Sicher surfen mit Google Chrome

Anleitung im Thema "Sicher surfen"

Mit Chrome hat Google einen eigenen Webbrowser ins Rennen um die Gunst der Websurfer geschickt. Was Sicherheit und Datenschutz angeht, ist allerdings nicht alles von Hause aus optimal voreingestellt. Wir zeigen Ihnen, an welchen Stellschrauben Sie noch drehen sollten.

Aktuell für Google Chrome Version 31 (Nov. 2013)

Inhalt

Google Chrome herunterladen und installieren 2
Sicherheitseinstellungen anpassen 3
"Passwörter und Formulare" verwalten 3
Die Kontrolle über "Downloads" behalten 4
"HTTPS/SSL" – Serverzertifikate überprüfen lassen 4
"Inhaltseinstellungen" – Webseiteninhalte unter Kontrolle bringen 5
"Bilder" anzeigen oder blockieren? 5
"JavaScript" gezielt einschränken 6
"Handler" für Protokolle festlegen 6
"Plug-ins" – Erweiterungen für Medieninhalte 7
Einstellungen für "Pop-ups" 8
"Plug-in-Zugriff ohne Sandbox" 8
"Automatische Downloads" 8
Datenschutzeinstellungen anpassen 10
Einstellungen für Cookies 11
Einstellungen für Standort-Daten 12
Geschützte Inhalte (nur Windows, ChromeOS) 12
Zugriff auf Mikrofon und Kamera 13
Anonymes Browsen und Löschen von Datenspuren 14
Surfen im "Inkognito-Fenster" 14
Datenspuren löschen 14
Chrome-Einstellungen sichern und synchronisieren 15
Nutzungsbedingungen für Google Chrome 15

ANHANG: Abbildungen in Großformat 16

Google Chrome herunterladen und installieren

Sie können Google Chrome kostenlos von den Webseiten des Unternehmens herunterladen. Dort finden Sie Installationspakete zur jeweils aktuellen Version des Browsers für Windows, Mac OS X und Linux.

Google Chrome aktualisiert sich automatisch, sobald neue Updates zur Verfügung stehen. Daher müssen Sie sich nicht um Sicherheitsaktualisierungen für den Browser kümmern. War der Browser bereits geöffnet, bevor die Aktualisierung gestartet wurde, müssen Sie den Browser erneut starten, um die neue Version zu aktivieren.

Neben den üblichen Funktionalitäten eines Browsers bietet Chrome eine enge Anbindung an die vielen Online-Dienste, die Google anbietet. Einige von Googles Online-Diensten sind bereits direkt in den Browser integriert, für andere können Sie entsprechende Erweiterungen für Google Chrome installieren. In dieser Anleitung beschränken wir uns allerdings auf den Browser und lassen die integrierten Dienste und Erweiterungen außen vor.

Zur Verbesserung der Sicherheit und des Schutzes Ihrer persönlichen Daten beim Websurfen sollten Sie nach der Installation einige Änderungen in den Einstellungen des Browsers vornehmen. In den nachfolgenden Abschnitten erfahren Sie, wie Sie Google Chrome optimal einrichten.

Sicherheitseinstellungen anpassen

Nachdem Sie Google Chrome installiert haben, sollten Sie aus Sicherheitsgründen vor der ersten Nutzung einen kurzen Abstecher in die Browser-Einstellungen machen und dort einige Änderungen vornehmen.

Abbildung 1: Menüsymbol

Um die Einstellungen zu öffnen, klicken Sie auf das Menüsymbol (drei waagerechte Balken) rechts oben in der Navigationsleiste (siehe nebenstehende Abbildung) und wählen im erscheinenden Menü-fenster den Punkt "Einstellungen". In der Mac-OS-X-Version können Sie auch alternativ im Menü "Chrome" den Punkt "Einstellungen" wählen.

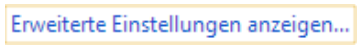

Abbildung 2: Link "Erweiterte Einstellungen"

Nun erscheint im Browserfenster die Einstellungen, die Google als die wichtigsten erachtet. Ganz unten auf der Seite sehen Sie einen Link "*Erweiterte Einstellungen anzeigen…*". Klicken Sie auf diesen Link, um auch die restlichen Einstellungen anzuzeigen. Hier befinden sich auch die für Sicherheit und Datenschutz relevanten Abschnitte.

"Passwörter und Formulare" verwalten

Abbildung 3: Abschnitt "Passwörter und Formulare"

Im Abschnitt "Passwörter und Formulare" legen Sie fest, wie Google Chrome mit Passwörtern und Web-formularen umgehen soll. Die Speicherung von Passwörtern durch den Browser und die automatische Vervollständigung von Webformularen (sogenannte "AutoFill"-Funktion) erleichtern die Handhabung der verschiedenen Dienste im Internet. So müssen Sie nicht jedes Mal die passenden Zugangs- und Formulardaten von Hand eingeben.

In beiden Fällen gilt allerdings: Wird der Computer im selben Benutzerkonto von mehreren Personen genutzt, oder wenn es sich um einen öffentlich zugänglichen Computer handelt, dann sollten Sie die Speicherung von Passwörtern und Formulareingaben durch den Browser abschalten. Denn Ihre Zugangsdaten könnten sonst auch von anderen verwendet werden.

In der Standardeinstellung von Chrome sind beide Funktionen aktiviert. Um sie auszuschalten, entfernen Sie einfach die Häkchen vor der jeweiligen Einstellung.

Außerdem können Sie jede der Einstellung "verwalten" (Link unter der jeweiligen Einstellung anklicken): Bei AutoFill die gespeicherten Adressen und Kreditkartendaten, und bei "Passwörter" die gespeicherten Passwörter sowie eine Liste von Websites, für das Sie keine Passwörter gespeichert haben möchten.

Die Kontrolle über "Downloads" behalten

Abbildung 4: Einstellung "Downloads"

Im Abschnitt "*Downloads*" können Sie einstellen, dass Sie vor dem Herunterladen von Dateien nach dem Speicherort gefragt werden. Haben Sie diese Einstellung aktiviert, erscheint vor jedem Download ein Dialogfenster, in dem Sie den gewünschten Speicherort festlegen können. Dadurch verhindern Sie auch, dass Dateien unter Umständen ohne Ihr Wissen auf den Computer heruntergeladen werden.

Abbildung 5: Inhaltseinstellung "Automatische Downloads"

In den Inhaltseinstellungen gibt es darüber hinaus den Abschnitt "*Automatische Downloads*". Es gibt offenbar Fälle, in denen mehrere Dateien automatisch hintereinander heruntergeladen werden, obwohl der geklickte Download-Link dies nicht deutlich machte. Mit der Einstellung "*Automatische Downloads*" wird in solchen in der voreingestellten Alternative ein Warnungsdialog angezeigt. Man kann aber auch einstellen, dass solche Mehrfach-Downloads immer unterbunden ("*Keiner Website gestatten,…*") oder immer erlaubt werden ("*Allen Websites gestatten,…*"). Für einzelne Websites lassen sich über die Schaltfläche "*Ausnahmen verwalten*" diese Einstellung ändern.

