

Vereinfachter Zugriff – sicherer Zugriff?

Will ein Unternehmen Kunden und Mitarbeitende einheitlich bedienen, ist ein einfacher Zugriff auf die verschiedenen internen Systeme und Applikationen unabdingbar. Dies zeigt das Beispiel der Generali Versicherungen, die ihre Web-Authentifizierungsplattform für die Brokersysteme komplett ersetzt haben. Auch privat wünschen wir uns einfachere, aber dennoch sichere Lösungen für den Internetzugang. Wird der Single Sign-on auf verschiedenste Portale auch für Privatanutzer Realität?

Generali Versicherungen – sichere Brokersysteme

2012 entschied Generali Schweiz, ihre Sicherheitslösung für Brokersysteme zu ersetzen und auf eine neue Standardlösung zu migrieren. Zu diesem Schritt führten Kostenüberlegungen, die Komplexität der bestehenden Lösung und der hohe Aufwand für Anpassungen an der bestehenden Plattform. Dem Unternehmen war wichtig, eine flexible Lösung zu finden, die Sicherheit bietet sowie die Anbindung komplexer Systeme mit vielen Schnittstellen erlaubt. Auch die Skalierbarkeit für mögliche künftige Anwendungen wie beispielsweise ein Kundenportal musste durch die neue Lösung gegeben sein. Angestrebt wurde eine integrierte Lösung aus einer Hand.

Die Vereinfachung ist gelungen

Das bestehende System basierte auf fünf verschiedenen Produkten von drei unterschiedlichen Herstellern. Generali suchte eine passgenaue Lösung aus einer Hand und entschied sich darum für die Web Application Firewall Airlock in Kombination mit der Authentifizierungsplattform Medusa.

Das Projekt wurde mit einem sportlichen Ziel gestartet: In nur sechs Monaten sollten Airlock und Medusa aufgeschaltet sein. Alle Termine konnten eingehalten werden, das Ziel der Vereinfachung wurde klar erreicht. So kommt die neue Lösung zum Beispiel mit 7 Servern aus, während bisher 24 Server notwendig waren. Die neue Lösung erlaubt auch eine Entflechtung zwischen den Brokerportalen und der Authentifizierungslösung und ermöglicht den Partnern der Generali Versicherungen einen einfachen und sicheren Zugang zu den internen Applikationen.

Ziel war aber nicht nur, die Komplexität zu reduzieren – auch die Usability der Nutzer sollte erhöht und damit die

Kosten gesenkt werden. Zuvor war insbesondere der User-Support ein wichtiger Kostenfaktor. Mit der neuen Lösung liess sich dieser Aufwand deutlich reduzieren. Durch die vereinfachte Bedienung der beiden Portale stieg auch die Akzeptanz bei den Nutzern. Zudem zeigte sich, dass sich mit den Ergon-Produkten über 50 Prozent der laufenden Kosten einsparen lassen.

Glossar

Authentifizierung ist die Verifizierung einer Entität (Person, Gerät, Dokument oder Information), die dabei z.B. durch ihr Passwort und ein Security-Token beweist, dass sie wirklich diese Entität ist.

Autorisierung definiert, welche Entität auf welche Dienste und Systeme zugreifen darf. Oft wird unterschieden zwischen Grobautorisierung (darf eine Entität zugreifen?) und Datenautorisierung (welche Daten darf eine Entität sehen?).

Identity and Access Management umfasst die Identitäts- und Zugangsverwaltung und ermöglicht einer Entität den Zugriff auf definierte Systeme zu definierten Zeitpunkten.

Single Sign-on bedeutet, dass sich ein Benutzer einmalig anmeldet (Authentisierung) und danach direkten Zugriff auf alle Applikationen und Dienste hat, für die er berechtigt (autorisiert) ist.

SAML steht für Security Assertion Markup Language und ist ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen.

OAuth ist ein offenes Protokoll, das eine sichere und standardisierte Autorisierung für Desktop-, Web- und Mobile-Applikationen erlaubt.

SuisseID ist der erste standardisierte elektronische Identitätsnachweis der Schweiz, mit dem sowohl eine rechtsgültige elektronische Signatur wie auch eine sichere Authentifizierung möglich sind.



Sichere Authentifizierung mittels Token

Single Sign-on im Internet?

Welche Bedeutung wird Single Sign-on (SSO) für ein durchschnittliches Schweizer Unternehmen in fünf bis zehn Jahren haben?

SSO für Unternehmen wird von grösster Bedeutung und bis dann auch Realität sein. Es wird sehr wichtig sein, Kunden und Mitarbeitende über alle Medien und Systeme einheitlich zu bedienen. Bei den Mitarbeitenden sind Einfachheit und Effizienz wichtig, im B2B-Bereich sind es schnell nutzbare Leistungen und im B2C-Umfeld einfache und nachvollziehbare Angebote. Wir merken die zunehmende Bedeutung des Themas in unserer täglichen Arbeit deutlich, wegen entsprechender Anfragen unserer Kunden.

Welche Herausforderungen gibt es auf dem Weg dorthin noch zu bewältigen?

Ein Unternehmen muss pro Benutzer eine zentrale Identität erfassen und die Durchgängigkeit über alle Systeme sicherstellen. Technische Standards für die Authentisierung wie SAML und OAuth sind vorhanden und werden

breit eingesetzt. Für die Autorisierung trifft dies aber noch nicht zu. Zudem müssen Rollen und Attribute einfach verwaltbar sein, teilweise auch durch den Benutzer selbst. Das ist alles machbar, aber für Firmen eine komplexe logistische Aufgabe. Sie ist mit einigem Aufwand verbunden, damit der einheitliche Zugang über alle Systemgrenzen und für alle Medien und Kanäle funktioniert.

Gibt es im Internet je ein Single Sign-on für Privatanutzer?

Bis heute hat sich keines der national unterstützten Systeme wie z.B. SuisseID durchgesetzt. Technisch wäre ein SSO machbar: Authentisierungsstandards wie SAML oder OAuth existieren. Die Frage ist vielmehr: Will ich überhaupt, dass über ein Log-in gleichzeitig Twitter und mein E-Banking zugänglich sind? Eine zentrale Identität würde eine extreme Bedeutung bekommen. Soll dies über eine staatliche Instanz koordiniert werden? Eigentlich möchte ich lieber selber definieren, was alles verknüpft ist. Ich gehe davon aus, dass es nie einen einzigen SSO geben wird, sondern nur innerhalb von bestimmten Themen,

z.B. dem SwissPass im öV. Ich erwarte ausserdem eine Gegenbewegung zu den vielen Gratisangeboten wie Whatsapp, wo ich beim Datenschutz Kompromisse machen muss. Die Nutzer dürften bereit sein, etwas für Dienste zu bezahlen, wenn dafür der Datenschutz gewährleistet ist.



Adrian Berger, VP Finance & Security Solutions