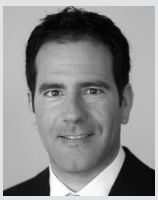
Ulrich Pordesch, Katja Seitz, Jan Steffan, Roland Steidle

Chrome mit Kratzern

Google's Webbrowser und der Datenschutz

Anfang September 2008 hat Google seinen neuen Webbrowser „Chrome" in einer Testversion auf den Markt gebracht, seit Dezember ist eine fertige Version 1.0 verfügbar. Der neue Browser soll eine bessere Performance als vergleichbare Produkte aufweisen, neue Funktionen beinhalten und zudem stabiler laufen. Er hat daher viele Nutzer von Anfang an begeistert. Allerdings gab es auch kritische Stimmen, insbesondere wegen datenschutzrechtlicher Aspekte einzelner Funktionen. Der Beitrag erläutert die wesentlichen neuen Funktionen von Chrome und deren Risiken, bewertet diese datenschutzrechtlich und schließt mit einer Empfehlung für den Unternehmenseinsatz.



Dr. Roland Steidle

ist Rechtsanwalt bei Waldeck Rechtsanwälte in Frankfurt am Main

E-Mail: roland.steidle@waldeck.eu

Jan Steffan

ist wissenschaftlicher Mitarbeiter am Fraunhofer Institut für Sichere Informationstechnologie (SIT)

E-Mail: jan.steffan@sit.fraunhofer.de

Katja Seitz

ist wissenschaftlicher Mitarbeiter am Fraunhofer Institut für Sichere Informationstechnologie (SIT)

E-Mail: katja.seitz@sit.fraunhofer.de

Dr. Ulrich Pordesch

ist IT-Sicherheitskoordinator an der Fraunhofer Gesellschaft e.V.

E-Mail: ulrich.pordesch@zv.fraunhofer.de

1 Ein neuer Webbrowser

In den vergangenen Jahren hat sich die Nutzung des World Wide Web auf vielfältige Art geändert und auf neue Geschäfts- und Lebensbereiche ausgedehnt. Es gibt einen erkennbaren Trend hin zu webbasierten Anwendungen. Nach eigener Aussage möchte die Firma Google Inc. dieser Entwicklung durch einen von Grund auf neu konzipierten Webbrowser Rechnung tragen. Der seit September 2009 verfügbare neue Browser Google Chrome soll einfacher zu benutzen, schneller, stabiler und sicherer sein als andere verfügbare Browser.

Die für Benutzer augenfälligste Neuerung von Chrome ist die multifunktionale Adressleiste, „Omnibox" genannt. Diese dient nicht nur, wie üblicherweise bei anderen Browsern, dem Aufruf eingegebener Web-Adressen (URLs) nach Betätigen der „Enter-Taste", sondern nimmt auch Suchanfragen an eine Suchmaschine (standardmäßig Google) entgegen und versucht, URLs schon während der Eingabe zu vervollständigen, um Tipparbeit zu sparen.

Weiter bietet Chrome einen so genannten „Inkognito-Modus". In diesem Modus vermeidet es der Browser, potenziell für die Privatsphäre relevante Daten wie persistente Cookies oder den Referer-Header an Webseiten zu übermitteln. Außerdem werden im Inkognito-Modus keine Cookies, Cache-Dateien und Verlaufsprotokolle dauerhaft auf dem Rechner des Nutzers gespeichert, um auch dort Spuren zu vermeiden.

Weitere Innovationen von Google Chrome betreffen dessen Architektur und sind für Benutzer nicht direkt sichtbar. So erfolgt beispielsweise eine weitgehende Trennung von in verschiedenen Seiten oder „Tabs" geladenen Webseiten. Dies soll Abstürze des gesamten Browsers auf Grund von Fehlern in einer einzelnen Seite vermeiden und die Stabilität erhöhen, was insbesondere bei einer künftigen Nutzung webbasierter Anwendungen von Bedeutung ist.

Die Veröffentlichung von Google Chrome erntete viel Aufmerksamkeit durch die Presse, führte aber auch zu Irritationen. Ein Teil der Kritik war darauf zurückzuführen, dass Google Chrome sich noch im Beta-Stadium befand und insbesondere die ersten veröffentlichten Versionen eine Reihe von Sicherheitslücken enthielten. Daneben unterlief Google bei der Formulierung der Nutzungsbedingungen ein Fehler, der Firmen und Institutionen teilweise dazu veranlasste, die Benutzung von Chrome durch Mitarbeiter wegen rechtlicher Bedenken zunächst zu verbieten. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) riet in einer Stellungnahme davon ab, Chrome einzusetzen.[1] Hauptkritikpunkt des BSI war,

* Der Artikel basiert auf einer Studie der Autoren für die Fraunhofer Gesellschaft e.V. Er gibt jedoch nur die persönliche Meinung der Autoren wieder.

1 Kurzmeldung des BSI, http://www.bsi.bund.de/presse/kurzmeldung/090908chrome.htm.

dass Google eine Beta-Version von Chrome mit entsprechenden Sicherheitslücken veröffentlichte, ohne deutlich auf den unfertigen Entwicklungsstand hinzuweisen.

