JRCTRAINING
Seminare | Kommunikation | Prozesse

Sicher(er) bewegen im Internet

Methoden der verdeckten Datenerhebung
Mehr Schutz vor Datenmissbrauch mit einfachen Mitteln

JRC Training J. Roth
Walter-Gieseking-Str. 14 | 30159 Hannover
Tel. 0511-4751840 | E-Mail info@jrc-training.com
www.**JRC-TRAINING**.com

Inhaltsverzeichnis

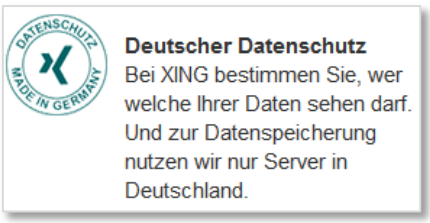
1. Warum Sicherheit auch für den eigenen PC wichtig ist

"Datensicherheit" ist in aller Munde und wird zunehmend als Kaufargument genutzt, da die Industrie erkannt hat, dass auch mit inhaltsleeren Begriffen geworben werden kann.

In der Lebensmittelbranche etwa wird gerne mit der Aufschrift "Spitzenqualität" geworben, die aber keine überprüfbare Qualitätsstufe bedeutet.

Das Internet-Pendant ist der Spruch "Ihre Datensicherheit ist uns wichtig", der sich unisono auf vielen Seiten findet; gefolgt von dem Satz, dass ich Cookies und andere Schnüffelfunktionen "für ein besonderes Surferlebnis" akzeptieren muss.

Gerne geben sich Internetseiten auch selbst erstellte Siegel, wie z.B. Xing, dem selbsternannten führenden Kontaktnetzwerk für Berufskontakte, um zusätzliches Vertrauen zu schaffen:

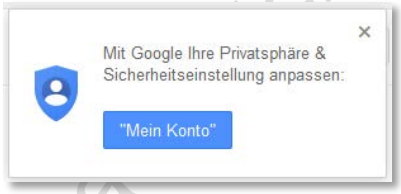


Tatsächlich versucht Xing, seinen Serverstandort zu verschleiern (Stand 10-19):

Hostname	www.xing.com	Internetdienstanbieter	New Work SE
Kontinent	Europa	Nationalflagge	?
Land	Unbekannt	Ländercode	Unbekannt
Region	Unbekannt	Lokale Zeit	22 Oct 2019 09:56 CEST
Stadt	Unbekannt	Postleitzahl	Unbekannt
IP-Adresse	109.233.155.204	Breitengrad	47
		Längengrad	8

Unabhängig davon können auch als "privat" gekennzeichnete Daten abgerufen werden (z.B. mit Google-Parametern oder OSint-Tools), Daten bleiben also für jedermann sichtbar. Hier wäre mehr Aufklärung nötig, dass "privat" eine Empfehlung und keine einklagbare Sicherheitseinstellung bedeutet.

Noch weiter mit der Irreführung treibt es Google selber: Seit Juni 2015 kann ich meine Spuren auch bei Google anonymisieren:



Auch hier soll die selbsterfundene Polizei-Vignette Vertrauen schaffen, also "besonders sicher"; "Mein Konto" deutet es aber an: Nur, wenn ich mich bei Google anmelde, werden die Spuren gelöscht.

Und auch das nur begrenzt: Google legt sofort wieder Schnüffelfunktionen auf dem eigenen PC ab, wie Cookies mit Langzeitstempeln (siehe dazu unten).

Wer sich die Mühe macht, Sucheinträge bei Google entfernen zu lassen (Google ist dazu nicht verpflichtet, sondern Sie müssen einen Antrag dazu stellen!), kann sich die Mühe sparen: Sobald Sie Zugriff auf die amerikanische Seite von Google haben, z.B. über www.google.com**/ncr**, können auch "entfernte" Sucheinträge wieder sichtbar gemacht werden.

Sie müssen sich also selber schützen vor unkontrolliertem Ausspähen, und genau hierbei soll diese Unterlage Sie unterstützen.

1.1 Rechtliche Inhalte

Sie finden hier eine lose Sammlung von Informationen zum Thema Datensicherheit, die aus verschiedenen Workshops, Präsentationen und Vorträgen zusammengestellt ist.

Zielgruppe ist der "normale" Anwender, sprachlich vermeiden wir darum, wo nicht benötigt, zu tiefe technische Erklärungen, unnötige Fachbegriffe und Anglizismen und versuchen, Vorgänge umgangssprachlich und verständlich zu halten. Wir nehmen dazu technische Ungenauigkeiten in Kauf, das Ziel "mehr Datensicherheit" zählt.

Hier werden Techniken und Tools vorgestellt, die sowohl von Hackern als auch von Sicherheitsexperten eingesetzt werden. Sie selber können diese Techniken nutzen, um die Sicherheit des eigenen Netzwerks oder WLANs zu prüfen. Bei "fremden" Netzen drohen bei der Verwendung dieser Techniken strafrechtliche Konsequenzen (§ 202 a-c StGB, der "Hacker-Paragraph").

Dies gilt auch für die Verwendung von Software, die speziell für diesen Zweck programmiert wurde.

Zudem erhebt die Sammlung keinen Anspruch auf Vollständigkeit, sondern wird ständig ergänzt und aktualisiert.

Stand 02-2020.

1.2 Vom Irrglauben eines sicheren Internets: 7 falsche Aussagen

"Ich besitze keine wertvollen Informationen" oder: "Ich habe nichts Interessantes zu verbergen".	*Jeder* Computernutzer besitzt wertvolle Daten: Passwörter für Online-Banking, Kennwörter für E-Mail- oder Web-Accounts etc. etc.: Gerade diese Infos sind für Identitätsdiebe besonders wertvoll! Und außerdem: Warum wollen staatliche Institutionen oder auch andere unbedingt wissen, dass ich nichts zu verbergen habe?
"Das Internet ist zu groß, um gerade mich anzugreifen."	Hacker setzen vollautomatisierte Angriffs-Tools ein, um Schwachstellen aufzudecken. Ein neuer, ungeschützter Computer, der erstmalig mit dem Internet verbunden wird, ist innerhalb von sieben Minuten kompromittiert, also im Netz bloßgestellt[1].
"Ich lösche stets alle kritischen Daten auf meiner Festplatte - damit sind sie weg."	Es wird nur der Verweis, nicht die Datei selber entfernt: Auch wenn die Datei nicht mehr angezeigt und gefunden wird. Sie bleibt, bis sie irgendwann mit einer neuen Datei überschrieben wird. Nur mit speziellen Löschprogrammen wie CCleaner, die freien Speicherplatz mehrfach und sektorweise überschreiben, werden Daten endgültig gelöscht. Und nie Festplatten in alten PCs lassen!
"Mein Computer ist sicher weil, wie überall empfohlen, mit Antivirus und Firewall geschützt."	Jedes internetfähige Gerät birgt potenzielle Schwachstellen für Angreifer, z.B. offene Ports und IP-Adressen. Cookies und Tracker schaffen ein unkontrollierbares Gefahrenpotential: Nur eine Kombination von Antiviren- und Antischnüffelsoftware sowie spezifischen Grundeinstellungen des PCs schaffen mehr Sicherheit.
"Ich bekomme mit, wenn mein Computer infiziert wurde: Er reagiert dann anders."	Die Entwicklung ist mittlerweile so weit fortgeschritten, dass kaum ein Nutzer merkt, wenn der PC als Teil eines Botnetzes zum Versenden von Spam missbraucht wird oder über Trojaner andere Computer angreift.
"Gefährliche Webseiten lassen sich schon an der Optik erkennen."	Cyberkriminelle tun alles, um eben das zu verhindern: Sie entwickeln Websites, die seriös und professionell aussehen oder vertrauten Internet-Diensten eins zu eins gleichen: Es reicht dann ein einziger Klick auf einen Link, und der ahnungslose Besucher sitzt in der Falle, sein PC wird dann z.B. gesperrt und nur gegen Bezahlung wieder freigegeben.
"EMails von Freunden und Infos bekannter Dienste kann ich gefahrlos öffnen, bei allen anderen bin ich vorsichtig."	Es ist einfach, sich beim Versenden einer Mail als jemand anders auszugeben: Parameter von Google benutzen, etwas im Social Web herumstöbern, überzeugende Argumente, ein falscher Name im Absender-Feld, eine geklaute oder kaum sichtbar abgeänderte EMail-Adresse als Absender und gefährliche Links in der EMail oder deren Anlage - fertig ist die Falle für den Empfänger.

