DAASI International

Access Control

In der IT gibt es verschiedenste Modelle, auf deren Basis Zugriffsregeln über bestimmte Eigenschaften bzw. Attribute definiert und verwaltet werden können. Welches Modell das richtige ist, hängt dabei von den individuellen Anforderungen und Sicherheitsansprüchen der jeweiligen Organisation ab.

WHITE PAPER

Mit Access Control, zu deutsch Zugriffskontrolle, kann auf Basis zuvor festgelegter Eigenschaften der Zugriff auf eine bestimmte Ressource eingeschränkt werden. Im täglichen Leben funktioniert die Zugriffskontrolle zu Gebäuden oder Veranstaltungen oft ähnlich. Bei einem Konzert wäre die entscheidende Eigenschaft der Besitz der Eintrittskarte oder aktuell auch der Nachweis einer Corona-Impfung.

MANDATORY ACCESS CONTROL (MAC)

Bei Access Control nach MAC erhalten alle Benutzer*innen Labels, die jeweils einem bestimmten Freigabelevel entsprechen. Die Berechtigungen werden für jede Nutzer*in einzeln angelegt und zentral verwaltet; sie können von den Nutzer*innen nicht geändert werden. Insgesamt ist MAC recht rigide und skaliert schlecht und ist damit oft nicht für dynamisch organisierte oder große Organisationen geeignet.
Für kleine Organisationen oder für einzelne Organisationseinheiten mit hohen Sicherheitsanforderungen ist MAC jedoch eine gute Wahl, da es die sicherste Methode zur Zugriffsregelung ist.

DISCRETIONARY ACCESS CONTROL (DAC)

DAC fokussiert bei der Rechtevergabe die zu schützenden Ressourcen bzw. Ressourcen-Gruppen, selbst. Den Ressourcen werden Access-Control-Listen (ACL) zugeordnet. Diese bestimmen, welche Benutzer*innen zugreifen dürfen und prüft, ob diese beispielsweise nur Lese- oder auch Schreibrechte haben, mit denen sie die Ressourcen verändern dürfen. Die Listen können sowohl zentral als auch durch die jeweiligen Ressourcen-Besitzer*innen verwaltet und angepasst werden. DAC kann mit MAC kombiniert werden, indem in die Listen und die jeweiligen Labels anstelle individueller Profile aufgeführt werden.
Mit DAC können Benutzer*innen, vor allem in großen Organisationen, über spezifische Ressourcen-ACLs auch zeitlich begrenzt Zugriff erhalten, um sie mit den für ein Projekt benötigten Rechten auszustatten. Leider liegt hierin auch ein großer Nachteil dieses Access-Control-Modells, da die Mitgliedschaft in mehreren ACL (etwa Standard und projektbezogen) zur Folge haben kann, dass die verschiedenen Rechtestrukturen sich gegenseitig überschreiben oder sich widersprechen. Nutzer*innen können dadurch zu viele Rechte erhalten oder vorhandene Rechte verlieren. Da ACL in der Regel sehr komplex sind, ist es nicht immer einfach den Überblick zu behalten, um

solchen Konflikten vorgreifen zu können. Besonders große Organisationen mit voneinander getrennten Einheiten können dieses Modell dennoch sehr gut einsetzen, um Mitarbeiter*innen von anderen Einheiten schnell onboarden zu können.

ROLE-BASED ACCESS CONTROL (RBAC)

In einem RBAC-Modell werden Berechtigungen auf Basis von Rollen vergeben, wobei das Prinzip des sogenannten „least Privilege" (geringstes Privileg) gilt. Dies bedeutet, dass allen Nutzer*innen über Rollen zunächst nur minimale Rechte eingeräumt werden, bis sie innerhalb der Organisation über weitere Rollen mit mehr Rechten ausgestattet werden. Benutzer*innen können folglich auch mehrere Rollen mit verschiedenen Berechtigungen innehaben. Eine Rollen-Struktur kann individuell an jede Organisation angepasst und, je nach Größe der Organisation, zentral und/oder dezentral verwaltet werden. Hierarchische Strukturen erlauben es auch, zwischen Administrator*innen, die für einen bestimmten Systemteil verantwortlich sind, und Superadministrator*innen, die auf oberster Ebene für das Gesamtsystem verantwortlich sind, zu unterscheiden.
Scheidet eine Person aus der Organisation aus, können der Identität die entsprechende(n) Rolle(n) entzogen werden, womit automatisch auch alle Berechtigungen widerrufen werden. Das funktioniert auch bei einem temporären Ausscheiden. Bei Wiedereintritt kann die Rolle der Identität ohne großen Aufwand erneut zugeordnet werden. Das RBAC-Modell ist demnach besonders dynamisch und einfach zu handhaben. Es ist deswegen eine der am häufigsten verwendeten Zugriffskontrollstrategien. Die Einführung von RBAC benötigt unter Umständen eine längere Anlaufzeit. Rollen- und Berechtigungskonzepte müssen wohl durchdacht sein, damit das Modell auch effektiv angewendet wird.