2 Funktionen und ihre Risiken

Zur Beurteilung der geäußerten Kritikpunkte wurde Google Chrome in verschiedenen Nutzungssituationen von den Autoren bei der Fraunhofer Gesellschaft untersucht. Das Augenmerk lag vor allem auf der Datenübermittlung von Google Chrome an durch Google betriebene Web-Server. Die dabei gewonnenen Erkenntnisse werden im Folgenden dargestellt. Die Untersuchungen erfolgten im Dezember 2008 an der finalen Version 1.0.154.36 sowie an Vorabversionen von Google Chrome. Nachfolgend werden nur die wesentlichen Besonderheiten von Chrome gegenüber anderen Browsern erläutert:

2.1 Vorschlagfunktion der Omnibox

Die Vorschlagfunktion der Omnibox dient dazu, die URL, die vom Nutzer in die Adresszeile eingetippt wird, automatisch zu vervollständigen. Dazu wird bei jedem Tastendruck die noch unvollständig eingegebene URL an Google übermittelt. Alle Zeichen, die in die Omnibox eingetippt werden, werden somit an Google gesendet. Die Datenübertragung erfolgt, ohne dass die eingetragene Adresse per Tastatur bestätigt werden muss.

Gelangt man durch einen Link auf eine Seite, die nicht existiert, versucht Chrome auch hier durch Anfrage bei der voreingestellten Suchmaschine (standardmäßig Google) zu helfen. Diese spezielle Funktion „Vorschläge für Navigationsfehler" lässt sich getrennt von der gewöhnlichen Vorschlagfunktion deaktivieren.

Weiterhin werden die übertragenen Daten zumindest teilweise von Google gespeichert und mit anderen Daten kombiniert: Auf Nachfrage äußerte sich ein Google-Sprecher, „*man wolle etwa zwei Prozent der über die Omnibox anfallenden Daten speichern – und zwar in Verknüpfung mit der IP-Adresse des jeweils benutzten Computers. Das heißt konkret: Selbst was ein Nutzer nur eingetippt, aber nicht durch Druck auf die Enter-Taste hinaus ins Web geschickt hat, kann auf den Google-Servern landen.*"[2] Diese Funktion ist aus mehreren Gründen kritisch zu beurteilen:

- Sämtliche in die URL-Zeile händisch oder per cut and paste eingegebenen URLs (auch Parameter und andere Texte) werden an Google übermittelt. Dazu zählen beispielsweise auch Adressen von Servern im Intranet eines Unternehmens und auch Parameter und Texte der URL-Zeile, wie eventuell Personen- oder Dokumentennamen.
- Ist die Vorschlagfunktion für Navigationsfehler aktiviert, so werden URLs sogar dann an Google gesendet, wenn sie nicht händisch eingegeben wurden, also wenn sie etwa über den Link einer anderen Seite aktiviert wurden. Damit würden beispielsweise Links eines schlecht gepflegten Intrawebs häufig an Google bzw. eine andere voreingestellte Suchmaschine im Internet weitergeleitet.
- URLs werden auch dann übermittelt, wenn sie vom Nutzer gar nicht per Tastatur-Bestätigung aufgerufen sondern beispielsweise noch korrigiert werden. Dies widerspricht der gängigen Annahme, dass erst nach dem Drücken der Return-Taste Daten übermittelt werden.
- Die übermittelten Daten bieten potenziell die Grundlage für vielfältige statistische Auswertungen über das Nutzerverhalten, beispielsweise die Dauer der Browsernutzung, die am häufigsten besuchten Web-Seiten und inhaltliche Interessen eines Nutzers.
- Da bei der Übertragung der Anfragen teilweise IP-Adressen gespeichert und insbesondere immer Cookies mit gesendet werden, die von anderen personalisierbaren Google-Diensten wie etwa Google Mail gesetzt wurden, ist eine Zuordnung zu einem bestimmten Nutzer möglich.[3]
- Die Daten werden unverschlüsselt übertragen, so dass auch Angreifer mit Zugriff auf die Kommunikation die gleichen Informationen erhalten wie Google.

2.2 Nutzungsstatistiken und Ausfallberichte

Sofern die Funktion des Sendens von Nutzungsstatistiken und Absturzberichten aktiviert ist, werden Beschreibungen von Programmfehlern zusammen mit einer eindeutigen Identifikationsnummer (User-ID) und der aufgerufenen URL an Google gesendet.

Während der Installation und in den Einstellungen des Browsers ist es möglich, das automatische Senden von Nutzungsstatistiken und Ausfallberichten an Google zu aktivieren. Standardmäßig ist diese Funktion deaktiviert. In den Nutzungsstatistiken soll festgehalten sein, wie intensiv bestimmte Features, wie zum Beispiel die Vorschlagfunktion, genutzt werden.[4] Zu den Ausfallberichten gibt Google lediglich an: „*Ausfallberichte enthalten Informationen aus Dateien, Anwendungen und Diensten, die zum Zeitpunkt eines Problems ausgeführt wurden.*"[5]

Während der Tests gelang es nicht, die Nutzungsstatistiken und Ausfallberichte zu erzeugen und einzusehen. Aus diesem Grund kann keine Aussage darüber gemacht werden, welche Daten und Informationen tatsächlich an Google übertragen werden.