[1] *nach Schätzungen des BSI (Bundesamt für Sicherheit in der Informationstechnik)*

1.3 Beispiel eines ungeschützten Routers: So wird gehackt

Nur Geräte ohne eine Netzwerkverbindung und Router ohne WLAN sind sicher vor Hacker-Angriffen:

Unbefugte kommen dann nur an Daten heran, wenn sie direkten Zugang zum Gerät haben oder Spionage-Software etwa über einen USB-Stick einschleusen. Geräte ohne Netzwerk bzw. Internetanbindung sind aber inzwischen die Ausnahme ("Internet of Things"). Und ein WLAN ist natürlich noch leichter zu hacken, weil es über die Grenzen der Wohnung hinaus funkt.

Der ausdrückliche Hinweis: Hier werden Techniken und Tools vorgestellt, die sowohl von Hackern als auch von Sicherheitsexperten eingesetzt werden. Sie selber können diese Techniken nutzen, um die Sicherheit des eigenen Netzwerks oder WLANs zu prüfen. Bei "fremden" Netzen drohen bei der Verwendung dieser Techniken strafrechtliche Konsequenzen (§ 202 a -c StGB "Hackerparagraphen").

Dasselbe gilt, wenn Sie Programme verwenden, die genau zu diesem Zweck programmiert wurden.

Die Geräte in Ihrem lokalen Netzwerk sind standardmäßig zwar nicht von außen erreichbar, auf sie kann aber über die Hauptschwachstelle aller Geräte mit Netzwerkanschluss, der eindeutigen IP-Adresse, über das Internet (und dort über Umwege) zugegriffen werden:

- Eine IP-Adresse ist für jedes Gerät eindeutig, um es ganz klar identifizieren und ansprechen zu können.
- Diese IP-Adresse besteht aus 4 Zahlen, mit einem Punkt voneinander getrennt, jeweils zwischen 0-255, Bsp.: Die aktuelle IP-Adresse meines Notebooks, an dem ich gerade diesen Satz schreibe lautet 192.168.2.201
- Die IP-Adresse wird innerhalb Ihres Netzwerkes von Ihrem Router vergeben: Die Verbindung zwischen Dem Dienstanbieter ("Provider") und Ihren Geräten. Der Router selber behält immer eine Adresse fix, zB. 192.168.2.1
- Der Provider, zB. Telekom, stellt dem Router eine Adresse zur Verfügung, die -während Sie im Netz sind- stets gleich bleibt. Diese Adresse kann aber beim nächsten Einloggen neu vergeben werden. Aktuell hat zB. mein Internetzugang die Adresse 84.190.93.13.

Über die Kette -> Internetadresse/Portscan -> Routeradresse -> Gerätadresse wird Ihr WLAN angreifbar.

1.4 Beobachten, ausspähen, nachverfolgen - Webbeacons

Internetseiten ermitteln über das Internet Ihre IP-Adresse:

- Javascripte und neue Browsertechniken wie HTML5 erlauben Inhalte abzufragen,
- "Web-Beacons": Auf der angeklickten Internetseite, z.B. ebay, werden Scan-Methoden anderer Seiten, z.B. facebook verborgen wie präparierte Bilder, die sich nicht auf der Webseite befinden, sondern auf fremden Rechnern, die beim Laden Ihre IP-Adresse erfahren.

Eingesetzt wird diese Technik bei facebook: Der "Gefällt mir"-Button ist als iFrame-Objekt auf vielen Seiten eingebettet, facebook kann jetzt sehen wo sich welcher User aufhält. Facebook verbindet Surfstatistiken *direkt* mit Ihrem useraccount[2], wobei die Informationen bei Facebook liegen und uns "Eigentümern" nicht zur Verfügung gestellt werden.

> So weit geht nur Facebook, darum: Sie finden auf unseren Seiten keinen "Like"-Button, Ihren Daten zuliebe können Sie auch kein "Fan" von uns bei Facebook werden!

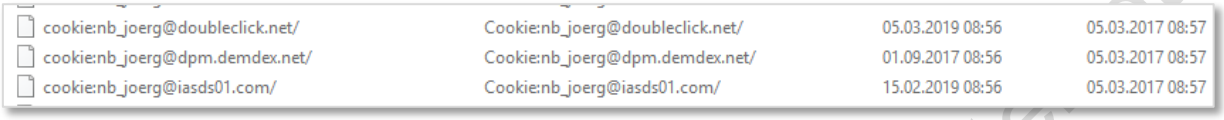
Ziel dieser Methoden: Ihnen angepasste (Schleich-)Werbung einzublenden bzw. Meinung zu manipulieren, sog. Filter-Blasen.

[2] http://www.sebbi.de/archives/2010/04/27/5-grunde-warum-mir-der-gefallt-mir-button-von-facebook-nicht-gefallt/

1.5 Cookies - Die Zecken des Internets

Cookies sind kleine Textdateien. also harmlos? Webseiten veranlassen Ihren Browser, Cookies zu speichern. Wenn Sie dies verhindern, wird in der Regel die Seite gesperrt, da Sie dann beim Surfen nicht mehr verfolgt werden können.

Es gibt mehrere Datenschutzrisiken im Zusammenhang mit Cookies: Werbe- und Statistikdienste einer Webseite, wie z.B. eBay, missbrauchen die Möglichkeiten mithilfe sogenannter Drittseiten-Cookies dazu, sie über mehrere Webseiten hinweg unbemerkt zu verfolgen, also z.B. alle Seiten beobachten, die Sie nach eBay besuchen.



Aber selbst, wenn Sie diese Drittseiten-Cookies sperren, können Webseiten Sie immer noch anhand der Erstseiten-Cookies wiedererkennen, die direkt von der jeweils besuchten Webseite gesetzt werden. Um Sie langfristig zu verfolgen, setzen Provider und VPN-Dienste gerne solche Erstseiten-Cookies selbst und lesen mithilfe von unsichtbaren Weiterleitungs-Seiten im Hintergrund die Cookies wieder aus[3].

Cookies sind für Onlinedienste eine einfache und effiziente Methode zur Verfolgung von Websurfern - sofern sie nicht von diesen blockiert werden. Ist das der Fall, können aber noch zahlreiche andere Methoden, wie nachfolgend beschrieben, zu Ihrer Verfolgung eingesetzt werden

Empfehlung vorweg: Cookies von Drittanbietern IMMER sperren und beim Schließen Ihres Browsers auch andere Schnüffel-Funktionen automatisch löschen.

