

# Starke Login für ein sicheres Online-Leben

Wir kennen es alle: Die Logins und Passwörter für Facebook, Google, Yahoo, Xing & Co. stapeln sich.

Auf der anderen Seite wollen unsere digitalen Identitäten gut geschützt sein.

Wie kann man als Businessbenutzer bequem und sicher mit verschiedenen Logins umgehen?



Niall Sweeney ist Solution und Software Architekt bei ELCA mit den Schwerpunkten IAM und Applikationssicherheit in Internetapplikationen.

Die meisten Menschen leben im Privaten wie im Beruf mit mehreren Identitäten. Gemeint sind hier nicht Persönlichkeitsmerkmale, sondern Identifikationen. Während unsere Identität in der realen Welt per Pass oder Identitätskarte einfach nachzuweisen ist, sind unsere digitalen Identitäten, mit denen wir uns etwa im Web ein- und ausloggen, weit weniger gut definiert. Das wird zunehmend zum Problem, auch weil die Anzahl unserer digitalen Identitäten steigt. Hatte man früher gerade mal ein Webmail-Konto, sind wir heute registrierte User von Google, Facebook, YouTube oder Amazon sowie Dutzenden von weiteren Online-Shops und Informationsportalen. Nicht nur Heimbenutzer, sondern auch Businessbenutzer verwenden und vernetzen sich über zahlreiche Plattformen wie LinkedIn, Xing, Plaxo oder SlideShare und unterhalten dort verschiedene digitale Identitäten.

Auf fast allen Websites müssen wir unsere Identität durch einen Benutzernamen und ein Passwort nachweisen. Da wir oft mit Millionen von anderen Usern auf der gleichen Site registriert sind, können wir nicht immer den gewünschten Benutzernamen für uns beanspruchen. So generieren wir über die Zeit mehrere Benutzernamen und verschiedene Passwörter. Alle diese Login-Daten müssen erinnert oder auf sicheren Listen gespeichert werden. Deshalb vereinfachen wir unser Online-Leben meist durch die Benutzung desselben Passworts. Doch dies birgt ein vielfach unterschätztes Gefahrenpotenzial: Sollte ein Hacker oder ein Krimineller auf einer Website Zugriff auf unsere Daten bekommen, stehen ihm somit Tür und Tor offen zu unseren vielen anderen Webaccounts. Man hört oft von solchen Datendiebstählen. Dennoch halten es Viele für unwahr-

scheinlich, dass ausgerechnet ihre eigenen Daten gestohlen werden könnten.

---

**«Bekommt ein Hacker auf einer Website Zugriff auf unsere Daten, stehen ihm Tür und Tor zu unseren anderen Webaccounts offen»**

---

Leider kommen solche Angriffe immer häufiger vor und werden immer erfolgreicher, wie die folgenden zwei Beispiele zeigen. So haben Anfang Juli 2011 Hacker den Twitter-Account des US-amerikanischen Nachrichtensenders Fox News in Beschlag genommen. Sie twitterten im Namen von Fox News, dass der amerikanische Präsident Barack Obama einem Attentat zum Opfer gefallen und tot sei. Bereits Anfang 2011 wurde das Playstation Network von Sony angegriffen, und die Daten von Millionen von Benutzern, teilweise inklusive Kreditkartennummern, wurden gestohlen. Erfolgreiche Angriffe bedeuten nicht nur Probleme für die Betreiber der Websites – das Playstation Network war für ein paar Wochen offline –, sondern auch für die Benutzer, deren Daten auf dem Schwarzmarkt angepriesen werden. Kriminelle, die in den Besitz dieser gestohlenen Identitäts- und Kreditkartendaten kommen, gelangen auch leicht an fremdes Geld. Die Opfer wissen meist nicht, dass ihre Daten gestohlen wurden und missbraucht werden, bis sie merken, dass ihr Bankkonto geplündert wurde. Es gibt verschiedene Methoden, einen



bequemeren Umgang mit so vielen digitalen Identitäten zu finden. Software zur Verwaltung von Logins ist eine Möglichkeit. Eine noch bequemere Variante bietet OpenID. OpenID ist ein Identity Provider, vergleichbar mit einer Behörde, die in der realen Welt die Identitätskarten und Pässe ausstellt, nur ist OpenID rein virtuell und nicht amtlich. Die von OpenID ausgestellte Identität ist ein Login, das auf vielen Seiten (z. B. Google, Yahoo, MySpace, etc.) verwendet werden kann, sofern diese OpenID unterstützen. Das heisst, bei diesen Seiten muss man nicht mehr von Grund auf seinen Identitätsnachweis mit spezifischem Benutzernamen und Passwort neu erbringen. Die von OpenID ausgestellte Identität ist glaubhaft genug. OpenID macht sich dabei die SingleSign-on-Funktionalität (SSO) zu Nutze. Single Sign-on heisst nur einmal einloggen – sobald der Benutzer mittels seiner OpenID in eine Website eingeloggt ist, kann er andere Websites, die OpenID unterstützen, im Browser öffnen und wird automatisch eingeloggt. In der Online-Welt lebt es sich dadurch etwas bequemer.