"HTTPS/SSL" – Serverzertifikate überprüfen lassen

Abbildung 6: Einstellung "HTTPS/SSL"

Im Abschnitt "*HTTPS/SSL*" der erweiterten Einstellungen können Sie die Option "*Serverzertifikate auf Sperrung prüfen*" aktivieren. Anhand eines Serverzertifikats stellt Ihr Browser sicher, dass er mit dem "richtigen" Server kommuniziert. Das Zertifikat darf allerdings nicht in die Hände von Angreifern gelangen, da diese das Zertifikat dazu benutzen können, ihren eigenen Server als den ursprünglich zertifizierten Server auszugeben. Besteht der Verdacht, dass dies geschehen sein könnte, wird das Zertifikat gesperrt, das heißt in eine Sperrliste eingetragen.

Durch Aktivieren der genannten Option überprüft Chrome bei jeder verschlüsselten TLS/SSL-Verbindung ("https"), ob das vom Server übermittelte Zertifikat noch gültig ist oder bereits gesperrt wurde. Dies kostet zwar etwas Zeit, bietet aber ein höheres Maß an Sicherheit.

"Inhaltseinstellungen" – Webseiteninhalte unter Kontrolle bringen

Eine Webseite besteht in der Regel aus einer Kombination von Texten, Bildern, multimedialen Inhalten und Programmcode (Skripten). Diese Inhalte stammen oft nicht allein vom Anbieter der von Ihnen angesteuerten Webseite ("Erstanbieter"), sondern werden von Drittanbietern zugeliefert und eingebunden. Ganz häufig geschieht das bei der Anzeige von Werbung.

Nicht in jedem Fall sind die zugelieferten Inhalte allerdings harmlos. Immer wieder kommt es auch vor, dass Angreifer Sicherheitslücken ausnutzen, um bösartige Skripte oder andere Inhalte unterzuschieben. Aus diesem Grunde sollten Sie vorsichtig mit den Inhalten von Webseiten umgehen. Der Chrome-Browser unterstützt Sie dabei und erlaubt es Ihnen, die Anzeige von Inhalten kontrolliert zuzulassen oder zu verbieten.

Abbildung 7: Fenster "Inhaltseinstellungen" (Ausschnitt)

Im Abschnitt "*Datenschutz*" finden Sie die Schaltfläche "*Inhaltseinstellungen*". Darüber gelangen Sie zu den Einstellungen für die Anzeige von Webseiten-Inhalten. Viele dieser Einstellungen betreffen sowohl die Sicherheit als auch den Datenschutz. Wir führen hier die Einstellungen auf, die vorwiegend sicherheitsrelevant sind.

"Bilder" anzeigen oder blockieren?

Im Abschnitt "*Bilder*" legen Sie fest, ob Bilder auf Webseiten automatisch angezeigt oder blockiert werden sollen. Bilder können unter Umständen dazu ausgenutzt werden, Ihr Surfverhalten auszuspionieren (als sogenannte "Web-Wanzen") oder Schadcode auf Ihren Computer zu schleusen. Da allerdings die meisten Webseiten Grafiken einsetzen, schränkt die Option "Keine Bilder anzeigen" den Surfkomfort sehr ein und ist daher nur sinnvoll, wenn aufgrund einer Sicherheitslücke eine Warnung und Empfehlung dazu ausgesprochen wurde. Über die Schaltfläche "Ausnahmen" können Sie außerdem individuelle Regelungen für einzelne Webseiten festlegen.

Abbildung 8: Inhaltseinstellung "Bilder"

"JavaScript" gezielt einschränken

Abbildung 9: JavaScript über die Adressleiste blockieren

Im Abschnitt "*JavaScript*" legen Sie fest, ob JavaScript grundsätzlich zugelassen oder blockiert werden soll. Da JavaScript mittlerweile von sehr vielen Webseiten verwendet wird, ist ein komplettes Abschalten nicht ratsam. Auf der anderen Seite ist ein uneingeschränktes Erlauben von JavaScript mit Sicherheitsrisiken verbunden.

Sie können den Einsatz von JavaScript gezielt einschränken, indem Sie die Option "*Ausführung von JavaScript für keine Website zulassen*" aktivieren und dann Ausnahmen für vertrauenswürdige Seiten hinzufügen. Diese Ausnahmen jedes Mal von Hand einzutragen ist jedoch relativ umständlich.

Einfacher geht es über ein kleines Symbol (ein Dokument mit einem kleinen roten Kreuz) in der Adressleiste: Wenn JavaScript auf einer Webseite blockiert wurde, zeigt Chrome dieses Symbol in der Adressleiste an. Mit einem Klick auf das Symbol haben Sie die Möglichkeit, eine Ausnahmeregel für diese Website zu erstellen und JavaScript zuzulassen. Danach müssen Sie die Seite erneut laden, um die Änderung zu übernehmen.

"Handler" für Protokolle festlegen

Abbildung 10: Inhaltseinstellung "Handler"

Als "Handler" wird ein Programm bezeichnet, welches eine bestimmte Anwendung (genauer: ein technisches "Protokoll") bereitstellt.

Ein Beispiel: Auf Webseiten gibt es immer wieder Links, die nicht zu einer Webseite führen. Stattdessen beginnen Sie mit der Kennung für das Protokoll "E-Mail", "`mailto:`", gefolgt von einer E-Mail-Adresse. Klickt man darauf, dann wird automatisch ein E-Mail-Programm geöffnet und ein Formular "Neue E-Mail verfassen" mit der Adresse aus dem Link gezeigt. Der Browser Chrome hat für das hierbei für das Protokoll "`mailto:`" den "Handler", also das E-Mail-Programm, mit der E-Mail-Adresse aus dem Link geöffnet.

Chrome ermöglicht es nun auch Web-Diensten, diese Aufgabe zu übernehmen und als sogenannter "Handler" für die genannten Protokolle aufzutreten. Beim Anklicken eines E-Mail-Links wird dann beispielsweise eine entsprechende Webseite (des festgelegten Webdienstes) geöffnet, in der Sie die E-Mail direkt verfassen können.

Mit der Option "*Registrierung von Websites als Standard-Handler für Protokolle zulassen*" erlauben Sie es Websites, Sie zu fragen, ob die Dienste der Website für die

genannten Protokolle genutzt werden sollen. Wenn Sie das nicht wollen, wählen Sie dagegen die Option "*Verarbeitung von Protokollen für keine Website zulassen*".

"Plug-ins" – Erweiterungen für Medieninhalte

Mit dieser Einstellung können Sie die Ausführung von installierten Plug-ins kontrollieren. Plug-ins dienen dazu, die Darstellung von interaktiven oder Medieninhalten von PDF-Dateien über Flash-Videos bis zu Java-"Applets" im Browserfenster zu ermöglichen.

Abbildung 11: Inhaltseinstellung "Plug-ins"

Mit der von Google empfohlenen Voreingestellung werden alle Plug-ins automatisch ausgeführt. Dies ist aber ein Sicherheitsrisiko, da auf diese Weise auch bösartige Inhalte geladen und ausgeführt werden, die Sicherheitslücken in Plug-ins ausnutzen und Ihren Computer infizieren. Um sich davor zu schützen, gibt es zwei mögliche Alternativen: Das "Click-to-Play", oder die vollständige Blockierung mit Zulassen von Ausnahmen.

