

# Sicher surfen im Internet?

Frank Olzog | Computer- und Medienservice, Hard- und Softwareservice | frank.olzog@cms.hu-berlin.de

Diese Frage kann sicherlich leicht mit „das geht nicht“ beantwortet werden. Doch geht es mir hier nicht darum zu beweisen, dass es nicht möglich ist, einen Computer im Internet zu benutzen und ihn gleichzeitig so sicher einzurichten, dass alle eventuellen Gefahren vermieden werden können. Vielmehr möchte ich an dieser Stelle einige Tipps und Anregungen zum Umgang mit dem Webbrowser geben. Wie fast immer, wenn es um Sicherheit geht, ist eine der größten Schwachstellen der Mensch. Und da meine ich nicht nur die Soft- und Hardwareentwickler, sondern vor allem auch die Computernutzer. Da sich die Entwickler von Soft- und Hardware kaum beeinflussen lassen (vielleicht durch Verweigerung?), muss das eigene Verhalten der jeweiligen Situation angepasst sein. Dieses Verhalten ist der sicherheitsrelevante Faktor beim Umgang mit dem Computer und der installierten Software.

Wenn über Sicherheit gesprochen wird, sollten wir uns zunächst vor Augen führen, was geschützt werden soll. Denken wir an das Internet, fällt uns vermutlich zuerst ein, unsere persönlichen Daten vor der unbefugten Kenntnisnahme durch Dritte zu schützen – wir wollen die Vertraulichkeit unserer Daten wahren. Und selbstverständlich soll auch verhindert werden, dass Daten auf unserem Computer gelöscht werden. Ebenso fatal kann es sein, wenn diese Daten, mit oder ohne unser Wissen, verändert werden. Mit anderen Worten, wir möchten die Integrität unserer Daten bewahren und auch möglichst jederzeit darauf zugreifen können. Jede böswillige Software, aber auch jede fehlerhafte Software, die auf unserem Computer

installiert ist, kann unsere Daten verändern, löschen und möglicherweise auch über das Internet weiterreichen. An dieser Stelle möchte ich Ihnen zwei Fragen stellen, auch wenn diese mit dem Thema des Artikels nur mittelbar zu tun haben: Wann haben Sie das letzte Mal Ihre Daten gesichert? Und wann haben Sie versucht, diese gesicherten Daten wiederherzustellen? Denn selbst wenn Sie sehr sorgfältig mit Ihrem Computer umgehen und die folgenden Hinweise beachten, kann beispielsweise Ihre Festplatte den Geist aufgeben.

## Halten Sie die Software Ihres Computers auf dem aktuellen Stand!

Selbstverständlich sollten Sie stets dafür Sorge tragen, dass die von Ihnen benutzte und installierte Software aktuell ist. Nur so können Sie vermeiden, dass bekannte Sicherheitslücken ausgenutzt werden. Und das Ausnutzen von Sicherheitslücken geht im Zeitalter des Internets schneller als geahnt. Ich weiß selbst, wie es ist, wenn nur schnell mal eine E-Mail gesendet werden soll und mitten im Verfassen dieser E-Mail der Computer neu starten möchte. Es gibt immer etwas zu tun, das wichtiger erscheint, als sich um den eigenen Computer zu kümmern. Und doch sollten Sie sich zuerst mit der Sicherheit des Computers befassen, bevor Sie ihn für die eigentliche Arbeit benutzen.

Benutzen und aktivieren Sie eine Firewall. Installieren Sie eine Antiviren-Software. Als Humboldtianer können

*Das Internet, und hier vor allem das WorldWideWeb, ist längst zu einer nicht mehr wegzudenkenden Informationsquelle geworden. Ob für Lehre, Forschung oder Studium, ohne die Nutzung dieser Informationsquelle kommt kaum ein Universitätsangehöriger aus. Zur Darstellung von Informationen aus dem WWW werden wie selbstverständlich Webbrowser benutzt. Was es dabei zu beachten gibt, wie das Surfen sicherer gestaltet werden kann und Empfehlungen zu gängigen Webbrowsern soll der folgende Artikel zeigen.*

Sie diese kostenlos bei uns bekommen (<https://amor.cms.hu-berlin.de/>). Achten Sie selbst darauf, dass die Updates für Ihr Betriebssystem und Ihre Software, Ihre Antivirensoftware „up to date“ sind – überlassen Sie diese wichtige Kontrollaufgabe nicht einfach einer Software.