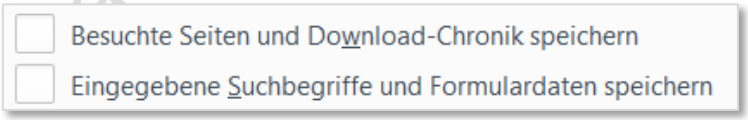
1.5.1 Authentifizierung durch Chroniken

In Browsern ist es möglich, dass Webseiten versteckte Authentifizierungsdaten an Drittseiten senden. Beispiel: http://Session:934523542@ipcheck.info/auth.css.php.

Dies kann entweder direkt auf der aktuellen Seite oder in einem sog. iFrame erfolgen, und benötigt KEIN JavaScript: Wenn zusätzlich iFrames und JavaScript verwendet werden, kann sogar die aktuell geladene Seite Ihre ID auslesen.

Diese Daten haben dieselbe Wirkung wie Drittseiten-Cookies und werden beim Schließen des Browsers in der Regel nicht gelöscht.

Empfehlung: Ihr Browser sollte keine HTTP-Authentifizierungsdaten an Drittseiten senden: Im Browser können Sie das Speichern von Informationen sperren.



[3] Techniken wie diese werden etwa vom Dienstleister Phorm (http://www.phorm.com) angeboten.

1.5.2 Referer verraten, woher Sie kommen

Der Referer verrät über den Klick auf einen Link in einer Webseite, welche Seiten sie vorher/danach besucht haben. Werbedienste nutzen dies natürlich zur Profilbildung von Websurfern. Google und Reiseportale "merken" sich so, was Sie auf anderen Seiten machen.

Empfehlung: Der Referer sollte nicht informiert werden, wenn Sie zu einer anderen Webseite wechseln und unverändert bleiben, solange Sie sich auf derselben Webseite bewegen.
Sie können dazu das bereits erwähnte Add-on "Smart Referer" benutzen.

Oder einfach: Die Link-Adresse per Kopieren manuell in ein neues Browser-Tab einfügen - schon ist der Referer weg!

2. Vorsorge beginnt am PC: Wichtige Grundeinstellungen

Schutz beginnt schon am eigenen Computer, der grundsätzlich so eingerichtet ist, dass er Ihnen möglichst viel "Komfort" bietet (Marketingdeutsch), also kaum Sperren hat. Hier ist es zunächst wichtig, dem ungehemmten Zugriff von außen einen Riegel vorzuschieben.

2.1 Der PC selber: wichtige PC-Grundeinstellungen

Wie bereits erwähnt, ist ein neuer, ungeschützter Computer im Schnitt innerhalb von 7 Minuten als ungeschützt erkannt, wenn er sich das erste Mal mit dem Internet verbindet.

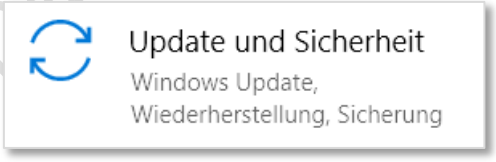
Treffen Sie daher zunächst ein paar Sicherheitsvorkehrungen

2.1.1 Sichern, Sichern, Sichern - Updates aktivieren

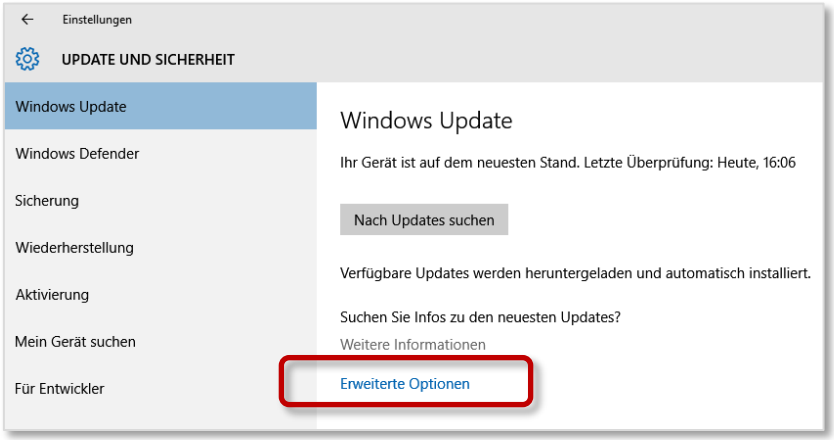
Nicht ein alter PC, sondern ein ***ver***alteter PC ist ein potentielles Opfer: Nur aktuelle Software mit regelmäßigen Sicherheits-Updates schließt auftretende Lücken.

- Klicken Sie auf das **Start-Symbol** unten links des Desktops und wählen den Befehl **Einstellungen** (Symbol Zahnrad). Alternativ: (**WindowsTaste) + i**

- Klicken Sie in dem Einstellungsfenster auf das Symbol **Update und Sicherheit**.



- Klicken Sie im Fenster Update und Sicherheit auf **Erweiterte Optionen**.



Dort können Sie den Stand der Updates kontrollieren und ggf. ein Update starten.

- Im Fenster Erweiterte Optionen können Sie weitere Update-Einstellungen vornehmen.

2.1.2 Windows - Schnüffeln einschränken: SmartScreen und ID-Scannen abschalten

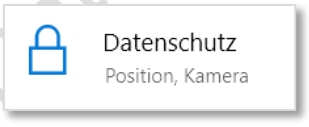
Der "SmartScreen"-Filter soll uns Anwender vor Download-Dateien mit schädlichem Inhalt warnen und ist ab Windows Version 8 vollständig im System integriert.

Klickt man statt auf "OK" auf den Link "Weitere Informationen" wird die Option "Trotzdem ausführen" angezeigt - und der Virus ist auf dem PC….

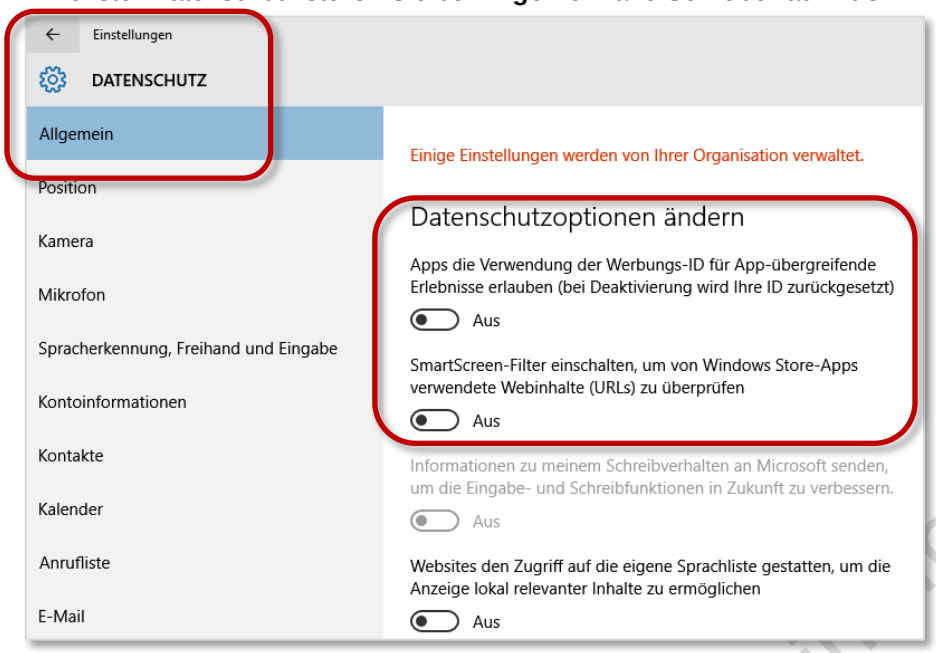
Nebeneffekt dieser Funktion: Sie informieren Microsoft mit jedem Klick / Download über Ihr Surfverhalten, da jede angeklickte Seite an Microsoft übermittelt und dort mit deren Datenbanken abgeglichen wird. Außerdem hat Microsoft sich seit Windows 10 die Möglichkeit geschaffen, mit Werbungs-IDs Ihren Standort weltweit eindeutig zu identifizieren.

