Clauth

Starke Authentisierung von und für die Cloud

von Martin Brunner

Starke Authentifizierung ist heutzutage wichtiger denn je. Der mobile Zugriff auf Systeme, Anwendungen sowie Daten eines Unternehmens werden von immer mehr Mitarbeitern, Kunden, Partner und Drittparteien gewünscht und auch genutzt. Die Wahl der richtigen Authentifizierungslösung spielt eine zentrale Rolle, um auf der sicheren Seite agieren zu können.

Bereits vor Jahren begannen die Unternehmen, die Grenzen des Perimeters zu verschieben. Mit der Einführung von Technologien wie VPN wurde den Mitarbeitern der Fernzugriff auf Firmendaten ermöglicht. Heute wird der Perimeter nicht mehr verschoben, er löst sich mehr und mehr auf. Zu einem nicht unerheblichen Teil liegt das an der weit verbreiteten Nutzung von Cloud-Diensten und anderer Online-Angebote. In zunehmendem Masse werden Software und Infrastruktur als Dienste über das Internet bezogen, anstatt im Unternehmensrechenzentrum installiert zu werden.

Fundamentale Auswirkungen

Dieser Schritt hat fundamentale Auswirkungen auf das Sicherheitsverständnis in Bezug auf die Authentisierung von Benutzern. In der Vergangenheit konnte der Zugang zu unternehmenseigenen Applikationen mit einfachen Authentisierungsmitteln wie Passwörtern geregelt werden. Man wusste, dass nur ein begrenzter Benutzerkreis innerhalb des eigenen Perimeters Zugriff auf die jeweiligen Applikationen hat. Die zeit- und kostenintensive Verwaltung der Benutzer und deren applikationsspezifischen Passwörtern wurde aufgrund der moderaten Sicherheitsanforderungen und mangels kostengünstiger und einfach zu intergierenden Alternativlösungen hingenommen.

Heute sind Unternehmen gefordert, den Zugang zu unternehmenseigenen- und Cloud-basierten Applikationen sicher und kosteneffizient zu ermöglichen und die damit zusammenhängende Verwaltung der Benutzer über verteilte Systeme sicherzustellen. Zudem soll der Helpdesk entlastet und über Single-Sign-On (SSO) die Benutzerakzeptanz und Benutzerfreundlichkeit erhöht werden.

Starke Authentisierung

Eine starke Authentisierung (oder Zwei-Faktor-Authentisierung) gegenüber Cloud-basierten Applikationen ist aus Gründen der Sicherheit ein Muss. Sie ist definiert durch erstens etwas, dass der Benutzer weiss (zum Beispiel ein Passwort oder ein PIN) und zweitens etwas, dass der Benutzer hat (zum Beispiel ein Smartphone oder ein Token).

Eigenschaften moderner Authentisierungslösungen

Die Wahl der richtigen Authentisierungslösung spielt hierbei eine zentrale Rolle. Sie sollte folgende wichtige Anforderungen erfüllen:

- Zentrale Benutzerverwaltung
  Automatische Integration der Benutzer von bestehenden Systemen (AD, LDAP, IDM) sowie einfache und effiziente Verwaltung der Benutzer, deren Rechte und Token.

- Self-Service und Self-Enrollment
  Benutzer sollen in der Lage sein, ihre Tokens eigenständig zu beantragen, auszutauschen und zu verwalten. Dies soll auf der Basis vordefinierter Benutzer- und Sicherheitsrichtlinien erfolgen.

- Integration und Migration
  Einfache Integration in unternehmenseigene- und Cloud-basierten Applikationen sowie einfache Migrationsszenarien, die bestehende Lösungen nahtlos in die neue Lösung überführen können.

- Schnittstellen
  Unterstützung aller gängigen Schnittstellen für unternehmenseigene- und Cloud-basierten Applikationen, insbesondere RADIUS und SAML und Federated Identities. Bereitstellung von sogenannten Agenten für Applikationen, die keine standardisierten Schnittstellen anbieten. Auf dieser Basis kann einfach und effizient ein Single-Sign-On unter Verwendung von Tokens umgesetzt werden.

- Administration und Monitoring
  Einfache und übersichtliche Administration der Benutzer und deren Zugänge zu den jeweiligen unternehmenseigenen- und Cloud-basierten Applikationen. Automatische Widerrufung der Berechtigungen im Falle von definierten Aktionen oder Prozessen (zum Beispiel Austritt eines Mitarbeiters aus dem Unternehmen).

- Tokens
  Unterstützung aller gängigen Mobiltelefone (Apps und SMS) und dedizierter Tokens und Streichlisten (auch von Drittanbietern).

- Wirtschaftlichkeit und Nachhaltigkeit
  Die Lösung muss skalierbar, flexibel, wirtschaftlich und nachhaltig in Bezug auf zu unterstützende Applikationen und Systeme sowie Anzahl Benutzer, Standorte und möglicher Mandanten sein.

SafeNet Authentication Service

Der Authentication Service von SafeNet erfüllt alle zuvor genannten Anforderungen und kann als Service aus der Cloud bezogen werden oder eigenständig im Unternehmen installiert und betrieben werden. Im Falle der Cloud-basierten Authentisierungslösung profitiert der Kunde von einer kostengünstigen und stufenlos skalierbaren Plattform, die es ihm ermöglicht, eine unbegrenzte Anzahl unternehmenseigener und Cloud-basierter Applikationen, Benutzern und Tokens zu integrieren und zu verwalten. Die jeweilige Verwaltung erfolgt über eine mandantenfähige Plattform, die herstellerübergreifende Technologien unterstützt. Die Lösung benötigt keine zusätzliche Infrastruktur und kann somit auch rasch und effizient für ein Proof of Concept integriert werden. Dies gibt dem Kunden die Möglichkeit, die Vorteile der Lösung unter realen Einsatzbedingungen zu prüfen. ■

Martin Brunner

ist Security Consultant / IT-Sales bei der keyon AG.

www.keyon.ch