Click-to-Play: Bei dieser Einstellung wird Ihnen beim Surfen für jeden Plug-in-Inhalt ein Platzhalter angezeigt. Sie wählen dann explizit durch Klick auf den oder die Platzhalter, welches der Inhalte geladen und ausgeführt werden soll. So könnte beispielsweise auf einer Seite ein Flash-Video, zwei Flash-Werbeanzeigen und ein (versteckter) Plug-in-Inhalt mit Schadcode vorhanden sein. Sie sehen dann vier Platzhalter, und können durch Klicken das Flash-Video abspielen, während die anderen drei Inhalte ungeladen bleiben.

Abbildung 12: Plug-ins (Adressleiste)

Vollständige Blockierung: Bei dieser Einstellung werden alle Plug-in-Inhalte grundsätzlich blockiert. Möchten Sie diese aber für für eine Website zulassen, dann können Sie Ausnahmen angeben. Sehen Sie also beim Surfen eine Seite mit einem oder mehr blockierten Plug-ins, dann erscheint in der Adresszeile rechts ein Puzzle-Stück-Symbol mit kleinem rotem Kreuz. Mit einem Klick auf dieses Symbol können Sie die Option "*Plug-ins auf* [Name der Website] *immer zulassen*" wählen, oder die Schaltfläche "*Dieses Mal alle Plug-ins ausführen*" betätigen. Mit erster Option "*immer zulassen*" wird die Website in die Liste der Ausnahmen von der Blockierung aufgenommen, mit letzterer nicht. In beiden Fällen werden die Plug-ins auf der gewählten Seite aktiviert.

Einstellungen für "Pop-ups"

Im Abschnitt "*Pop-ups*" können Sie den Umgang mit Pop-up-Fenstern festlegen. Die Einstellung "*Anzeige von Pop-ups für keine Website zulassen*" ist hier bereits standardmäßig ausgewählt und kann im Normalfall auch beibehalten werden. Pop-up-Fenster werden häufig für Werbung eingesetzt und können das Surfen im Internet beeinträchtigen.

Abbildung 13: Inhaltseinstellung "Pop-ups"

Chrome zeigt Ihnen mit einem kleinen Symbol (Fenster mit kleinem roten Kreuz) in der Adressleiste an, wenn Pop-up-Fenster blockiert wurden. Mit einem Klick auf dieses Symbol können Sie sich die blockierten Fenster anzeigen lassen. Weiterhin haben Sie die Möglichkeit, Pop-up-Fenster für diese Website grundsätzlich zuzulassen (Änderungen werden erst beim erneuten Laden der Seite aktiv). So können Sie einfach und gezielt reagieren, sollte eine Website ohne Pop-up-Fenster nicht richtig nutzbar sein.

"Plug-in-Zugriff ohne Sandbox"

Eine weitere Einstellung im Zusammenhang mit Plug-ins findet sich fast am Ende der Inhaltseinstellungen. Die "Sandbox" ist ein Sicherheitsmechanismus, mit der das Plug-in in Chrome isoliert ausgeführt wird. Sollte Schadsoftware versuchen, eine Sicherheitslücke des Plug-ins auszunutzen, könnte es wegen der Sandbox nicht auf den Computer übergreifen. Allerdings benötigen Plug-ins manchmal Zugriff auf den Computer, etwa wenn es für einen Videochat auf Mikrofon und Kamera zugreifen muss. Daher ist die voreingestellte Option "Eingabeaufforderung anzeigen…" hier sinnvoll. Dann können Sie jedesmal entscheiden, ob Sie einem Plug-in den Zugriff auf den Computer ermöglichen oder nicht. Alternativ können Sie alle Zugriffe blockieren und mit "Ausnahmen verwalten" per Hand ausgesuchten Plug-ins den Zugriff erlauben.

Abbildung 14: Inhaltseinstellung "Plug-in-Zugriff ohne Sandbox"

"Automatische Downloads"

Wenn Sie eine Datei von einer Webseite herunterladen, dann kann es vorkommen, dass diese Webseite nicht nur eine, sondern gleich mehrere Dateien zurücksendet. Dies hört sich komfortabel an (Sie müssen nicht jede einzeln herunterladen). Aber dies könnte auch von

Abbildung 15: Inhaltseinstellung "Automatische Downloads"

Angreifern ausgenutzt werden, um so versteckt schädliche Dateien in Ihren Computer zu laden.

Mit der Einstellung "*Automatische Downloads*" legen Sie fest, wie sich Chrome in solchen Fällen verhalten soll.

Die empfohlene Voreinstellung ("*Mich fragen, wenn eine Website versucht, Dateien nach der ersten Datei automatisch herunterzuladen*") ist sinnvoll. Denn dann erhalten Sie eine explizite Meldung, und können wählen, was geschehen soll.

Chrome bietet für andere Situationen auch an, solche automatisch zuzulassen oder ganz zu blockieren. Auch können Sie über die Schaltfläche "*Ausnahmen*" für bestimmte Websites bestimmen, von der Einstellung abzuweichen.

Datenschutzeinstellungen anpassen

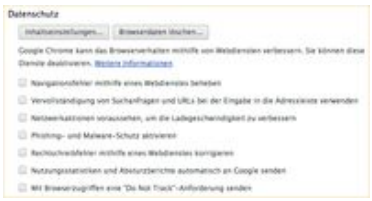

Abbildung 16: Einstellungen "Datenschutz"

Die wichtigsten Datenschutzeinstellungen finden Sie in den "*erweiteren Einstellungen*". Dort bietet der Abschnitt "*Datenschutz*" eine Reihe von Einstellungen, die im Folgenden kurz erläutert werden:

Navigationsfehler mithilfe eines Webdienstes beheben: Wird eine Webseite nicht gefunden, dann wird normalerweise eine Fehlermeldung angezeigt. Ist diese Option eingeschaltet, schlägt Google automatisch Links zu ähnlichen Webseiten vor. Dazu werden Ihre IP-Adresse und Informationen aus gespeicherten Cookies an Google übermittelt, womit Vorschläge mit Ihrer Person verknüpft werden könnten. Wenn Sie dies nicht möchten, dann schalten Sie diese Option aus.

Vervollständigung von Suchanfragen und URLs bei der Eingabe in die Adressleiste verwenden: Bei Google Chrome fallen Suchfeld und Adressleiste zusammen. Sie geben sowohl Suchbegriffe als auch komplette Webadressen in dasselbe Eingabefeld ein. Wenn diese Einstellung aktiviert ist, zeigt Ihnen Chrome bereits während der Eingabe Vorschläge für Webadressen an. Damit dies funktioniert, werden Ihre Eingaben an Google geschickt, dort ausgewertet, und gespeichert. Nach Angaben von Google werden nur zwei Prozent aller Nutzereingaben statistisch erfasst und nach 24 Stunden anonymisiert. Wenn Sie jedoch das Übermitteln und Speichern Ihrer Eingaben verhindern möchten, dann schalten Sie diese Option aus.

