# Identity-based Security

oder: Was hat eigentlich Indiana Jones mit digitaler Sicherheit zu tun?

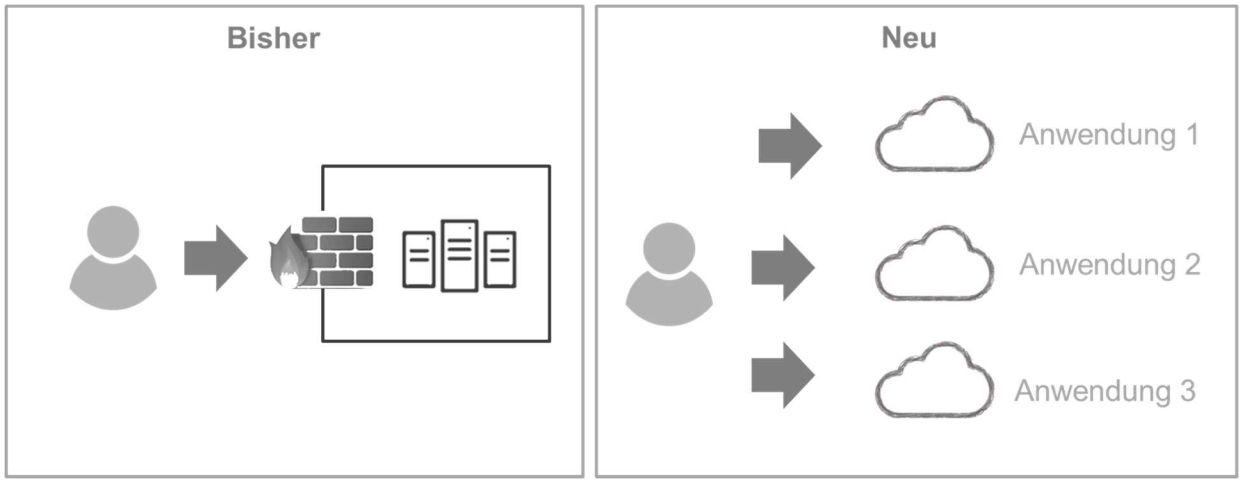
Thema Cloud Security

## Identity based Security

Das Prinzip ist bildlich eigentlich ganz einfach: Indiana Jones braucht keine Sicherheit – Indiana Jones ist die Sicherheit in Person. Es stellt sich lediglich die Frage, wie Sie aus Benutzern Indiana Jones machen?

Gerne nehmen wir Sie mit auf den abenteuerlichen Weg zum neuen heiligen Gral der Sicherheitswelt: Dem identitätsbasierten Sicherheits-Ansatz.

Doch nun einmal der Reihe nach: Cloud-Anwendungen sind aus einem digitalen Umfeld nicht mehr wegzudenken. Mit dem Einsatz von Cloud-Anwendungen findet eine grundlegende Änderung des Denkansatzes im Bereich Sicherheit statt. Eines der grundlegenden Sicherheitsprinzipien „Security by Separation“ funktioniert in der Cloud-Welt auf einer anderen Ebene. Bisher fand die Separierung von Systemen und Anwendungen auf Ebene des Netzwerks statt, z.B. über die Abschottung durch Perimeter-Systeme oder Netzwerkzonen. In der Cloud-Welt funktioniert dies nur noch teilweise, respektive auf Ebene der einzelnen Cloud-Anwendungen oder -Infrastrukturen.




Betrachtet man in der Cloud-Welt die Elemente, in denen Sicherheitsmassnahmen umgesetzt werden können, so stehen an erster Stelle die Benutzer selbst und damit deren digitale Identitäten. Einer der Schlüsselfaktoren der Sicherheit in einem verteilten System ist somit das Management von digitalen Identitäten, deren Authentisierung und Autorisierung.

Das Management von digitalen Identitäten stellt in einer Multi-Cloud-Umgebung eine grosse Herausforderung dar.

Dadurch, dass Anwendungen auf unterschiedlichen Cloud-Plattformen und von unterschiedlichen Anbietern angeboten werden, bestehen pro Anwendung und Anbieter ganz unterschiedliche, dezentrale Benutzerverwaltungen.

Dies kann einerseits aus Sicht des Datenschutzes ein Problem sein, da überall wo Personendaten in Kombination mit deren Verhalten aggregiert werden, z.B. ein erhöhter Schutzbedarf dieser Identitätsdaten entstehen kann. Andererseits bergen dezentrale Benutzerverzeichnisse das Risiko, dass diese ungenügend verwaltet und kontrolliert werden. Zudem kann es bei Sicherheitsvorfällen in Cloud-Umgebungen sehr schwierig sein, Identitäten rasch zu sperren oder Zugriffe und Angriffsmuster überhaupt nachzuvollziehen.

Nicht zuletzt stellen dezentrale Benutzerverwaltungen die Benutzer vor einen Wirr War an unterschiedlichen Zugriffsmitteln. An einen Single Sign-On wagen derzeit viele Organisationen gar nicht mehr erst zu denken.