## Benutzen Sie nur vertrauenswürdige Software!

Kann einer Software überhaupt vertraut werden? Auch so eine Frage, die bei der gerade aktuellen Diskussion um den Bundestrojaner (was für ein Unwort!) kaum mit „Ja“ beantwortet werden kann. Deshalb sollten Sie sich vor der Installation jeder Software gerade die erste der folgenden Fragen ehrlich beantworten:

- Benötige ich diese Software auch tatsächlich?
- Wo habe ich diese Software her?
- Was sagen andere zu dieser Software bzw. welche Software benutzen andere für den gleichen Zweck?

## Welcher Webbrowser sollte benutzt werden?

Ich möchte hier keinen ideologischen Streit vom Zaune brechen. Ohne jedwede Wertung kann behauptet werden, dass es für Angreifer umso attraktiver ist, eine Software zu hacken, je weiter diese Software verbreitet ist, also je mehr potentielle Opfer es gibt. Und es leuchtet ein, dass je offener der Quelltext einer Software gelegt ist, desto eher Sicherheitslücken bekannt und meist auch beseitigt werden. Allerdings muss an dieser Stelle berücksichtigt werden, dass aus diesen Vorteilen auch Nachteile folgen können. Ein bekannter Quelltext macht es auch Hackern leichter. Sie können so Sicherheitslücken leichter ausfindig machen oder auch ohne viel Aufwand Veränderungen an der Software vornehmen. Und Software, die nicht so sehr verbreitet ist, ist häufig nicht fehlerfrei und selten benutzerfreundlich. Ausgehend vom Vertrauen in die Software, sieht meine Hitliste der Webbrowser folgendermaßen aus, selbstverständlich in den jeweils neuesten Versionen:

- Mozilla Firefox (Linux, MS Windows, Mac OS)
- Safari (Mac OS X, MS Windows)
- Opera
- Internet Explorer (IE) – neuere Versionen nur für MS Windows

Der Favorit ist – mit Abstand – das Programm, dessen Quelltext offengelegt ist (Firefox). Dies schafft Vertrauen, auch wenn man selbst nicht in der Lage sein sollte, das Programm zu prüfen. An zweiter Stelle stehen die Produkte, die nicht ganz so weit verbreitet sind wie der Internet Explorer von Microsoft (Safari, Opera).

Da es uns die Webmaster nicht gerade leicht machen – weil es die Webbrowser den Webmastern nicht gerade leicht machen – alle Seiten mit unserem Lieblingsbrowser korrekt anzeigen zu können, kommen wir nicht darum herum, mehrere Browser zu nutzen.

Holen Sie sich die Installationssoftware Ihrer Webbrowser stets direkt von den Herstellerseiten. Googlen Sie nicht danach – die Anbieter von Suchmaschinen bewerten die Suchergebnisse nicht nach ihrer Vertrauenswürdigkeit.

- Firefox: <https://www.mozilla.org/>
- Safari: <https://www.apple.com/>
- Opera: <http://www.opera.com/>
- IE: <https://www.microsoft.com/>

Benutzen Sie, wann immer möglich, die abhörsichere Variante zum Abrufen von Webseiten (mit https), so können angeforderte und gesendete Daten unterwegs nicht einfach verändert werden. Nutzen Sie die vom Hersteller angebotenen Möglichkeiten zur Prüfung der Korrektheit Ihrer Downloads (Prüfsummen/Hashwerte).

