Martin Meints, Denis Royer

Der Lebenszyklus von Identitäten

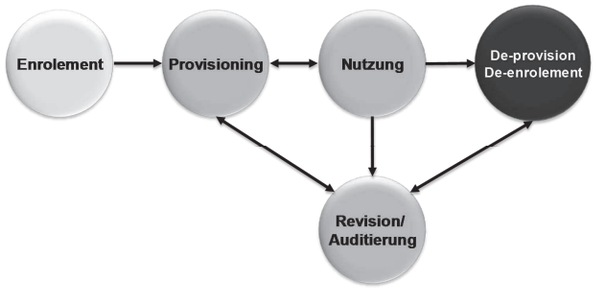
Auditoren für Datenschutz und Datensicherheit kennen das Phänomen: In fast jedem System, besonders aber in zentralen Identitätsmanagementsystemen (IMS), finden sich nicht mehr benötigte Konten oder Nutzer die deutlich mehr Rechte haben, als sie aktuell benötigen.

Eine kleine Anekdote aus der Praxis beleuchtet das Problem: „Ein Auditor versuchte während einer Auditierung herauszufinden, wer in einem mittelständischen Unternehmen die meisten Zugriffsberechtigungen für die IT-Systeme des Unternehmens besaß. Das Ergebnis überraschte nicht nur ihn, sondern auch die Geschäftsführung: Es war ein Praktikant am Ende seines Praktikums. In sechs Wochen, in welchen er durch alle Abteilungen gegangen war, hatte er die jeweils benötigten Zugangsrechte zugewiesen bekommen. Beim Wechsel in die nächste Abteilung wurden diese aber nie wieder entzogen..

Welche Identität betrachten wir in diesem Kontext eigentlich? Wie im Zusammenhang mit IMS üblich sprechen wir nicht von den Identitäten von (physischen) Personen, sondern von deren so genannten partiellen Identitäten innerhalb eines bestimmten kommunikativen Kontexts (s. auch die Definition von partieller Identität im Beitrag von Herrn Hühnlein in diesem Heft). Diese Betrachtungsperspektive macht auch deutlich, dass wir bei Identitätsmanagementsystemen nicht an reinen IT-Systemen denken können, sondern auch die papier- oder kartengestützte Systeme wie etwa klassische Ausweise einbeziehen müssen. Ferner gehören zum Management von Identitäten neben den technischen Systemen auch alle hierfür benötigten Prozesse. Speziell die Prozesse zum Management der Lebenszyklen von (partiellen) Identitäten nehmen hierbei eine Schlüsselrolle ein.

Welche Phasen des Lebenszyklus von Identitäten sind nun zu beachten? Hierzu gibt es eine Reihe von verschiedenen Modellen, die aber alle die folgenden Phasen, teilweise jedoch mit variierenden Begriffen kennen (vgl. Abbildung 1):

Abbildung 1 | Darstellung des Lebenszyklus von (partiellen) Identitäten.



Enrolment: Ein Benutzerkonto wird angelegt, die Bindung zwischen dem Identifier und der physischen Person hergestellt. Benötigte Informationen für die Authentifizierung werden erhoben und gespeichert.

- ***Provisioning oder Management:*** dem Benutzer werden die benötigten Rechte zugewiesen oder entzogen (De-provisioning)
- ***Nutzung:*** Nutzung von Rechten (Authentisierung / Authentifizierung / Autorisierung)
- ***Revision/Auditierung:*** Überwachung / Auditierung der Identitätsmanagementprozesse und zugehörigen Systeme
- ***De-provisioning und De-enrolment:*** Hierzu zählen Deaktivierung / Sperrung / Anonymisierung und letztlich Löschung der Benutzerkonten im Identitätsmanagementsystem.

Erfahrungsgemäß treten vor allem beim Management der Identitäten in den Teilprozessen Provisioning und De-provisioning / De-enrolment Probleme auf. Häufig ist die mangelhafte Integration der Identitätsmanagementprozesse in die Organisation die Ursache dafür. So wird z.B. die Betreuung des IMS und der dazugehörigen Nutzerkonten in der IT-Abteilung angesiedelt. Gleichzeitig stellt man aber nicht sicher, dass alle benötigten Informationen für die Pflege der Rechte in den Systemen dort auch zeitnah und vollständig zur Verfügung gestellt werden.

Auch findet die Vergabe der benötigten Zugangsrechte an Mitarbeitern zum Teil ad-hoc und „*auf Zuruf*“ statt. Gibt es in einer solchen Situation eine interne Auditierung, so bleibt sie weitgehend unwirksam: Infolge fehlender Dokumentation der Beauftragung und Umsetzung von Erteilung und Entzug von Rechten kann man den IST-Stand der bestehenden Rechte zwar feststellen, aber nicht bewerten. Fehlt die Auditierung, bleiben die genannten Probleme möglicherweise gänzlich unbemerkt – hoffentlich ohne negative Folgen für die betroffene Organisation.

Wie kann nun eine Lösung aussehen? Die Beauftragung und die Umsetzung von Änderungen bei Benutzerrechten muss durch standardisierte Prozesse lückenlos dokumentiert und unterstützt werden. Bietet das IMS hierfür keine eigenen Funktionalitäten zur technischen Unterstützung dieser Prozesse, kann man sog. Ticket-Systeme, die auch für die Dokumentation von Serviceanfragen der Nutzer verwendet werden, einsetzen. Ticket-Systeme bieten oft auch Reporting-Funktionen. Kombiniert man diese mit regelmäßigen Reports aus dem IMS über die aktuelle vergebene Rechte, so hat man eine gute Grundlage für eine Auditierung.

Soweit die Theorie, die für kleine und mittlere IMS auch praktikabel ist. Bei großen IMS werden diese Reports schnell derart umfangreich, dass eine sinnvolle Auswertung mit Standardwerkzeugen nur noch unzureichend möglich ist. Hier hilft nur der Einsatz leistungsfähiger Spezialwerkzeuge, welche die in der Organisation für die Auditierung benötigten Informationen auswählen und zusammenführen können. Ein Beispiel hierfür ist die Extraktion der vorgenommenen Änderungen und tatsächlich vergebene Rechte aus Log-Dateien.