Social ID – der einfachste Weg zum Kunden

Dipl.-Ing. oec. Sebastian Rohr

Der große Erfolg der Social Media Netzwerke hat dazu geführt, dass sich viele Unternehmen im Bereich Marketing auch um ihre attraktive Präsentation in eben diesen Netzen bemühen, um Aufmerksamkeit für die eigenen Marken, Produkte und Dienstleistungen oder die eigene Website zu schaffen. Trotz „Tracking Cookies und Co." bleibt es für einen Großteil der Aktivitäten jedoch schwer nachvollziehbar, welche Auswirkungen diese haben und ob wirklich eine nachhaltige Bindung der Nutzer an die eigenen Dienste möglich ist. Insofern suchen Unternehmen nach Möglichkeiten, die den Weg zum Kunden abkürzen und die sogenannte „Conversion Rate" erhöhen. Viele Anwender von Webanwendungen oder mobilen Services haben die Zeichen der Zeit erkannt, und bieten im Registrierungsprozess die Option „Benutze Dein Facebook Konto". Doch mit der Nutzung der Social ID im Registrierungsprozess sind nicht nur Vorteile verbunden. Auch aus Datenschutzgründen lohnt eine Analyse.

Protokolle mit Mehrwert

Benutzerdatenabhängige Web- und Mobile-Anwendungen müssen in irgendeiner Form die Daten des Benutzers erfassen. Der offensichtliche Weg über Formulare stellt den Benutzer vor die Entscheidung: „Entweder du füllst das Formular aus, oder du gehst! [*Login Wall*]"

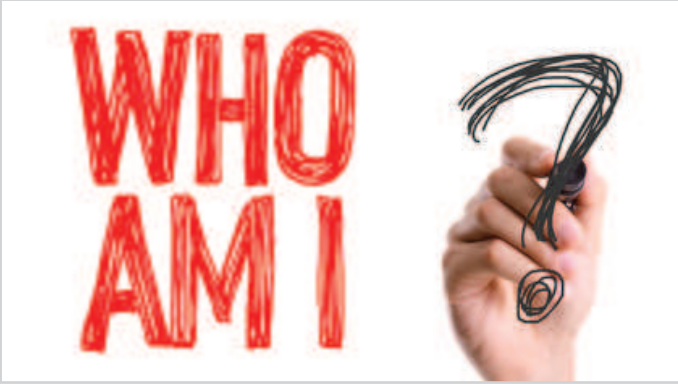
Dadurch verliert der Betreiber dieser Anwendung jene potenziellen Benutzer, welche sich für Letzteres entscheiden [*] – nämlich zu gehen. Eine verbreitete Alternative zum manuellen Erfassen der Daten ist die Integration in vorhandene Systeme, in die der Benutzer bereits sein Profil eingepflegt hat. Soziale Netzwerke bieten sich für diese Aufgabe wunderbar an. Mithilfe von OAuth2.0 oder auf OAuth2.0 aufbauenden Protokollen wie OpenID Connect, können Web- und Mobile-Anwendungen ihren Benutzern anbieten, sich über Facebook, Google+, Twitter oder andere Identitätsprovider anzumelden. Identitätsprovider müssen dabei nicht zwingend soziale Netzwerke sein – allerdings liegt deren Integration besonders nahe, da sie sehr verbreitet sind und somit eine große Menge an potenziellen Nutzern abdecken.

Benutzerdaten zu erfassen ist grundsätzlich ein Prozess, der für den Benutzer Mehraufwand bedeuten kann. Folglich steht die Frage im Raum, wie sich dieser Aufwand minimieren lässt ohne Passwörter zu teilen. Auch in diesem Kontext sind die Protokolle OAuth2.0 oder OpenID Connect hilfreich, da sie weitaus nützlicher und flexibler sind, als gemeinhin vermutet wird. Anwendungen oder auch „Apps" mit einem Social Login Flow zu versehen, ist nämlich nur eines der möglichen Einsatzgebiete von OAuth2.0. Das Protokoll wurde vielmehr entwickelt, um für dritte Anwendungen den Zugriff auf Ressourcen zu autorisieren – und gleichzeitig das Passwort als