## Gleich nach der Installation erledigen!

Nach der Installation lassen Sie den neu installierten Webbrowser selbst prüfen, ob es Updates gibt und installieren Sie diese. Das gilt im Übrigen für jede Software, die eine Online-Update-Funktion bietet. Bei der Aktualisierung des Internet Explorers können Sie gleich auch das ganze Betriebssystem updaten. Ähnlich

kann unter Mac OS X die gesamte installierte Software aktualisiert werden. Sie erreichen die Update-Funktion für die verschiedenen Webbrowser/Betriebssysteme wie folgt:

- Firefox: Hilfe → Firefox aktualisieren
- Safari: Apfel-Symbol → Softwareaktualisierung ...
- Opera: Hilfe → Auf Updates überprüfen
- IE: Extras → Windows Update

## Zertifikate der HU installieren

Um sichere, verschlüsselte Verbindungen mit dem Webbrowser herstellen zu können, müssen die Zertifikate der Webserver im Webbrowser installiert sein. In der Installationssoftware der Webbrowser sind viele Zertifikate bereits integriert. Dies ist auch ein Grund, die Webbrowser nur von den Herstellerseiten zu laden. Als Surfer auf Webseiten der Humboldt-Universität sollten Sie sich auf jeden Fall auch die folgenden Wurzelzertifikate installieren:

- Deutsche Telekom Root CA 2  
Fingerprint=85:A4:08:C0:9C:19:3E:5D:51:58:7D:CD:D6:13:30:FD:8C:DE:37:BF
- DFN-PKI-Global  
Fingerprint=F0:28:8F:DA:C6:3A:F7:9A:31:9A:E9:72:F3:95:09:0E:A3:EF:E9:45
- HU-CA  
Fingerprint=59:67:2F:EF:A0:AF:99:12:1D:A7:63:C0:A6:31:B4:01:BE:1A:3C:DA

Diese Zertifikate und die Beschreibungen zur Installation bekommen Sie hier: [http://www.cms.hu-berlin.de/dl/zertifizierung/index\\_html](http://www.cms.hu-berlin.de/dl/zertifizierung/index_html)

Insbesondere immer dann, wenn Sie selbst Daten ins Internet senden (z. B. bei jedem Login), ist es wichtig, eine verschlüsselte und damit abhörsichere Verbindung zu verwenden. Zu erkennen ist dies am kleinen geschlossenen Vorhängeschloss im Webbrowser. Ein Klick auf dieses Symbol zeigt Ihnen weitere Informationen zur bestehenden Verbindung an.

## Aktive Inhalte abschalten

Sobald Sie aktive Inhalte im Webbrowser abschalten, verringern Sie die Gefahr, dass sich ein Schad-Code auf Ihrem Computer einnisten kann.

Zu den aktiven Inhalten zählen vor allem Java, JScript, JavaScript, ActiveX. Aber auch jede andere Zusatzkomponente, beispielsweise Plug-ins, Add-ons, Adobe Flash, MS Silverlight, kann die Gefahr aus dem Internet vergrößern. Es gilt wie bei der Installation von Software, drei Fragen ehrlich zu beantworten (siehe oben). Jede zusätzliche Software erhöht die Wahrscheinlichkeit, dass neue Schwachstellen im eigenen System, sowohl Betriebssystem als auch Webbrowser, entstehen.

Ehrlicherweise muss jedoch zugeben werden, dass der gewünschte Inhalt aus dem Internet nicht immer angezeigt werden kann, wenn aktiver Inhalt deaktiviert wurde. Doch wo die Nutzung vermieden werden kann, sollte sie auch vermieden werden. Hier finden Sie die Einstellungen zu den aktiven Inhalten:

- Firefox: Extras → Einstellungen → Inhalt
- Safari: Edit → Preferences... → Security
- Opera: Extras → Einstellungen → Erweitert → Inhalt
- IE: Extras → Internetoptionen → Sicherheit → Sicherheitsstufe → Sicherheitsstufe anpassen

Abgesehen davon, dass dies im IE meiner Meinung nach eine Zumutung für fast jeden Nutzer ist, finden Sie eine hilfreiche Beschreibung dieser Einstellungen unter: <http://www.bsi-fuer-buerger.de/browser/checkIE7/iexpl7schritt3.htm>

## Cookies

Cookies stellen im Grunde keine Gefahr dar. Es sind kleine Dateien, die es den Betreibern von Webangeboten ermöglichen, Sie und auch Ihr Surfverhalten wiederzuerkennen, auch wenn Sie zwischendurch mal auf anderen Webseiten surfen. Wenn Ihnen dies unheimlich ist, deaktivieren Sie das Speichern von Cookies oder löschen Sie sie regelmäßig, günstigerweise automatisch beim Schließen des Webbrowsers. Wie bei den ak-

tiven Inhalten kann das Deaktivieren dazu führen, dass Sie bestimmte Webangebote nicht nutzen können.

