Webbugs – Wanzen im Internet

Michael Sonntag

Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM),
Johannes Kepler Universität Linz,
A-4040 Linz, Altenbergerstr. 69
sonntag@fim.uni-linz.ac.at

Schlagworte: Webbugs, Datenschutz, Cookies, Datenerhebung, Datenübermittlung

Abstract: Webbugs sind eine weit verbreitete Möglichkeit, unbemerkt Daten über Personen beim Besuch von Webseiten oder dem Lesen von E-Mails bzw. Dokumenten zu sammeln. Besondere Bedeutung erhalten sie durch große Probleme, die sich bei ihrer Abwehr stellen. Es wird ein Überblick über Webbugs gegeben, deren Verwendung dargestellt, sowie die Rechtslage in Österreich (bzw der EU) erläutert (Zulässigkeit, Zustimmungsmöglichkeiten).

1. Einleitung

Datenschutz ist ein wichtiges Element für Endbenutzer im Internet. Dem gegenüber steht das legitime Interesse der Wirtschaft, möglichst viel über ihre Besucher/Kunden zu erfahren. Eine der dabei verwendeten Methoden wird hier untersucht: Webbugs[1]. Es handelt sich fast immer um eine „geheime" Methode in dem Sinne, daß Benutzer nicht informiert werden, daß Daten über sie gesammelt werden bzw welche dies sind.

2. Über Webbugs

Klassische[2] Webbugs[3] sind Grafiken auf einer Webseite oder in einem Dokument, die automatisch von externen Quellen geladen werden und zur Verfolgung des Benutzers dienen. Die typische Form ist in HTML co-

---

[1] Electronic Frontier Foundation: *Smith, R. M.:* Web Bug FAQ.
http://www.eff.org/Privacy/Marketing/web_bug.html (25.3.2002),
Haas, F. G./Sosna, A.: Was versteht man unter WebBugs?
htpp://members.surfeu.at/privacy/definitions/webbugs.html (25.3.2002).

[2] Siehe http://www.bugnosis.org/ (19.3.2002) für eine Erläuterung und ein Programm zur Erkennung (aber nicht Abwehr) derselben.

[3] Auch genannt: „Clear GIF", „1-by-1 GIF", „Invisible GIF", „Beacon GIF", „Tracker GIF". Es handelt sich meist um Grafiken im GIF Format (technisch günstig da kleine Dateien); dies ist jedoch keine Voraussetzung.

diert, doch das Prinzip ist universell anwendbar. In der Regel treffen auf Webbugs noch andere Kriterien zu: Sie sind 1x1 Pixel groß (muss nicht sein; auch normal große Werbebanner können derart verwendet werden), durchsichtig, und lesen bzw. setzen Cookies. Als „externe" Quelle ist bei Dokumenten jede Quelle anzusehen, die nicht im Dokument selbst oder sonst lokal ist, zB ein Webserver. Bei Webseiten bezieht sich dies darauf, dass der Webbug von einem dritten Server stammen muss[4]. Der daraus folgende typische Aufbau ist in Abbildung 1 dargestellt.

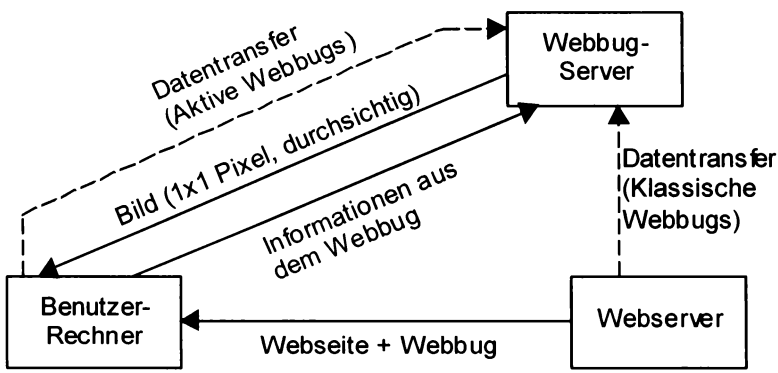

Abbildung 1: *Typische Konfiguration bei Webbugs*

Hiervon zu unterscheiden sind aktive Webbugs, bei welchen zusätzlich noch Java bzw. Javascript Verwendung finden. Es wird der URL, mit dem anschließend das Bild geladen wird, dynamisch auf dem Benutzerrechner zusammengestellt. Dies erlaubt es, sonstige Informationen[5] zu sammeln und an den Webbug-Server weiterzuleiten. Aktive Webbugs sind daher auch dann sinnvoll, wenn sie vom Rechner der Webseite stammen.

