Föderierte Autorisierung und
ein Umdenken im Privilegienmanagement

Organisationsübergreifend arbeiten – aber sicher!

Die moderne Welt ist eine Welt der Kooperationen und Interaktionen – „Einzelkämpfer" sind weitgehend abgemeldet. Damit Unternehmen und Organisationen dieser Herausforderung gerecht werden können, ist ein Paradigmenwechsel bei der Autorisierung von Nutzern notwendig. Etablierte Rollen-basierte Autorisierung und Domain-zentrierte Sicherheitskonzepte sind nicht mehr in jeder Situation zielführend. Eine Lösung bilden Richtlinien- und Attribut-basierte Ansätze und neue Standards, die eine dynamische Rechtezuweisung an föderierte Identitäten ermöglichen.

Organisationsübergreifend arbeiten zu können, ist eine typische Herausforderung in der heutigen vernetzten Geschäftswelt. Damit steigen die Gefahren für die schützenswerten Informationen der beteiligten Organisationen. Täglich neue Nachrichten über den Missbrauch von Diensten und Daten bestätigen dies. Zehntausende geheime Dokumente wurden beispielsweise auf der Online-Enthüllungsseite WikiLeaks veröffentlicht. Angesichts der zunehmenden Kooperationen von Unternehmen ist es immer häufiger notwendig, Identitäten organisationsübergreifend zu verknüpfen. Diese Identitäten werden als „föderiert" bezeichnet. Beispielsweise muss ein Notarzt im Falle einer Operation Informationen über den Patienten in den Datenbeständen einer fremden Klinik einsehen können. Dazu benötigt er ad hoc eine Autorisierung, die ihm exakt die notwendigen Rechte für diesen Vorgang auf dem fremden Dienst einräumt. Insbesondere der Gesundheitssektor sieht hier klare Regelungen und Sanktionen bei Missbrauch vor.

Wozu ein Umdenken im Privilegienmanagement?

Der stark wachsende Daten- und Informationsaustausch sowie die Nutzung von Anwendungen und Diensten über Organisationsgrenzen hinweg bedeuten neue Herausforderungen für ehemals nach außen abgeschottete IT-Systeme. Trends und Technologien wie Service-orientierte Architekturen (SOA), Software as a Service (SaaS) und das Outsourcing von Kern-Funktionen des IT-Managements sind in vielen Organisationen umgesetzt oder geplant. Sie führen dazu, dass etablierte Sicherheitsbarrieren und Domain-zentrierte Sicherheitskonzepte den Anforderungen nicht mehr genügen. Eine Organisation muss nicht mehr nur Identitäten und Zugangsberechtigungen für interne Benutzer verwalten, sondern auch für ständig wechselnde externe Benutzer. Die für die IT-Sicherheit fundamentalen Autorisierungs- und Zugriffskontrollmechanismen einer Organisation dürfen hierdurch natürlich nicht außer Kraft gesetzt werden. Der Zugriffsschutz muss entsprechend angepasst werden, damit die Sicherheit gewährleistet bleibt. Diese Anpassungen sind allerdings fundamental und führen zu einem Paradigmenwechsel im Access Management. Durch den Einsatz und die optimale Verwaltung von Privilegien, welche die Erlaubnis zur Durchführung einer Aktion beinhalten, gibt es die Chance, erfolgreich Access Management zu betreiben. Das Privilegienmanagement (PvM) regelt, wie mit Privilegien für IT-Systeme umzugehen ist.

Aber wie genau kann PvM organisationsübergreifend funktionieren? Wie können Privilegien dynamisch und zeitnah an Nutzer adressiert werden? Wie können feingranulare Autorisierungsentscheidungen, anhand einer Vielzahl von Informationen, über Organisationsgrenzen hinweg sicher verwirklicht werden? Wie müssen etablierte Sicherheitsmechanismen, insbesondere Domain-zentrierte Sicherheitskonzepte, umgestaltet werden, um Identitätsföderationen mit Partnern abzusichern? Neben diesen Fragen ist auch relevant, ob für eine Lösung bereits praktikable Methoden und Standards existieren.

