Was ist ein Cookie und welche Gefahr besteht?

(Quelle: pixabay.com/bykst)

Ein Cookie plaudert gerne aus, was Ihnen gefällt. Gleichzeitig gehören sie zum Internet und ermöglichen die komfortable Nutzung vieler Internetseiten. Wir erklären, was Cookies sind. Außerdem erfahren Sie, welcher Nutzen und welche Gefahr von Cookies ausgeht.

Machen Cookies den Verbraucher zum gläsernen Bürger? Im Zusammenhang mit dem Internet denken die wenigsten Nutzer bei dem Begriff Cookies an süße Naschereien. Viele Verbraucher wissen, dass mit Cookies irgendetwas gespeichert wird. Doch was sind Cookies genau und können diese die Privatsphäre des Nutzers gefährden?

Als Cookie werden kleine Textdateien bezeichnet, die über den Webbrowser auf dem Computer des Nutzers gespeichert werden. Die Dateien enthalten Informationen über Ihr Surfverhalten und werden bei einem erneuten Besuch der Webseite wieder ausgelesen. Sie sind dann kein unbeschriebenes Blatt mehr. Die Dateien werden im temporären Speicher des Webbrowsers gespeichert und sind in der Regel zeitlich beschränkt gültig.

Name:	variant.configname_eue
Content:	2014-04-22
Domain:	.1und1.de
Pfad:	/
Senden für:	Jede Verbindungsart
Für Skript zugänglich:	Ja
Erstellt:	Montag, 9. Mai 2016 um 10:11:06
Läuft ab:	Samstag, 27. Mai 2084 um 13:25:13

Diese Informationen enthält ein Cookie beispielsweise.

Cookies werden normalerweise von der Webseite, die Sie gerade besuchen, erstellt und gespeichert. Doch zunehmend gelangen auch Textdateien von Webseiten auf Ihren Computer, die Sie niemals besucht haben. Diese Dateien werden als Drittanbietercookies bezeichnet.

Vorteile und Nachteile von Cookies

Aus dem Internet sind Cookies heute kaum noch wegzudenken. Sie sind dafür verantwortlich, dass Webseiten Sie wieder erkennen, wenn Sie diese ein zweites Mal besuchen. Dieser Umstand trägt zu mehr Komfort bei, wenn Sie sich beispielsweise nicht bei jedem Besuch neu einloggen müssen. Nützlich kann auch sein, wenn der Browser Ihnen auf einer Webseite anzeigt, welche Seiten Sie schon besucht haben und wo Sie weiterlesen können.

Doch es gibt auch Schattenseiten. Im schlimmsten Fall speichern Cookies vertrauliche Daten, was Ihre Privatsphäre gefährden kann. Zudem ist es mit den Textdateien möglich, Sie als Nutzer eindeutig zu identifizieren und zu verfolgen. Sie selbst merken im Normalfall nichts davon. Um Ihnen personalisierte Werbung anzeigen zu können, werden Ihre Interessen und Ihr Surfverhalten gespeichert und verfolgt sowie ein Profil angelegt. Besonders unüberschaubar wird das in Zusammenhang mit den Drittanbietercookies. Sie kennen das vom Online-Marketing, wenn Ihnen plötzlich überall Produkte oder Reisen angeboten werden, nach denen Sie tatsächlich im Internet gesucht haben.

Was in Cookies gespeichert wird

Letztlich setzt nur die Kreativität der Cookie-Programmierer Grenzen bei der Speicherung von Informationen als Cookie. Nachfolgend zählen wir einige Daten auf, die in einem Cookie auf Ihrem Rechner abgelegt und von der Webseite jederzeit wieder gelesen werden können:

- Anmeldedaten von Webseiten
- besuchte Webseiten
- eingegeben Suchbegriffe
- Ihr Name, die E-Mail-Adresse, Ihre Anschrift oder Telefonnummer
- aufgerufene Produkte
- abgegebene Bewertungen
- Ihre IP-Adresse
- und vieles mehr

Wichtig ist, dass nur die Informationen gespeichert werden können, die Sie vorher übermittelt haben. Die besuchte Webseite kann also beispielsweise Ihre Telefonnummer nicht allein ermitteln, sondern diese nur abspeichern, nachdem Sie diese beispielsweise in ein Formular eingegeben haben.

Drittanbietercookies sind in Bezug auf Ihre Privatsphäre besonders gefährlich, da diese Sie von Webseite zu Webseite verfolgen können. Auf diese Weise können die Dateien immer weiter mit Informationen angereichert werden.

Cookies und der Datenschutz

In Bezug auf den Datenschutz sind Cookies nicht nur umstritten, sondern unserer Meinung nach auch sehr kritisch einzuschätzen. Je nach Browsereinstellung werden Sie zwar auf das Setzen des Cookies und damit der Speicherung der Daten hingewiesen, wissen jedoch nicht, was genau in welchem Umfang gesichert wird. Ebenfalls kritikwürdig ist, dass Sie nicht wissen und kontrollieren können, wer auf diese Daten zugreifen kann.

Eine Richtlinie der Europäischen Gemeinschaft (2009/136/EG) hat bereits im Jahre 2009 festgelegt, dass Verbraucher in verständlicher Form informiert werden müssen, wenn auf dem Computer des Verbrauchers Daten gespeichert oder abgerufen werden.

> *„[...] Es ist denkbar, dass Dritte aus einer Reihe von Gründen Informationen auf der Endeinrichtung eines Nutzers speichern oder auf bereits gespeicherte Informationen zugreifen wollen, die von legitimen Gründen (wie manchen Arten von Cookies) bis hin zum unberechtigten Eindringen in die Privatsphäre (z. B. über Spähsoftware oder Viren) reichen. Daher ist es von größter Wichtigkeit, dass den Nutzern eine klare und verständliche Information bereitgestellt wird, wenn sie irgendeine Tätigkeit ausführen, die zu einer solchen Speicherung oder einem solchen Zugriff führen könnte. Die Methoden der Information und die Einräumung des Rechts, diese abzulehnen, sollten so benutzerfreundlich wie möglich gestaltet werden. [...]“*
>
> *Auszug aus der Richtlinie 2009/136/EG des europäischen Parlaments und des Rates*

In Deutschland wurde die Richtlinie der EU noch nicht umgesetzt. Die Bundesregierung sieht aktuell keinen Handlungsbedarf, da sie die Vorgaben des Telemediengesetzes für ausreichend hält. Anderer Meinung sind die Datenschutzbeauftragten des Bundes und der Länder, die Ihre Auffassung im Februar 2015 in einer Umlaufentschließung mitgeteilt haben:

> *„[...] Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann zum Beispiel auf sie zugeschnittene Werbung anzuzeigen. [...] Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Artikel 5 Absatz 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. [...] Die Datenschutzbeauftragten des Bundes und der Länder halten diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. [...]“*
>
> *Auszug aus der Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015*

Aufgrund der unklaren Rechtslage können die Nutzer nur selbst aktiv werden, indem sie die technischen Möglichkeiten der Webbrowser nutzen.

Geht es auch ohne Cookies?

Ja. In den Einstellungen Ihres Browsers legen Sie selbst fest, wie dieser mit Cookies umgehen soll. Normalerweise erfahren Sie nicht, wann eine Webseite einen Cookie auf Ihrer Seite ablegen möchte. In den Einstellungen des Webbrowsers legen Sie fest, dass Sie vor dem Speichern des Cookies gefragt werden möchten. So können Sie den Cookie nicht nur zulassen, sondern auch ablehnen. Drittanbietercookies lassen sich in den meisten Browsern vollständig blockieren. Zudem lassen sich in den Einstellungen des Browsers bereits gespeicherte Cookies löschen. In unserer ausführlichen Anleitung erfahren Sie, wie Sie in Google Chrome, Mozilla Firefox, Safari und Microsoft Edge Cookies verwalten.

In Bezug auf Cookies schützen Sie Ihre Privatsphäre auch durch die Nutzung des privaten Modus. Angelegte Cookies werden gelöscht, wenn Sie den Browser schließen. Wir zeigen Ihnen, wie Sie den privaten Modus in verschiedenen Webbrowsern aktivieren.

Zusammenfassung: Cookies sind Risiko und Chance zugleich

Grundsätzlich besteht durch Cookies tatsächlich die Gefahr, dass Sie mit der Zeit zu einem gläsernen Internetnutzer werden. Doch die kleinen Textdateien sind auch nützlich und sorgen dafür, dass wir Webseiten komfortabel nutzen können. Wenn Sie wert auf Ihre Privatsphäre legen, sollten Sie die Speicherung von Cookies über die Browsereinstellungen steuern. Dann bestimmen Sie selbst, welche Webseite Daten speichern darf.