- Firefox: Extras → Einstellungen → Datenschutz
- Safari: Edit → Preferences... → Security
- Opera: Extras → Einstellungen → Erweitert → Cookies
- IE: Extras → Internetoptionen → Datenschutz

## Surfverhalten

Wie eingangs beschrieben, bringt das Nutzerverhalten selbst das größte Sicherheitsrisiko mit sich. Beherrzigen Sie daher die folgenden Hinweise:

- Surf-Konto einrichten  
Wenn möglich, richten Sie sich ein extra Benutzerkonto, ein Gastkonto, mit eingeschränkten Rechten zum Surfen ein. Surfen Sie niemals als Administrator oder als Benutzer mit Administratorrechten (auch wenn Sie zur Installation einer Software unter Umständen Administrator sein müssen, können Sie dennoch den Download dieser Software als Gast durchführen).
- Googlen versus nicht googlen  
Googlen Sie sich nicht zu Webseiten durch, wenn Sie vorhaben, persönliche Daten zu übermitteln. Tippen Sie in solchen Fällen stets die Ihnen bekannte URL in der Adresszeile Ihres Webbrowsers ein – auch wenn dies ein wenig mehr Arbeit macht.
- E-Mail-Klick  
Klicken Sie niemals auf Links, die Ihnen in einer E-Mail zugesandt wurden. Woher eine E-Mail wirklich kam, können Sie nur feststellen, wenn diese digital signiert wurde und Sie diese Signatur prüfen können.
- Geben Sie persönliche Daten nur dann ein, wenn Sie sich sicher sind, dass es sich um ein seriöses Angebot handelt und Sie auch eine entsprechende Gegenleistung bekommen.
- Speichern Sie keine Eingaben (Autovervollständigen, Passwörter!!!)
- Nutzen Sie nicht die Funktion Ihres Webbrowsers, eigene Eingaben zu speichern. Wo immer es möglich ist, geben Sie Daten nur dann ein, wenn eine sichere Verbindung per https

zum Webserver besteht (erkennbar am geschlossenen Vorhängeschloss).

## Sicherheits-Checks

Das Bundesamt für Sicherheit in der Informationstechnik (<http://www.bsi.bund.de/>) bietet einen Service für Bürger. Hier können Sie für die folgenden Webbrowser prüfen, ob die grundlegenden Einstellungen sicher gestaltet sind: <http://www.bsi-fuer-buerger.de/browser/browsercheck.htm>

- Firefox 2.0
- Mozilla 1.7.12
- Opera 8.0
- Internet Explorer 7
- Internet Explorer 6

Auch im Online-Angebot des Zeitschriftenverlags Heise (<http://www.heise.de/>) finden Sie weiterführende Informationen zur Sicherheit im Webbrowser. Hier können Sie Ihren Webbrowser auch online testen: <http://www.heise.de/security/dienste/browsercheck/>

## Zusammenfassung

- Sichern Sie regelmäßig Ihre Daten, prüfen Sie diese Sicherungen.
- Installieren Sie nur Software, die Sie tatsächlich benötigen.
- Halten Sie jede installierte Software aktuell (Betriebssystem, Antivirensoftware, Webbrowser, ...)
- Gehen Sie nicht als Administrator zum Surfen ins Internet.
- Nutzen Sie alle verfügbaren Sicherheitsmechanismen (https, Zertifikate, Verschlüsselung)

Surfen Sie mit Köpfchen, denn:  
Einen absoluten Schutz gibt es nicht!

## Weiterführende Informationen

- Bundesamt für Sicherheit in der Informationstechnik (BSI): [www.bsi.de](http://www.bsi.de)
- Heise Zeitschriftenverlag: [www.heise.de](http://www.heise.de)
- Die freie Online-Enzyklopädie (Wikipedia): [de.wikipedia.org](http://de.wikipedia.org)