Wie sieht das Management von Privilegien heute aus?

Zur Beantwortung der aufgeworfenen Fragen müssen zunächst etablierte Lösungsansätze für PvM innerhalb des Access Managements betrachtet werden. Das PvM verwaltet Zusammenhänge zwischen Rechten und digitalen Identitäten. Eine digitale Identität besteht aus Attributen wie dem Namen und einer E-Mail-Adresse. Sie ist eine Untermenge aller Daten und Informationen einer Entität (Mensch, Maschine, Dienst etc.). Die Attribute ermöglichen es, eine Entität eindeutig von einer anderen Entität zu unterscheiden. Ein Privileg wiederum besteht aus dem Recht einer digitalen Identität, etwas in einem bestimmten IT-System tun zu dürfen. Privilegien gewähren den kontrollierten Zugriff auf Daten oder auf eine Funktion. Das kann bspw. die Erlaubnis zur Anpassung einer Datenbank sein. Privilegien müssen intern für jede digitale Identität definiert und anschließend in die IT-Systeme übertragen werden. Dies schafft die Voraussetzung dafür, Zugriffe auf Ressourcen kontrollieren zu können (Access Control).

Die Verwaltung von Privilegien wird auf Basis eines **Role-Based Access Control (RBAC)**-Modells gelöst. Privilegien werden nicht manuell an eine digitale Identität vergeben, sondern über deren Zugehörigkeit zu einer Rolle, zum Beispiel Arzt und Krankenpfleger. Privilegien, die ganze Nutzergruppen benötigen, können somit zusammengefasst werden. Hier ist zu beachten, dass Rollenmodelle mehrstufig sind. Es gibt die organisatorische Rolle mit Fokus auf Organisationshierarchien, bspw. Oberarzt und Stationsarzt, die technische Rolle auf IT-Ebene, zum Beispiel Domänenbenutzer, und die Elementarrolle für einzelne Systeme, bspw. Administrator. Eine grundsätzliche Aufteilung der Rollen in diese drei Bereiche gibt der RBAC-Standard ANSI INCITS 359-2004 vor.

Bei RBAC werden Privilegien auf mehreren, unterschiedlichen Systemen zu Rollen gruppiert. Anschließend werden die Nutzer dieser Systeme den Rollen zugeordnet. Die Implementierung ist schwierig, da Nutzer oft eine Vielzahl von Rollen einnehmen, welche in Konflikt stehende Privilegien in-

nerhalb eines Systems beinhalten können. Die in vielen Organisationen bestehende strikte Funktionstrennung führt bei einer Vielzahl von Applikationen und Rollen zu Problemen. Sobald eine Verletzung der Funktionstrennung auftritt, zum Beispiel weil eine Rolle Privilegien für IT-Systeme in unterschiedlichen Domänen beinhaltet, welche funktional getrennt werden sollen, muss diese Verletzung durch eine Anpassung der betroffenen Rolle gelöst werden. Oftmals führt eine solche Anpassung dazu, dass Funktionen anderer Nutzergruppen nicht mehr getrennt werden, weil diese ebenfalls die nun geänderte Rolle nutzen. Das Problem ist vergleichbar mit einem niemals endenden Sudoku (siehe Abb. 1).

