IAM und die Grenzen der Technik

Thomas Zweifel, Tom Sprenger

Laut einer Studie von IDC Ende 2012 hat sich das digitale Universum in den letzten zwei Jahren auf unvorstellbare 2,8 Zettabyte verdoppelt. Die Auswertung und Verknüpfung dieser Daten bieten Unternehmen und Institutionen neue Möglichkeiten. Gleichzeitig wird es zur Herausforderung, den Zugriff auf die eigenen Daten zu steuern.
Klassische Mechanismen wie Role-Based Access Control oder Proxies und VPN stossen zunehmend an Grenzen: Durch den Einsatz von Cloud-Services lassen sich Daten nicht mehr einfach in einem organisationsinternen Netzwerk zusammenfassen und zentral verwalten. Mit der Zusammenarbeit zwischen Organisationen wird auch die Nutzergemeinde immer disperser. Durch die Verknüpfung können an sich unbedenkliche Daten mehr Information preisgeben als gewünscht und damit schützenswert werden. All diese Entwicklungen sprechen dafür, beim Zugriffsmanagement neu von den Daten auszugehen.

Thomas Zweifel
Senior IT Consultant
AdNovum Informatik AG
thomas.zweifel@adnovum.ch

Dr. Tom Sprenger
CTO
AdNovum Informatik AG
tom.sprenger@adnovum.ch

Den Behörden steht heute eine ständig wachsende Menge und Vielfalt von Daten zur Verfügung. Da das Übertragen von Daten immer einfacher und schneller und das Speichern immer günstiger wird, werden Daten immer häufiger dezentral gehalten und repliziert. Obwohl vor allem als Datenerheberinnen wahrgenommen, können Behörden auch für sich selbst beachtlichen Nutzen aus den Daten ziehen. Daten aus Verkehrszählern beispielsweise können zur Modellierung von Pendlerströmen dienen. Selbst Daten, die auf den ersten Blick nichts miteinander zu tun haben, können kombiniert interessante Schlüsse zulassen: Google beispielsweise nutzt das Wissen über die Anzahl Suchabfragen zu gewissen Stichworten, um durch Verknüpfung mit Daten aus den Vorjahren Höhepunkte von Grippewellen zu errechnen.

Daten gezielt schützen

Mit der vermehrten Verbreitung, Nutzung und Verknüpfung von Daten stellt sich die Frage nach ihrem Schutz. Insbesondere bei der Verknüpfung und Auswertung von Personendaten stehen Behörden schnell in der Kritik. Dabei sind nicht alle generierten Daten schützenswert. Oft ist der Erzeuger der Daten sogar selbst daran interessiert, sie möglichst weit zu streuen. So wollen zum Beispiel zahlreiche Open-Data-Initiativen vorhandene Daten über einfache neue Interfaces öffentlich zugänglich machen.
Aber auch sensible Daten werden heute immer häufiger dezentral abgelegt, oft in einer Cloud. Die Verknüpfung der dezentralen Datenpools bringt zusätzlichen Nutzen, kann jedoch dazu führen, dass auch Daten, die per se als unbedenklich gelten, in Kombination mit komplementären Daten als schützenswert eingestuft werden müssen.

Zugriffsmanagement stösst an Grenzen

Durch die Dezentralisierung und die Explosion der Datenmenge wird es immer schwieriger, Daten mit klassischen Mitteln zuverlässig zu schützen. Das Paradigma der Perimetersicherheit, also der physischen und/oder logischen Separierung von «intern» und «extern» mit Kontrolle der Zugänge, gerät zunehmend unter Druck. Die vermehrte Einbindung externer Dienste und die wachsende Vernetzung von Behörden weichen die Perimeter auf. Auch die Nutzergruppen werden immer vielfältiger. Zu den internen kommen externe Nutzerstämme hinzu, und die zentrale Verwaltung von Benutzerrechten stösst an Grenzen.
Diese Masse an Identitäten und Berechtigungen kann über kurz oder lang nur automatisiert verwaltet werden. Die Zugriffskontrolle über Access Control Lists (ACL), die festlegen, welche Benutzerinnen und Benutzer Zugriff auf ein Objekt haben, wurden bereits durch die Role-Based Access Control (RBAC) abgelöst. Bei der RBAC werden Berechtigungen in Rollen gruppiert, wodurch sich die Anzahl individueller Berechtigungszuweisungen stark reduziert. Bei der Attribute-Based Access Control (ABAC) wird die Rollenverwaltung durch automatisierte Generierung und Zuweisung von Rollen und Berechtigungen auf der Basis von Attributen weiter vereinfacht. So erhalten Mitarbeitende zum Beispiel auf der Basis ihrer Daten automatisch Zugang zum richtigen Gebäude und Zugriff auf die Kollaborationsumgebung ihres Teams.

Umsetzung nicht trivial

Die Anzahl wohldefinierter statischer Attribute, die solche Zuweisungen erlauben, ist allerdings selbst innerhalb einer Organisation begrenzt. Noch rarer sind solche Attribute, wenn organisationsübergreifend gearbeitet wird. Mit Hilfskonstruktionen wie Gastzugriffen für Endkunden oder Zulieferer kann zwar Abhilfe geschaffen werden, doch ist eine konsistente Integration externer Daten schwierig und nicht selten aufwendig. Die Daten müssten durch Provisionierung automatisiert abgeglichen werden, was nicht nur zeit- und kostenintensiv, sondern unter Umständen auch datenschutzrechtlich problematisch ist.
Die attributbasierte Zugriffskontrolle (ABAC) ermöglicht zwar eine gewisse Automatisierung bei der Berechtigungsverwaltung, doch bleibt der Aufwand für die Verwaltung der Attribute hoch. In einem weiteren Automatisierungsschritt können die Attribute durch Policies ersetzt werden: Die Policy-Based Access Control (PBAC) wertet die Attribute der Systeme basierend auf Policies aus und kann dadurch Zugriffsberechtigungen überwachen. Die Komplexität solcher Policies sowie der unternehmensweiten Standardisierung und Homogenisierung der Attribute ist jedoch nicht zu unterschätzen. Neben der technischen

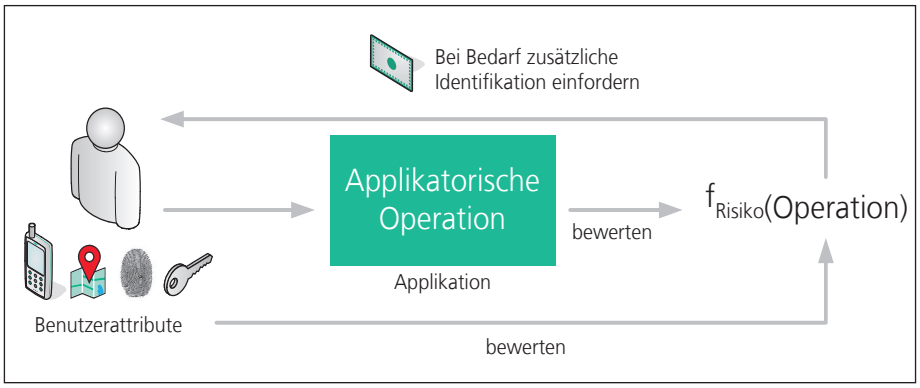

Abbildung 1: Risk-Adaptive Access Control (RAdAC)

Umsetzbarkeit stellen sich Fragen zur Haftung, falls Policies versagen und es zu Datendiebstahl oder Missbrauch kommt.

Dynamische Einstufung von Zugriffen

Eine zusätzliche Möglichkeit zur Risikobewertung bei Zugriffen erhält man durch dynamische Auswertung der Umgebungsfaktoren der Userinnen und User: Dieses Vorgehen wird Risk-Adaptive Access Control (RAdAC) genannt und bezieht Faktoren wie Infrastruktur, Lokation, Authentisierungsmittel oder Frequenz der Anfragen ein. Werden die für die Daten errechneten Limiten überschritten, wird entweder der Zugriff gesperrt und intern alarmiert oder ein zusätzlicher Identifikationsprozess mit manueller Interaktion gestartet (s. Abbildung 1).

Gewinnt die Usability?

Dieses System schneidet auch bezüglich Usability gut ab, denn Sicherheitsfragen zur zweifelsfreien Identifikation zu beantworten oder Sonderrechte zu beantragen, ist nur dann nötig, wenn ein Fall als kritisch eingestuft wird. Im Mobile-Zeitalter, in dem die Benutzerinnen und Benutzer bei der Zusammenarbeit und dem Datenaustausch den Komfort von Cloud-Lösungen wie der Dropbox erwarten, ein nicht zu unterschätzender Vorteil. Allerdings wird damit das Verhalten einer Applikation für den Benutzer weniger berechenbar, da er beispielsweise beim hundertsten Zugriff auf eine Schnittstelle überraschend in eine höhere Risikokategorie eingestuft werden kann.

Risikobewertung über Metadaten

Für die Umsetzung adaptiver Systeme werden Daten und Applikationen mit der Sicherheitsinfrastruktur verknüpft. Ohne diese Verknüpfung kann die Infrastruktur nicht wissen, auf welchem Risikolevel sich eine Kundin oder ein Kunde bewegt und wann zusätzliche Checks nötig sind. So werden Applikationen, Datenbanken und IAM-Systeme wieder miteinander verbunden, die man über Dekaden aus Sicherheitsgründen separiert hat. Eine adaptive Lösung kann jedoch gerade in einem heterogenen dezentralen Umfeld zielführend sein, wo eine zentrale Verwaltung utopisch und ein Datenabgleich mittels Provisionierung aus datenschutzrechtlichen und politischen Gründen nur beschränkt umsetzbar ist.

RAdAC: noch nicht verbreitet

Beispiele von RAdAC gibt es bereits, es handelt sich jedoch in der Regel um Insellösungen für einzelne Anwendungsgebiete. Facebook zum Beispiel nutzt Risikofaktoren, um Identitätsdiebstahl zu erschweren. So kann es sein, dass man beim ersten Zugriff von einem neuen Gerät aus oder aus einem anderen Land zusätzliche Sicherheitsfragen beantworten oder Freunde auf Fotos identifizieren muss. Analog lösen in E-Banking-Anwendungen Abweichungen vom Nutzerprofil zusätzliche Sicherheitsüberprüfungen aus: So wird zum Beispiel bei einer Überweisung an einen neuen Begünstigten eine separate Transaktionssignatur verlangt. Auch in der Kreditkartenbranche kommen Profiling und Fingerprinting zur Erkennung und Prävention von Betrugsversuchen zum Einsatz. Wird die Kreditkarte ausserhalb eines eingeschätzten Verhaltensmusters eingesetzt, so kann sie gesperrt werden.
All diese Lösungen setzen Metadaten ein. Zusätzlich sollte eine Risikoabschätzung Informationen zur Qualität, Gültigkeit und Quelle der Metadaten und zum vorgesehenen Einsatzrahmen einbeziehen.

Daten statt Applikationen im Zentrum

Trotz allen Herausforderungen sollten Behörden vorhandene Daten im Rahmen ihrer rechtlichen Möglichkeiten nutzen. So können sie neue Services anbieten und über Benutzeranalysen Partner sowie Kundinnen und Kunden besser kennenlernen und Services optimieren.
Zentral ist dabei die Vorgehensweise beim Umgang mit der wachsenden Datenflut und der Dezentralisierung. Hier zeichnet sich eine Verschiebung vom Paradigma der Applikations- und Systemverantwortlichen hin zur Data Ownership ab, also zur Verantwortung für Daten über System- und Applikationsgrenzen hinweg. Nur so können die rechtlichen Vorgaben eingehalten und Daten übergreifend geschützt werden.

Schutzkategorien für Daten

Ein erster Schritt ist die Einteilung der Daten in Schutzkategorien: «nicht schützenswert», «nicht schützenswert, aber mit Missbrauchspotenzial (zum Beispiel bei Verknüpfung mit anderen Daten)», «publizierbar, von ökonomischem Wert und darum nur für kontrollierte Zugriffe freizugeben» und «schützenswert, Zugang nur für klar definierte Benutzer». Die vier Kategorien müssen unterschiedlich behandelt werden: Bei schützenswerten und kommerziell zu nutzenden Daten geht es um die Identifikation der Benutzerin oder des Benutzers, bei der Missbrauchsprävention eher um die Detektion von Anomalien bei Datenabfragen. Die Kategorisierung beziehungsweise die Risikoabwägung kann also nicht allein auf der Basis der Daten geschehen, sondern muss auch adaptive Faktoren wie Datenmengen, Zugriffspatterns oder die Verknüpfung mit anderen Daten berücksichtigen.
Weiter gilt es, die Datenflüsse zu analysieren und auf der Basis von Risikoeinschätzungen Zugriffsprozesse zu definieren. Ebenfalls zentral ist, dass regelmässige Reviews und Audits eingeplant werden, um Veränderungen frühzeitig zu erkennen. Soweit möglich sind dabei Mechanismen vorzusehen, um die Datenalterung zu handhaben. In den Metadaten soll zudem Information über die Qualität der Daten mitgeführt werden.

IAM neu verstehen

Insgesamt empfehlen wir, bei der Umsetzung eines datenorientierten Zugriffsmanagements evolutionär vorzugehen. Etablierte IAM-Lösungen lassen sich durch schrittweise Integration von RAdAC-klassierten Daten und Metadaten zu Lösungen erweitern, mit denen grosse Mengen von dezentralen Daten sicher und nachvollziehbar verwaltet und vor unberechtigtem Zugriff geschützt werden können. Identity- und Access-Management ist dann nicht mehr nur ein Sicherheitsservice, sondern kann auch dabei helfen, die Benutzerinnen und Benutzer und ihre Bedürfnisse besser zu verstehen, ganz im Sinne von «Know your E-Gov-Customer».