2.3 User-ID

In jeder installierten Kopie von Chrome ist eine eindeutige Identifikationsnummer enthalten, die sogenannte User-ID. In den Anmerkungen zum Datenschutz von Chrome heißt es: „*Ihre Kopie von Google Chrome enthält mindestens eine eindeutige Anwendungsnummer.*"[6] Diese wird bei der Installation und auch bei jeder Update-Anfrage an Google gesendet.

In der Fachpresse wurde die Einführung einer eindeutigen User-ID besonders kritisiert: „*In Verbindung mit einem Google Account und den eingesetzten Cookies erhält Google erstmals einen ‚gläsernen Internet-Surfer'.*"[7] Denn über die User-ID ist eine Zuordnung von Cookies und in die Omnibox eingetippten URLs, die ebenfalls von Google gesammelt werden, zu einem Nutzer möglich. In Kombination mit den Daten aus personalisierten Google-Diensten oder mit Google verbundenen Diensten dritter Anbieter können diese eindeutigen Profile auch einer namentlich identifizier-

2 Spiegel Online, http://www.spiegel.de/netzwelt/tech/0,1518,576186,00,html.

3 Auch wenn ein Nutzer nicht bei einem anderen Google-Dienst registriert ist, ist eine Zuordnung möglich, beispielsweise über Kombinationen aus der IP-Adresse oder der eindeutigen User-ID (s.u.).

4 Zu den Nutzungsstatistiken s. http://www.google.com/support/chrome/bin/answer.py?answer=96817&hl=de.

5 Datenschutz von Google Chrome, http://www.google.com/chrome/intl/de/privacy.html.

6 Nutzungsbedingungen von Google Chrome, http://www.google.com/chrome/eula.html.

7 Computerbild, http://www.computerbild.de/artikel/cb-News-Internet-Google-Chrome-Neuer-Browser-greift-Inter3287940.html.

ten Person zugeordnet werden. Als Schutzmaßnahme kursieren daher im Internet bereits zahlreiche Anleitungen, Tipps und sogar Software zum Entfernen der User-ID aus den Konfigurationsdateien.

Ein weiteres Problem ist, dass *„die Chrome User-ID auch bei einer Deinstallation des Chrome-Browsers im System erhalten bleibt."*[8] Bei einer Neuinstallation von Chrome oder möglicherweise auch von einer anderen Google-Anwendung kann folglich die vorhandene User-ID weiter genutzt werden und ermöglicht so weitere Zuordnungen.

2.4 Cookies

Die von Google gesetzten Cookies enthalten eine zufällige ID, die bei jedem Setzen des Cookies neu generiert wird. Beim Start von Chrome, bei der Verwendung der Vorschlagfunktion und allen anderen Aufrufen von Google, etwa bei den 30-minütigen Hash-Abfragen zum Phishing-Schutz oder Update-Anfragen, werden jeweils sämtliche für die Domain google.com beziehungsweise google.de gesetzten Cookies zusammen mit dem Request an Google gesendet. Dazu gehören auch Cookies, die von anderen Google-Diensten gesetzt wurden (z. B. Google Mail).

Über die bei Update-Anfragen gesendete eindeutige User-IDs könnten diese Cookies einer Browser-Installation zugeordnet werden – leichter noch als etwa über eine (ggf. dynamische) IP-Adresse des Nutzers. Da die User-ID vom Benutzer mit normalen Mitteln nicht entfernt werden kann, könnte Google die Cookies eines Benutzers speichern und über die User-ID auch dann einem Nutzer zuordnen, wenn dieser alle Cookies zum Schutz seiner Privatsphäre regelmäßig löscht und meint, damit seien ihm die Cookie-Informationen nicht mehr zuzuordnen. Durch die Verknüpfung mit Google-Diensten oder verbundenen Diensten Dritter ist zudem eine Zuordnung der User-ID zu persönlichen Daten wie Name und E-Mail-Adresse möglich.

Kritisch ist auch, dass der einmalige Aufruf der Web-Seite www.google.com bei jedem Start von Chrome nicht unterbunden werden kann. Hierdurch kommt es pro Sitzung mindestens zu einem Aufruf und einer Übermittlung der Cookies an Google.