Die Klassifizierung der Nutzer, die Rollendefinitionen und insbesondere die notwendige Konfliktlösung machen RBAC, je nach Komplexität der Organisation, bisweilen zu einer hochkomplexen Aufgabe. Ein weiterer Schwachpunkt ist, dass Privilegien auf Basis von RBAC nur innerhalb einer Organisation, meist begrenzt auf einzelne Domänen, korrekt erteilt und durchgesetzt werden können. Bedingt durch den abweichenden Kontext, dem eine Fremdrolle entstammt, ist PvM über RBAC daher entsprechend eingeschränkt. Muss beispielsweise der in Klinik A angestellte Arzt mit seiner Fremdrolle „Notarzt" in Klinik B eingebunden werden, bekommt er dort eine oder mehrere neue Rollen. Dies kann zum Beispiel eine neue Rolle „externer Notarzt aus Klinik A" sein, welche eine Teilmenge der internen Rolle „Notarzt" von Klinik B darstellt. Eine Schnittmengenbildung ist jedoch denkbar aufwendig. Rollendefinitionen sind fast nie einheitlich, selbst in einer einzelnen Organisation. Passende Schnittmengen von Rollen zwischen Organisationen zu finden, ist daher nahezu unmöglich. Das Anlegen neuer Rollen für Externe führt bei Identitätsföderationen außerdem zu einer Explosion der Rollenanzahl. Externe Rollen in RBAC einzugliedern, funktioniert nur dann, wenn deren Anzahl überschaubar bleibt, sie strukturell in das vorhandene Modell passen und sie sich nicht dynamisch ändern. Identitätsföderationen verlangen also nach einer neuen Art von föderierter Autorisierung, welche nicht ausschließlich auf Rollen basiert und eine dynamische und flexible Zuweisung von Privilegien ermöglicht.

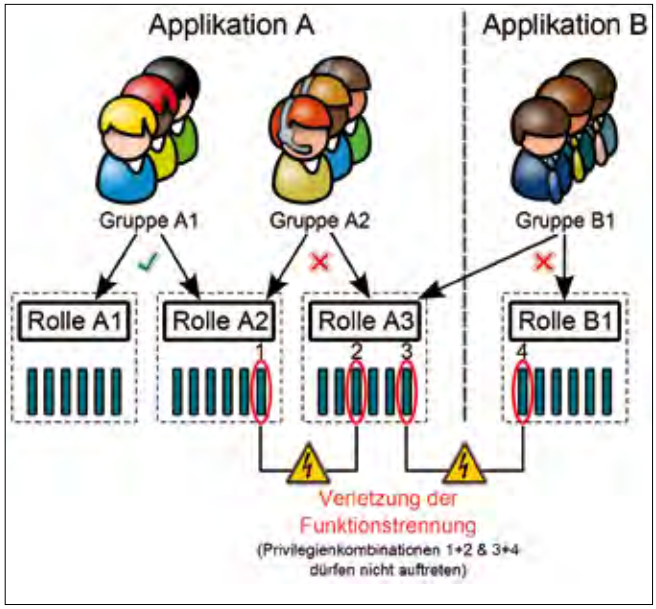

Abb. 1: Applikationsübergreifende Durchsetzung der Funktionstrennung trotz Privilegienmanagement mittels Rollen: Ein niemals endendes Sudoku

Wie kann ein organisationsübergreifendes Privilegienmanagement funktionieren?

Ein Problem von externen Rollen ist, dass sie ohne Kenntnis ihres ursprünglichen Kontextes nicht für Autorisierungsentscheidungen genutzt werden können. Die im vorigen Beispiel erwähnte, in Klinik B generierte Rolle „externer Notarzt aus Klinik A" zeigt es: Im Kontext von „Klinik A" kann eine entsprechend mächtige Infrastruktur entscheiden, dass dieser Notarzt eventuell nur eingeschränkt autorisiert werden darf und ihm zum Beispiel nur der Zugriff auf Notfall-Patienten-Daten erlaubt ist.

Organisationsübergreifend Autorisieren heißt also, Zugriffe auf Ressourcen feingranular festleg- und durchsetzbar zu machen. Feingranularität bedeutet hier, dass zusätzliche Attribute, zum Beispiel zum Kontext einer Aktion, berücksichtigt werden müssen. Ein solches Attribut stellt durch seinen Wert Informationen über Objekte bereit, wie bspw. Formatierungsinformationen im Sinne von Kodierung=UTF-8. Attribute sind in einer Vielzahl von Quellen, zum Beispiel Verzeichnisdiensten, vorhanden. Externe Quellen müssen ebenso berücksichtigt werden. Wichtig ist, dass sie vertrauenswürdig sind. Die Attribute müssen qualitativ hochwertig sein. Ein sicherer und überprüfbarer Austausch der für eine Autorisierungsentscheidung notwendigen Attribute ist bspw. durch Kopplung von Verzeichnisdiensten möglich. Die Security Assertion Markup Language (SAML) des OASIS-Konsortiums stellt hierfür den Quasi-Protokoll-Standard dar.