geheime Information zwischen dem Identitätsprovider und dem Benutzer zu wahren. Auf diese Weise kann der Identitätsprovider seine Nutzer übrigens optimal an sich binden. Insbesondere dem Endanwender bleibt so erspart, sich an einer weiteren Website oder für eine weitere App einen Benutzernamen auszudenken und sich ein Passwort zu erstellen, dass vermutlich in Kürze mühsam durch Passwortrücksetzung neu definiert werden muss, da der Anwender es vergessen hat. Falls das genutzte Social Media Netzwerk zudem über eine Zweifaktor-Authentisierung verfügt (2FA) bzw. diese unterstützt, profitiert der Anbieter des Services gleich zweifach: Erstens muss er sich nicht um die Verwaltung von Nutzernamen und Passworten kümmern (was auch mögliche Haftungsfragen bei einer ungewollten Veröffentlichung dieser personenbezogenen Daten ausschließt) und kann sich voll auf die Erweiterung seines Dienstes kümmern, zweitens nutzt er komplett kostenfrei die 2FA Infrastruktur des Netzwerks und muss sich weniger Sorgen um einen möglichen Missbrauch der Daten durch Dritte machen.

Wanted: Social ID

Die soziale Identität rückt also immer weiter in den Mittelpunkt des digitalen Kosmos: Nahezu jeder Web- oder Mobil-Anwendungsanbieter will sie haben. Doch diese Entwicklung hat ihre Tücken. Denn je größer der Fundus an autorisierten Apps und Services wird, desto zentraler wird die Rolle des Identitätsproviders für den Benutzer. Soziale Netzwerke hingegen haben ein natürliches Interesse daran, den Kampf um die Singularität zu gewinnen.



Als zentrale Drehscheibe für Informationen über ihre eigenen Nutzer haben die sozialen Netzwerke den Mehrwert „angeschlossener“ Seiten schnell erkannt. Die Möglichkeit, sich mit den im sozialen Netzwerk angegeben Details bei anderen Diensten anmelden zu können, ist mit Blick auf den Komfort ein Mehrwert für den Anwender – der Betreiber des Netzwerks erhält im Gegenzug weitere Informationen über die Vorlieben und das Verhalten des Mitglieds bei der Nutzung von Diensten Dritter. Diese Win-Win Situation können sich Dienstanbieter zunutze machen, indem sie wiederum gezielt für die „Verbindung“ des Benutzers mit dem eigenen Dienst in dessen Netzwerk werben bzw. im Gegenzug die Vorlieben und Mitgliedschaften des Benutzers im Sozialen Netz analysieren, um weitere Interessenten gezielter finden und anwerben zu können.

Login-Mauern wiederum würden den Benutzer abschrecken und das Wachstum einer neuen Anwendung schnell ausbremsen. Insofern ist es nur zu verständlich, dass Anwendungsanbieter alles versuchen, um solche Mauern gar nicht erst entstehen zu lassen.

Nutzen sie die Brücke „Social ID“ profitieren sie zudem von weiteren Vorteilen: Immerhin haben sie neben der größeren Benutzerakzeptanz nur einen geringen wenn nicht sogar überhaupt keinen Wartungs- und Administrationsaufwand mit den Benutzerdaten. Diese Reduktion des eigenen Aufwands für die Erstellung und Erhaltung einer eigenen Benutzerdatenbank ist schon ein guter Grund für die Nutzung der Social ID. Überzeugend ist aber noch ein anderer Aspekt: Verzichten Anwendungsanbieter auf das Vorhalten der Benutzerdaten, tragen sie auch nicht die Verantwortung, diese Datenbank mit teilweise sensiblen Personen bezogenen Informationen über die Benutzer vor unerlaubtem Zugriff und Missbrauch zu schützen. Weniger Informationen führen zwangsläufig zu geringeren Kosten bei der Gewährleistung des Datenschutzes und somit geringeren Auflagen bei der Erstellung des eigenen Services. Die so entfallenden Aufwände können in die strategische Verbesserung des eigenen Produktes fließen, anstatt in die Errichtung zusätzlicher Barrieren für den Zugriffsschutz.

Der einzige Nachteil, der offensichtlich auftritt, ist die enge Bindung an die sozialen Netzwerke und deren „ID Service“. Ohne den Zugriff auf das soziale Netzwerk wird die Anmeldung am eigenen Dienst stark erschwert und im Zweifel unmöglich gemacht. Da die sozialen Netze jedoch üblicherweise über eine erheblich bessere Ausfallsicherheit verfügen als man selbst für sinnvolle Beträge erreichen kann, ist selbst dieser Nachteil fast schon ein Vorteil – es sei denn, man überwirft sich mit dem Betreiber des Netzwerks oder möchte aus anderen Gründen die Verbindung lösen.