Diese Funktion kann daher getrost deaktiviert werden.

- Gehen Sie in die Einstellungen (Zahnradsymbol oder WindowsTaste+i) und klicken auf **Datenschutz**.



- Im Fenster Datenschutz stellen Sie bei **Allgemein alle Schieber** auf **Aus**.

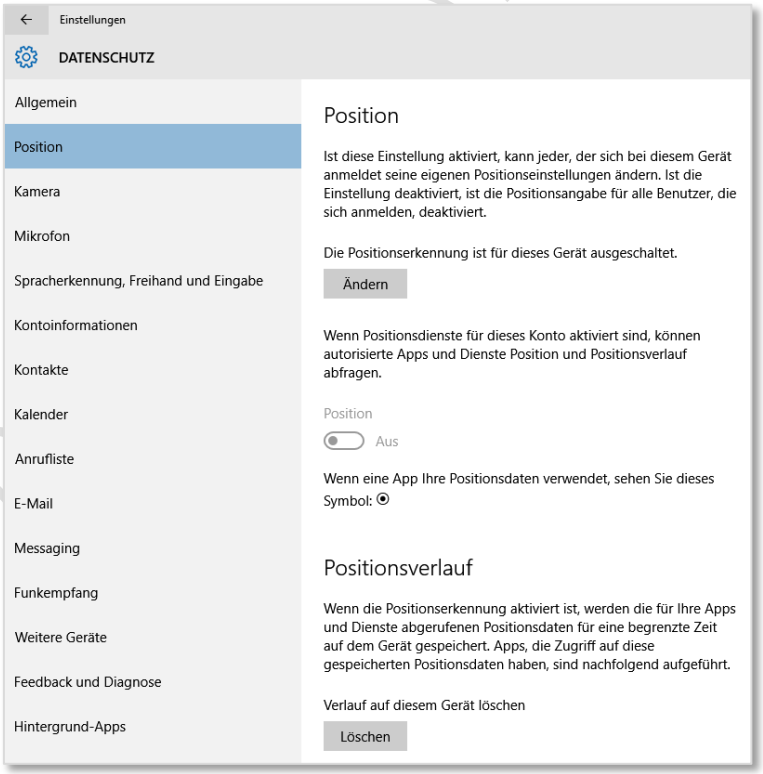


- Auf jeden Fall auch alle anderen Optionen abschalten!

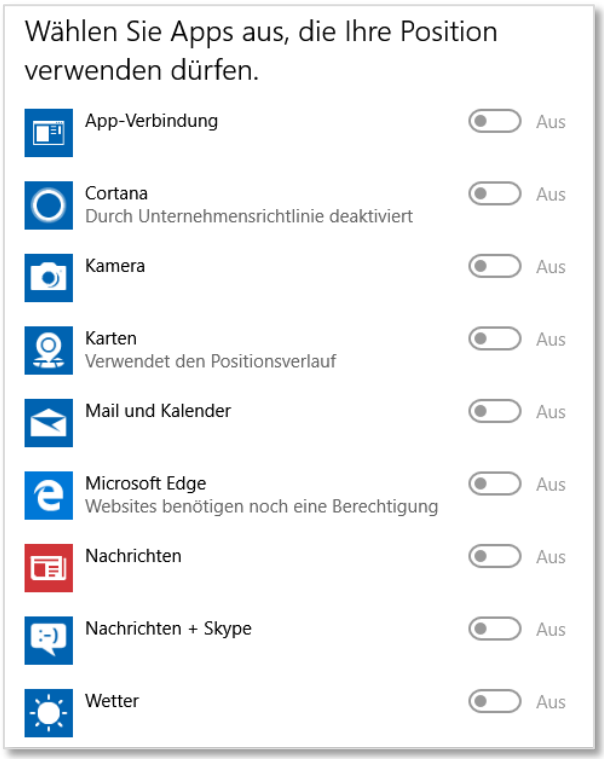
2.1.3 Positionsverlauf deaktivieren

Noch weiter treibt es Microsoft mit dem Positionsverlauf: Hiermit kann Microsoft weltweit die Position und die Bewegungen Ihres Gerätes feststellen.

- In den Datenschutz-Einstellungen klicken Sie auf **Position**.
- Schalten Sie **alle** Funktionen ab, insbesondere **Positionserkennung**

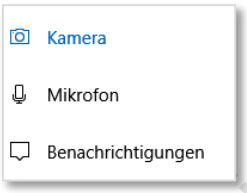


- Weiter unten im selben Fenster können Sie die Positionskennung von "Apps" deaktivieren: Prüfen Sie, ob jedes Programm wirklich Ihre Bewegung aufzeichnen muss.



2.1.4 Sonstige Einstellungen der "Sicherheit"

Kontrollieren Sie insbesondere auch die Einstellungen bei Kamera, Mikrofon, Benachrichtigungen und Kontoinformationen: Entscheiden Sie hier selber, ob und welche Anwendungen diese Geräte übernehmen und bedienen können.



2.2 Virenscanner und mehr: Eine Checkliste wichtiger Zusatz-Software

Nun, wo Sie Ihren PC grundsätzlich vorbereitet haben auf den Zugang in das Internet, ist es erforderlich, weitere Schutzfunktionen einzurichten, die Ihnen Microsoft Windows nicht bietet:

- Der Schutz vor Angriffen durch einen Virenscanner
- Der ideale Browser zum Surfen im Internet
- Das Entfernen von Spuren und Schnüffelfunktionen
- Und überhaupt: Erkennen, wann es gefährlich wird.

2.2.1 Der Virenscanner

Unerlässlich ist es, einen Virenscanner zu installieren, um zumindest einen Großteil von Angriffen abzuwehren. Nicht notwendig ist es, dafür zu bezahlen: Hier gibt es eine Vielzahl von kostenlosen

Programmen wie Antivir (www.avira.de). Sie erhalten zwar die eine oder andere Werbeeinlage in der kostenlosen Version, aber er ist schnell und als Basisschutz genauso ausreichend wie kostenpflichtige Programme. Außerdem weit verbreitet, so dass die Virendefinitionen auch stets aktuell sind und automatisch ein Update stattfindet.

