VON DER AUSSENKANTE ZUM INNEREN KERN

Bild: funkschau Quelle: 123rf

Oberstes Gebot bei der Verwaltung von Identitäten ist die größtmögliche Sicherheit. Fachbereiche fordern hingegen ein hohes Maß an Flexibilität, um digitale Services erfolgreich zu machen. Sollen diese, auf den ersten Blick widersprüchlichen, Anforderungen in Einklang gebracht werden, braucht es eine serviceorientierte Standardinfrastruktur.

Autorin: Silvia Hänig ***Redaktion: Diana Künstler***

➤ Die Tatsache, ob sich ein Mitarbeiter gerade innerhalb oder außerhalb seiner Firma befindet, wenn er einen Online-Dienst abruft, wird immer mehr zur Nebensache. Zumindest für den Anwender. Die einst klar abgesteckten und gut geschützten Grenzen im Unternehmensnetzwerk, die genau definierten, was innen und außen war, werden durch die aktuelle Arbeitspraxis – in der orts- und zeitunabhängig gearbeitet wird – zunehmend entwertet. Was zählt ist: Zwischen jedem Nutzer, der auf einen Online-Dienst zugreift und jedem Unternehmen, das diesen Dienst anbietet, wird eine unkomplizierte und dennoch sichere Verbindung erwartet. Ob das aus dem Homeoffice oder vom Urlaubsort aus passiert, spielt für Endkunden oder Mitarbeiter keine Rolle.

Das Analystenhaus Kuppinger Cole setzt sich schon seit einigen Jahren damit auseinander, was diese Entwicklung für das Zusammenspiel von

Identitäts- und Sicherheitsmanagement heißt: „Eine sichere Identität verlagert damit die Grundlage für Sicherheit dorthin, wo sie benötigt wird“, erklärt der Analyst Matthias Reinwarth. Aber welche Konsequenzen zieht so eine Dynamisierung von Sicherheit nach sich, wenn sie auf proprietäre IAM-Systeme stößt?

Inhouse-IAM-Infrastruktur gehört auf den Prüfstand

Genau hier liegt die große Herausforderung. Traditionelle IAM-Infrastrukturen inklusive selbst entwickelter Authentifizierungs-Bausteine sind „von Haus aus“ nicht wirklich kompatibel mit den aktuellen Anforderungen an digitale Identitäten, über die der Nutzer von überall auf unterschiedliche Dienste zugreift. Im Gegenteil: Sie fußen auf monolithischem Design sowie einer klassischen Implementierung und wurden für lokale Rechenzentren entwickelt. Denn damit war man bisher immer gut gefahren. Genau diese eher gewachsene IAM-Infrastruktur mitsamt ihrer Identitätssilos muss jetzt auf den Prüfstand, damit digitale Identitäten mit digitalen Diensten korrespondieren können. „Wenn diese Home-Grown-Lösungen auf die Welt da draußen mit Corona und Cyberattacken treffen, knirscht es“, weiß auch Matthias Reinwarth.

Tatsächlich stellen sowohl Quantität als auch Qualität von Cyberattacken die On-Premise-IAM-Landschaften auf eine harte Probe. Beim Credential Stuffing etwa werden Nutzerdaten in großem Stil in Bruchteilen von Sekunden über frei verfügbare Listen im Internet heruntergeladen, um diese dann möglichst gewinnbringend im Netz weiter zu veräußern. Schutzwälle wie Firewalls und Intrusion-Detection-Systeme zum Schutz der Außengrenzen werden damit zwar nicht zwangsläufig überflüssig, dennoch brauchen die Entwickler und Administratoren ergänzende Lösungen, um über ihre Eigenentwicklungen der dynamischen Bedrohungslage jederzeit Herr werden zu können. Und zwar möglichst ohne, dass die selbst entwickelten IAM-Funktionen gleich über Bord geworfen werden müssen. Nur: Das kostet Zeit und Geld.

Gefahr: Kostengrab Eigenentwicklungen

Das Weiterentwickeln von eigenen IAM-Funktionen für jeden zusätzlichen digitalen Dienst kostet nicht nur mehr Entwicklerstunden, sondern im Zweifel auch lange Marktführungszeiten. Hinzu kommt, dass das Management von Identitäten schnell komplex werden kann, da nahezu täglich neue Zugriffswege und Authentifizierungsmöglichkeiten hermüssen, um die Customer Journey zu bedienen. Das kennt auch Andre Priebe, CTO des Systemintegrators iC Consult, aus seiner Beratungspraxis nur zu gut: „Am Anfang geht es meist um die Entwicklung weniger Funktionen, die man gut in den Griff bekommt. Aber mit zunehmender Anzahl an Providern und Partnern, die es zu integrieren gilt, wächst auch die Anzahl an Funktionen und Protokollen. Dann wird Identitätsmanagement schnell vielschichtig und unter

Umständen zum Millionengrab.“ Sein Identitätspartner Auth0 liefert die entsprechenden Zahlen dazu: „Rund 50 Prozent unserer Kunden haben ihre IAM-Funktionen selbst weiterentwickelt, bis sie merkten, dass es so auf Dauer nicht funktionieren kann. Denn noch während der Entwicklungszeit wurden sie von den Anwendungsbedürfnissen überholt“, weiß Steven Rees-Pullman, Senior Vice President International des US-Anbieters. Man stelle sich allein die Einbindung und Verknüpfung diverser Accounts – zum Beispiel von Social-Logins bei Facebook, Google oder Apple – vor.