Die Sache mit den Daten

Die Qualität der Daten ist zunächst einmal abhängig vom Identitätsprovider. Bei sozialen Netzwerken ist es sogar möglich, dass für zwei verschiedene Benutzer ganz unterschiedliche Datenqualitäten und -mengen vorliegen. Hierbei empfiehlt es sich, den kleinsten gemeinsamen Nenner (Benutzer ID) zu nutzen, und bei Bedarf weitere Stammdaten zu erfassen. Die Benutzer ID bringt dabei folgende, wesentliche Eigenschaften mit:

- Sie ist einzigartig innerhalb des Identitätsproviders.
- Sie kann einem Benutzer zugeordnet werden.

Der Identitätsprovider stellt die Authentizität des Benutzers sicher und sorgt für die Integrität der Aussagen, welche der Benutzer über sich selbst getroffen hat. Genau wie bei dem Erfassen über ein Formular, hat der Benutzer die Kontrolle über den Wahrheitsgehalt der Aussagen. Ob diese Aussagen nun dem Dienstbetreiber gegenüber bei der Registrierung gemacht wurden oder im sozialen Netz erhoben wurden, ist dabei nahezu bedeutungslos. Die Wahrscheinlichkeit, relevante und korrekte Daten zu erhalten, ist beim Zugriff auf „gut vernetzte“ Social IDs jedoch deutlich höher, als bei einer direkten Registrierung.

Aus datenschutzrechtlicher Sicht besteht für den Benutzer ebenfalls kein Grund zur Sorge. Vielmehr profitiert auch er von spürbaren Vorteilen, da er beispielsweise keine multiplen Identitäten verwalten muss und folglich Zeit spart. Das ist in der heutigen Zeit ein wichtiges Argument, folglich ist der Single-Sign-On (SSO)- Effekt auch auf dem Siegeszug.

Dabei meldet sich der Benutzer bei seinem Identitätsprovider einmalig an und autorisiert externe Anwendungen für den Zugriff auf eine Auswahl seiner Daten. Nun kann er sich bei den autorisierten externen Anwendungen per Knopfdruck ohne großen Aufwand anmelden. Einfacher geht es kaum – obwohl es sich bei dieser Vorgehensweise zugegebenermaßen um ein unechtes SSO handelt.

Licht und Schatten

Trotz all der Vorteile auf allen Seiten – für den Anbieter, für den Nutzer und für den Identitätsprovider, schlummern in der Nutzung der Social ID auch Risiken. Bei der Frage nach den Sicherheitsrisiken muss allerdings differenziert werden. Dabei wird gemeinhin in drei Sicherheitsziele (CIA) unterteilt, die bei Bedarf erweiterbar sind. Für die Thematik „Social ID“ sind folgende fünf Sicherheitsziele hilfreich:

- Vertraulichkeit (C)
- Integrität (I)
- Authentizität (A)
- Verbindlichkeit
- Verfügbarkeit.

Vertraulichkeit

Zwischen dem Identitätsprovider und der Anwendung werden potenziell sensible Daten ausgetauscht. Der Benutzer liefert einen Zugriffstoken (access Token), die Anwendung wiederum einen symmetrischen Schlüssel (client_secret). Beim Client Secret ist der Name Programm: Er muss nämlich von der Anwendung und dem Identitätsprovider geheim gehalten werden. Der Zugriffstoken ist für einen definierten Zeitraum gültig und wird vom Identitätsprovider nur für einen authentifizierten Benutzer ausgestellt. Der Benutzer übermittelt den Zugriffstoken über einen Kommunikationskanal (meist https) der Anwendung. Um vertrauliche Informationen zu schützen, sollten weitere auszutauschende Informationen dann ebenfalls verschlüsselt übertragen werden – was durch die Nutzung von SSL/TLS und entsprechende Schlüssel ebenfalls leicht gewährleistet werden kann.