Tabelle 1 |

Wann wird übertragen?	Cookie	User-ID	IP	URL	Deaktivierbar?
Beim Start	Ja	Nein	Ja	Nein	Kann nicht unterbunden werden
Vorschlagfunktion	Ja	Nein	Ja	Ja	Kann deaktiviert werden, oder andere Suchmaschine kann verwendet werden
Vorschlagfunktion bei Navigationsfehlern	Ja	Nein	Ja	Ja	Kann deaktiviert werden, oder andere Suchmaschine kann verwendet werden
Malware-/Phishing-Schutz	Ja	Nein	Ja	Ja, aber nicht ganz	Kann deaktiviert werden.
Update Anfrage	Ja	Ja	Ja	Nein	Kann nicht deaktiviert werden.
Anderer Google-Dienst	Ja	Nein	Ja	Nein	
Nutzungsstatistiken	Ja	Ja	Ja	Ja	Kann deaktiviert werden
Deaktivierbar?	komplett deaktivierbar	mit Aufwand deaktivierbar			

2.5 Malware- und Pishingschutz

Die Safe-Browsing Funktion dient dazu, besuchte Web-Seiten mit einer Liste bekannter Malware- und Phishing-Seiten abzugleichen, um den Nutzer gegebenenfalls vor dem Öffnen der Seite zu warnen. Der Malware- und Phishingschutz ist standardmäßig aktiviert.

Ist der Malware- und Phishingschutz aktiviert, so aktualisiert Chrome alle 30 Minuten eine beim Nutzer lokale gespeicherte Liste mit Hash-Werten gelisteter URLs. Die Listen werden von einem Google-Server bereitgestellt. Es werden jedoch nicht die vollständigen 256 Bit langen Hash-Werte übertragen, sondern jeweils nur die ersten 32 Bit. Falls eine URL geöffnet werden soll, deren Hash-Wert in den ersten 32 Bit mit einem gelisteten Wert übereinstimmt, erfolgt eine erneute Anfrage an Google nach allen 256-Bit aller Hash-Werte, die in den ersten 32 Bit übereinstimmen.[9]

Durch die Verwendung gekürzter Hash-Werte ist kein direkter Rückschluss auf die geöffnete URL möglich. Kritisch ist jedoch, dass bei jeder Anfrage wiederum alle für die Domain google.com gesetzten Cookies des Benutzers übertragen werden.

2.6 DNS Prefetching

Zur Beschleunigung des Seitenaufbaus startet Chrome beim Öffnen einer Web-Seite eine DNS-Abfrage für jeden darin enthaltenen Link. Beim Start von Chrome erfolgen DNS-Anfragen für die zehn am häufigsten besuchten Web-Seiten des Nutzers entsprechend dessen Verlauf-Ordner.[10] Hierdurch kann der Seitenaufbau schneller erfolgen, da die DNS-Namensauflösung schon beim Start durchgeführt wurde.

Diese Funktion lässt sich in der neuen Version 1.0 von Chrome deaktivieren.

2.7 Google als Standardsuchmaschine

Chrome erlaubt es, eine alternative Standardsuchmaschine an Stelle von Google auszuwählen. Bei Nutzung der Suchfunktion werden Cookies dann von der alternativen Suchmaschine gesetzt und an diese gesendet. Dies kann eine Verbesserung bedeuten, falls die andere Suchmaschine datenschutzfreundlichere Nutzungsbedingungen hat.

3 Datenschutzrechtliche Relevanz

Wie Google Daten verarbeitet, wird in den Google Datenschutzbestimmungen erläutert. Diese gliedern sich in einen allgemeinen Teil zu Google[11] sowie einen Teil speziell zu Google Chrome.[12]

Das Datenschutzrecht kennt den allgemeinen Grundsatz, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn eine Rechtsvorschrift dies erlaubt

8 Blog zum Thema Chrome, http://www.planet.vaovaoweb.de/2008/09/12/webworker/firefox-und-chrome-telefonieren-mit-google/.

9 Client specification for the Google Safe Browsing v2.1 protocol, http://code.google.com/p/google-safe-browsing/wiki/Protocolv2Spec.

10 Chromium Developer Documentation, DNS Prefetching, http://dev.chromium.org/developers/design-documents/dns-prefetching.

11 S. http://www.google.com/intl/de/privacy.html.

12 S. http://www.google.com/chrome/intl/de/privacy.html.

oder der Nutzer eingewilligt hat (sog. präventives Verbot mit Erlaubnisvorbehalt). Dieser Grundsatz ist im Bundesdatenschutzgesetz in § 4 Abs. 1 BDSG sowie für den Bereich des Internets im Telemediengesetz in § 12 Abs. 1 TMG festgelegt.

Im Rahmen üblicher Datenverwendungen, insbesondere zum Zweck der Erfüllung gegenseitiger vertraglicher Pflichten, legitimieren beispielsweise die §§ 14 f. TMG die Datenverwendung bei Telemedien und allgemein § 28 BDSG, so dass es keiner expliziten Einwilligung bedarf. Werden dagegen Zwecke verfolgt, die über eine Vertragserfüllung zwischen Vertragspartnern hinausgehen, oder werden personenbezogene Daten von Dritten verwendet, ist eine Datenverarbeitung regelmäßig nur eingeschränkt zulässig und bedarf einer Einwilligung der Betroffenen.

