ENDLICH PASSWORTFREI?

Neue offene Standards wie OAuth 2.0 und OpenID Connect treten an, um das Management von Benutzeridentitäten und Zugriffsrechten zu revolutionieren. Gewachsen aus den Anforderungen des Web 2.0 versprechen sie, den unzähligen Benutzerkonten und Passwörtern ein Ende zu setzen. Auf ihrem Siegeszug machen sie auch vor der Unternehmens-IT keinen Halt.

→ **VON DR. MARTIN BURKHART**

Die Zeiten sind vorbei, als man sich nur eine PIN für seine Bankkarte merken musste. Egal ob man Facebook benutzt, Kinokarten bestellt, Superpunkte sammelt, oder auch nur einen Kommentar in ein Forum stellen möchte – überall wird ein Passwort gebraucht.

DIE KRUX MIT DEN PASSWÖRTERN

Natürlich sollten die Passwörter möglichst lang und kompliziert sein. Ebenfalls sollte man dasselbe Passwort nicht für verschiedene Konten benutzen. Aufschreiben ist natürlich verboten und wechseln sollte man sie mindestens monatlich, wie uns gerade die Heartbleed-Lücke wieder schmerzlich bewusst gemacht hat. Der durchschnittliche «Homo Interneticus» kann die erforderliche Passwort-Hygiene kaum bei mehr als zwei Passwörtern befolgen, braucht aber mindestens zwei Dutzend davon. Browser und Passwort-Tools eilen dem gestressten Benutzer zur Hilfe und speichern die vielen Passwörter an einem zentralen Ort, was die Sicherheit nicht eben erhöht.

Wir hassen die Passwörter, kommen aber scheinbar nicht los davon. Gleichzeitig vernetzen sich moderne Internetapplikationen immer stärker und integrieren gegenseitig Funktionen. Diese Mischung führt mitunter zu einem giftigen Cocktail bekannt unter dem Namen «Passwort-Anti-Pattern». Was ist damit gemeint? Falls ein Benutzer seine Kontakte beispielsweise bei Google gespeichert hat, kann dies für eine Webplattform zur Verwaltung von Business-Kontakten sehr interessant sein. Eine solche Plattform würde die Kontakte natürlich gerne durchforsten und Personen vorschlagen, die der Benutzer offenbar kennt und die bereits bei dieser Plattform registriert sind. Was liegt also näher, als dem armen Benutzer die mühsame Arbeit abzunehmen? Alles was die Plattform dazu braucht, ist die Email-Adresse und das Passwort für das Google Konto! Die Plattform loggt sich dann anstelle des Benutzers ein und holt sich die relevanten Informationen gleich selbst. Die Bekanntgabe des Passworts kommt allerdings einer generellen Vollmachtserteilung auf dem gesamten Konto gleich. Der Benutzer hat keine Möglichkeiten, die Aktivitäten der Plattform zu kontrollieren, einzuschränken oder nachzuvollziehen.

OAUTH 2.0 UND OPENID CONNECT

Eine Alternative zum «Passwort-Anti-Pattern» bietet OAuth 2.0, ein HTTP-basiertes Framework zur Autorisierung von Zugriffen auf geschützte Ressourcen. Der Benutzer verwaltet dabei selbst, welche Applikationen auf welchen Teil seiner Daten zugreifen dürfen.

OAuth 2.0 definiert verschiedene Entitäten wie Clients, Resource Owners, den Authorization Server, Resource Server und User-Agents. Ein Client ist eine Applikation, die auf eine geschützte Ressource auf dem Resource Server zugreifen möchte. Nehmen wir als Beispiel die Plattform LinkedIn, die auf die geschützte Ressource «Kontaktliste bei Google» lesend zugreifen möchte. Der Benutzer ist der Resource Owner und entscheidet, welche Clients in welchem Ausmass auf seine Ressourcen zugreifen dürfen. Der Authorization Server übernimmt die Authentifizierung der Clients und stellt, basierend auf der Freigabe des Resource Owners, Access Tokens aus, die für den Zugriff auf geschützte Ressourcen berechtigen. Ein Access Token kann vom Client beim Authorization Server bezogen werden und muss beim Zugriff auf die Ressource vorgewiesen werden. Die Tokens können mit kurzer Gültigkeitsdauer versehen werden, damit sie regelmässig beim Authorization Server erneuert werden müssen. Dies erlaubt es dem Resource Owner, erteilte Berechtigungen wieder zu entziehen, beziehungsweise nicht mehr zu erneuern. Der User-Agent schliesslich ist das Programm, über das auf den Authorization Server zugegriffen wird, typischerweise ein Browser oder eine Smartphone-App. Abbildung 1 zeigt den typischen Ablauf einer Autorisierung mittels OAuth 2.0.