2.2.2 Der beste Browser?

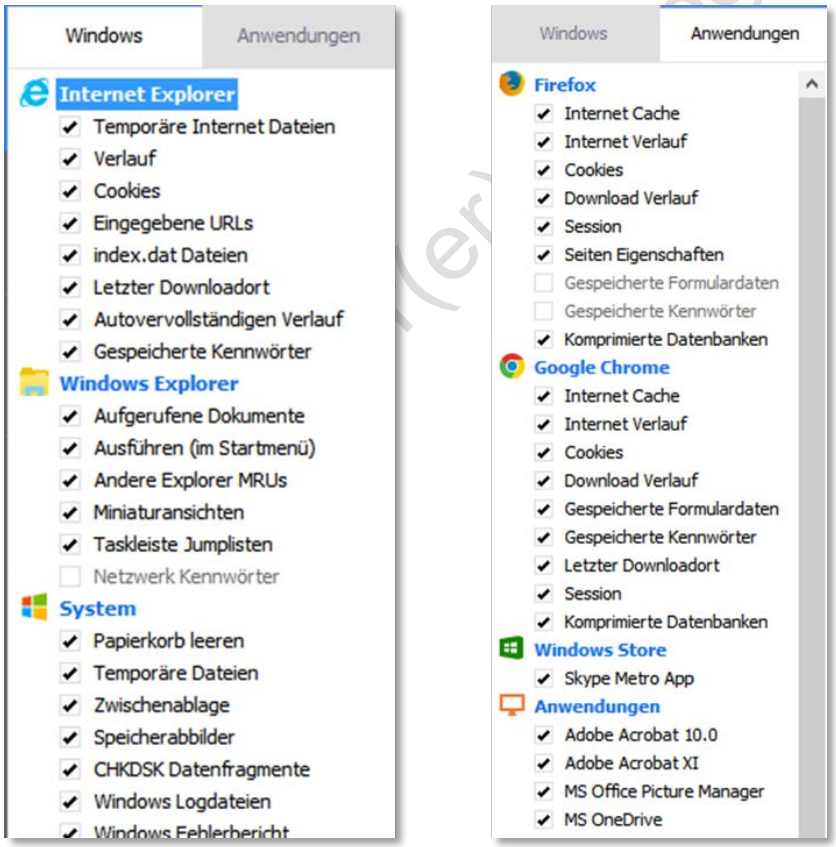
Die schlechteste Wahl ist der Internet Explorer: Dieser bietet nur sehr wenig Möglichkeiten, sich vor Auspionieren zu schützen und die dazu nötigen Einstellungen sind für normale Benutzer mehr als wenig verständlich erklärt. Außerdem ist es nicht möglich, sinnvolle Add-Ons (s. dort) zu ergänzen, um den Schutz zu erhöhen.

Unsere Empfehlung: **Mozilla Firefox**: Dieser Browser bietet die meisten Möglichkeiten, Sicherheitseinstellungen vorzunehmen und ist ehrlich: Die eingebauten Schnüffelfunktionen können hier deaktiviert werden. Diese Unterlage bezieht sich im Weiteren ausschließlich auf das Surfen mit Mozilla Firefox. Ebenfalls empfehlenswert: Opera oder Safari.

2.2.3 CCleaner: Spuren komfortabel vom PC entfernen

Hier bietet sich das Programm CCleaner von piriform.de an: Ein kostenloses Zusatzprogramm, das auf einen Schlag alle Spuren und sonstwie gesammelten Informationen über Ihr Verhalten auf Ihrem PC entfernt.

CCleaner listet unter "Windows" und "Anwendungen" die bei Ihnen installierten Anwendungen auf, die typischerweise Datenspuren hinterlassen:



Wichtig hier: Die Einstellungen kontrollieren zu **Startmenü, Desktop, Microsoft Office** und ggf. deaktivieren: Ansonsten werden auch *Ihre* individuellen Einstellungen bei jedem Start entfernt.

2.2.4 Gesundes Misstrauen beim Surfen: Gefährliche Websites und Emails erkennen

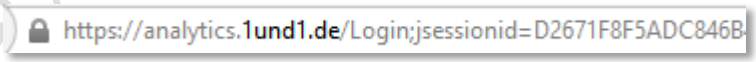
Ob beim Online-Banking oder -Shopping: Mit gefälschten Webseiten ziehen Hacker Ihnen das Geld aus der Tasche. Wie können Sie Fallen erkennen?

Ein klassischer Fall von Phishing: Sie sollen eine TAN eintippen und folgen der Anweisung, weil die gefälschte Bankseite der tatsächlichen täuschend echt ähnelt. Wenige Tage später fehlen 650 oder auch 950 Euro auf ihrem Konto - der übliche Betrag beim Phishing. Statt an die Bank übermittelt das Opfer Passwörter und TANs an kriminelle Dritte. Keine Bank wird von Ihnen verlangen, so viele TANs auf einmal einzugeben. Aber wenn Kriminelle behutsam vorgehen, wird es auch für erfahrene Surfer gefährlich. Täuschend echt nachgebaute Internetseiten liegen heute schon zuhauf als Köder im Internet aus.

Aktuelle Themen: Gutscheine, Paketankündigungen, "versehentlich" falsch adressierte Mails mit Überweisungsankündigungen.

Eine sehr beliebte Täuschungs-Methode von Online-Kriminellen sind **lange und komplizierte Links**. Das Opfer soll den Schwindel nicht schon anhand des Links erkennen. Oder: Der Link enthält zwar den Namen Ihrer Bank – etwa „postbank.de“ – aber an der falschen Stelle: pish**.ru**/postbank.de. Die wahre Domain führt nach Russland oder China.

So erkennen Sie den Schwindel:

Suchen Sie nach dem ersten Schrägstrich nach dem Suffix, hier ".de" bzw. „https://“. Was davor steht, ist der wahre Domain-Name.	https://Kunden.**postbank.de/**Login
Ein verspätetes „postbank.de“ irgendwo weiter hinten zählt nicht.	http://Kunden.**deafanddump.com/**583416/**postbank.de/**Login
Firefox hebt den tatsächlichen Domainnamen optisch hervor.	
Tipp: Das (kostenlose) Firefox-Addon "Flagfox" verrät Ihnen den Server-Standort einer Webseite.	 Warum sollte z.B. Ihre Bank die Webseite in China betreiben? Spätestens jetzt sollten Sie kritisch und genauer hinschauen.

3. Sicher(er) im Internet bewegen - Einstellungen und Hilfsmittel

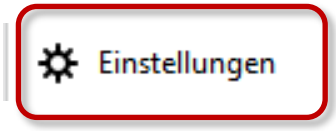
3.1 Firefox einstellen

Auch Firefox ist nicht besser als die anderen: Um das Produkt weiterzuentwickeln bzw. den "Surfkomfort nicht einzuschränken", möchte Firefox gerne Ihr Surfverhalten beobachten, d.h. alle Informationen wandern unkontrolliert und nicht einsehbar an Firefox und auch das dauerhafte Ablegen von Schnüffeldateien wie Cookies wird ungehindert zugelassen.

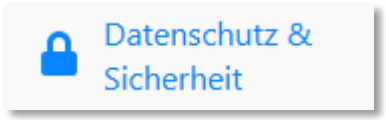
Was dafür in Ordnung ist: Im Gegensatz zu den Mitbewerbern werden die von Ihnen vorgenommenen Veränderungen bei einem Software-Update nicht einfach (und klammheimlich) wieder zurückgestellt.

- Um die Grundeinstellungen anzupassen, klicken Sie in der oberen rechten Ecke auf das **Menü einstellen** - Symbol.

- Klicken Sie dann auf den Befehl **Einstellungen**.