3.1 Verwendung personenbezogener Daten

Personenbezogene Daten sind nach der Legaldefinition in § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Da § 3 Abs.1 BDSG auch auf die Bestimmbarkeit abstellt, wird klargestellt, dass personenbezogene Daten bereits dann vorliegen, wenn die nicht ganz unwahrscheinliche Möglichkeit besteht, den Betroffenen zu bestimmen. Die Frage des Personenbezugs ist damit eine Frage nach der Wahrscheinlichkeit, einen Personenbezug herzustellen. Ausreichend ist es, dass der Personenbezug auch nur unter Zuhilfenahme Dritter oder zusätzlicher Kenntnisse und zusätzlicher Datenerhebungen hergestellt werden kann.[13]

Beispiele für personenbeziehbare Daten können etwa Geburtsdaten oder Kfz-Kennzeichen sein. Bei der Internet-Nutzung können auch Cookies personenbezogen sein, wenn Sie Angaben enthalten, die direkt oder mit Hilfe anderer Daten einer Person zuordenbar sind. Sogar dynamische IP-Adressen werden in der Rechtsprechung bereits als personenbezogen angesehen, allerdings nicht durchgängig.[14]

Sofern daher Google bei der Nutzung von Chrome personenbezogene Daten wie beispielsweise IP-Adressen oder Nutzer-Kennzeichen verwendet, bedarf es einer legitimierenden Rechtsgrundlage. Diese könnte in einer expliziten Einwilligung der Nutzer entsprechend den Anforderungen von § 13 Abs. 2 TMG liegen, welche jedoch weder bei der Installation von Chrome noch bei der späteren Nutzung eingeholt wird.

Die Rechtsgrundlage könnte ferner in einer gesetzlichen Grundlage zu sehen sein, wenn die konkrete Datenverwendung dazu dient, einen Telemediendienst gemäß § 15 Abs. 1 Satz 1 TMG zu erbringen oder sonst der Zweckbestimmung des Lizenzvertrages mit dem Nutzer gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG dient.

3.2 Übermittlung von IP-Adresse und Cookies

Ausweislich der allgemeinen Datenschutzbestimmungen werden von Google Cookies gesetzt, IP-Adressen gespeichert und möglicherweise mit Daten anderer Google Dienste oder Drittanbieter kombiniert. In der Rubrik „Datenschutzüberblick" heißt es unter „Umfang":

- „Google sammelt persönliche Informationen, wenn Sie sich für einen Google-Service anmelden oder anderweitig derartige Informationen freiwillig bereitstellen. Wir kombinieren unter Umständen die von Ihnen eingeholten Informationen mit denen von anderen Google-Services oder Drittanbietern, um die Nutzererfahrung zu optimieren, einschließlich der Anpassung von Inhalten an Ihre Anforderungen.
- Google verwendet Cookies und andere Technologien, um Ihre Onlineerfahrung zu verbessern und um zu erfahren, wie Sie die Google-Services nutzen. So lässt sich die Qualität unserer Services optimieren.
- Mithilfe von Google-Servern werden Informationen automatisch erfasst, wenn Sie unsere Website aufrufen oder unsere Produkte verwenden. Diese Informationen umfassen unter anderem URL, IP-Adresse, Browserart, Sprache sowie das Datum und die Uhrzeit Ihrer Anfrage."

In den speziellen Datenschutzbestimmungen zu Google Chrome heißt es entsprechend unter der Rubrik „Bei der Verwendung von Google Chrome an Google gesendete Informationen":

- „Zum Verwenden und Herunterladen von Google Chrome müssen keine persönlichen Informationen angegeben werden. Falls Sie Google Chrome herunterladen oder zum Herstellen einer Verbindung mit den Servern von Google verwenden, empfängt Google nur standardmäßige Protokollinformationen wie die IP-Adresse Ihres Computers und einige Cookies. Sie können Google Chrome wie hier erläutert so konfigurieren, dass keine Cookies an Google oder andere Websites gesendet werden."

In der Praxis kann weder die Übermittlung von IP-Adressen noch von Cookies ohne gravierende Nutzungseinschränkungen unterbunden werden. Cookies können in Chrome nur global für sämtliche Webseiten deaktiviert werden, was viele Webseiten unbenutzbar macht.

Die Übermittlung der IP-Adresse ist zur Verbindungsherstellung notwendig. Sie könnte zwar durch die Verwendung eines Anonymisierungsdienstes unterbunden werden, was jedoch mit Performance-Einschränkungen verbunden sein kann.

Über die IP-Adressen wie auch über Cookies und die User-ID kann eine Zuordnung zu einem Endgerät bzw. einem Nutzer möglich werden.[15] Diese Möglichkeit ist nicht unwahrscheinlich, sondern

13 Ausführlich Dammann, in: Simitis BDSG, § 3 Rn. 21ff.; Roßnagel, in: Roßnagel Handbuch Datenschutzrecht, Kap. 7.9 Rn. 50 ff.