OpenID Connect fügt dem OAuth 2.0 Token ein weiteres Token mit standardisierten Informationen zur authentisierten Benutzeridentität hinzu. Das OpenID-Connect-Token ist der digital signierte Beweis dafür, dass sich der Benutzer korrekt authentisiert hat und ist diesbezüglich vergleichbar mit einer SAML-Assertion.

Zum Autor

Dr. Martin Burkhart arbeitet als Airlock Product Manager in der Abteilung «Web Application Security» bei Ergon Informatik AG.

Zum Unternehmen:
Die Softwarefirma Ergon ist führend in der Realisierung von individuellen Softwarelösungen und Anbieterin der beiden Sicherheitslösungen Airlock und Medusa, die Applikationen im Internet schützen und eine starke vorgelagerte Authentisierung ermöglichen. Das Unternehmen mit 200 Mitarbeitenden wurde 1984 gegründet.

Mehr Informationen:
www.ergon.ch

ergon

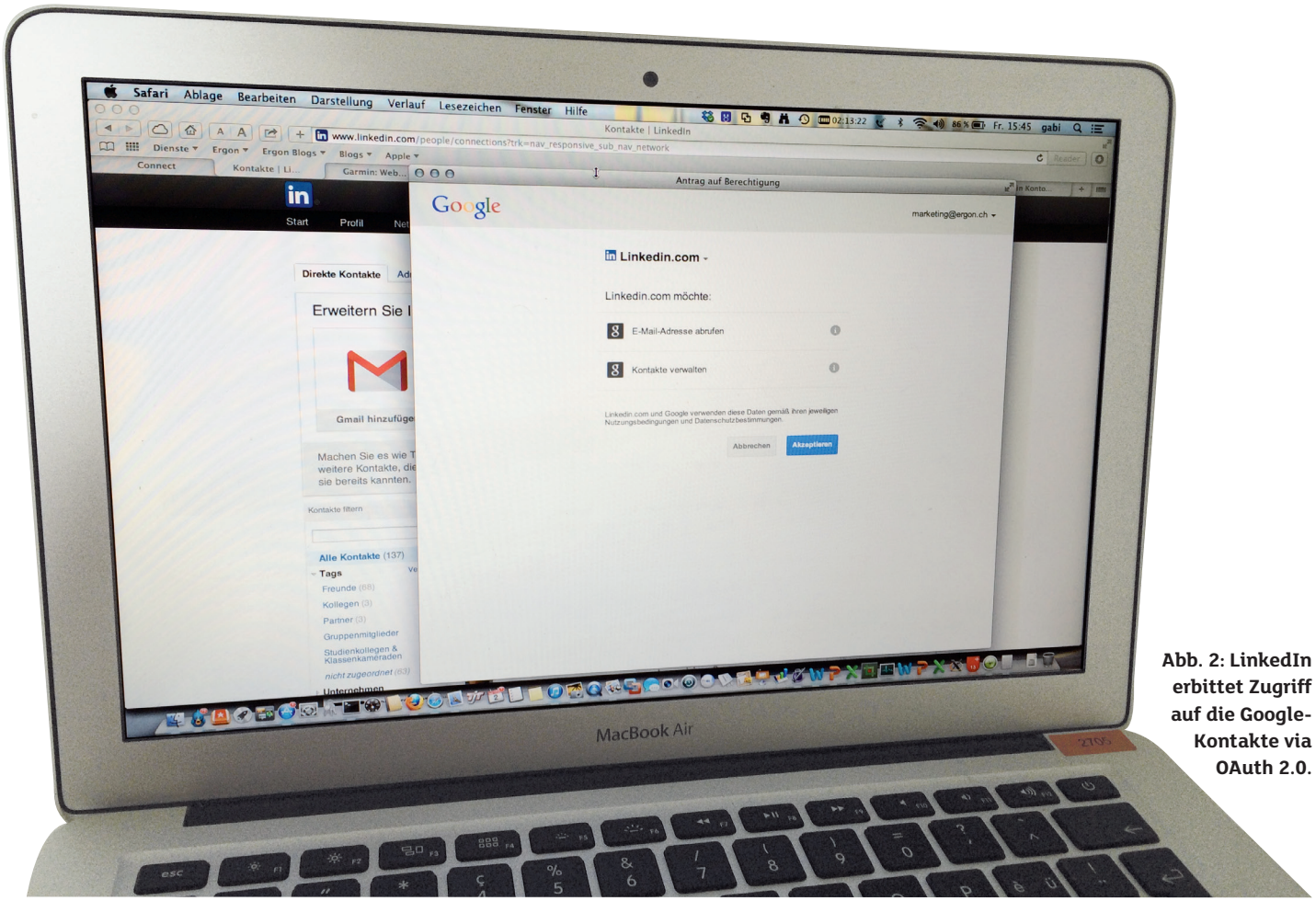

Abb. 2: LinkedIn erbittet Zugriff auf die Google-Kontakte via OAuth 2.0.