Bisher fehlte aber ein Modell, das anhand einer Menge von Attributen Autorisierungsentscheidungen treffen konnte. Hierzu wurden **Attribute-Based Access Control (ABAC)** beziehungsweise **Policy-Based Access Control (PBAC)** erdacht. Letzteres ist jedoch lediglich eine erweiterte Variante des Ersteren. Beide arbeiten Attribut- und Richtlinien-basiert und ermöglichen sehr flexibel definier- und anwendbare Zugriffsrichtlinien. Möglich wird dies durch die Auslagerung der Autorisierungsentscheidungen in separate Komponenten, sog. Policy Decision Points (PDP), welche auf Basis von Richtlinien arbeiten. Innerhalb dieser Richtlinien bilden Attribute und deren Werte, zum Beispiel „Rolle=Chefarzt", die Basis für Regeln. Eine Regel könnte zum Beispiel „Wenn Rolle=Chefarzt und Ressource=Patientenverzeichnis ist, dann Zugriff erlauben." lauten. Algorithmen zur Kombination dieser Regeln werten diese pro Richtlinie aus und liefern ein eindeutiges Ergebnis. Ein gemeinsames Verständnis der Attribute muss daher zwingend bei allen Partnern einer Föderation vorhanden sein. Die Richtlinien müssen auf einem gemeinsamen Standard aufbauen. Dieses kann nur durch Übereinkommen der Partner erreicht werden, ist also in erster Linie ein organisatorisch zu lösender Aspekt.

Wie soll ein solches Modell beziehungsweise die zugrundeliegende Infrastruktur umgesetzt werden?

Den technischen Teil können vorhandene Standards abdecken. SAML erlaubt neben der sicheren Übertragung von Attributen auch die Übertragung von Autorisierungsentscheidungen. Letztere ist jedoch zu ein-

geschränkt, so dass ein dedizierter Standard für Autorisierungsentscheidungen entworfen wurde. Dieser ebenfalls von OASIS stammende Standard **eXtensible Access Control Markup Language (XACML)** wird bald in Version 3.0 verabschiedet. XACML bedient sich eines Komponentenmodells (siehe Abb. 2). Dessen grundlegender Gedanke ist es, dass Dienste, Applikationen oder ganze Systeme mit **Policy Enforcement Points (PEP)** ausgestattet werden. Diese dienen als Kontrollpunkte, welche beim Zugriff auf definierte Ressourcen vollautomatisch den Programmverlauf abfangen. Sie formulieren eine Zugriffsanfrage und schicken diese an einen **Policy Decision Point (PDP)**. Dieser kennt im Prinzip alle für sein Umfeld gültigen Richtlinien und kann durch sie die Entscheidung berechnen. Der PDP schickt diese zurück an den PEP. Je nach Entscheidung erlaubt oder verweigert der PEP den Zugriff. Zusätzlich kann er den Zugriff mit Auflagen versehen, wie bspw. ein Mitschnitt des Zugriffsversuches.

Die Vorteile dieser Architektur liegen auf der Hand: Es lassen sich neben detaillierten Regeln auch umfassende Sets von Richtlinien erstellen, welche sehr feingranulare Autorisierungsentscheidungen ermöglichen. Neue Richtlinien werden über die Verwaltungskomponente, den **Policy Administration Point (PAP)**, eingepflegt. Hierdurch kann sichergestellt werden, dass alle angeschlossenen Systeme vom Zeitpunkt der Inkraftsetzung einer Richtlinie an diese tatsächlich auch befolgen. Zudem werden alle für eine bestimmte Domäne relevanten Attribute an einer für diese Domäne zentralen Stelle, dem **Policy Information Point (PIP)**, gespeichert und verwaltet.