OpenID ist jedoch nicht nur Convenience. Vielmehr kann damit auch die Sicherheit des Logins verbessert werden. Zum einen hat ein Benutzer nur noch ein Login und kann ein komplexeres und deshalb weniger vorhersehbares Passwort benutzen. Zum anderen sind Benutzername und Passwort nicht bei den individuellen Webseiten hinterlegt, so dass selbst bei einem Angriff auf die entsprechende Webseite die Logindaten nicht gestohlen werden können.

Einziger Pferdefuss: Für einen Datendiebstahl lohnt sich ein Angriff auf OpenID umso mehr. Sollte jetzt ein Angreifer der OpenID-Logindaten einer Person habhaft werden, hat er Zugriff auf deren Daten auf

allen von ihr besuchten Websites, welche OpenID unterstützen. Die Konsequenzen eines erfolgreichen Angriffes können viel gravierender sein, als wenn der Benutzer mehrere Benutzerkonten hätte.

Um Benutzer und deren Transaktionen auf Websites besser zu schützen, verwenden viele kritische Websites wie etwa Online Banking Sites mehr als nur Benutzername und Passwort zur Authentifizierung des Benutzers. Hier wird zusätzlich überprüft, ob der Benutzer auch im Besitz eines bei der ersten Registrierung übergebenen Gegenstandes ist. Beispiele sind Streichlisten, kleine Kartenleser in der Form eines Taschenrechners, USB-Sticks, Tokens (eine Art elektronischer Schlüssel) oder auch Mobiltelefone, welche via SMS den benötigten Eingabecode liefern können.

Werden nun zusätzlich solche Authentifizierungsmassnahmen eingesetzt, kann die Sicherheit von OpenID massgeblich erhöht werden, da der Angreifer nicht nur ein statisches Passwort abfangen muss, sondern weitere Faktoren zu überwinden hat.

Die oben aufgeführten Beispiele (Streichlisten, Tokens, SMS, etc.) sind weitverbreitete Authentifizierungslösungen mit ihren Vor- und Nachteilen, die es für jeden spezifischen Gebrauch genau abzuwägen gilt. Eine neuere Lösung ist ELCARDm, eine Authentifizierungslösung, die speziell für Smartphones mit Touchscreen entwickelt wurde. Der Benutzer verwendet eine „App“, welche mit benutzerspezifischen Daten initialisiert wird. Diese Software verwandelt das Smartphone in ein Gerät zur Erzeugung von „Einmalpasswörtern“. Das Einmalpasswort wird nach der Eingabe einer „Signatur“ – vergleichbar mit einer Unterschrift –, die der Benutzer selbst wählt, erzeugt. Nach der Eingabe

des Benutzernamens und Passworts auf einer Website wird der Benutzer über das Handy aufgefordert, seine Unterschrift, also seine Signatur auf dem Touchscreen einzugeben. Die korrekte eingegebene Unterschrift auf dem Smartphone authentifiziert den Benutzer schliesslich bei der Website. Der Benutzer kann sich somit bequem und vor allem sorgloser in der digitalen Welt bewegen.

---

### «Der Benutzer sollte sich sorgloser und dennoch bequem in der digitalen Welt bewegen können»

---

Ein potenzieller Angreifer müsste also über Benutzernamen und Passwort verfügen, zudem das Benutzerhandy besitzen sowie die Signatur kennen. Letzteres ist jedoch weder auf dem Smartphone noch bei einem Provider gespeichert, es existiert einzig im Gedächtnis des Benutzers und ist somit schwer zu ergattern. Allerdings bleiben auch trotz den sichersten Verfahren zur Authentifikation Restrisiken, die schwer zu vermeiden sind, da selbst mit einer sicheren Authentifizierung kleinste Lücken in der Implementation von Webseiten durch kriminelle Hacker aufgefundnen und ausgenutzt werden können.