Zu beachten ist, dass nicht jedes kleine und unsichtbare Bild ein Webbug sein muss. Um ein bestimmtes Layout zu erreichen, werden derartige Bilder ebenfalls eingesetzt („Spacer GIF"). In diesem Fall stammen sie

---

[4] Webbugs vom selben Server bedeuten in der klassischen Form keine (zusätzliche) Gefahr: Alles was an Daten herausgefunden werden kann, ist bereits beim Abruf der Seite selbst bekannt. Zusätzliche Probleme stellen sich jedoch bei aktiven Webbugs.

[5] ZB: Bildschirmauflösung, Farbtiefe, Betriebssystem, lokales Datum, Browser-Version, Java-Version usw.

vom Server der Webseite und setzen keine Cookies. Eine weitere Verwendungsmöglichkeit ist ein Hinweis für Blinde: Hierbei ist der Alternativ-Text des Bildes klar lesbar und kann mittels eines Links auf eine spezielle (zB frame-lose) Seite führen.

3. Verwendungsmöglichkeiten

Die Verwendungsmöglichkeiten sind vielfältig und werden daher nach Webseiten und E-Mails (sonstige Dokumente[6] werden hier nicht behandelt, sind aber meist ähnlich zur Verwendung bei E-Mail) getrennt.

3.1. Webseiten

Durch die Verwendung von Webbugs können Benutzer über mehrere Server verfolgt werden: Der Webbug wird immer vom selben Server geladen und der Benutzer (bzw sein Rechner) über ein Cookie identifiziert. Dies erlaubt es, Benutzerprofile über einen langen Zeitraum sowie verschiedenste Anbieter zu erstellen. Die Einstellung, Cookies nur an den Rechner zu schicken, von dem sie stammen, ist hier wirkungslos.

Da die meisten Suchmaschinen die Anfrage im URL kodieren (um Bookmarks auf Suchergebnisse zu ermöglichen) und dessen Format bekannt ist, können auch diese ausgewertet werden: Wird direkt vom Suchergebnis auf eine Seite mit Webbug verzweigt, so wird der Such-URL als Referer automatisch mitgeschickt[7].

Wurden auf einem Server persönliche Daten eingegeben (zB die Kundeneigenschaft), so kann ein anderer Server, welcher denselben Webbug-Provider verwendet, diese Daten einer ihm bisher unbekannten Person zuordnen[8] (bzw auch in der Gegenrichtung). Hierzu ist jedoch eine zusätzliche (Webbug-externe) Kommunikation[9] sowohl mit dem Webbug-Server als auch der Datenquelle erforderlich.

---

[6] Etwa MS Word: *Garfikel, S/ Spafford, G.:* Web Security, Privacy & Commerce[2]. Chapter 8. *O'Reilly* 2001 http://www.oreilly.com/catalog/websec2/chapter/ch08.html (25.3.2002).

[7] *Schaar, P.:* Persönlichkeitsprofile im Internet. DuD 25 (2001) 7, 383.

[8] Ist man auf Server A namentlich registriert, so kann Server B über den Webbug (für diesen ist die Person auf beiden Rechnern zB als Benutzer Nr 0815 bekannt) diesen Namen (der direkt von A an ihn geschickt werden muß) einem von seinen (bisher anonymen) Accounts zuordnen und damit die Anonymität aufheben.

[9] *Hillenbrand-Beck, R./Greß, S.:* Datengewinnung im Internet. DuD 25 (2001) 7, 390 f.

Ein direkter Datentransfer vom Webserver zum Webbug-Server ist über den Benutzerrechner möglich (siehe dazu auch unten). Hierbei kann der Server der Webseite beliebige Informationen an den Webbug-Server übermitteln. Ein Transfer in der anderen Richtung (Webbugs-Server → Webserver) ist auf diese Weise jedoch nicht möglich.