Integrität

Die Daten des Benutzers, welche im Identitätsprovider verwaltet werden, sind Aussagen, die der Benutzer über sich selbst getroffen hat oder generierte Informationen. Diese Informationen dürfen

nur über definierte Wege und nur von berechtigten Parteien geändert werden. Gegenüber den externen Anwendungen muss sichergestellt werden, dass diese nicht verändert wurden. Hierfür eignen sich typische Hashverfahren wie HMAC oder SHA256.

Authentizität

Sobald jemand Zugriff auf den Social Network Account des Benutzers erlangt hat, hat er auch Zugriff auf alle autorisierten Apps und angeschlossenen Dienste. Er kann zudem weitere Apps und Dienste autorisieren, oder Daten manipulieren – bis hin zur Ausführung von Transaktionen im Namen des eigentlichen Benutzers. Folglich ist es von hoher Wichtigkeit, dass die ausgewählten Social Networks die Möglichkeit zur Nutzung von 2FA bieten und dies auch propagieren. Es bietet sich ein gelegentlicher Hinweis an die eigenen Nutzer an, dass die Nutzung 2FA bei der Anmeldung an Social Networks sinnvoll ist, um die eigenen Daten zu schützen!

Verbindlichkeit

Kann die Verbindlichkeit der Transaktionen der Benutzer gewährleistet werden? Im Rahmen des Social Logins spielen Authentisierung und Autorisierung zwar eine umfassende Rolle, aber ohne die Verwendung von 2FA ist die Vertrauenswürdigkeit aller Identitäten aus Social Networks eher gering, da zu viele Benutzer zu sorglos mit ihren Benutzerkennungen und Passworten umgehen und nur ein Bruchteil die 2FA Funktionen der Netze wirklich nutzen. Folglich ist für die Verbindlichkeit eine klare Absage zu erteilen – ohne ein Login per validierter Identität, wie sie etwa durch den deutschen Personalausweis mit der eID angeboten wird, sind alle Aktivitäten der Social Media Nutzer als „nicht verbindlich“ zu werten. Bevor finanz-relevante Transaktionen durchgeführt werden, sollte also eine weitergehende Anreicherung des Social Network Datensatzes mit validierbaren Attributen oder eine Prüfung der Identität – etwa per PostIdent – erfolgen.

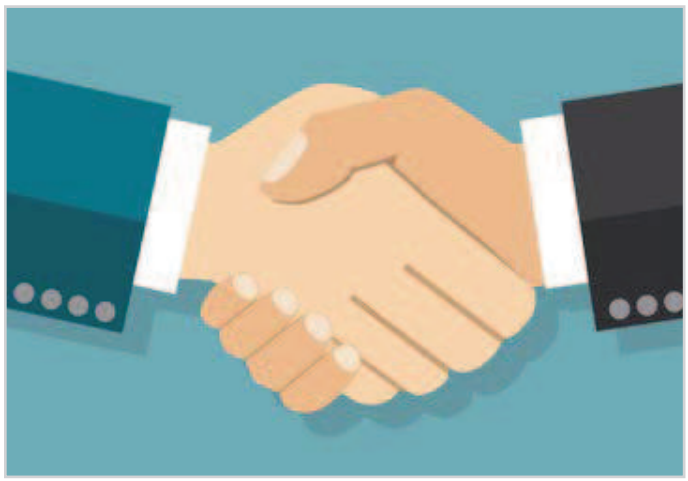
Verfügbarkeit

Das Auslagern von Kernfunktionalitäten wie das Authentifizieren von Benutzern bedeutet auch, dass dem externen Dienst vertraut werden muss, verfügbar zu bleiben. SLAs mit sozialen Netzwerken sind unüblich. Hier muss auf den Selbsterhaltungstrieb der sozialen Netzwerke gebaut werden.

Grundsätzlich ist die mangelnde Kontrolle über die Sicherheitsrichtlinien eines Social ID Providers problematisch und kommt im Grunde einem Kontrollverlust gleich. Darüber hinaus sind „Social Login Buttons“ nicht auf jeder Webseite ansehnlich und können dem Design der Anwendung schaden.

Die zentrale Frage: Vertrauen?