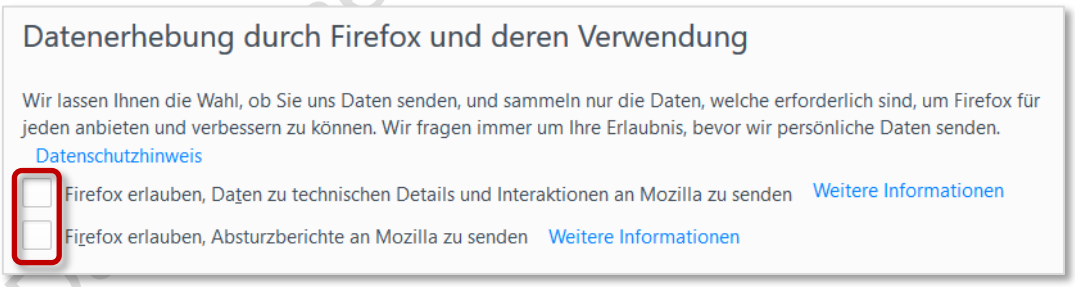
- Die Einstellungen werden in der Navigationsleiste links zum Eintrag bei **Datenschutz und Sicherheit** vorgenommen.



3.1.1 Firefox das Schnüffeln unterbinden

Wichtigste Einstellung zunächst: Das permanente Schnüffeln zumindest stark einschränken.

Datenerhebung durch Firefox... : Deaktivieren Sie alle Funktionen; Sie erlauben Firefox ansonsten einen vollständigen Überblick über Ihr Surfverhalten.



3.1.2 Daten(un)sicherheit: Cookies etc.

Auch Cookies werden mit einem Vollzugriff abgelegt, d.h. allen Internetseiten wird gestattet, über Cookies Ihr Surfverhalten zu protokollieren. Zudem erlaubt Firefox diesen Anbietern, auch Cookies von Dritten wie z.B. Marktforschungs- und Werbeunternehmen auf Ihrem PC zu platzieren, sozusagen in Ihrem stillschweigenden unwissentlichen Einverständnis.

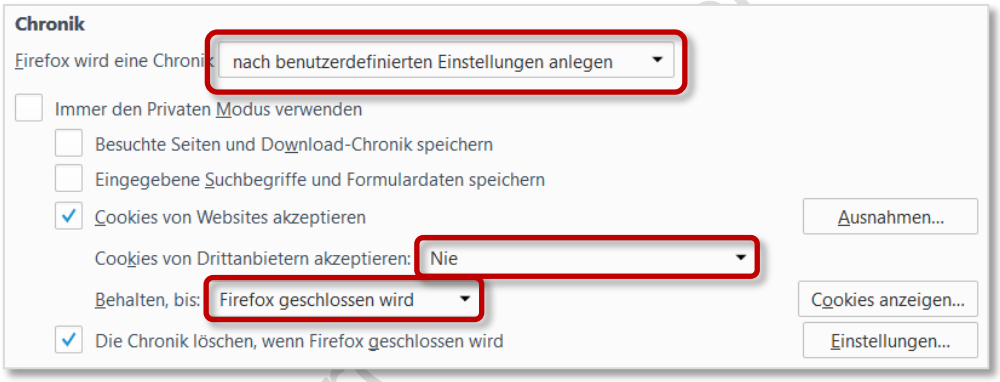
Schieben Sie auch hier einen Riegel vor: Sie können zwar das Setzen von Cookies nicht ganz verhindern (Internetseiten können nicht mehr aufgerufen werden), aber zumindest soweit einschränken, dass nur wenig Informationen (=der der aktuellen Sitzung) abgelegt werden können.

Chronik: Legen Sie hier zunächst fest, dass Firefox Seiteninformationen nur entsprechend IHRER Vorgaben speichert.

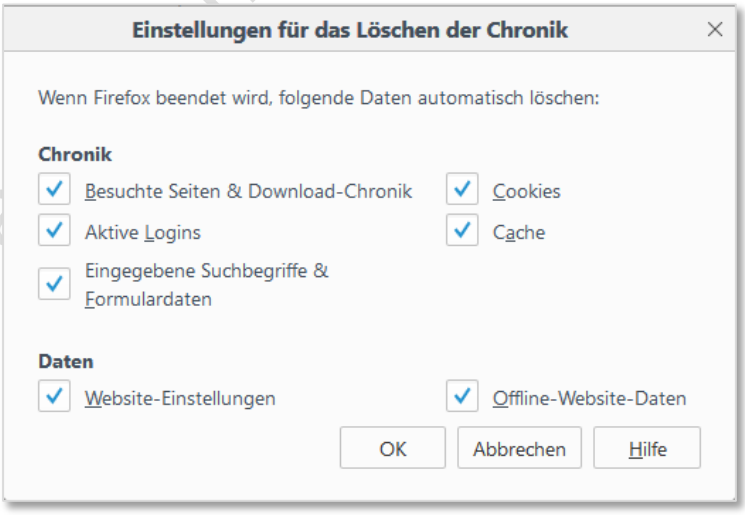
Wichtig hier:

- Sie müssen Cookies akzeptieren (sonst können Sie eine Internetseite erst gar nicht aufrufen),
- Aber: Aktivieren Sie unbedingt "Behalten, bis: **Firefox geschlossen wird**". Der in Cookies enthaltene Zeitstempel zum dauerhaften Ausschnüffeln Ihrer Aktionen im Internet (bei Google z.B. 20 Jahre!) wird somit pauschal auf "Ende der Sitzung" verkürzt. So kann eine Seite nur solange schnüffeln, wie sie sie besuchen.

  Für Fans von Seiten wie "Facebook" o. ähnlichen Erscheinungen: Über die Schaltfläche Ausnahmen können Sie solchen Seiten erlauben, trotzdem Cookies anlegen zu lassen, um den Seiten einen besseren Überblick über Ihr Surfverhalten zu geben.



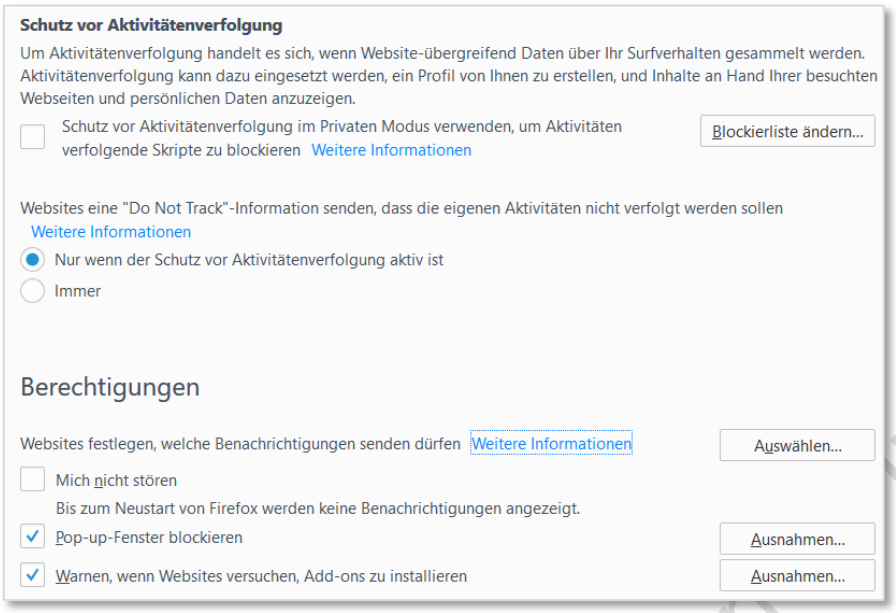
- Kontrollieren Sie hier aber unbedingt über die Schaltfläche **Einstellungen**, was gelöscht wird. Am besten alles.