Netzwerkaktionen voraussehen, um die Ladegeschwindigkeit zu verbessern: Normalerweise ermittelt ein Browser die (nummerische) IP-Adresse für eine Webseite (genauer: der Domainname) erst, wenn Sie auf deren Link klicken. Wenn diese Einstellung aktiviert ist, dann ermittelt Chrome automatisch im Hintergrund die IP-Adresse für alle Links auf der Webseite. Damit soll das Laden einer Webseite, dessen Link sie anklicken, beschleunigt werden. Der Geschwindigkeitsgewinn ist allerdings in der Regel gering. Aber es werden keine persönlichen Daten an Google übermittelt. Aus Datenschutzsicht ist diese Option daher unbedenklich. Sie können hier trotzdem die Option ausschalten, wenn Sie diese Funktion nicht wünschen.

Phishing- und Malwareschutz aktivieren: Diese Einstellung betrifft die so genannte "Safe Browsing"-Funktion. Google verwaltet und aktualisiert eine Liste von als

gefährlich eingestuften Websites. Steuern Sie eine dieser Websites an, dann zeigt Chrome Ihnen zunächst eine Warnung an. Dazu wird die Adresse jeder Website, die Sie anwählen, zusammen mit der IP-Adresse Ihres Computers und Cookie-Daten an Google übermittelt. Das "Safe Browsing" ist ein sinnvolles Instrument zum Schutz gegen gefährliche Websites. Wenn Sie sich dies aber nicht mit der Übermittlung Ihrer Daten an Google 'erkaufen' möchten, dann schalten Sie diese Option aus.

Rechtschreibfehler mithilfe eines Webdienstes korrigieren: Wenn Sie einen Text in ein Webformular eingeben, so wird dieser an Google gesendet und und auf Rechtschreibung geprüft, wenn Sie diese Option aktiviert haben. Es ist unklar, inwiefern Google diese Daten speichert. Möchten Sie also die Übermittlung an Google verhindern, dann schalten Sie diese Option aus.

Nutzungsstatistiken und Absturzberichte automatisch an Google senden: Diese Option dient der Weiterentwicklung von Chrome. Allerdings werden dazu unter Umständen persönliche Informationen an Google übermittelt.

Mit Browserzugriffen eine "Do Not Track"-Anforderung senden: Im Gegensatz zu den anderen Optionen wird hier kein Webdienst von Google in Anspruch genommen. Wenn diese Option aktiviert ist, so wird an alle Webanbieter, deren Seiten Sie aufrufen, eine Mitteilung gesendet, dass Sie nicht möchten, dass der Anbieter Ihre Daten zum Zwecke des "Tracking" (der Erstellung von Surfprofilen) speichert und verarbeitet. Der Anbieter ist derzeit nicht gesetzlich verpflichtet, dieser Aufforderung nachzukommen. Wenn Sie aber trotzdem diese Aufforderung senden möchten, können Sie diese Option anschalten.

Einstellungen für Cookies

Lesen Sie hierzu auch unsere Anleitung "Cookies verwalten in Google Chrome"

Im Abschnitt "*Cookies*" in den "*Inhaltseinstellungen*" (in den *erweiterten Einstellungen*) legen Sie fest, inwiefern Cookies im Browser gespeichert werden sollen. In den Einstellungen wird statt "Cookies" teilweise auch der etwas allgemeinere Begriff "lokale Daten" verwendet.

Abbildung 17: Inhaltseinstellung "Cookies"

Cookies sind aus Datenschutzgründen bedenklich, da sie auch dazu benutzt werden, Ihre Surfgewohnheiten zu erfassen. Viele Webseiten setzen jedoch den Einsatz von Cookies voraus, sodass die Auswahl "Speicherung von Daten für alle Websites blockieren" mit Einschränkungen beim Websurfen verbunden sein kann.

Mit den Optionen "*Speicherung lokaler Daten nur für aktuelle Sitzung zulassen*" und "*Cookies und andere Website- und Plug-in-Daten beim Schließen des Browsers löschen*" können Sie aber dafür sorgen, dass alle gespeicherten Cookies beim Beenden des Browsers wieder entfernt werden.

Über die Schaltfläche "*Ausnahmen verwalten*" können Sie für einzelne Webseiten unabhängig von der gewählten Option festlegen, ob Cookies grundsätzlich, nur für die laufende Sitzung oder gar nicht zugelassen werden sollen.

Über die Schaltfläche "*Alle Cookies und Websitedaten*" können Sie sehen, welche Cookies gerade im Browser gespeichert sind. Dort können Sie alle oder einzelne Cookies von Hand löschen.

Cookies von Drittanbietern werden häufig für die Anzeige von Werbung eingesetzt. Sie können sie daher in der Regel blockieren, ohne große Einbußen beim Surfkomfort hinnehmen zu müssen. Aktivieren Sie dazu die Option "*Setzen von Drittanbieter-Cookies blockieren*". Alle Drittanbieter-Cookies werden dann blockiert, auch von Websites, deren Cookies Sie unter "*Ausnahmen verwalten*" explizit zugelassen haben.

Einstellungen für Standort-Daten

Abbildung 18: Inhalts-einstellung "Standort"

Im Abschnitt "*Standort*" der "*Inhaltseinstellungen*" finden Sie die Einstellungen zur Chrome-Standort-funktion. Wenn sie diese zulassen, dann werden unter anderem Informationen über ihr Gerät (z.B. die IP-Adresse), WLAN-Router und Sendemasten in Ihrer Nähe oder die Stärke Ihrer WLAN- bzw. Mobilfunk-verbindung zur Verarbeitung von Standortanfragen (im Rahmen der "Google Location Services") an Google oder andere Website-Betreiber übermittelt. Wenn Sie diese Angaben über Ihren aktuellen Standort nicht übermitteln möchten, dann schalten Sie die Standortfunktion ab. Alternativ können Sie sich für jede Anfrage eine Bestätigung anzeigen lassen, ob Sie diese zulassen wollen oder nicht. Auch hier bietet Chrome an, dass Sie für Ihre Wahl der Einstellung Ausnahmen angeben.

Geschützte Inhalte (nur Windows, ChromeOS)

Abbildung 19: Inhalts-einstellung "Geschützte Inhalte"

Unter Windows und ChromeOS hat der Chrome-Browser einen Mechanismus installiert, mit der Websites Ihren Computer eindeutig identifizieren können. Dies wird dazu benutzt, um in Chrome gekaufte Medieninhalte an Ihren Computer zu binden.

Wenn Sie keine Medieninhalte in Chrome kaufen, dann sollten Sie diese Einstellung deaktivieren, da sie möglicherweise von Webseiten generell dazu benutzt werden könnte, Sie beziehungsweise Ihren Computer stets eindeutig zu identifizieren.

Zugriff auf Mikrofon und Kamera

Abbildung 20: Inhalts-einstellung "Medien"

Webseiten können inzwischen auch ohne die Hilfe von Plug-ins den Zugriff auf Kamera und Mikrofon anfordern, um beispielsweise einen Videochat zu ermöglichen. Damit dies nicht heimlich geschehen kann, gibt Chrome hier die Möglichkeit, dass vor dem Zugriff nachgefragt wird (voreingestellt), oder der Zugriff ganz verboten wird. Für Webseiten, denen Sie vertrauen, können Sie zusätzlich hier Ausnahmen eintragen.