3.2. E-Mails

Ein Webbug kann auch in eine HTML-E-Mail eingebaut werden.[10] In diesem Fall erhält der Webbug-Server Informationen, die ihm sonst nicht zugänglich wären. Hierzu zählt insbesondere die Tatsache, dass, und der genaue Zeitpunkt wann, die E-Mail angezeigt wurde.[11] Ist in dem URL des Bildes die E-Mail-Adresse oder sonst ein eindeutiges Kennzeichen inkludiert, so kann genau auf den Empfänger zurückgeschlossen werden.[12] Bei manchen E-Mail-Programmen reicht es hierzu bereits aus, wenn die Mail in der Vorschauansicht angezeigt wird (zB MS Outlook/Outlook Express), ohne dass sie geöffnet wird.[13]

Selbst ohne eine derartige Markierung läßt sich etwa feststellen, wann ein einzelner Empfänger eine E-Mail gelesen hat (da außer dem Sender nur er den URL „kennt"). Wird diese E-Mail weitergeleitet, so erhält man auch die IP-Adressen aller weiteren Empfänger. Dies ist daher zB innerhalb einer Firma sehr gut zur Überwachung geeignet, da von jedem Mitarbeiter bekannt ist, wann er welchen Computer benützt.

Wird zum Laden des Bildes nicht HTTP sondern FTP verwendet, so wird (zumindest bei älteren Browsern) zusätzlich noch die E-Mail Adresse als Passwort für den anonymen Zugang angegeben. Auf diese Weise können sowohl Adressen gesammelt als auch Personen identifiziert werden.

---

[10] Siehe *Magee, M.*: MS accused of ignoring email security. http://www.theinquirer.net/28080103.htm (25.3.2002). Die Möglichkeit des Einbaus von Webbugs kann jedoch eher nicht als „Sicherheitsproblem" bezeichnet werden, sondern ist Konsequenz einer (sonst durchaus nützlichen) Funktion.

[11] *Köhntopp, M./Köhntopp, K.*: Datenspuren im Internet. CR 4/2000, 253.

[12] Wichtig insbesondere für Spam-Versender: Diese E-Mail Adresse ist gültig und wird auch abgefragt, wodurch ihr Wert stark ansteigt. Siehe hierzu sowie zu amerikanischer Rechtsprechung zu Webbugs: *Opsahl, K./Infantino, S.*: Privacy and the Use of Pixel Tags. http://www.perkinscoie.com/resource/ecomm/pixel.htm (25.3.2002).

[13] In Eudora 5.1 etwa kann das laden externen Bilder in E-Mails abgeschaltet werden.

4. Datenerhebung

Werden mittels Webbugs Daten durch den Webbug-Server erhoben, so ist die Zulässigkeit analog der von Cookies zu beurteilen. Zu beachten ist, dass der Betreiber des Webserver zwar selbst keine Daten erhebt (außer durch Logs oder eigene Cookies; diese sind gesondert zu beurteilen), doch dies ohne seine Mitwirkung (=Beitrag) nicht möglich wäre. Erfolgt die Verarbeitung auf dem Webbug-Server nach seinen Vorgaben, so ist er als Auftraggeber zu behandeln, ansonsten nur als dessen Gehilfe (er selbst sieht die Daten nie, daher liegt keine Verarbeitung durch ihn vor).

Erlaubt sind Webbugs sofern kein Personenbezug der Daten besteht.[14] Bei einer statischen IP Adresse oder zusätzlichen Daten (Benutzername, Rechnername, aber auch Cookies[15]) ist jedoch von diesem auszugehen. Ebenso ist von insgesamt geschützten Daten auszugehen (also auch rückwirkend), wenn diese zwar anfangs anonym sind, jedoch später eine Identifizierung des Benutzer erfolgt (zB durch zusätzliche Daten).[16] Weiters wäre die Erhebung/Verwendung erlaubt, wenn kein Geheimhaltungsinteresse besteht. In der Regel wird dieses jedoch anzunehmen sein: Die vorher besuchte Webseite, Verfolgung über mehrere Websites, Eingaben in Suchmaschinen, verwendetes Betriebssystem bzw. Browserversion etc; Ausnahmen sind hier Statistiken, zB die übliche Bildschirmauflösung der Besucher als Richtlinie für das Design von Webseiten. Eine Genehmigung durch den Benutzer kommt nicht in Frage, da es sich um versteckte Elemente handelt und dieser daher überhaupt nichts davon weiß.[17] Dass er eventuell mit deren Existenz rechnen oder sie vermuten muss und trotzdem die Seite besucht, reicht für eine konkludente Zustimmung nicht aus. Siehe dazu auch unten.

---

[14] Dieser muss beim Webbug-Server gegeben sein, da dort die Erhebung stattfindet. Ein Personenbezug beim Webserver wird erst bei Datenverknüpfung relevant, oder falls mittels des Bugs personenbezogene Daten übermittelt werden (siehe nächster Abschnitt). Bloß potentieller Personenbezug (Cookies können nicht sicher anonymisiert werden), wie von *Ihde, R.*: Cookies – Datenschutz als Rahmenbedingung der Internetökonomie, CR 7/2000, 417 für third-party-cookies angenommen, reicht nicht aus.

[15] Eine Identifikation des Benutzers ist bei dynamischen IP-Adressen auch durch Cookies möglich, da diese oftmals für jeden Benutzer gesondert gespeichert werden und daher direkten Personenbezug herstellen.

[16] Dies ist analog zu der Verwendung von Cookies und kann daher von diesen übertragen werden; in Bezug auf diese siehe *Schaar, P.*: Cookies: Unterrichtung und Einwilligung des Nutzers über die Verwendung. DuD 24 (2000) 5, 276.

[17] *Jahnel, D.*: Datenschutz im Internet. ecolex 2001, 88 zur gleichen Lage bei Cookies.

5. Datenübermittlung

Bei der Datenübermittlung werden bereits vorher bekannte Daten (wie auch immer erhoben) vom Webserver über den Benutzer an den Webbug-Server weitergeleitet. Sofern der Webbug-Server nicht als Dienstleister des Webservers tätig wird, liegt daher eine Übermittlung vor.

Es handelt sich hierbei nicht um eine Übermittlung (bzw Bekanntgabe) der Daten vom Benutzer an den Webbug-Server, da dieser in der Regel keine Kenntnis von diesem Vorgang hat. Weiters kann er die Daten nicht beeinflussen und bei Verschlüsselung nicht einmal erkennen, welche Daten enthalten sind. Auch aus der Sicht des Empfängers kann nicht davon ausgegangen werden, dass die Daten direkt vom Benutzer stammen: Die Anforderung eines einzelnen unsichtbaren Bildes anhand eines speziellen URLs ist keine übliche Vorgangsweise. Es lässt sich daher sagen, dass bei dieser Übermittlung der Rechner des Benutzers nur als technische Zwischenstation verwendet wird und daher auf die Zulässigkeit der Übertragung keine Auswirkung hat.

Besonders zu beachten ist hier der Personenbezug. Dieser kann nicht nur schon beim Webserver bestehen, sondern sich auch erst auf dem Webbug-Server ergeben, indem die Daten mit anderen verknüpft werden.

Im Sinne des TKG handelt es sich bei hierbei übertragenen Daten (zumindest teilweise: besuchte Webseite, IP-Adresse des Benutzers usw) um Vermittlungsdaten. Diese unterliegen dem Fernmeldegeheimnis (§ 88 TKG; Tatsache des Webseitenabrufs, genauer Zeitpunkt usw). Sie dürfen gem. § 91 TKG nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Betroffenen[18] übermittelt werden. Obwohl die Daten vom Benutzerrechner aus an den Webbug-Server gesendet werden, liegt hier eine Übermittlung vor, da diese Übertragung vom Webserver ausgeht und dieser den Benutzerrechner lediglich als technisches Übermittlungsgerät verwendet (kein Wissen des Benutzers, keine realistische Verhinderungsmöglichkeit[19], aus Sicht des Webbugs-Servers stammen die Daten inhaltlich vom Webserver).

---

[18] Als Antwort auf ein gesondertes Ersuchen des Betreibers: *Jahnel, D.:* Datenschutz im Internet. ecolex 2001, 85.

[19] „Mangelnde Schutzmöglichkeit": *Buxel, H.:* Die sieben Kernprobleme des Online-Profiling aus Nutzerperspektive. DuD 25 (2001) 10, 582.

6. Zustimmungsvoraussetzungen

Eine konkludente Zustimmung zur Datenerhebung bzw. -übermittlung setzt voraus, dass diese nach Verkehrssitte sowie Gewohnheiten und Gebräuchen eindeutig als solche zu verstehen ist. Zusätzlich ist hier jedoch zu überlegen, ob der Besuch einer Webseite bzw das Verfolgen von Links überhaupt als Erklärung gedeutet werden kann und nicht vielmehr Schweigen vorliegt (Erklärungsbewusstsein). Eine adäquate Verursachung durch den Benutzer liegt aufgrund des Versteckens jedoch nicht vor, insbesondere da im Gegensatz dazu der Webbug-Server genau weiß, dass der Großteil der Benutzer deren Existenz nicht bemerken werden. Es liegt daher in der Regel nicht einmal eine Erklärung vor. Weiß der Benutzer vom Webbug, so wird jedoch ebenfalls eine konkludente Erklärung ausscheiden, da es jedenfalls keine allgemeine Verkehrsauffassung gibt, Daten beim normalen surfen jemand anderem als dem Webserver bekannt zu geben.