## Wie erreichen Sie eine identitätszentrierte Sicherheit?

Ok, akzeptiert, Indiana Jones hat sich ja auch nicht in einer Ritter-Burg versteckt, sprich der Perimeter war gestern! Nur: Wie stellen Sie denn nun eine Identitäts-basierte Sicherheit in Ihrer Organisation um? Vorweg einmal: Einen solchen Sicherheitsansatz zu entwickeln und umzusetzen erfolgt nicht innert weniger Tage oder Stunden. Ganz grundsätzlich bestehen zwei Möglichkeit, den Sicherheitsansatz umzugestalten. Idealerweise findet ein Umbau Top down, also abgeleitet aus einer Sicherheits- oder IAM-Strategie resp. entsprechender Richtlinien oder der Anpassung bestehender Richtlinien statt. Nicht selten erfolgt die Umsetzung des Sicherheitsansatzes in einem Bottom up Approach, das heisst das Thema wird aus der Technik heraus forciert.

Bei beiden Vorgehensweisen sollten folgende Punkte grundlegend geklärt werden:

1) Erstellung & Identitätsüberprüfung

2) Verteilung der Identität (Provisionierung)

3) Authentisierung & Autorisierung

4) Federation & Assertions

5) Management des Identitäts-Lebenszyklus

6) Detection & Response

### 1) Erstellung & Identitätsüberprüfung

Je nach Schutzbedarf der Daten, auf welche mittels einer digitalen Identität zugegriffen wird, muss die digitale Identität ein entsprechendes Qualitätsniveau aufweisen. Es gibt unterschiedliche Stufenmodelle, um diese Qualitätsniveaus festzulegen. Die Qualitätsniveaus von Identitäten können über einfache Selbst-Registrationsprozesse bis hin zu staatlich geprüften Identitäts-Verifikationsverfahren erreicht werden.

### 2) Verteilung der Identitäten (Provisionierung)

Im Bereich der Provisionierung von Zielsystemen etablieren sich derzeit bei den unterschiedlichen Cloud-Anbietern unterschiedliche Standards, wie z.B. System for Cross-domain Identity Management (SCIM), Just-In-Time-Provisionierung, usw. Alle diese Provisionierungs-Verfahren haben unterschiedliche Vor- und Nachteile, welche einander gegenübergestellt werden müssen.

### 3) Authentisierung & Autorisierung

Auf unterschiedlichen Cloud-Anwendungen stehen unterschiedliche Mechanismen für die Anmeldung zur Verfügung. Ziel ist die Erreichung eines Single Sign-Ons. Einmal zentral angemeldet, sollten die Benutzer nicht mehrfach zur Eingabe von Anmeldeinformationen aufgefordert werden. Um dies zu erreichen muss zunächst einmal klar sein, auf welchen Credentials die Anmeldung zu erfolgen hat. Damit jedoch nicht genug. Eine Anmeldung, ohne die entsprechenden Rechte in einem Cloud-Service zu verfügen macht keinen Sinn. Neben den Credentials ist auch das übergreifende Management der Rollen und Rechte zu klären.

### 4) Federation & Assertions

Um schliesslich einen effektiven Single Sign-On umsetzen zu können, müssen die Informationen über die Anmeldung und die einem Benutzer zugewiesenen Rollen und Rechte dem Cloud Service mitgeteilt werden. Das hierzu notwendige Verfahren wird als Federation bezeichnet. Um dieses Verfahren umzusetzen, werden entsprechende Assertions (Zuweisungen) benötigt. Die Ausgestaltung dieser Assertions ist von zentraler Wichtigkeit für die Sicherheit, die Benutzerfreundlichkeit sowie die Betreibbarkeit einer Cloud-Umgebung.

### 5) Management des Identitäts-Lebenszyklus

Über die Dauer der Existenz einer digitalen Identität können diverse Mutationen an der digitalen Identität entstehen. Einige Beispiele hierfür sind: Rollen und Rechte ändern, der Name der digitalen Identität muss geändert werden, Attribute wie Mobil-Telefonnummer, Adresse, Funktion werden geändert.

Ausserdem muss geregelt sein, wie digitale Identitäten de-aktiviert, archiviert und gelöscht werden. Hier spielen alsbald Themen wie Archivierungsvorgaben, Nachvollziehbarkeit und Datensparsamkeit eine wichtige Rolle.

### 6) Detection & Response

Last but not least stellt sich nun die Frage, inwiefern und wie Anomalien der Nutzung von digitalen Identitäten festgestellt werden können und dürfen. Die Herausforderung dabei liegt darin, dass die Zugänge zu Cloud-Services schlecht überwacht werden können. Nichts desto trotz müssen Fehllogins, unerlaubte Rechte-Kummulationen oder die verdächtige Nutzung von Zugängen mit erhöhten Rechten festgestellt (detektiert) werden und es werden entsprechende Response-Verfahren im Falle von Abweichungen benötigt.

## Fazit

Ein Identitäts-basierter Sicherheitsansatz in einem verteilten System mit mehreren Cloud-Anwendungen stellt einiges an Herausforderungen. Um alle diese Herausforderungen zu meistern, ist ein gut geplantes Vorgehen in einzelnen Etappen zu empfehlen. Auf dem Weg gibt es einige Fallen, welche vermieden werden können, was letztendlich viel Geld spart.

Durch unsere langjährige Erfahrung in komplexen Identitäts- und Accessmanagement-Projekten und -Umgebungen, steht Ihnen mit Syracom ein Team von ausgewiesenen Experten zur Verfügung, welches Ihnen den Weg an diesen Traps vorbei zeigt. Zögern Sie nicht uns zu kontaktieren.


syracom im brand eins Ranking
der >> Beste Berater 2020<<

syracom

Gunter Dobratz
Leiter Produkte und Lösungen

**Syracom Schweiz AG**
Fon: +41 78 956 64 33
gunter.dobratz@syracom.ch
www.syracom.ch