Anonymes Browsen und Löschen von Datenspuren

Surfen im "Inkognito-Fenster"

Beim Websurfen hinterlassen Sie im Browser Spuren, die einiges über Ihre Surfgewohnheiten aussagen. Zum Beispiel finden sich Informationen zu besuchten Webseiten im Browser-Verlauf, in gespeicherten Cookies oder hinterlegten Zugangsdaten. Schutz bietet der mittlerweile von vielen Browsern angebotene private Modus, in Google Chrome "Inkognito-Fenster" genannt.

Abbildung 21: Inkognito-Fenster

Mit dem "Inkognito-Fenster" bietet Ihnen Chrome die Möglichkeit, im Internet zu surfen, ohne die genannten Spuren im Browser zu hinterlassen. Nutzungsdaten wie besuchte Webseiten, Cookies, eingegebene Formular- und Zugangsdaten werden beim Schließen des Fensters gelöscht. Daten aus Nicht-"Inkognito"-Browserfenstern bleiben dabei erhalten.

Das Websurfen im Inkognito-Fenster ist insbesondere dann zu empfehlen, wenn Sie mit einem fremden oder öffentlich zugänglichen Computer (z.B. im Internet-Café) ins Internet gehen.

Sie öffnen ein neues Inkognito-Fenster, indem Sie im Schraubenschlüsselsymbol-Menü den Menüpunkt "Neues Inkognito-Fenster" wählen. Daraufhin erscheint ein neues Browser-Fenster mit einem speziellen Agenten-Symbol in der linken oberen Ecke des Fensters. Hier können Sie nun wie gewohnt im Internet surfen. Schließen Sie danach das Fenster, damit Chrome alle Surfspuren für dieses Fenster löscht.

Datenspuren löschen

Sie können die beim Websurfen entstandenen Datenspuren im Browser löschen. Dazu klicken Sie in den erweiterten Einstellungen im Abschnitt "Datenschutz" auf die Schaltfläche "*Browserdaten löschen…*". Oder Sie klicken im Browserfenster auf das Menüsymbol oben rechts und wählen im Menüpunkt "*Tools*" die Option "*Browserdaten löschen…*".

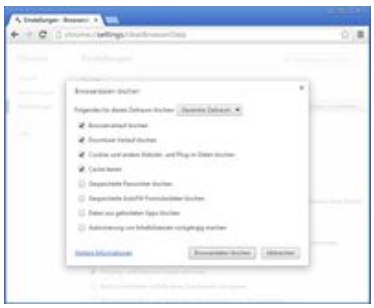

Abbildung 22: Einstellung "Browserdaten löschen"

Im erscheinenden Fenster "*Browserdaten löschen*" können Sie wählen, welche der gespeicherten Daten

(z.B. Browser- oder Download-Verlauf, Cookies, Passwörter) Sie löschen möchten. Außerdem können Sie den Zeitraum wählen, für den die Daten gelöscht werden sollen, also beispielsweise alle Daten der vergangenen Woche löschen.

Wichtig: Das Inkognito-Fenster und das Löschen der Browserdaten wirken sich nur auf die Spuren aus, die *in Ihrem Browser gespeichert werden*. Daten, die beim Besuch einer Webseite *beim Webseitenanbieter gespeichert* werden, werden durch den Inkognito-Modus nicht erfasst.

Chrome-Einstellungen sichern und synchronisieren

*Lesen Sie auch unseren Artikel "*Das Google-Konto: Ihr Tor zu Googles Diensten*"*

Die Synchronisierungsfunktion in Chrome ermöglicht es Ihnen, Ihre Browser-Einstellungen, Lesezeichen und Browser-Designs zu sichern und auf mehreren Computern zu verwenden, ohne die Änderungen auf jedem Computer vornehmen zu müssen. Diese Daten werden dazu in Ihrem Google-Konto gespeichert. Wenn Sie noch kein Google-Konto besitzen, müssen Sie zunächst ein solches erstellen, um die Synchronisierungsfunktion verwenden zu können.

Durch die Online-Speicherung sichern Sie die Daten auch für den Fall, dass diese auf Ihrem Computer beschädigt oder gelöscht werden. Ihre Lesezeichen werden außerdem in Googles Online-Dienst "Text & Tabellen" hinterlegt, sodass Sie auch von anderen Browsern aus Zugriff auf Ihre Lesezeichen haben.

Um die Synchronisierungsfunktion zu aktivieren, klicken Sie auf die Schaltfläche "*In Chrome anmelden*" im Abschnitt "*Anmelden*" der Chrome-Einstellungen (praktischerweise hat Google diese Einstellung an die erste Stelle positioniert).

Nutzungsbedingungen für Google Chrome

Bevor Sie Google Chrome herunterladen und installieren können, müssen Sie den Google-Chrome-Nutzungsbedingungen zustimmen. Darin erklärt Google, welche Rechte und Pflichten Sie bei der Chrome-Nutzung haben. Unter anderem sind hier die Datenschutzbestimmungen für die Chrome-Nutzung aufgeführt. Sollten Sie mit den Nutzungsbedingungen nicht einverstanden sein, dann dürfen Sie Google Chrome nicht benutzen.

ANHANG: Abbildungen in Großformat

Abbildung 1: Menüsymbol

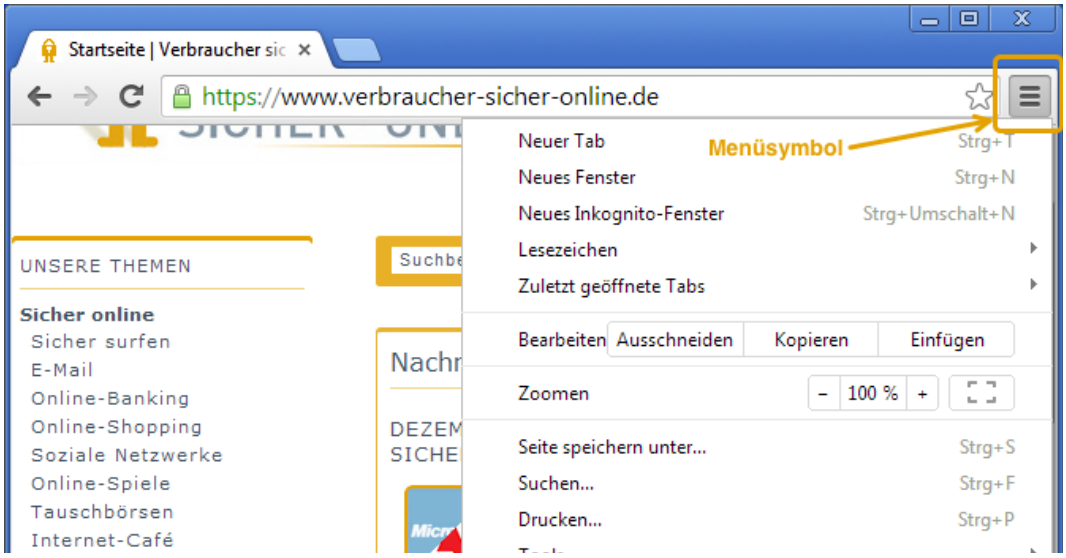

Abbildung 2: Link "Erweiterte Einstellungen"