14 Urteil des Landgerichts Darmstadt vom 25.1.2006, Az.: 25 S 118/05 = MMR 2006, 330 ff; Das Landgericht hat eine Speicherung von IP-Adressen über das Ende des Nutzungsvorgangs hinaus für unzulässig erachtet. Ebenso Urteil des Landgerichts Berlin vom 6.9.2007, Az.: 23 S 3/07. Das Landgericht hat eine Speicherung von IP-Adressen durch das Bundesjustizministerium über das Ende des Nutzungsvorgangs hinaus für unzulässig erachtet. I.Ü. Tätigkeitsbericht des Innenministeriums Baden-Württemberg 2007 nach § 39 Landesdatenschutzgesetz, 97 unter Verweis, dass dies von allen Datenschutzbehörden in Deutschland so gesehen werde; Jahresbericht des Berlinerischen Beauftragten für Datenschutz und Informationsfreiheit 2004, 152; Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" der Artikel-29-Datenschutzgruppe der EU, 19; Büchting, in: Beck'sches Rechtsanwaltshandbuch, 2007, C27 Rn. 81; ohne Differenzierung auch der europäische Datenschutzbeauftragte Peter Hustinx (http://www.edps.europa.eu/EDPSWEB/edps/lang/de/pid/1), etwa in der Computerwoche v. 22.01.2008, http://www.computerwoche.de/1853312. Anders jedoch zuletzt das AG München, Urteil vom 30.9.2008 – 133 C 5677/08, noch nicht rechtskräftig, wobei fraglich ist, ob damit eine Änderung der Rechtsprechung verbunden sein wird.

15 Dies gilt bei statischen IP-Adressen gleichermaßen wie bei Verwendung einer eindeutigen ID und ist bei dynamischen IP-Adressen oftmals möglich, wenn diese mit Daten Dritter kombiniert werden. Lediglich bei Verwendung von Proxy-Servern, hinter denen eine Vielzahl von Endgeräten stehen, ist eine Zuordnung über die IP-Adresse wenig erfolgversprechend.

technisch durchführbar und nach den Datenschutzbestimmungen ausdrücklich vorgesehen.[16] Bei jedem Start von Chrome und bei jeder Nutzung der Vorschlagsfunktion werden alle von Google für die Domain google.com bzw. google.de gesetzten Cookies an Google übertragen. Die Cookies können zusammen mit der eindeutigen User-ID, die Dienste übergreifend verwendet wird, oder über IP-Adressen einer bestimmten Person zugeordnet werden. Dies ist zumindest nicht auszuschließen, wenn Nutzer sich bei anderen Diensten wie beispielsweise Google-Mail angemeldet haben. Es ist daher davon auszugehen, dass die IP-Adressen und Cookies der Nutzer in vielen Fällen personenbeziehbar sind.

Google gibt weiterhin selbst an, diese Daten mit anderen Diensten und auch Drittanbietern – also beispielsweise mit Zugangs-Providern oder Diensten, bei denen sich ein Nutzer angemeldet hat wie etwa im Versandhandel – zu Zwecken zu kombinieren, die über die Diensteerbringung hinausgehen.

Sieht man mit einem Teil der Rechtsprechung und den Aufsichtsbehörden in der IP-Adresse ein personenbezogenes Datum, so bedarf der über die Verbindungsherstellung zum Surfen im Internet hinausgehende Vorgang der Speicherung und weiteren Verwendung von IP-Adressen und Cookies[17] einer Rechtsgrundlage. Da jedoch weder eine Einwilligung des Nutzers eingeholt wird noch die Speicherung und Übermittlung an Google zur Erfüllung des Lizenzvertrags erforderlich ist, fehlt es an einer Rechtsgrundlage. Die Verwendung der IP-Adressen in Kombination mit Cookies zu Zwecken, die nichts mit der Benutzung des Webbrowsers zu tun haben, muss daher ohne Einwilligung des Nutzers als unzulässig betrachtet werden.

3.3 Vorschlagsfunktion, Omnibox, Phishing-Schutz

In den Datenschutzbestimmungen zu Google Chrome heißt es ferner:

- „In die Adressleiste eingegebene URLs oder Suchanfragen werden an Google gesendet, damit von der Vorschlagsfunktion automatisch gesuchte Begriffe oder URLs empfohlen werden können. Falls Sie Nutzerstatistiken an Google senden möchten und Sie eine vorgeschlagene Suchanfrage oder URL akzeptieren, sendet Google Chrome diese Information ebenfalls an Google. Sie können diese Funktion wie hier erläutert deaktivieren.
- Von Ihnen aufgerufene nicht vorhandene URLs werden möglicherweise an Google gesendet, damit wir Ihnen bei der Suche nach der gewünschten URL helfen können. Sie können diese Funktion wie hier erläutert deaktivieren.
- Die Funktion Sicheres Durchsuchen stellt regelmäßig eine Verbindung zu den Servern von Google her, um die aktuellste Liste bekannter Phishing- und Malware-Websites herunterzuladen. Zusätzlich wird, wenn Sie eine Website besuchen, die eine Phishing- oder Malware-Website sein könnte, von Ihrem Browser eine verschlüsselte Kopie eines Teils der URL dieser Website an Google gesendet, so dass wir weitere Informationen über diese potentiell gefährliche URL senden können. Google kann die reale URL, die Sie besuchen, aus diesen Informationen nicht bestimmen. Weitere Informationen erhalten Sie hier."

