Webserver übermittelt werden.

Beispiel: IP-Adresse, verwendeter Browser

Aktives Fingerprinting: Informationen, die sich durch JavaScript oder Flash auslesen lassen.

Beispiel: Betriebssystem-Informationen, Zeitzone, Schriftarten, Auflösung, Fenstergröße

Wenn eurer Browser im Internet also durch seine Konfiguration mit Plugins und Addons einzigartig ist, lässt er sich auch immer eindeutig zuordnen und euch als diesen einen Surfer wiedererkennen

“Eigentlich mag ich gar keine Kekse”



**Cookies sind kleine Textdateien, die
- ohne dass du es merkst -
gespeichert werden**

**Cookies speichern Informationen wie z. B. die bevorzugte Sprache
Bildschirmauflösung, installierte Schriften u.ä., um dich
wiederzuerkennen**

**Cookies können eine Vielzahl von Informationen beinhalten,
die dich eindeutig identifizierbar machen
(wie Namen, Adresse, E-Mail-Adresse oder Telefonnummer)**

**Eine Website hat jedoch nur Zugang zu persönlichen Daten,
die DU selbst bereitstellst.**

**So kann eine Seite z.B. nicht deine E-Mail-Adresse ermitteln.
Eine Website kann auch nicht auf andere Dateien
auf deinem Computer zugreifen.**

Ganz böse Kekse

- Third party cookies
diese Kekse stammen von “fremden” Seiten
- Sie dienen einzig und allein dazu euch auszuspionieren
- Es interessieren vor allem
- Wie lange Du eine Seite besuchst
- Wo du zuvor warst
- Welche Links du angeklickt hast
- Die Gesamtheit dieser Informationen liefert ein gutes Bild von dir, denn hier kann nicht nur nachverfolgt werden, wofür Du dich innerhalb einer Domain interessiert, sondern über mehrere Domains hinweg. Third Party Cookies erlauben damit die Erstellung von umfangreichen Nutzerprofilen

“Jet zo laache” Was luschediges

Third Party Cookies – der Datenschutz

Es gibt zwar eine europäische Richtlinie zur Verarbeitung, Speicherung, Nutzung und Weitergabe persönlicher Daten – die E-Privacy-Richtlinie (auch Cookie Richtlinie genannt) – diese wurde in Deutschland jedoch noch nicht umgesetzt.

- Gemäß der E-Privacy-Richtlinie muss der Nutzer ausdrücklich zustimmen, dass seine Daten getrackt werden. Die Umsetzung sollte durch die sogenannte Opt-in/Opt-out Funktion erfolgen.
- Deutschland hat zwar die Richtlinie nie aktiv umgesetzt, d.h. kein Gesetz dazu erlassen, geht aber davon aus, dass die Umsetzung auch nicht notwendig gewesen wäre, weil die deutsche Rechtslage (durch das Telemediengesetz) bereits diese Vorgaben erfüllt hätte.

Javascript machts möglich

- Erfunden von Brendan Eich um Interaktion im Browser zu ermöglichen
- Kann direkt in die Webseite eingefügt werden, oder aus dem HTML-Code heraus der Skriptcode einer separaten JavaScript-/JScript-Datei aufgerufen werden
- unzählig oft weitere Fenster zu öffnen und damit eine Art Denial-Of-Service-Angriff auf den Anwenderrechner zu verursachen
- Im schlimmsten Fall erhält ein Außenstehender vollständigen Zugriff auf den Rechner.
- Möglichkeiten, mit JScript/JavaScript-Elementen den Anwender zu täuschen. So können ganze Eingabefenster von vertrauenswürdigen Webseiten simuliert werden, wodurch beispielsweise Benutzernamen, Passwort oder andere sensible Daten wie Kreditkarteninformationen abgefangen und übertragen werden können.
- Über spezielle Funktionen kann die Statusleiste des Web-Browsers verändert werden, so dass die dort angezeigte Adresse nicht der der tatsächlich verlinkten Webseite entspricht.
- Unter JavaScript/JScript können jedoch durch Verschleierung entsprechender HTML-Tags mit JavaScript/JScript-Funktionen beispielsweise Java-Applets auf dem lokalen Rechner des Anwenders ausgeführt werden, auch wenn die Firewall die Applets eigentlich herausfiltern sollte.
- Nachfolgend ein Beispiel für die Verschleierung von HTML-Tags:

```
document.write('<APP');  
document.write('LET\n');  
document.write('CODE=client.Main.class \n>');  
document.write('CODEBASE=base \n>');  
document.write('ARCHIVE=clientapplet.jar \n>');  
document.write('</APPLET>') ;
```