- "**Cookies von Drittanbietern**" unbedingt auf "**Niemals**" stellen: Nur so können Sie dem unkontrollierbaren Zugriff auf Ihre Daten durch Werbe- und Marktforschungsinformanten halbwegs entgehen.

3.1.3 Schutz vor Aktivitätenverfolgung / Berechtigungen

- Hier können Sie zunächst einmal einstellen, ob Sie ein vollständiges Beobachten Ihrer Aktivitäten durch Webseiten wünschen (natürlich **NICHT**!)



Diese Funktion hat Ähnlichkeit mit der sog. "Robinson"-Liste in den 80er-Jahren: Hier konnte man sich eintragen lassen, um keine Werbung zu erhalten. Allerdings wurde das nur von Firmen beachtet, die sich ihrerseits dazu verpflichteten, die Robinson-Liste zu beachten. Die wurden immer weniger, es machte also keinen Sinn mehr, sich dort einzutragen weil keiner sie beachtete.

Hier kommt noch der Effekt dazu: *Gerade weil* Sie der anderen Seite mitteilen, *nicht* verfolgt zu werden, haben die die Information bekommen, WER nicht verfolgt werden will mit dem Effekt: Es gibt dann erst recht Werbung…

3.2 Sinnvolle Add-ons

Add-Ons (auch "Erweiterungen" oder "Apps") sind kleine Zusatzprogramme und können die Sicherheit beim Surfen deutlich erhöhen:

- Entweder warnen sie vor gefährlichen Inhalten (ghostery, flagfox)
- Oder sperren diese (ghostery, facebook Container)
- oder täuschen die Gegenseite mit falschen Spuren (ublock origin, anonymox)

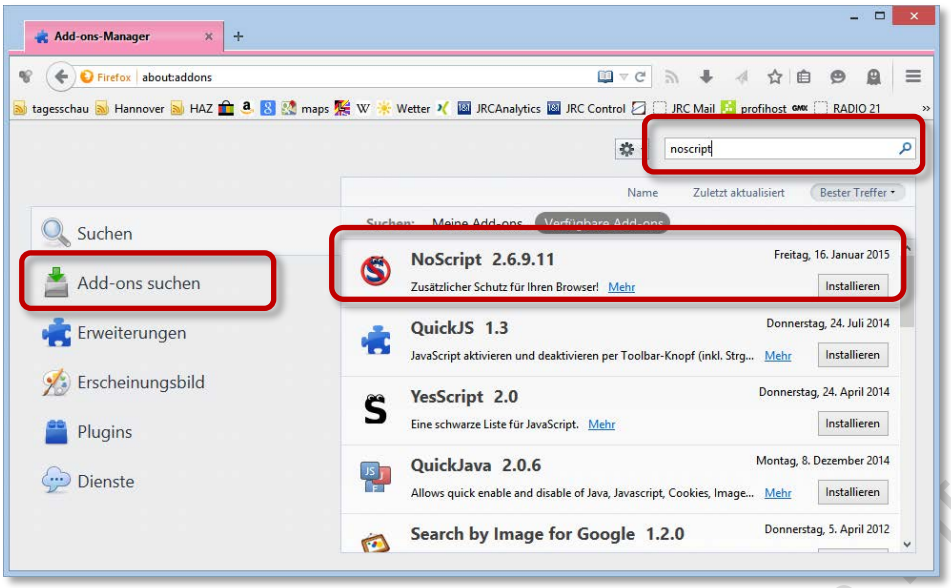
3.2.1 Installation von Add-ons

Gerade für Mozilla Firefox gibt es eine Vielzahl nützlicher Zusatzprogramme, die Sie über die Einstellungen direkt installieren können, hier am Beispiel des add-on "NoScript", was das Ausführen gefährlicher Funktionen verhindert:

- Klicken Sie oben rechts auf das Symbol **Menü öffnen**

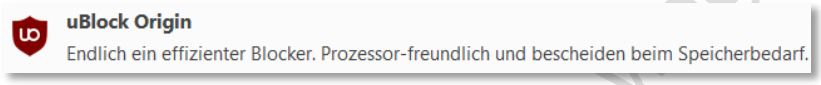
- Dort auf den Eintrag **Add-Ons**

- Hier klicken Sie auf **Erweiterungen** und geben oben rechts den Namen des Add-ons an.



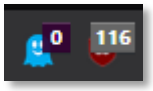
- Drücken Sie die Enter-Taste: Die Treffer werden nun im Fenster angezeigt, Sie können das Programm nun installieren.

3.2.2 UBlock Origin



Sich selbst öffnende Fenster, verlinkte Schleichwerbung und Facebook-Fallen wie versteckte Like-Button auf einer Seite werden entfernt. Zumindest weitestgehend.

GoogleMaps greift z.B. extrem häufig auf Daten zu, da bei jeder Kartenbewegung versucht wird, im Hintergrund Werbung für den angezeigten Ausschnitt zu platzieren.



Auch Seiten wie chip.de oder wetter.de versuchen hemmungslos auf den Rechner zuzugreifen:

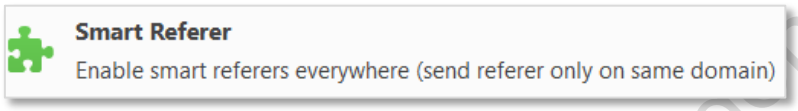
(chip.de)

(wetter.de)

Stark mit solchen Funktionen "Verseuchte" Seiten werden vollständig gesperrt:

Temporär können solche Seiten dann angezeigt werden. Ublock Origin ist ein idealer Ersatz für Adblock, dass seinen Funktionen nicht mehr gerecht wird, s. dort.

3.2.3 Smart Referer

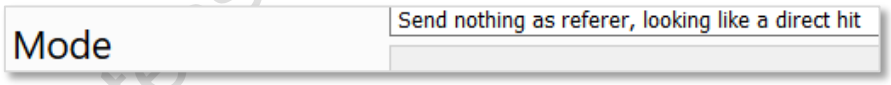


Wie bereits unter *1.5.2 Referer verraten, woher Sie kommen* erwähnt, können Internetseiten nachverfolgen, welche andere Seiten Sie auch noch besuchen, wenn Sie die anderen Seiten direkt von der ersten Internetseite aufrufen (und nicht direkt als neue Seite eintippen). Bsp.: Google "lebt" von diesen Links: So kann beim nächsten Besuch von Google Ihr Suchergebnis besser angepasst werden an das, was Sie sehen sollen.

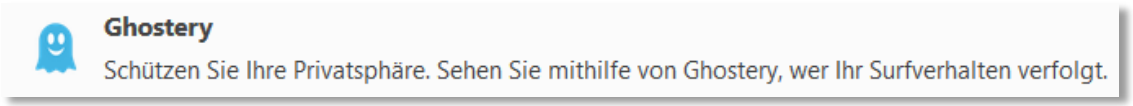
Gerade, wenn eine Internetseite wie Google als Startseite eingerichtet ist, neigen viele Leute dazu, die eigentlichen Internetseiten auch nur noch über Google und nicht mehr direkt aufzurufen. Ideal für Google festzustellen, welche Seiten ein User bevorzugt.

Nun ist es aber auch umständlich, jede Seite direkt einzugeben: Smart Referer verschleiert einer Seite das Ziel so, als wenn Sie direkt aufgerufen wurde. Google kann den Verweis nun nicht mehr auswerten.