Indem URLs oder Suchanfragen automatisch an Google übermittelt werden, erfährt Google einiges über die Interessen eines Nutzers. Im Arbeitsumfeld auch insofern, als sich Interessen auf Arbeitsinhalte beziehen. In Kombination mit der IP-Adresse und/oder den Cookies kann damit ein Interessenprofil des Nutzers erstellt werden. Ob Google dies tatsächlich durchführt, wird explizit nicht angegeben, bislang aber auch nicht ausgeschlossen. Die in den Datenschutzbestimmungen angelegte Kombinationsmöglichkeit mit Informationen anderer Google Dienste oder Dritten deutet jedoch darauf hin.

Ohne eine Einwilligung ist das Anlegen personenbeziehbarer Nutzungsprofile entsprechend den vorstehenden Ausführungen nicht zulässig.[18]

3.4 Eindeutige User-ID

Weiterhin wird laut den Datenschutzbestimmungen von Google Chrome eine eindeutige User-ID in der Konfigurationsdatei angelegt, die jedoch, im Gegensatz zu den Cookies, nur bei bestimmten Aktionen regelmäßig an Google übermittelt wird:

- „Ihre Kopie von Google Chrome enthält mindestens eine eindeutige Anwendungsnummer. Diese Nummern und Informationen zur Installation des Browsers (z. B. Versionsnummer, Sprache) werden bei der erstmaligen Installation und Verwendung der Anwendung und bei der automatischen Update-Prüfung von Google Chrome an Google gesendet. Falls Sie Nutzungsstatistiken und Ausfallberichte an Google senden, werden uns diese Informationen sowie eine eindeutige Anwendungsnummer vom Browser übermittelt. […]."

Über die User-ID kann ein Nutzer eindeutig, wenngleich nicht unmittelbar namentlich, identifiziert werden. Mehr noch als über regelmäßig dynamische Vergebene IP-Adressen ist es Google sowie mit Google verbundenen Drittdiensten damit möglich, umfangreiche Nutzerprofile zu einer ID zu erstellen. Da sich die ID nicht ändert und grundsätzlich auch nach der Deinstallation des Browsers gespeichert bleibt, kann mindestens bei jeder Update-Anfrage eine eindeutige Zuordnung von Daten zu einer Installation erfolgen, etwa zu Daten aus der Omnibox, zu Daten aus anderen Google-Diensten oder zu Diensten Dritter.

Dies kann auch durch das Nicht-Akzeptieren bzw. Löschen von Cookies oder die Verwendung eines Anonymisierungsdienstes zur Unterdrückung der IP-Adresse nicht verhindert werden. Indem sich Google eine Kombination mit anderen Informationen auch Google-externer Dienste vorbehält, kann auch nicht ausgeschlossen werden, dass die zu einer User-ID gespeicherten Daten mit personenbezogenen Daten verbunden werden, etwa mit Adressdaten eines Versandhändlers. Insofern kann die User-ID wie auch eine IP-Adresse als personebeziehbares Datum qualifiziert werden, deren Verwendung einer Einwilligung des Nutzers bedürfte.

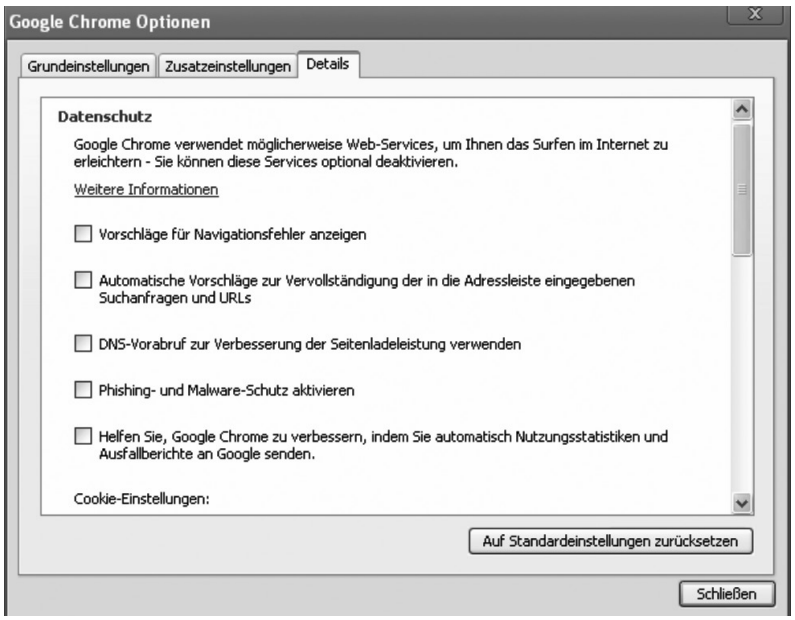
Die Verwendung einer eindeutigen User-ID in Verbindung mit den Cookies stellt damit aus Sicht des Datenschutzrechts eine ebenfalls kritische Funktion von Chrome dar. Im Vergleich zu anderen

16 Auch andere Browser und Webseiten wie etwa Microsoft IE oder Firefox übermitteln IP-Adressen, wobei jedoch nicht klar ist, ob und in welchem Umfang sie von anderen Unternehmen gespeichert und mit weiteren Daten kombiniert werden.