BEDEUTUNG FÜR DIE UNTERNEHMENS-IT

Gartner prognostiziert, dass bis Ende 2015 die Hälfte aller neuen Kundenaccounts auf Social-Network-Logins basieren werden. Zusammen mit föderierten Identitäten und Mobile Computing wird dies die klassische IAM-Welt nachhaltig verändern. Das heisst, Unternehmen werden ihre Applikationen vermehrt über «Login via Facebook» zugänglich machen statt dem Benutzer ein weiteres Konto und Passwort aufzuzwingen. Hier bieten sich OAuth 2.0 und OpenID Connect nicht nur für den Login an, sondern auch für die Integration von Social-Networking-Funktionen (z.B. ein «Tweet this»-Button) in eigene Applikationen und Smartphone Apps.

Getrieben durch soziale Netzwerke wird die Revolution an der Schnittstelle zum Endkunden zuerst einsetzen. Ein Fortschreiten in Richtung B2B ist jedoch absehbar. OAuth 2.0 ist HTTP-basiert und daher von Haus aus bestens gerüstet, um RESTful-Webservices zu schützen. Wenn es also um die Autorisierung von Enterprise APIs geht, beispielsweise um Partnern den Zugriff zu ermöglichen, können die neuen Standards ihr Potenzial bestens ausspielen. Auch in Architekturen, die eine Föderation von Benutzeridentitäten und eine Komposition von APIs aus verschiedenen Bereichen vorsehen, sollte man die neuen Standards in Betracht ziehen. Einige Branchen setzen bereits heute erfolgreich auf föderierte Architekturen, wie beispielsweise die Plattform BrokerGate® des Vereins IG B2B (www.igb2b.ch), die Versicherer und Broker vernetzt, oder das Projekt eCH (www.ech.ch), das Standards für E-Governement definiert.

OAuth 2.0 und OpenID Connect werden die Unternehmens-IT an der Schnittstelle zum Kunden und zu Partnern mittelfristig revolutionieren. Inwiefern sie allerdings ins firmeninterne IAM vordringen werden, wo hierarchische LDAP-Strukturen und zentrale Verwaltungen dominieren, wird die Zukunft weisen. ←

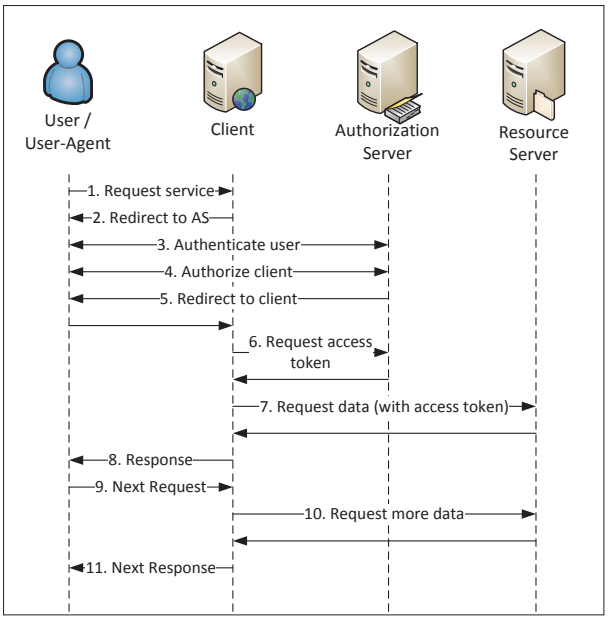

Abb. 1: Authentisierung und Autorisierung mit OAuth 2.0.

Prognose

«By the end of 2015, 50 percent of new retail customer identities will be based on social network identities, up from less than 5 percent today, according to Gartner, Inc. Along with federation technologies and mobile computing, social identity adoption will have a major impact on the practice of identity and access management (IAM) in 2013 and beyond.»

Gartner Press Release: gartner.com/newsroom/id/2326015