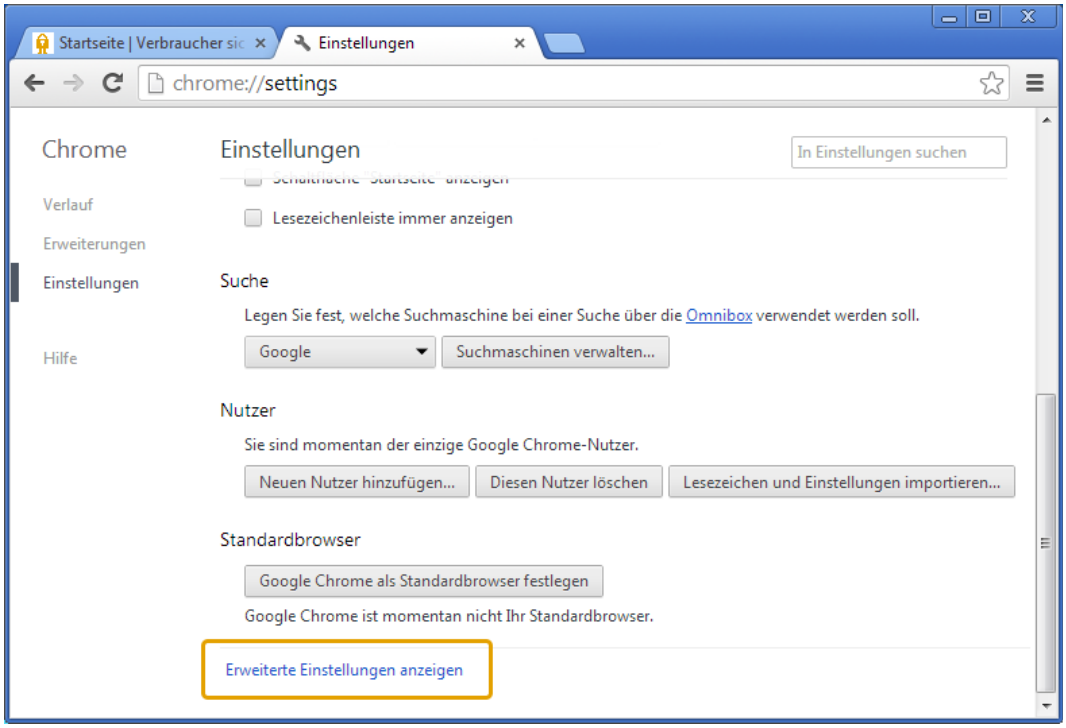

Abbildung 3: Abschnitt "Passwörter und Formulare"

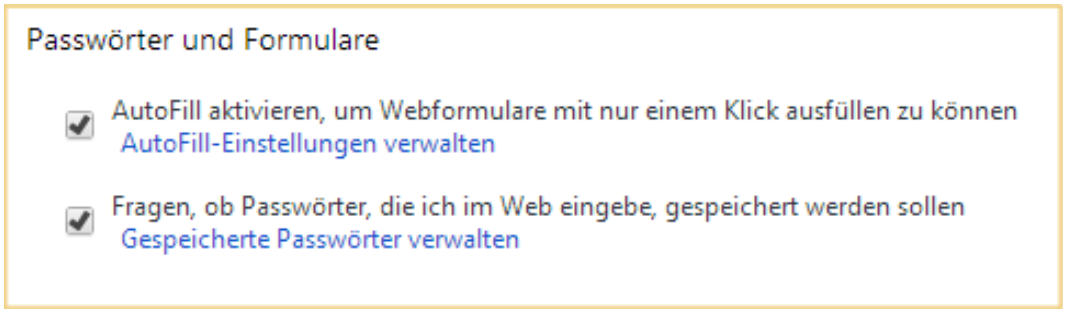

Abbildung 4: Einstellung "Downloads"

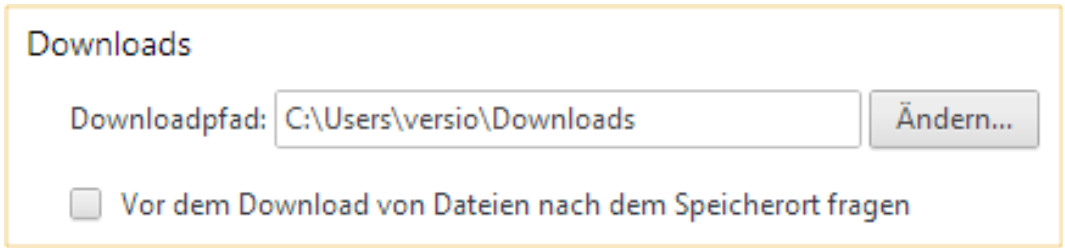

Abbildung 5: Inhaltseinstellung "Automatische Downloads"

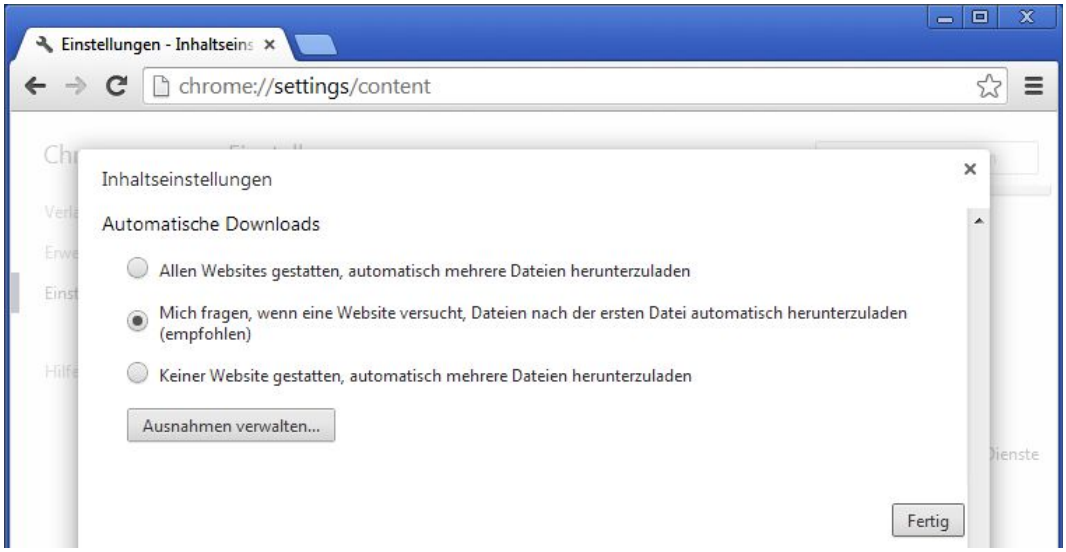

Abbildung 6: Einstellung "HTTPS/SSL"

Abbildung 7: Fenster "Inhaltseinstellungen" (Ausschnitt)