Risiken den Schutzzielen zuzuordnen ist ein wichtiger Schritt. Dennoch bleibt eine entscheidende Frage offen: Wer trägt welches Risiko? Die meisten Risiken werden gegenüber dem Benutzer durch den hohen Komfortfaktor verschleiert. Ob bewusst oder unbewusst, wenn Sicherheit im Design nicht berücksichtigt wurde, dann wird der Benutzer zwar nicht vor eine Login Wall gestellt, aber vor eine tiefgreifende Entscheidung: Kann ich der Anwendung Zugriff auf meine beim Identitätsprovider hinterlegten Daten gewähren? Wie wird denn nun sichergestellt, dass meine Daten so verwendet werden wie angegeben?



Sehr schnell bewegen wir uns hier in rechtlichen Gefilden, die am Ende des Tages auf eine Vertrauensfrage hinsichtlich des Social Networks hinaus laufen: Kann ich der Anwendung und dem Social Network trauen, meine Daten sorgsam zu verarbeiten und vor unerlaubtem Zugriff zu schützen? Da die meisten Benutzer der Netzwerke diese Bedenken bereits mit dem Beitritt zum Netzwerk implizit „über Bord“ geworfen haben, bleibt die Frage als Dienstanbieter: Welche möglichen negativen Konsequenzen kann ein Missbrauch der Benutzerdaten beim Social Network für meinen Dienst haben? Diese Frage muss jeder Dienstanbieter für sich ergründen und dann eine Entscheidung für oder gegen eine Rolle „Relying Party“ für einen oder mehrere „Identity Provider“ aus den Reihen der Social Networks treffen.

Best practice Lösungsansätze

Die Nutzung von OAuth 2.0 und OpenID Connect sowie die Verwendung von SAML2.0-basierten Föderationen sind eine sinnvolle Erweiterung und Bereicherung des World Wide Webs. Die Steigerung der Benutzerfreundlichkeit durch die erleichterte Registrierung, Anmeldung und Nutzung von Diensten Dritter durch deren Anbindung an andere Identity Provider sind Schlüsselfaktoren für das schnelle Wachstum der Nutzeranzahl für neue Services. Bei der Verknüpfung von Cloud Diensten mit internen Benutzerkonten zeigen die „klassischen“ Föderationskonzepte auf SAML Basis volle Wirksamkeit, die beim Sprung auf die mobilen Endgeräte durch Nutzung OAuth 2.0 fortgeführt werden können. Die accessec GmbH empfiehlt im Zuge dessen, die interne Nutzung von Diensten und die Bereitstellung von Diensten an Dritte über Application Programming Interfaces (APIs) durch eine entsprechende API Management Infrastruktur zu sichern und diese in das Konzept zur einfachen Integration mit Social ID Providern einzubinden.

Fazit

Social IDs lassen sich optimal nutzen, um die eigene Anwendung auf das Siegertreppchen zu führen. Dennoch sind sie kein Allheilmittel – insbesondere dann nicht, wenn der originäre Datenprovider Sicherheitslücken offen lässt oder technische Probleme sichtbar werden. Fällt der Identitätsprovider nämlich aus, bleibt dem Anwendungsanbieter nichts anderes übrig, als eigene Ressourcen zu schaffen – und die vorgehaltenen Daten sach- und fachgerecht zu sichern. Dass es soweit nicht kommen muss, beweisen zahlreiche aktuelle Beispiele. Die Praxis zeigt nämlich, dass mit Hilfe moderner Lösungen wie etwa der Integration einer API Management Infrastruktur und deren Zusammenspiel mit den Social ID Providern, bestehende Risiken abgefedert werden können.

Autor

Dipl.-Ing. oec.
Sebastian Rohr

2001 erhielt Sebastian Rohr seinen Abschluss als Wirtschaftsingenieur, Fachrichtung Produktionswirtschaft, an der TU Hamburg-Harburg. Über Stationen als Sicherheitsberater bei der Siemens AG von 1998 bis 2002, Forscher für Netzwerksicherheit im Fraunhofer Institut für Sichere Informationstechnik (SIT) von 2002 bis 2004 sowie als Solution Strategist für die Sicherheitslösungen von CA (Computer Associates) von 2004 bis 2006 kam Rohr als Chief Security Advisor zu Microsoft. Nach seiner Tätigkeit bei Microsoft gründete er Ende 2007 mit zwei weiteren Gesellschaftern die accessec GmbH und ist dort als technischer Geschäftsführer maßgeblich am Erfolg des Unternehmens beteiligt.

www.accessec.com
info@accessec.com