Neben diesem Komponentenmodell ist XACML in erster Linie eine XML-Sprache, welche sich als eine Art Grammatik zum Austausch von Informationen über Zugriffe beschreiben lässt. Wo in einem ganzen Satz Subjekt, Prädikat, Objekt und adverbiale Konstrukte stehen, dort verfügt XACML über Subjekt, Aktion, Ressource und Umgebung. Eine Anfrage wird wie folgt aufgebaut: WER (Subjekt) will WAS (Aktion) WOMIT (Ressource) unter welchen BEDINGUNGEN (Umgebung) tun? Die einzelnen Bestandteile werden jeweils mit spezifischen Attributen beschrieben. Der Standard legt eine Grundmenge fest, erlaubt aber die Definition weiterer Attribute. In der Umsetzung ist dies durch Absprachen der Partner lösbar. Der Umgang mit Richtlinien kann hingegen nicht rein organisatorisch gelöst werden.

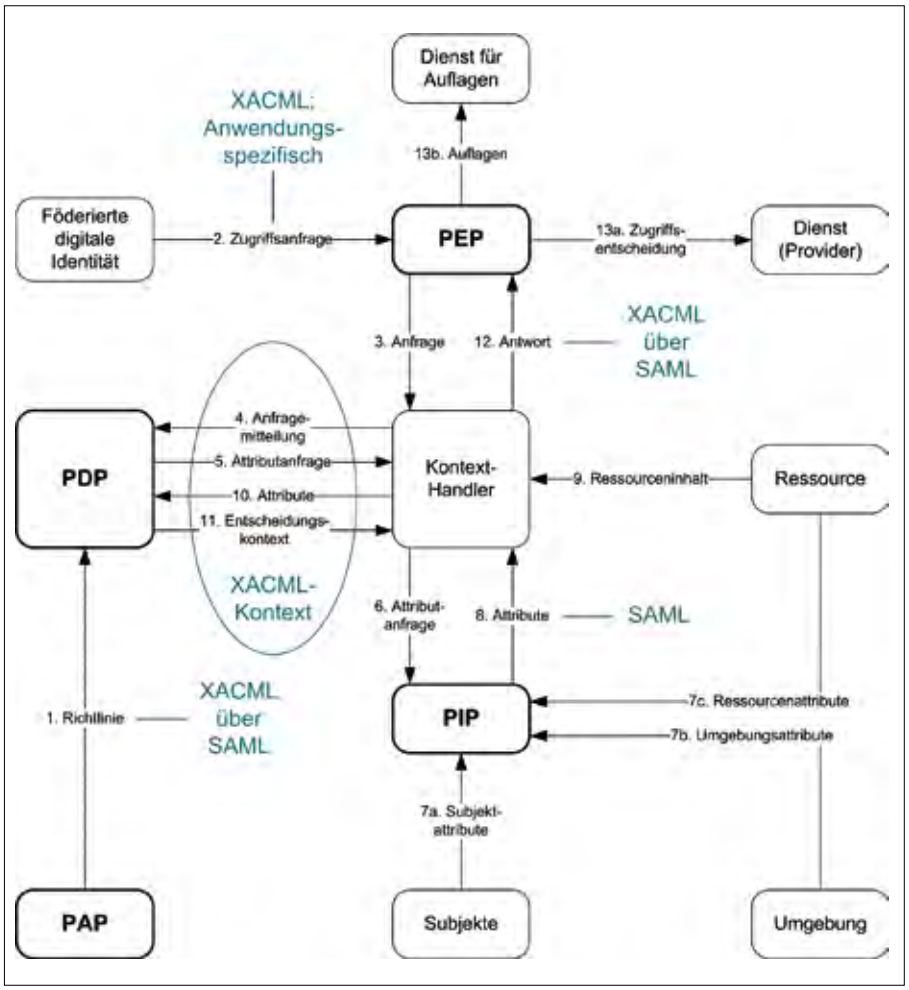

Abb. 2: Erweitertes Komponentenmodell inkl. Zuordnung der Standards auf Basis des XACML-Referenzmodells

Sind leistungsfähige Administrations-Werkzeuge für Richtlinien der Schlüssel zum Erfolg?