Ich weiss auch wo deine Haus wohnt

- JS ermöglicht deinen Standort zu ermitteln und zu übertragen

“Mit der Geolocation API können sie den Standort des Clienten ermitteln. Dies ist besonders interessant, um Benutzern maßgeschneiderte Antworten auf Suchanfragen, zielgerichtete Werbung und regionale Informationen zukommen zu lassen.[1] Neben den Daten zum Standort können die **Genauigkeit der Koordinaten, Geschwindigkeit und Richtung der Bewegungen** aufgezeichnet werden. “

```
var button=document.getElementById('los');
• button.addEventListener('click', ermittlePosition);
• var ausgabe = document.getElementById('ausgabe');
•
• function ermittlePosition() {
•   if (navigator.geolocation) {
•     navigator.geolocation.getCurrentPosition(zeigePosition);
•   } else {
•     ausgabe.innerHTML = 'Ihr Browser unterstützt keine Geolocation.';
•   }
• }
•
• function zeigePosition(position) {
•   ausgabe.innerHTML = "Ihre Koordinaten sind:<br>Breite: " + position.coords.latitude +
•   "<br>Länge: " + position.coords.longitude;
• }
```

- JS verrät wo du dich im Web herumgetrieben hast

```
GET /data?title=ZEIT%20ONLINE%20%7C%20Nachrichten%2C%20Hintergr%C3%BCnde%20und%20Debatten&hostSiteUrl=http%3A%2F%2Fwww.zeit.de%2Findex&userAgent=5.0%20(X11)&userLang=en-US&color=24&os=Linux%20x86_64&timezone=-2&screen=1053x1920&event_id=page_view&_sid=97578&_ver=0.1.13&_seg=jsonp&_id=893025804693 HTTP/1.1
```

- Host: ups.xplosion.de
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
- Accept: */*
- Accept-Language: en-US,en;q=0.5
- Accept-Encoding: gzip, deflate
- Referer: https://www.zeit.de/index
- DNT: 1
- Connection: close

- Es wird analysiert, welche Beiträge bzw. Links ein Nutzer auf den News-Portalen anklickt. Anhand dieser Informationen entsteht ein Nutzerprofil bei emetriq, die jeden Klick erfassen also was dich interessiert, was Du für Videos schaust, Artikel liest usw. Somit was Du denkst!



Ich kenne alle deine Wege

• **Beispiel: verfolge jede Standortänderung**

```
var id, ziel, options;
• //Verfolgen beginnen
• id = navigator.geolocation.watchCurrentPosition(verfolgePosition);
•
• function verfolgePosition(pos) {
•   var aktuell = pos.coords;
•
•   if (ziel.latitude === aktuell.latitude && ziel.longitude === aktuell.longitude) {
•     console.log("Sie haben Ihr Ziel erreicht");
•     //Verfolgen beenden
•     navigator.geolocation.clearWatch(id);
•   }
• }
•
• ziel = {
•   latitude : 0,
•   longitude: 0
• };
•
• options = {
•   enableHighAccuracy: false,
•   timeout: 5000,
•   maximumAge: 0
• };
•
•
•
```

Brave new World HTML5

- Die Geolocation API ist eine HTML5 Javascript-Schnittstelle mit offiziellen W3C-Spezifikationen.
- Dabei werden vom Browser mehrere Methoden genutzt, um den besten Standort des Nutzers zu ermitteln. Das wären zum Beispiel: GPS-Sender
- WLAN-Netzwerke
- Funk-Signale (Handynetz)
- IP-Adresse
- Vom Benutzer definierter Standort

Richtig spannend wird die Geolocation API natürlich erst mit mobilen Geräten wie Smartphones oder Tablets, die sich immer größerer Beliebtheit erfreuen. Hier ist in fast alle Geräten ein GPS-Sender oder 3G-Modem verbaut und die Position des Nutzers lässt sich im Idealfall auf den Meter genau bestimmen.

Dieser Beschatter wird niemals müde!

Das WOT plugin und anderes Snakeoil

- User bewerten Seriösität einer Webseite

“A Safer Browsing Experience”

WOT checks every website before you visit it to let you know its safety and security rating.