Schon mit dem Handling der schieren Menge an Daten sind traditionelle IAM-Systeme eigentlich längst überfordert. Ohne professionelle Hilfe lässt sich dieser Kraftakt nur schwer bewältigen. Die IT- und Security-Fachbereiche sind aufgrund von Fachkräftemangel und reduzierten Budgets meist ohnehin gezwungen, mit einer ausgedünnten Mannschaft zu arbeiten, die schon genug damit zu tun hat, den Tagesbetrieb aufrechtzuerhalten.

IAM-Management muss skalierbar sein

Diese Erfahrung ist einer der Hauptgründe dafür, warum für viele Unternehmen das eigene Rechenzentrum nur noch eine von vielen Möglichkeiten ist, wenn es um die Weiterentwicklung der Identity-Infrastruktur für interne und externe Dienste geht. Denn im Hinblick auf Kosten und Time-to-Market gehen immer mehr Firmen dazu über, einen großen Anteil der neuen IAM-Infrastrukturen in die Cloud zu verlagern. Sie haben verstanden, dass sich ständig verändernde Kundenanforderungen und Bedrohungslagen, schnelle technische Innovationszyklen und der Wunsch nach Skalierbarkeit nicht mehr allein mit den klassischen Lösungsansätzen handhaben lassen.

Vielmehr geht es um ein tiefes Verständnis für Serviceorientierung in Kombination mit Standardisierung, sofern es mit dem modernen Identitätsmanagement klappen soll. „Die Skalierung, die ich zwischen innen und außen erreichen möchte, bekomme ich nur mit standardisierten Komponenten hin“, so Matthias Reinwarth. „Dort, wo beispielsweise gerade viel Authentifizierungslast benötigt wird, möchte ich schnell hochskalieren können. Das gelingt nicht auf Basis der Entwicklung individueller Authentifizierungs-Lösungen.“ Nur wenn es um die Konfiguration geht, so der Analyst, kann man individuelle Anpassungen vornehmen. Ansonsten sollte die Verbindung ausschließlich über standardisierte APIs laufen, um den Nutzer immer genau dort einen Service anzubieten, wo er sich gerade befindet.

Das stellt auch veränderte Anforderungen an die Eigenschaften, die eine digitale Identität braucht, um das richtige Sicherheitslevel für die Bereitstellung eines Dienstes verfügbar zu machen. Das können beispielsweise die Position des Anwenders oder auch das Gerät sein, von wo aus er den Dienst nutzen möchte. Trifft diese Dynamik jetzt beispielsweise auf eine statische Identität, erhöht sich automatisch die Gefahr von Identitätsdiebstahl und es hagelt im Zweifel negative Nutzererfahrungen. Das zeigt, wer die Zugriffe auf Dienste über Geräte und deren Apps dynamisch kontrollieren und steuern möchte, kommt um das IDaaS-Modell im Standardansatz nur schwer herum.

Basis: eine einheitliche Identitätsinfrastruktur

Diesen Trend bestätigt hat auch eine Erhebung unter 426 US-Unternehmen. Demnach setzen dort bereits 74 Prozent aller Befragten auf ein SaaS-Modell. Dabei priorisieren sie vor allem die Bereiche Payment, Messaging und Authentifizierung. Um den Shift Richtung Serviceorientierung bewerkstelligen zu können, versorgt der US-Anbieter Unternehmen mit einer Art digitalem Identitäts-Backend, welches alle ID-Services in standardisierter Weise je nach gewünschtem Service bereitstellt, und zudem On-Premise-IAM-Systeme berücksichtigt. „Brauche ich also den Baustein Authentifizierung, muss ich sichergehen, dass alle Services mit einer einheitlichen Identitätsinfrastruktur reden können“, so Matthias Reinwarth. Das kann ebenfalls die komplette Umstellung auf digitale Geschäftsabläufe erheblich erleichtern, zumal die Bereitstellung digitaler Identitätsdienste und deren Zugangs-Steuerungen nur Sinn machen, wenn digitale Angebote auch entsprechend rege genutzt werden.

Die zentrale Frage für jeden IT- oder Security-Verantwortlichen darf daher nicht länger lauten: Wie können wir unser Identitätsmanagement bestmöglich weiterentwickeln? Sondern vielmehr: Inwieweit sind unsere eigenen Entwicklungen wirtschaftlich und sicherheitstechnisch mit der aktuellen Bedrohungslage und Anwenderpraxis vereinbar?

Silvia Hänig ist Communication Strategist bei iKom

Identitätsmanagement war noch nie so wichtig wie in Zeiten von Homeoffice und mobilen Arbeitsumgebungen. Eine sichere Identität optimiert das Risikomanagement. Doch jede Branche legt bei ihrer IAM-Stragie andere Schwerpunkte, welche eine aktuelle Studie des IDaaS-Anbieters LastPass aufzeigt. Bei Finanzdienstleistern stehen demnach Risikominderung und Integrationen im Vordergrund; die IT wiederum legt großen Wert auf Datensicherheit. Bei Medienunternehmen liegt der Fokus auf einer besseren Personalproduktivität.