Aufgrund der Komplexität der verwendeten Richtlinien sind XACML-basierte Infrastrukturen nicht unproblematisch. Richtlinien in der organisationseigenen Umgangssprache zu formulieren, ist bereits eine komplexe Aufgabe. Diese Richtlinien einem Softwaresystem zugänglich zu machen, bedeutet, umgangssprachliche Richtlinien unter Wahrung ihrer Semantik formalisieren zu müssen. Erst dann können sie in ausführbare Richtlinien umgewandelt werden.

Hier sind entsprechend leistungsfähige Administrations-Werkzeuge notwendig. Ebenso muss eine durch diese Werkzeuge gestützte Evaluierung erstellter Richtlinien möglich sein. Niemand kann die exakten Auswirkungen einer neuen Richtlinie auf eine bereits vorhandene Basis von Richtlinien kennen. Eine solche Basis kann aus tausenden von Richtlinien bestehen. Diese richten sich nach der Weisung der Verantwortlichen einer Ressource. Administratoren sind dafür verantwortlich, dass Richtlinien auf Basis jener Weisung korrekt erstellt, geprüft und in Kraft gesetzt werden. Während aber die Pflege der Sicherheitseinstellungen eines einzelnen Dienstes noch weitestgehend überschaubar ist, wird dies im Umfeld einer ganzen Organisation schwierig. Bei jeder neuen oder geänderten Richtlinie ist zu klären, ob sie den erwünschten Effekt erzielt, Konflikte auftreten, wie diese zu lösen sind und ob wirklich alle möglichen Zugriffe abgedeckt werden.

Eine auf dem XACML-Standard basierende Infrastruktur setzt daher eine vorherige Evaluierung der zu verwendenden Administrations-Werkzeuge voraus. Auf ein reichhaltiges Repertoire an Editier- und Prüffunktionen ist zu achten. Allerdings ist fraglich, ob in Zukunft die aktuellen Mechanismen ausreichen werden.

Welchem Ansatz gehört die Zukunft?

Einen Schritt weiter als ABAC/PBAC geht **Risk-Adaptable Access Control (RAdAC)** [1]. RAdAC erlaubt sehr feingranulare Autorisierungsentscheidungen durch die zusätzliche Einbeziehung von betriebsbedingten/-kritischen Erfordernissen, wie zum Beispiel „Leib und Leben in Gefahr", und den zugehörigen Sicherheitsrisiken, wie zum Beispiel „Veröffentlichung von vertraulichen Informationen an Unbefugte". Existieren dynamisch auftretende, betriebskritische Erfordernisse, so kann der Zugang zu Diensten und Informationen auch unbekannten digitalen Identitäten erlaubt werden. Jedoch nur, falls das Risiko für den Betrieb oder die Nicht-Erreichung eines Zieles höher ist als die durch die Gewährung des Zugriffs auftretenden Sicherheitsrisiken beziehungsweise ein möglicher Schaden.

RAdAC baut auf ABAC/PBAC auf, benötigt jedoch eine umfangreichere Infrastruktur und eine solide Festlegung aller Attribute durch vordefinierte Richtlinien, die in die Autorisierungsentscheidungen einfließen müssen (siehe Abb. 3). Die Entscheidungen selbst basieren auf einer nochmals erweiterten Policy-Basis, so dass ein extrem komplexes Gebilde entsteht, welches mit einigen Traditionen der IT-Sicherheit bricht.

