

Transfer

Unsere Identität(en) im Internet



*Roland Portmann,
Leiter Kompetenzzentrum Informations- und Softwaresicherheit,
Hochschule Luzern, Technik & Architektur, Luzern
roland.portmann@hslu.ch*

Das Internet wird zunehmend das zentrale Kommunikationsmedium unserer Gesellschaft und verdrängt klassische Kommunikationsinfrastrukturen wie Telefon und Post. Wir kaufen über das Internet ein, wir sind auf Portalen präsent, wir planen und buchen Reisen über das Internet, Vereine organisieren sich in Portalen, und selbst die öffentliche Verwaltung sucht zunehmend mit E-Government die Nähe zum Bürger.

Das Internet wird dadurch immer persönlicher:

- Beim Einkaufen geben wir unseren Namen und unsere Adresse an.
- Bei Suchmaschinen konfigurieren wir die Oberfläche gemäss unseren Präferenzen (iGoogle).
- Bei Portalen treten wir mit einem Pseudonym mit anderen Internetbenutzern in Kontakt.
- Bei Reisen geben wir die Kreditkarteninformationen und unsere Komfortansprüche (z.B. an ein Hotel) preis.

Durch diese Tätigkeiten übergibt der Internetbenutzer den aufgerufenen Webapplikationen Informationen. Diese Webapplikationen haben unterschiedliche Anforderungen an die Vertrauenswürdigkeit der übergebenen Informationen. Bei Anwendungen im Umfeld beispielsweise des E-Governments muss sichergestellt sein, dass der richtige Bürger mit der richtigen Verwaltung kommuniziert. Bei anderen Anwendungen stellt der Betreiber keine besonderen Anforderungen an

die Vertrauenswürdigkeit. So vertrauen heute die meisten Webshops den Angaben des Benutzers, beharren aber auf einer Vorauszahlung. Auf bestimmten Webseiten (z.B. Portalen) ist die Verwendung von Pseudonymen sinnvoll und üblich. Die dem Webseitenbetreiber übergebenen Informationen unterscheiden sich je nach Anwendung. Bei einem Portal für Kinder möchte sich der Betreiber auf das korrekte Alter und Geschlecht seiner Portalbenutzer verlassen können. Die Kinder sollen aber durchaus mit Pseudonymen arbeiten können. Bei Webshops ist normalerweise die Lieferadresse eine wichtige Information, bei einer Auslieferung über das Internet (Software) ist es aber die E-Mail-Adresse.

Aktuelle Probleme

Viele Webseiten erfordern heute eine Anmeldung mit Benutzername und Passwort. Die Benutzer müssen sich demnach vor der erstmaligen Verwendung der Webseite ein Konto (Account) einrichten. Dabei werden die für die Benützung der Webseite erforderlichen Informationen angegeben. Dies kann durchaus praktisch sein, so entfällt beispielsweise eine wiederholte Angabe einer Lieferadresse. Auf vielen Webseiten werden zusätzliche Informationen verlangt, die beispielsweise für Werbezwecke eingesetzt werden.

Jeder regelmässige Internetbenutzer hat heute viele Accounts. Diese Konten entspre-

chen digitalen Identitäten. Die wenigsten Internetbenutzer haben ihre Identitäten im Internet im Griff. Man verwendet den gleichen Benutzernamen (vielfach die E-Mail-Adresse) und das gleiche Passwort auf vielen Webseiten. Vergessene Passwörter und/oder Benutzernamen verursachen hohe Kosten bei den Hotlines der Webseitenbetreiber.

Verschiedene Webseitenbetreiber können zusammenarbeiten und die Informationen ihrer Benutzer zusammenführen, um damit aussagekräftigere Identitätsprofile zu erstellen. Auch kann nicht ausgeschlossen werden, dass Geheimdienste und/oder kriminelle Organisationen Interesse an möglichst detaillierten Identitätsinformationen der Internetbenutzer haben könnten. Schweizerische Datenschutzgesetze sind hier wirkungslos: Das Internet ist weltweit.

Management der Internet-Identitäten

Es stellt sich die Frage, wie Internetbenutzer bei der Verwaltung ihrer Identitäten unterstützt werden könnten. Ein solches Identitätsmanagementsystem müsste den folgenden Anforderungen genügen:

- Der Benutzer kann unterschiedliche Identitäten und Pseudonyme selbst verwalten.
- Der Internetbenutzer hat die Kontrolle darüber, welche Informationen an die Webseite weitergegeben werden.
- Es können Webapplikationen mit unterschiedlichen Ansprü-

chen an die Vertrauenswürdigkeit der Identitäten unterstützt werden.