Achten Sie bei den Einstellungen darauf, dass der Link wie eine neue Eingabe erscheint



3.2.4 Ghostery



Dieses Programm schützt gegen Schnüffelfunktionen wie …

…Web-Tracker

Dritte Parteien verfolgen nach, was Sie im World Wide Web surfen. Diese Tracker können sehen,

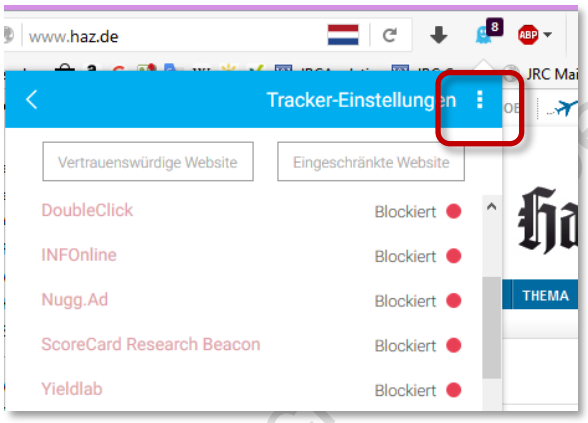
welche Webseiten Sie aufrufen, natürlich ohne dass Sie davon etwas mitbekommen. Zudem funktionieren diese Tracker auch über Webseiten verschiedener Anbieter hinweg, also generell.

Das Fraunhofer-Institut bietet dazu einen Link zum Aufspüren von Trackern und Hintergrundinformationen (02-2016):
https://www.sit.fraunhofer.de/de/track-your-tracker/worum-gehts/was-bedeutet-web-tracking/

… **Web-Beacon**
oder Zählpixel (engl. *Web Bug*; also passenderweise Web-Wanze): 1x1 pixelkleine Grafiken, versteckt in HTML-E-Mails oder auf Webseiten, die ein Bewegungsprofil erstellen können, IP-Adresse und (ungefähren) Standort feststellen bzw. mitteilen, ob und wann eine E-Mail geöffnet wurde.

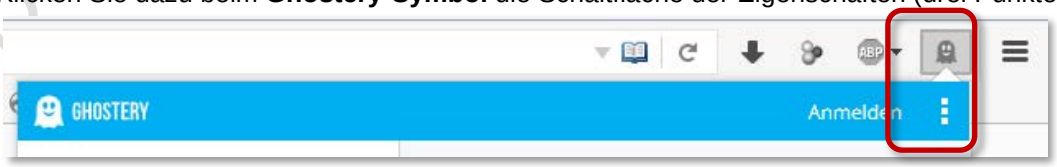
… **Cookies**
Dateien, in die beim Internetsurfen benutzerbezogene Daten auf dem PC des Anwenders zum späteren Wiederabruf durch die betreffende Website oder Webanwendung gespeichert werden, natürlich auch hier Browser- und Webanwendungsübergreifend.

Es ist dabei interessant zu sehen, welche "seriösen" Seiten dies in massiver Form nötig haben, z.B. die "Hannoversche Allgemeine" oder "Die Welt"[4]. Hier finden sich auch als besonders aggressiv und gefährlich eingestufte Datenschnüffler wie z.B. DoubleClick, aber auch google analytics:



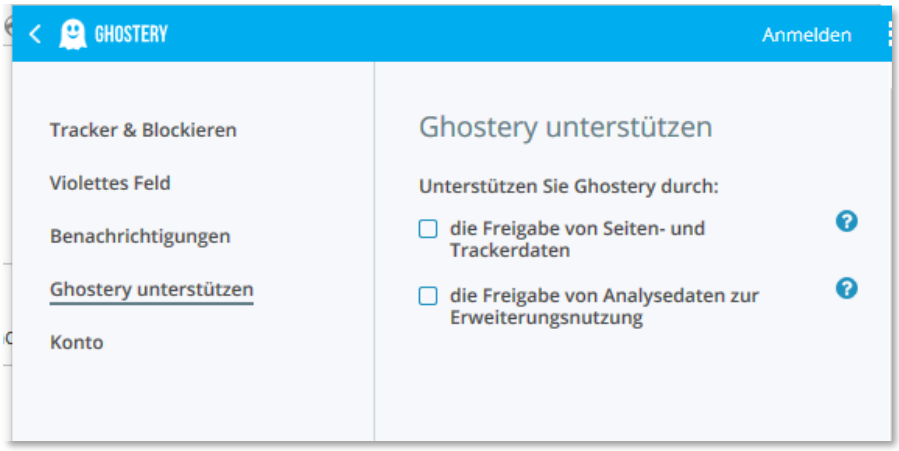
Prinzipiell ist Facebook ebenfalls "besonders gefährlich", Facebook-Fans können aber wie im Beispiel oben bei Ghostery Ausnahmen zulassen.

- Wichtig hier: Nach der Installation der Erweiterung die Einstellungen kontrollieren, Klicken Sie dazu beim **Ghostery-Symbol** die Schaltfläche der Eigenschaften (drei Punkte) an:



- Dort die **Einstellungen** anklicken: Deaktivieren Sie unter **Ghostery unterstützen** alle Einstellungen, sonst schnüffelt Ghostery selber!

[4] Was ist "normal" an Schnüffelfunktionen, warum sollen wir uns das gefallen lassen? "Normalerweise" möchte ich gefragt werden, wenn ich (marktforschungstechnisch oder sonstwie) beobachtet werde. Sagen wir 1-3 solcher Programme ist eventuell noch tolerierbar, 12-30, wie z.B. bei den Tageszeitungen "Hannoversche Allgemeine" oder "Die Welt" eingesetzt, ist aggressiv und rücksichtslos.



3.2.5 AdBlock / AdBlock Plus - Bitte nicht

Die Macher dieses Add-Ons (wird als Internetstandard zum Blockieren ungewünschter Fenster gehandelt) verdienen mittlerweile anscheinend mehr Geld damit, sich bezahlen zu lassen das AdBlock NICHT Seiten blockt (die eben dafür bezahlt haben).

Besser und zuverlässiger: UBlock Origin, s. Kapitel 3.2.2.

3.2.6 Flagfox

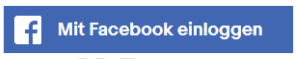
Das (kostenlose) Firefox-Addon "Flagfox" verrät Ihnen den Server-Standort einer Webseite

Warum sollte z.B. Ihre Bank die Webseite in China betreiben? Spätestens jetzt sollten Sie kritisch und genauer hinschauen.

Unsichere Länder sind Holland, Irland, USA: Datenschutzrechtliche Ansprüche gegen Seiten in diesen Ländern werden stets abgelehnt, in der Regel wird Ihnen nicht einmal geantwortet.

3.2.7 facebook Container

Das Firefox-Addon "facebook Container" ist ein echtes Ärgernis für facebook, die versuchen, Schattenprofile über Nichtmitglieder zu erstellen, z.B. indem auf einer Internetseite das facebook-Logo eingebunden wird, hier am Beispiel des Logins bei eBay:



Ohne die Schaltfläche anzuklicken, also mit bloßem Aufruf der Seite, wird das Bild vom facebook-Server geladen, Ihre IP-Adresse geht infolgedessen an facebook, als wenn Sie facebook direkt aufrufen. Über Cookies und andere Techniken kann facebook also Ihr Verhalten auf der eigentlichen Seite beobachten (siehe dazu Ausführungen oben).

Die App deaktiviert diese facebook-Hintergrundaktivitäten und zeigt Ihnen dies mit einem Sperrsymbol an: