

Der Browser als Bodyguard für das Web 2.0

Mit der Vielfalt der Angebotspalette nehmen Unübersichtlichkeit, Risiken und Gefahren im Netz zu. Der Browser der Zukunft ist deshalb kein passives Surfbrett mehr, sondern begleitet den Anwender auf allen Wegen im Web und beschützt ihn dabei aktiv.

Die Art und Weise, wie sich Menschen online bewegen und wie ausdauernd und intensiv sie das Internet für ihre Zwecke nutzen, hat sich in den vergangenen Jahren grundlegend verändert. Das reine «Blättern» im Web ist zwar nach wie vor die häufigste Tätigkeit. Aber die Umgebung sieht heute völlig anders aus. Aus einer losen Sammlung vor allem statischer Seiten ist ein komplexes Netzwerk entstanden, das diesen Namen tatsächlich verdient; mit vielfältig und dynamisch verknüpften Sites und Services, über die sowohl einzelne Anwender als auch ganze Gemeinschaften von überall her zugreifen und interaktiv miteinander kommunizieren. So verbrachten im gesamten Monat Juli dieses Jahres Menschen rund um den Globus durchschnittlich 31 Stunden und 46 Minuten auf über 1400 Seiten im Internet (Quelle: Nielsen Online). Dabei «konsumierten» sie



Dieter Mai

«Der Privatsphäre des Einzelnen im Web muss mehr Beachtung geschenkt werden.»

nicht einfach Informationen, sondern machten eifrig Gebrauch von aktuellen, personalisierten Inhalten, von Video, Online-diensten und verschiedensten Formen des sogenannten Social Networking.

Aktiver Schutz im Netz

Das Transportmittel für die Reise durch die schöne neue Welt des Web 2.0 ist – wie schon in den Anfangstagen des globalen Datennetzes – in der Regel der Browser. Es ergibt deshalb Sinn, in Sachen Privatsphäre und Datenschutz genau hier anzusetzen und dabei sehr viel kritischer Mechanismen zur Absicherung des Einzelnen zu konzipieren, als dies bisher der Fall war: Der Browser der Zukunft soll schnell, belastbar und absolut zuverlässig sein. Anders als früher darf er aber nicht mehr einfach passiv als Surfbrett dienen, sondern muss den Anwender quasi wie ein persönlicher Bodyguard auf allen Wegen im Web begleiten und aktiv beschützen. Denn mit der Vielfalt der Angebotspalette nehmen Unübersichtlichkeit, Risiken und Gefahren im Netz zu. Die Einfallstore, durch die Hacker und programmierte Bösewichte versuchen, den privaten PC zu kontrollieren, das Onlineverhalten der Anwender missbräuchlich zu überwachen oder sie dazu bringen, persönliche

Informationen preiszugeben, werden immer zahlreicher und ausgeklügelter.

Aktuelle Forschungsergebnisse untermauern die Notwendigkeit, der Privatsphäre des Einzelnen im Web künftig mehr Beachtung zu schenken: Die Sorgen um Identitätsdiebstahl, die unfreiwillige Publikation von persönlichen Daten und Informationen sowie die Nachvollziehbarkeit der eigenen Bewegungen, etwa auf Rechnern, die von mehreren Personen genutzt werden, wachsen stetig. Und nicht nur die Anwender, auch Verbraucher- und Datenschützer orten dringenden Handlungsbedarf: Menschen sollen jederzeit wissen, was mit den Informationen geschieht, die sie im Web angeben und darauf vertrauen können, dass diese Daten zum gewünschten Zweck und zu ihrem eigenen Nutzen verwendet werden.

«Trustworthy Browsing»

«Trustworthy Computing» ist eine langfristig angelegte Initiative von Microsoft, deren Zielsetzungen mehr Sicherheit, Zuverlässigkeit, Datenschutz und Integrität im Umgang mit Software und Computern sind. In diesem Zusammenhang investiert das Unternehmen in zukunftsweisende Technologien und optimiert die Funktionalität seiner Produkte laufend. Ein Beispiel ist das zweispurige «InPrivate»-Konzept, das zukünftig in den Internet-Browsern das Prinzip des aktiven Schutzes umsetzen soll. Mit der Funktion «InPrivate Browsing» kann der Anwender sicher sein, dass seine Bewegungen im Web von niemandem verfolgt werden, auch nicht im Nachhinein. Denn sie verhindert das Speichern von Verlauf, temporären Dateien oder Cookies. Dies ist zum Beispiel nützlich, wenn mehrere Personen den PC nutzen, etwa im Internetcafé oder als Gast. Mit «InPrivate Blocking» entscheidet der Anwender aktiv, wer mit ihm kommunizieren darf und wer nicht. In der Praxis: Oftmals finden sich auf Webseiten Angebote Dritter – Börsenticker, Wetterinformationen und dergleichen mehr, die den Anwender im Moment nicht interessieren. Alle Drittanbieter profitieren dabei ungefragt von verfügbaren persönlichen Daten wie der TCP/IP-Adresse. InPrivate Blocking erlaubt es hingegen, Inhalte gezielt zu blockieren und den Zugriff auf die eigenen Daten transparent zu regeln. Mit solchen und weiteren Funktionen wie etwa einem Smart-Screen-Filter, der vor Phishing und anderen Angriffen aus dem Web schützt, oder auch interaktiven Bookmarks, Übersetzungsdiensten und intelligenter Suche soll der Browser in Zukunft für den Anwender agieren – eben als Bodyguard, der voraus- und mitdenkt.

Dieter Mai ist Windows Business Group Lead bei Microsoft Schweiz.