Der Einbau einer Zustimmungserklärung in AGB's ist zwar möglich, doch da der „normale" Benutzer keinen Vertrag mit dem Webserver abschließt, sind diese nicht anwendbar. Falls ein Vertrag besteht (zB für die Nutzung besonderer Dienste), so ist eine derartige Zustimmung außer bei sensiblen Daten (ausdrückliche Zustimmung erforderlich; bei Webbugs wohl kaum relevant) möglich. Gleiches gilt für Benützungsbedingungen, welche über einen Link einsehbar sind: Die meisten Benutzer werden diese nicht einmal bemerken.

Dennoch ist es möglich, eine derartige Zustimmung auch ohne Vertrag zu erhalten: Durch Hinweis bei einer Registrierung oder Einblenden eine Vor-Seite (zusätzliche Fenster reichen wohl nicht, da diese sehr oft ohne sie zu lesen geschlossen werden). Es stellt sich jedoch auch hier die Frage, ob ein einfacher Mausklick als Erklärung gewertet werden kann. Ist ein Kästchen anzukreuzen, so wird dies ausreichen; zu entfernende Kreuze oder bloße Links wohl eher nicht[20]. In diesem Fall ist ein Hinweis auf durchgeführte Datensammlung mit Link zu genauen Details ausreichend. Zu beachten ist jedoch, dass diese Seite selbst (und damit die Startseite), frei von Webbugs sein muss, da vor deren Anzeige (und damit Aktivierung dieser Webbugs) keine Zustimmung eingeholt werden kann.

---

[20] Vergleiche hierzu *Stude, P.*: Informationen zum Umgang mit personenbezogenen Daten. http://www.infoquelle.de/Recht/Online_recht/Datenschutz.cfm (25.3.2002); jedoch zum dt Recht mit dessen besonderen Zustimmunerfordernissen. In dieser Hinsicht ist aber wohl eine Übertragung möglich.

Die Privacy Foundation brachte eine Liste von fünf Punkten als Richtlinien für die Verwendung von Webbugs[21] heraus, in denen ua eine sichtbare Darstellung, eine Unterrichtung des Nutzers über Art der Daten, Verwendung und Auftraggeber sowie eine Opt-out-Möglichkeit gefordert wird. Dies alleine wird nicht für eine konkludente Zustimmung ausreichen, sofern es sich nicht um ein standardisiertes und weithin bekanntes Bild handelt, da es ansonsten der Großteil der Benutzer nur als ein weiteres Werbebanner ansehen wird.

7. Zusammenfassung

Zusammenfassend kann gesagt werden, dass Webbugs grundsätzlich verboten sind, sofern sie dazu dienen, personenbezogene Daten zu erheben. Dies wird meistens der Fall sein (Ausnahmen: rein statistische Auswertungen bei denen die personenbezogenen Daten, sofern sie unvermeidbar anfallen, sofort gelöscht werden), da sie regelmäßig mit Cookies verbunden sind. Eine Zustimmung zu deren Verwendung ist zwar möglich, muss jedoch vor dem Einsatz erfolgen. Diese kann auch konkludent erfolgen (außer bei sensiblen Daten), sofern der Webbug-Server als Dienstleister für den Webserver tätig wird (der dann auch die Verantwortung für den Umgang mit den Daten trägt). Ansonsten ist eine schriftliche (dh eigenhändige Unterschrift oder sichere elektronische Signatur) Zustimmung zur Übermittlung erforderlich (TKG).

Gesondert zu untersuchen wären noch besondere Probleme der aktiven Cookies, bei denen der Webserver auf dem Benutzerrechner ein Programm für den Webbug-Server ausführen läßt, um weitere Daten zu sammeln.

---

[21] Privacy Foundation: New Proposal: Make Web Bugs Visible. (25.3.2002) http://www.privacyfoundation.org/privacywatch/report.asp?id=40&action=0.