- <https://www.kuketz-blog.de/wot-addon-wie-ein-browser-addon-seine-nutzer-ausspaecht/>
- WOT weist in seinen Nutzer- und Datenschutzbestimmungen darauf hin, dass die Daten seiner Nutzer anonymisiert und entpersonalisiert gespeichert und weiterverarbeitet werden. (Wikipedia)
- Die Datensätze, die der NDR von den Datenhändlern erwarb, ließen sich teilweise durch enthaltene Klarnamen oder E-Mail-Adressen in den URLs des Browserverlaufs eindeutig einem jeweiligen Nutzer zuordnen (Wikipedia)

War doch nur ein Katzenbild

Wie Trojaner und Malware dich erreichen

- Einfallstor Nr 1 Email
- Schadcode in harmlos erscheinender pdf oder Bilddatei versteckt (Steganografie)
- Versucht über Zwischenschritte höhere Rechte zu erlangen
- Baut tcp Verbindung zu Server auf
- Liest deine Festplatte aus
- Snifft den Netzwerktraffic mit (Passwörter)

Rootkits

Jetzt gehörst Du mir!

- Der Begriff „Rootkit“ stammt aus der Unix-Welt. Er bezeichnete eine Sammlung modifizierter Systemprogramme, die dem Angreifer illegalen Root-Zugriff („Root“ ist auf Unix-Systemen der Administrator) verschafften und die dadurch entstandenen Spuren verwischten.
- Rootkits "an sich" richten keinen Schaden an.
- Rootkits nutzen zur Verbreitung meist einen Trojaner, den der Nutzer über einen E-Mail-Anhang erhält oder selbst von einer Webseite herunterlädt. Ebenso können sie durch infizierte Dokumente (wie PDF-Dateien) oder Computerwürmer verbreitet werden.
- Es gibt vier Arten von Rootkits:
 - Application-Rootkits (mittlerweile unbedeutend)
 - Kernel-Rootkits (extrem gefährlich laufen im sog. Kernspace)
 - User-Mode-Rootkits (können nicht unmittelbar auf Speicherbereich anderer Anwendungen zugreifen jedoch mittels z.B. IAT oder Code injection in den Kernel-space "gelangen")
- Speicher-Rootkits lassen sich nur im Hauptspeicher eines Computers nieder
- Wird der PC aus unerfindlichen Gründen plötzlich langsam oder scheint die Internetverbindung immer wieder überlastet zu sein, spricht dies ebenfalls für einen möglichen Rootkit-Befall

Was tun?

- Oma und Mama Regeln befolgen!
- Wenn Du nicht erwischt werden möchtest – lass es einfach sein!
- Von Fremden nimmst Du nichts an!
- Fremden öffnest Du niemals die Tür!
- Benutze 3 verschiedene Browser! (Privat, beruflich, online shopping)
- Gegen auslesen und mitlesen hilft nur verschlüsseln!
- Traue nichts und niemandem das und den Du nicht persönlich kennst!
- Überprüfe alles vorher! (URLs, Signaturen, Schlüssel)
- Halte dein System sauber!
- Gib niemals deine privaten Schlüssel oder deine Passwörter heraus
- 1 Passwort für alles ist keine gute Idee
- Private Schlüssel und Passwörter gehören extern gespeichert! (usb Sticks)
- Tu es erst wenn Du es wirklich verstanden hast!!!!
- Verwende niemals Passwörter, die sich von deiner Person ableiten lassen oder aus einem Wörterbuch stammen!
- Nutze 2 oder besser Multiauthentifizierung!
- Biometrische Merkmale alleine sind unsicher!
- Zum Experimentieren gibt es virtuelle Maschinen!

Zusammenfassung

- Internet ist per se unsicher!
- Erst denken dann klicken!
- Es giebt niemals etwas für nichts auch nicht im Cyberspace!!!
- Gehe so sparsam mit deinen Daten um wie mit Geld!
- Vertraue im Netz nichts und niemand, das / den du nicht überprüfen kannst!
- Verschlüssele deine Daten und Emails
- Was dir komisch vorkommt lass liegen!
- Vorsicht mit add-ons und plugins!
- Sicherheit gibt es nicht umsonst!
- Verwahre deinen privaten Schlüssel und Passwörter niemals auf deinem Rechner!
- Halte dein Sytem stets aktuell!

Danke fürs zuhören / Fragen

- Uli Kleemann
Linux Sysadmin
office@ukleemann-bw.de



Credits & License

- Content by <Put Your Name>
<http://<PutYourWebsite>>
License: <Put Your License>
- OpenOffice.org template by Raphaël Hertzog
<http://raphaelhertzog.com/go/ooo-template>
License: GPL-2+
- Background image by Alexis Younes “ayo”
<http://www.73lab.com>
License: GPL-2+