ATTRIBUTE BASED ACCESS CONTROL (ABAC)

Nach einem ähnlichen Prinzip, allerdings feingranularer zu konfigurieren, gibt es neben RBAC auch ABAC. Hier wird das Recht auf Zugriff nicht prinzipiell über Rollen definiert, sondern über einzelne Attribute der Nutzer*innen, wie Security Clearance, Arbeitsort, Zugehörigkeit zu einer Organisationseinheit oder auch die Rolle als Attribut. Dieser Unterschied macht ABAC um einiges flexibler im Vergleich zu RBAC.
In föderierten Umgebungen erlaubt ABAC die Freigabe von externen Benutzer*innen, ohne dass alle Informationen geteilt werden müssen. Um die Ressourcen innerhalb einer Föderation nutzen zu können, muss mit ABAC nur das für die Freigabe relevante Attribut geteilt werden, sodass die meisten sensiblen Daten (wie insbesondere personenbezogene Daten) nicht weitergegeben werden müssen. Aufgrund des hohen Maßes an Flexibilität und Sicherheit sowie aufgrund der feingranularen Struktur eignet sich ABAC vor allem für große Organisationen mit komplexen Berechtigungsstrukturen.
Bei ABAC ist es besonders wichtig, optimale Grundvoraussetzungen zu schaffen, wie dem sicheren Management der relevanten Attribute, der genauen Definition von Business Logik und/oder den Policys. Der große Vorteil der feingranularen Struktur macht jedoch das Gesamtsystem eher unübersichtlich und es passiert leicht, dass Fehler im System entstehen. Bei größeren notwendigen Änderungen ist es oftmals besser, alles nochmal neu auszurollen, was jeweils mit hohen Aufwänden einhergeht.

RULE BASED ACCES CONTROLL (RUBAC)

Access Control kann auch funktionieren, ohne direkt auf Nutzerrollen einzuwirken. So arbeitet RuBAC mit einer festgesetzten Liste an Regeln, die stringent befolgt werden. Dabei wird eine Erlaubnis nur dann erteilt, wenn eine Regel dies explizit vorsieht, anstatt Zugriff zu gewähren, wenn etwas nicht ausgeschlossen ist („Least Privilege"). Eine Regel kann auch nur für einen bestimmten Zeitrahmen gültig sein, etwa um zu verhindern, dass außerhalb der Bürozeiten auf eine Ressource zugegriffen werden kann. Dies ist insbesondere bei der Verwaltung von vertraulichen Ressourcen hilfreich. Firewalls etwa arbeiten häufig mit RuBAC. Auf Organisationsebene ist RuBAC jedoch oft nicht ausreichend, da Regeln ständig überwacht und überprüft werden müssen, was Zeit kostet und die Flexibilität einschränkt. Da Regeln hier ohne Ausnahme und Nuance befolgt werden, ist es zudem schwierig, Business-Logik in RuBAC zu berücksichtigen.

PRIVILEGED ACCESS MANAGEMENT (PAM)

PAM ist keine generelle Zugriffsregelungsstrategie, sondern befasst sich ausschließlich mit privilegiertem Zugriff. Das betrifft Accounts, die grundsätzlich mehr Rechte benötigen als andere, wie Root-Accounts auf Rechnern oder sonstige administrative Accounts sowie Anwendungsaccounts, über die auf Datenbanken zugegriffen werden kann. PAM beruht auf dem Prinzip „Least Privilege". Dabei können Privilegien sowohl einzelnen Nutzer*innen individuell als auch bestimmten Nutzergruppen wie Administrator*innen zugeordnet werden. Ein Ziel von PAM ist dafür zu sorgen, dass Passwörter von privilegierten Accounts besonders lang und stark sind und häufig geändert werden müssen. Ein weiteres Ziel besteht darin, dass ungewöhnliches Verhalten oder andere Auffälligkeiten bei privilegierten Nutzer*innen, insofern sie überwacht werden, leicht entdeckt werden können. So wird es möglich, schweren Sicherheitslücken und kompromittierten Systemen vorzubeugen.
Solche Systeme sind jedoch oft sehr komplex und können nur wirklich effektiv eingesetzt werden, wenn die entsprechenden Ressourcen in der örtlichen IT-Abteilung zur Verfügung stehen. Sind Ressourcen kein Problem und die Administrator*innen bereit, sich auf ein solches System einzulassen, kann ein besonders hohes Maß an Sicherheit erreicht werden. Viele Best-Practice-Fallbeispiele für Access Control verweisen auf PAM als Modell ihrer Wahl.

FAZIT

Häufig ist es nicht ausreichend, lediglich festzulegen, worauf einzelne Nutzer*innen zugreifen können. Es muss auch sichergestellt sein, dass die Identität mit den Freigaben der Nutzer*innen zusammenpasst. Hier kommt Identity Management ins Spiel. Heutzutage werden beide Ausdrücke, Access Control und Identity Management, durchaus auch synonym verwendet. In der Regel findet man sie jedoch zusammengefasst unter dem Begriff Identity & Access Management (IAM). Dies zeigt, wie eng Identitätsmanagement und Zugriffskontrolle miteinander verbunden sind. Nur wenn Nutzeridentitäten mit sicheren Prozessen verwaltet werden und jeweils aktuell gehalten werden, können die Mechanismen der Access Control auch funktionieren. Dabei ist es oft von Vorteil, das Identity Management zu zentralisieren, um Dubletten in den verschiedenen Datenbanken der angeschlossenen Dienste zu verhindern und den Administrationsaufwand gering zu halten. Um ein möglichst flexibles und damit zukunftsfähiges System zu schaffen, setzt etwa die IAM-Software-Suite didmos auf die Vorteile von RBAC.

Nicht nur der Aspekt der Senkung des Administrationsaufwands und die damit verbundene Kostenersparnis sowie die verminderte Belastung der Mitarbeiter*innen sind die positiven Folgen eines ausgewogenen IAM-Systems. Mit einem gut durchdachten und auf Ihre Organisation angepasstem IAM-System – mit dem richtigen Access-Control-Modell – wird selbstverständlich auch die Systemsicherheit gewährleistet. Interne Prozesse können standardisiert und damit vereinfacht werden.