17 Zum Personenbezug bei Cookies s. bspw. bereits Schulz, in : Roßnagel RMD, zu § 1 TDDSG Rn. 38; Tinnefeld, in: Roßnagel Handbuch Datenschutzrecht 2003, Kap. 4.1 Rn. 21, 28.

18 Eine Zulässigkeit folgt auch nicht aus § 15 Abs. 3 TMG, s. dazu bei Google Analytics Pordesch/ Steidle, DuD 2008, 324 ff.

Abbildung 1 |



Browsern wie Microsoft Internet Explorer oder Firefox und in Kombination mit der Omnibox ist sie zudem ein negatives Alleinstellungsmerkmal von Chrome.

4 Vorschläge für eine datenschutzkonforme Verwendung

Einige der vorab untersuchten und kritisch bewerteten Funktionen lassen sich deaktivieren. Aus Sicht des Datenschutzes ist negativ zu bewerten, dass die Default-Einstellungen zunächst die meisten Funktionen aktivieren. Seit der Version 1.0 von Chrome sind jedoch einige Funktionen gebündelt und daher leichter zu deaktivieren. Die User-ID lässt sich allerdings nur über spezielle Tools entfernen, nicht aber über die Chrome Oberfläche.

Kritisch ist vor allem, dass bei der Kommunikation von Chrome mit Google-Servern Cookies mitgesendet werden, die von anderen Google-Diensten gesetzt wurden. Da schon bei der einfachen Verwendung der Google Suchmaschine ein mehrere Jahre gültiges Cookie gesetzt wird, ist so eine Zuordnung der von Chrome übermittelten Informationen möglich. Für Benutzer, die aktiv einen Dienst wie Google-Mail verwenden, kann sogar eine Zuordnung zu Namen, E-Mail Adresse und anderen dort gemachten persönlichen Angaben erfolgen.

In Unternehmen kann die Nutzung von Google Chrome das bereits aus der Suchmaschinennutzung bestehende Risiko, dass Interessen- und damit geschäftsrelevante Daten an Google abfließen, weiter verschärfen. Von jedermann einfach zu verstehende und zu nutzende Konfigurationen, die diese Risiken ausschalten, sind nicht vorhanden. Aus diesem Grunde raten maßgebliche IT-Sicherheitsbeauftragte in der Fraunhofer Gesellschaft Ihren Mitarbeitern und IT-Verantwortlichen derzeit davon ab, Google Chrome regelmäßig als Arbeitsbrowser zu nutzen.

Wenn Google Chrome dennoch verwendet werden soll, sollte der Browser so konfiguriert werden, dass möglichst wenige Daten übermittelt werden. Eine sinnvolle Konfiguration von Chrome wäre danach die folgende:

- Die Nutzungsstatistiken sollten ausgeschaltet werden. Hierzu ist in Chrome auf „Anpassen“ zu klicken (das Schraubenschlüssel-Symbol neben Omnibox), dann ist im Drop-Down-Menü „Optionen“ auszuwählen. Sodann ist im Reiter „Details“ unter der Überschrift „Datenschutz“ (siehe Abbildung) das entsprechende Häkchen bei „Helfen Sie, Google Chrome zu verbessern, indem Sie automatisch Nutzungsstatistiken und Absturzberichte an Google senden“ nicht zu setzen.
- Die Vorschlagfunktion sollte deaktiviert werden. Das Häkchen zur Deaktivierung befindet sich im gleichen Dialog wie die Nutzungsstatistiken. Die Funktionen „Automatische Vorschläge zur Vervollständigung der in die Adressleiste eingegebenen Suchanfragen und URLs“ und „Vorschläge für Navigationsfehler anzeigen“ sollten beide deaktiviert werden.
- Ebenfalls in diesem Dialog lässt sich das DNS-Prefetching (der DNS Vorabruf) ausschalten.
- Zusätzlich sollte die eindeutige Identifikationsnummer unterdrückt oder geändert werden. Dazu muss die Konfigurationsdatei geändert werden. Das genaue Vorgehen wird auf der folgenden Internet-Seite beschrieben:
  http://www.golem.de/0809/62216.html
- Nicht deaktiviert werden kann die Update-Funktion und der Aufruf von *www.google.com* mit Übermittlung aller Cookies bei jedem Start von Chrome.
- Wer ganz sicher gehen und die Übermittlung jeglicher Cookies an Google vermeiden will, kann auch den Phishing- und Malwareschutz ausschalten. Das Häkchen zur Deaktivierung befindet sich im gleichen Dialog wie die Nutzungsstatistiken.

Da der Quelltext von Chrome bereitgestellt wurde, war es der Firma SRWare möglich, einen darauf basierenden Browser namens Iron zu entwickeln, der alle Funktionen von Chrome ohne die in Bezug auf Datenschutz kritisierten bietet[19]. Ob Iron eine empfehlenswerte Alternative zu Chrome ist, hängt u. a. davon ab, ob die Firma SRWare in der Lage ist, zukünftig Sicherheitsupdates zuverlässig und zeitnah bereitzustellen.

19 SRWare Iron, http://www.srware.net/software_srware_iron.php