COOKIES UND WEBSITE-TRACKING: CHANCEN, RISIKEN UND NEBENWIRKUNGEN

Die Geschichte der Cookies ist eine Geschichte voller Missverständnisse. Bis heute gibt es zwei große Meinungsgruppen. Die eine hält Cookies für harmlos, die anderen für gefährlich. Beide haben recht. Wir möchten Ihnen aufzeigen, welche grundsätzlichen Arten es von diesen krümeligen Vertretern gibt und was diese letztendlich bewirken können.

Cookies, englisch für Keks oder Plätzchen, sind kleine Informationshäppchen, die auf einem Internetrechner von einer Website erzeugt werden können. Dabei kann man diese grundsätzlich in zwei Kategorien einordnen: die sog. Sitzungs-Cookies und die gespeicherten Cookies.

Sitzungs-Cookies

Wie der Name schon andeutet, sind diese Cookies nur für die Dauer einer Sitzung gültig und werden nicht gespeichert.

Diese Cookies sind ungefährlich und werden von vielen Websites benutzt, um Informationen über verschiedene Einzelseiten richtig verteilen zu können. Ein klassisches Beispiel dafür ist ein Bestellformular. Hier gibt man einige Daten ein und sendet das Formular ab. Ist ein Feld nicht korrekt ausgefüllt, so wird das ausgefüllte Formular nochmals angezeigt und man kann die Daten korrigieren. Ein Cookie hilft hierbei, die Formulardaten zu behalten.

Dabei kann leicht der Eindruck entstehen, dass die persönlichen Daten in diesem Cookie gespeichert werden. Im Regelfall ist das nicht so. Der Webserver, der hinter der Seite steht, merkt sich die Daten vorübergehend. Die Zuordnung erfolgt nur über eine temporäre Nummer, z.B. eine Session-ID. Damit bekommt man, wenn man eine Internetseite aufruft vom Webserver eine Nummer zugeteilt, beispielsweise 1256328. Diese wird im Sitzungs-Cookie gespeichert. Werden nun Formulardaten übertragen, so ordnet der Webserver diese Daten der vergebenen Nummer zu. Bei erneutem Aufruf des Formulars, kann der Server dann anhand dieser Nummer entscheiden, welche Daten angezeigt werden müssen.

Sitzungs-Cookies sind auch im allgemeinen dafür verantwortlich, dass man z.B. einige Seiten nur nach einer Benutzeranmeldung sehen kann oder das eine persönlich eingestellte Schriftgröße erhalten bleibt.

Natürlich gibt es im Bereich der Website-Programmierung Techniken, die auf Cookies verzichten. Allerdings ist es wesentlich leichter, mit Cookies zu arbeiten. Sitzungs-Cookies spielen beim Website-Tracking keine Rolle.

gespeicherte Cookies

Werden Cookies mit einem Ablaufdatum versehen, so werden diese auf dem lokalen PC gespeichert.

Auch in diesem Fall sind diese nicht generell als gefährlich zu betrachten. Gespeicherte Cookies enthalten z.B. Informationen über den Zeitpunkt des letzten Besuchs auf einer Seite oder auch den Namen, damit eine personalisierte Begrüßung möglich ist. Auf Shopseiten wird im allgemeinen auch gespeichert, für welche Produkte man sich interessiert hat. So kann bei erneutem Besuch auf dieser Seite gleich eine entsprechende Empfehlung gegeben werden. Dieses Verhalten kennt man vor allem von den großen Seiten wie Amazon.

Aber auch gespeicherte Cookies können wiederum in zwei Arten aufgeteilt werden; in Cookies von Erstanbietern und solche von sog. Drittanbietern.
Erstanbieter ist immer die Internetseite, die man aufgerufen hat. Ein Drittanbieter kann heute nahezu immer mit Werbung gleichgesetzt werden.

Noch vor ein paar Jahren war Werbung auf Internetseiten nichts anderes als die einfache Platzierung von ein paar statischen Grafikdateien. Heute verbirgt sich dahinter eine ganze Wissenschaft die mit Millionenumsätzen verbunden ist.
Schaden an Hard- oder Software können die kleinen Kekse nicht verursachen. In diesem Bereich geht es vielmehr um das Sammeln von Informationen, das Erstellen von Benutzerprofilen und das Verkaufen dieser Daten um Werbetreibenden möglichst hohe Umsätze zu ermöglichen.

Profile durch Cookies

Die Definition von Nutzerprofilen ist durchaus mehrschichtig. Ein Online-Shop kann dabei die Vorlieben seiner Kunden analysieren und entsprechende Produktvorschläge machen. Allerdings wäre es für viele Shops auch schön zu wissen, welchen Interessen der Nutzer sonst noch nachgeht.