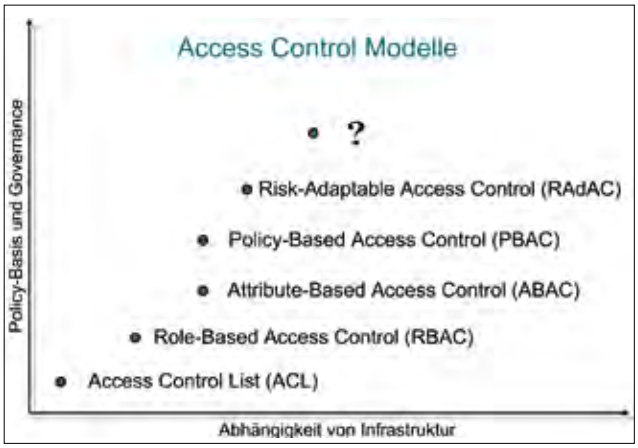

Abb. 3: Einordnung der Access-Control-Modelle bezüglich Voraussetzungen und Abhängigkeit

Eine gemeinsame Studie des National Institute of Standards and Technology (NIST) und der National Security Agency (NSA) geht zum Beispiel davon aus, dass RAdAC nicht vor 2016 im Bereich des U.S. Department of Defence einsetzbar sein wird. Im Gesundheitssektor oder im Unternehmensumfeld besteht hingegen die Hoffnung, dass erste Umsetzungen schon früher erfolgen.

Fazit

Die fortschreitende Entwicklung zu föderiertem Identity and Access Management [2] erfordert ein Umdenken beim Umgang mit Privilegien von Identitäten. Zur organisationsübergreifenden Authentisierung existiert der Quasi-Standard SAML, welcher in allen marktgängigen Produkten etabliert ist. Der kritischere Bereich der Autorisierung von Nutzern ist hingegen noch nicht so weit, da das notwendige Umdenken im Privilegienmanagement (PvM) noch nicht stattgefunden hat. PvM auf Basis von Rollen reicht in Föderationen nicht mehr aus. Es muss durch ein Berechtigungsmanagement abgelöst werden, das durch eine erweiterte Infrastruktur mit Attribut- und Policy-basiertem Access Control sein Potenzial entfalten kann. Es wird erreicht durch feingranulare Autorisierungsentscheidungen ausgelagerter Komponenten.

Mit Hilfe der international etablierten Standards SAML und XACML ist die Grundlage für organisationsübergreifende Infrastrukturen geschaffen. Diese Infrastrukturen erfüllen, mit Hilfe geeigneter, am Markt verfügbarer Administrations-Werkzeuge, die beschriebenen IT-Sicherheits-Anforderungen von föderierten IT-Systemen. Für immer komplexere Anforderungen steht mit RAdAC bereits ein neuer Ansatz bereit. Zeit und finanzielle Mittel sind für die Umstellungen und Erweiterungen der Infrastruktur für föderierte Autorisierung auf Basis von Richtlinien und Attributen notwendig. Potenzielle Partner haben das Umdenken im PvM jedoch eventuell bereits vollzogen und ihre Infrastruktur angepasst. Organisationen sollten daher bereits heute ihre derzeit eingesetzten Mechanismen im Access Management mit den Anforderungen abgleichen und früh die notwendigen Schritte einleiten, um auf sichere Art und Weise organisationsübergreifend agieren zu können. Ein erster Schritt ist die Absprache mit den Partnern, die an einer Identitätsföderation teilnehmen möchten. ■

Literaturhinweise:
[1] **McGraw, Robert W.:** "Risk-Adaptable Access Control (RAdAC)", 2009, http://csrc.nist.gov/news_events/privilege-management-workshop/radac-Paper0001.pdf
[2] **Forschungsbereich Identity and Access Management:** https://www.internet-sicherheit.de/de/forschung/aktuelle-forschungsprojekte/identity-management/

Prof. Dr. Norbert Pohlmann, Informatikprofessor für Verteilte Systeme und Informationssicherheit, Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de)

B.Sc. Michael Gröne, wissenschaftlicher Mitarbeiter des Instituts für Internet-Sicherheit und Projektleiter im Forschungsschwerpunkt Identity Management