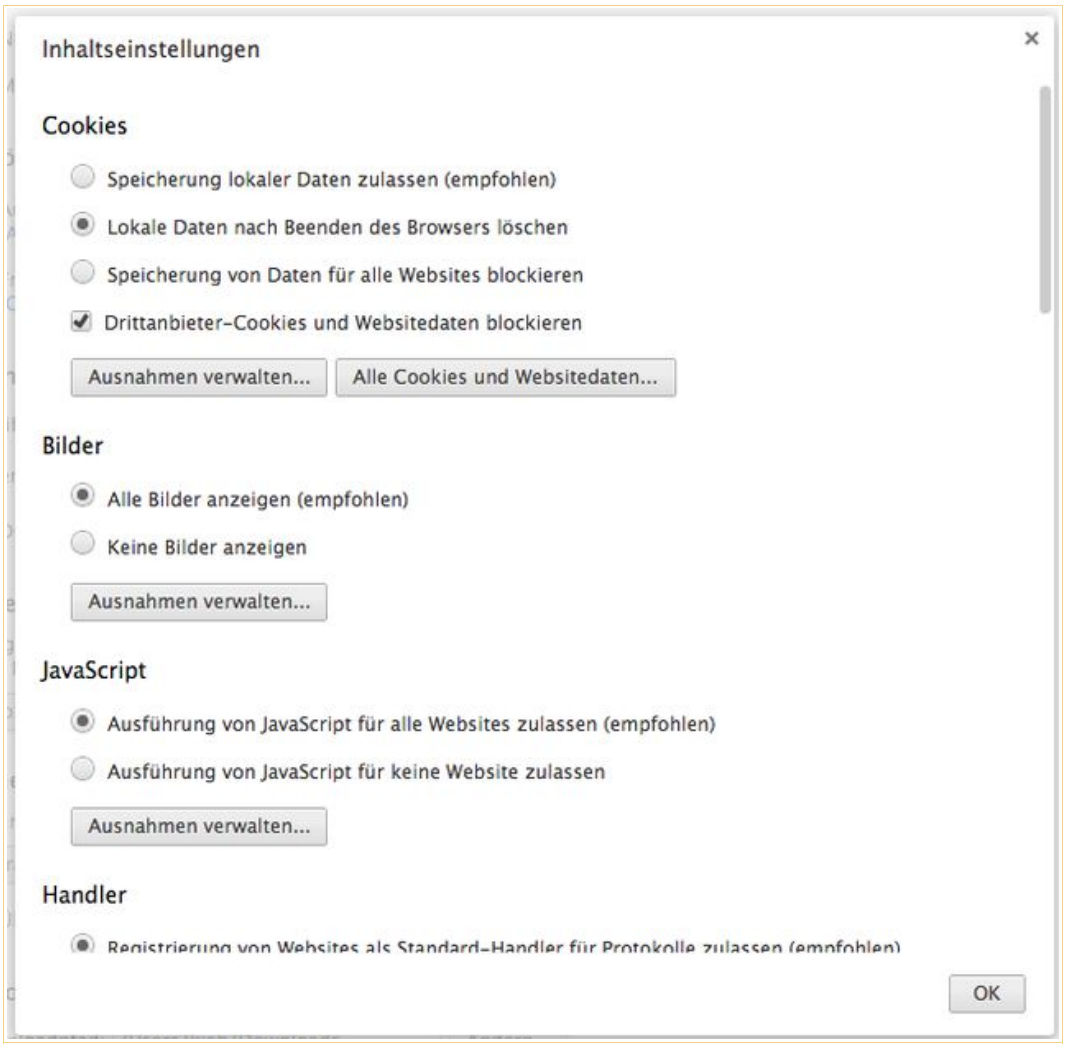

Abbildung 8: Inhaltseinstellung "Bilder"

Abbildung 9: JavaScript über die Adressleiste blockieren

Abbildung 10: Inhaltseinstellung "Handler"

Abbildung 11: Inhaltseinstellung "Plug-ins"

Abbildung 12: Plug-ins (Adressleiste)

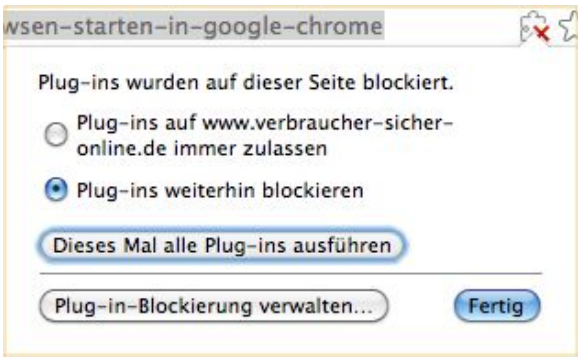

Abbildung 13: Inhaltseinstellung "Pop-ups"

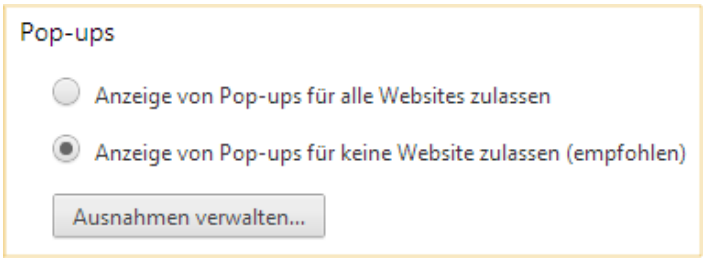

Abbildung 14: Inhaltseinstellung "Plug-in-Zugriff ohne Sandbox"

Abbildung 15: Inhaltseinstellung "Automatische Downloads"

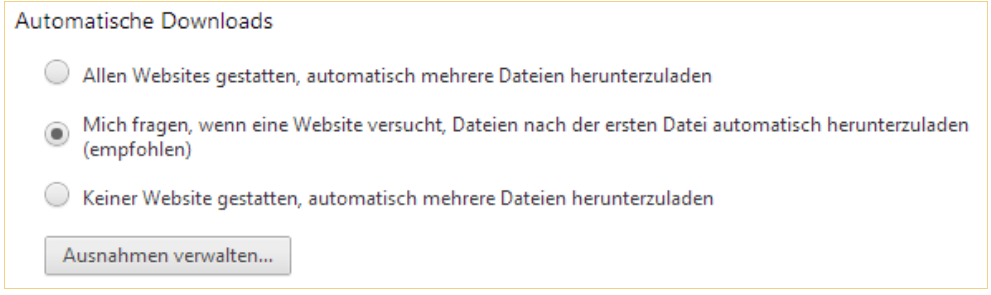

Abbildung 16: Einstellungen "Datenschutz"