- Die Vorgänge sind für den Internetbenutzer transparent.
- Das Identitätsmanagementsystem ist sicher.
- Es werden offene Standards verwendet, sodass das Identitätsmanagementsystem plattformübergreifend verwendet werden kann.

Lösungsansätze

Bereits vor einigen Jahren gab es erste Lösungsansätze, die sich aber nicht durchsetzten. So bot beispielsweise Microsoft mit Passport (LiveID) einen Identitätsdienst an, der auch von Nicht-Microsoft-Webseiten verwendet werden konnte. Die Verwaltung der Identitäten erfolgte über einen Dienst von Microsoft. Dieser Dienst erfüllte praktisch keine der oben formulierten Anforderungen. Daher erstaunt es nicht, dass der Erfolg dieser gut gemeinten Initiative ausblieb.

Mit dem Nachfolgerprodukt CardSpace werden die wesentlichen Anforderungen eines Identitätsmanagementsystems für das Internet erfüllt. Dieses Produkt ist Bestandteil der aktuellen Microsoft-Betriebssysteme. Der Internetbenutzer kann mehrere Identitäten verwalten. Die Identitäten (Cards genannt, in Analogie zu Business Cards) können vom Benutzer selbst oder von externen vertrauens-

würdigen Stellen (Identity Provider) ausgegeben werden. Jeder Identität können Attribute (Namen, E-Mail-Adresse, Postanschrift, ...) beigefügt werden. Es werden beliebig viele Identity Provider unterstützt. Ein besonders vertrauenswürdiger Identity Provider wird eine Card nur nach vorgängiger persönlicher Überprüfung mit einem amtlichen Ausweis ausstellen. Für Webshops könnten selbst ausgestellte Cards ausreichend sein. Es können spezielle Identity Provider für Kinder eingerichtet werden, die eine korrekte Altersangabe sicherstellen.

Im OpenSource-Umfeld wurden vergleichbare Technologien (Information Card, OpenID) entwickelt. Der neu gegründete Verbund «Information Card Foundation» (ICF) hat die Vereinheitlichung der Verfahren und Protokolle zum Ziel. Unter dem Namen Geneva stellt Microsoft eine Betaversion der Weiterentwicklung von Card Space zur Verfügung. Dieses Identitätsmanagementsystem strebt eine Kompatibilität mit anderen Initiativen wie beispielsweise Higgins (IBM, CA, ...) an.

Die Benutzersicht

Für den Internetbenutzer gestaltet sich der Umgang mit den Identitäten sehr einfach. Erscheint auf einer Webseite bei einer Anmeldemaske das abgebildete Symbol, werden

ihm mit einem Klick auf dieses Symbol seine zur Verfügung stehenden Identitäten angezeigt. Er kann auswählen, welche Identität und welche Informationen er dem Betreiber der Webseite übermitteln will.

Zusammenfassung

Mit Identitätsmanagementsystemen können viele bestehende Probleme, insbesondere Datenschutzprobleme, entschärft werden. Der Internetbenutzer muss lernen, bewusst mit seinen digitalen Identitäten umzugehen. Dies dürfte das grösste Problem sein, denn die Notwendigkeit, sich mit verschiedenen Identitäten im Internet zu bewegen und die preisgegebenen Informationen unter Kontrolle zu halten, ist selbst IT-Fachleuten nicht einfach zu erklären.

Für den seriösen Webseitenbetreiber hätte die Einführung eines Identitätsmanagementsystems Vorteile. Die Webapplikation könnte einfacher gestaltet werden. Die Probleme mit veralteten Daten wären gelöst.

Die Hochschule Luzern wird sich in diesem Jahr intensiv mit Identitätsmanagementsystemen befassen. Damit wird sichergestellt, dass die zukünftigen Absolventen mit diesen Technologien vertraut sind. Mit mehreren Initiativen wird zudem versucht, die Anwendungen dieser Technologien in der Schweiz zu fördern. ■

Literatur, weiterführende Links

- Informationen zu Geneva: <<http://msdn.microsoft.com/en-us/security/aa570351.aspx>>
- Informationen zu Higgins: <<http://www.eclipse.org/higgins>>