Dies wird heute durch eingeblendete Werbung realisiert. Die Werbung einer Seite wird zu großen Teilen über externe Dienstleister eingekauft. Diese blenden dann beispielsweise Werbebanner auf der Seite des Shopbetreibers ein. Die Werbung selbst wird dabei vom Server des Werbungsanbieters übertragen. Daher kann dieser Server dann auch Cookies setzen; den Drittanbieter-Cookie.

Viele, vor allem große Verkaufsseiten, kooperieren mit den Werbeanbietern, so dass dieser genauere Kenntnis darüber erhält, was bestimmte Kunden angeschaut oder bestellt haben. Die Personalisierung wird jedoch noch weiter verfolgt, denn der Werbeanbieter schaltet ja bei vielen seiner Kunden auch entsprechende Anzeigen. Das bedeutet, dass der Werbeanbieter weiß, das ein Kunde in einem Shop nach Badmöbeln gesucht hat und vielleicht bei einem Reiseanbieter nach Urlaubszielen in der Karibik. Diese Daten werden gespeichert, wobei in vielen Fällen im Cookie auch nur eine Identifikationsnummer steht.

Besucht dieser Kunde jetzt eine weitere Internetseite, die auch mit Werbung des gleichen Werbeanbieters versorgt wird, so erkennt dieser den Kunden und kann personalisierte Anzeigen schalten, z.B. um günstige Badmöbel zu bewerben. Diese Verzahnung von Internetseiten und die Datenauswertung wird als Website-Tracking bezeichnet: die Verfolgung eines Besuchers oder Kunden auf möglichst vielen Seiten, mit dem Zweck so viele Informationen über einen bestimmten User zu erhalten wie möglich.

Website-Tracking und Möglichkeiten

Die technischen Möglichkeiten gehen mittlerweile weit über den einfachen Einsatz von Cookies hinaus. Nach deutschen Bestimmungen ist z.B. die Weitergabe von Kundendaten nur mit dessen Zustimmung möglich, und der Einsatz von Cookies und Art und Umfang der Speicherung persönlicher Daten gehört in eine entsprechende Datenschutzerklärung auf die Seite. Doch viele Anbieter verstecken diese Erklärungen recht gut, so dass man schon teilweise aufwändig danach suchen muss oder unterliegen, wie viele der großen Shopbetreiber, nicht deutschem Recht.

Website-Tracking im eigentlichen Sinne ist also nur ein Weg der Informationsbeschaffung über potentielle Kunden. Die einzige Gefahr, die davon ausgeht ist die, das der Kunde Werbung erhält, die speziell auf seine Interessen ausgerichtet ist. Datenschützer sehen hier jedoch schon einen Eingriff in die Persönlichkeitsrechte. Immerhin versuchen die Werbeanbieter mit der Personalisierung den Kunden zu manipulieren.

Schon sehr bedenklich wird das Tracking, wenn einzelne Anbieter gezielt Informationen über einzelne Kunden an den Werbeanbieter weitergeben. Beispielsweise Adressdaten oder persönliche Daten wie Geburtstage oder Handynummern, aber auch Nummern von Kreditkarten. Laufen diese Daten dann bei einem Anbieter zentral in eine Datenbank, so ist die Personalisierung nahezu perfekt. Diese Phänomen ist ja bereits von Loyalitätsprogrammen auch außerhalb des Web bekannt, wie z.B. PayBack.

Website-Tracking ist in den letzten Jahren zunehmend ein Thema geworden und mittlerweile werden neue Browser mit Mechanismen ausgestattet, die diese Form der Informationsbeschaffung ausschließen sollten. So gibt es in jedem Browser die Möglichkeit die Cookiebehandlung zu definieren oder gesetzte Cookies nach Schließen des Browser komplett zu löschen. Nachteil einer zu restriktiven Einstellung können dann jedoch Einschränkungen in der Funktionalität einzelner Internetseiten sein.

Um die Zusammenhänge verschiedener Werbeanbieter nachvollziehen zu können, gibt es seit ein paar Wochen das FireFox-Plugin Collusion. Damit lassen sich die Vorgänge von Cookies grafisch darstellen und sind so auch für normale User nachvollziehbar.

Fazit

Cookies sind also nicht per se gefährlich, sondern eher die Intentionen und Ziele der Anbieter, die sich mit Hilfe dieser verwirklichen lassen. Selbst wenn Programmierer neue Browser mit erhöhten Sicherheitsstandards auf den Markt bringen oder viele Regeln innerhalb der Einstellungen realisierbar sind, bleibt letztendlich immer die persönliche Abwägung, wie wichtig einem jedem die persönlichen Daten sind.

Basierend auf den Ergebnissen diverser Umfragen macht sich der Durchschnittsuser nur selten Gedanken über Website-Tracking oder den Missbrauch seiner Daten. Daher darf zu Recht die Frage gestellt werden, ob in Zeiten sozialer Netzwerke wie Facebook das Website-Tracking ein Gefahrenpotential darstellt.