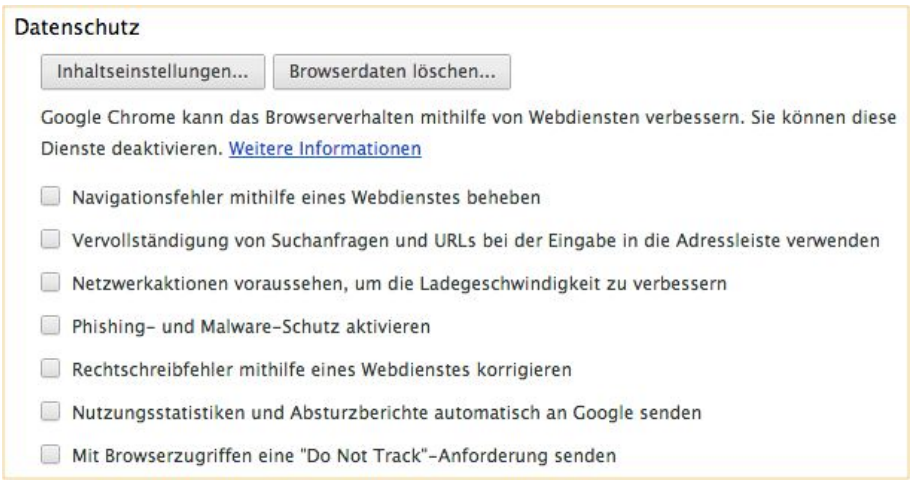

Abbildung 17: Inhaltseinstellung "Cookies"

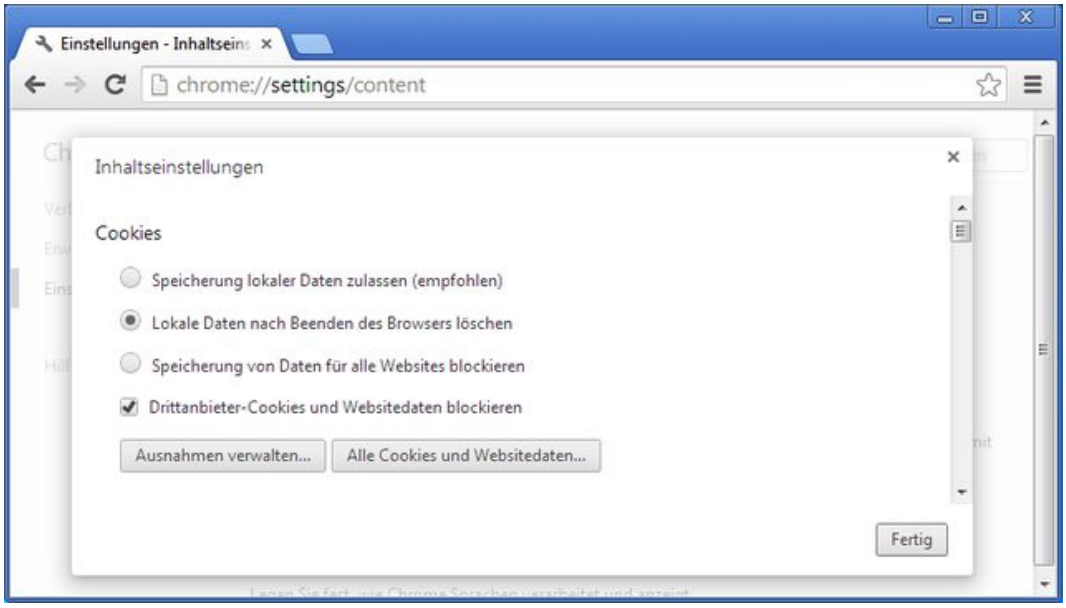

Abbildung 18: Inhaltseinstellung "Standort"

Abbildung 19: Inhaltseinstellung "Geschützte Inhalte"

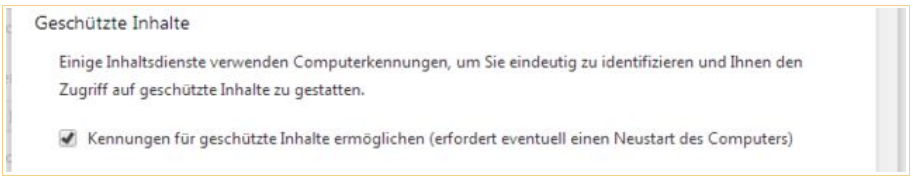

Abbildung 20: Inhaltseinstellung "Medien"

Abbildung 21: Inkognito-Fenster

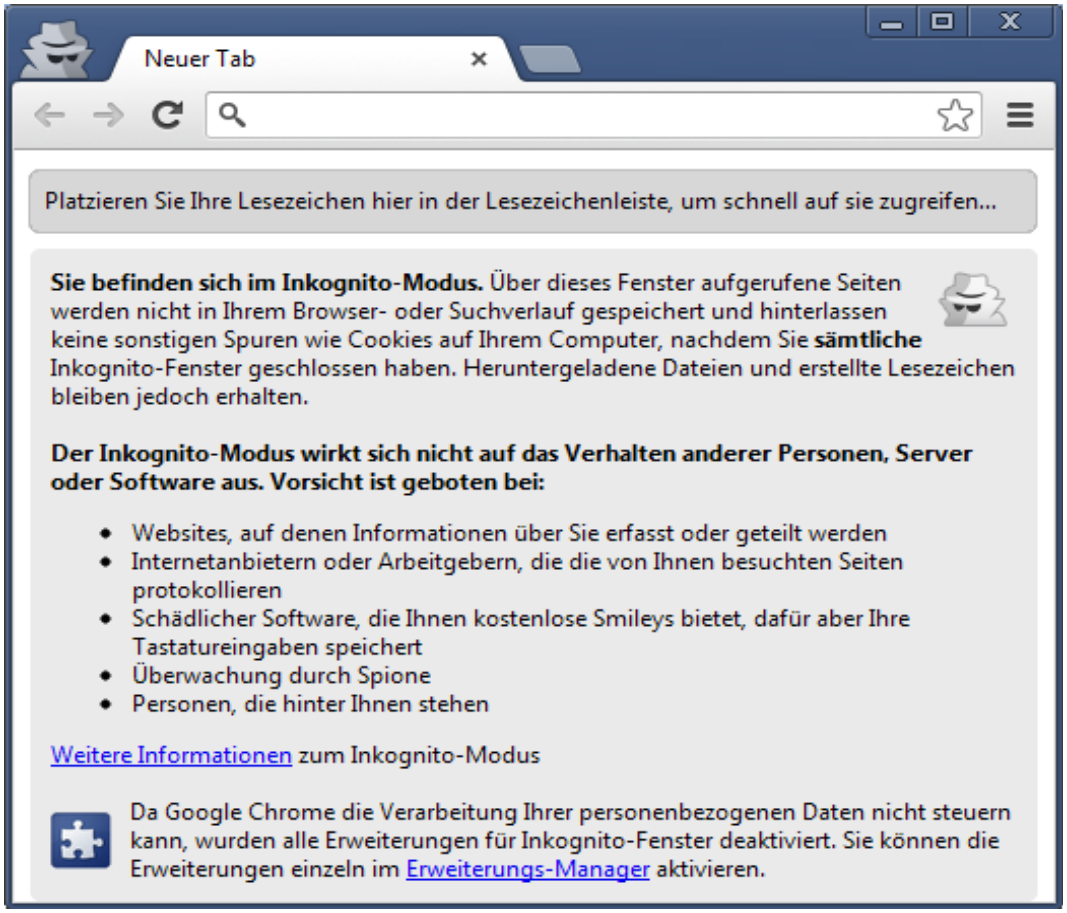

Abbildung 22: Einstellung "Browserdaten löschen"