Transfer

Zentrale Autorisierungsdienste

Roland Portmann, Leiter Kompetenzzentrum Informations- und Softwaresicherheit, HTA Luzern, roland.portmann@hta.fhz.ch

Gemäss Datenschutzgesetz dürfen Mitarbeiter einer Organisation nur Zugriff auf besonders schützenswerte Personendaten haben, die sie für Ihre Arbeit benötigen. Vergleichbare Anforderungen an den Schutz von Daten bestehen vermehrt auch für andere sensitive Daten (z. B. im Bankenumfeld). Für Datenmutation bestehen häufig noch feingranularere Zugriffsregelungen. Mit den verbreiteten statischen Zugriffsschutzmechanismen, die den Zugriff auf eine Klasse von sensitiven Daten (z. B. ein bestimmtes Feld in einer Datenbankapplikation) von der Identität des Benutzers abhängig machen, können komplexere Anforderungen häufig nicht erfüllt werden. Das Problem liegt darin, dass sehr grosse Datenmengen gleich klassifiziert sind und der Personenkreis, der auf Daten einer bestimmten Klassifizierung zugreifen kann, ebenfalls sehr gross sein kann. So müssen beispielsweise in Spitälern sehr viele Personen auf bestimmte Kategorien von Patientendaten zugreifen können. Applikationen, die in einem solchen Umfeld eingesetzt werden, unterstützen daher vielfach (aber nicht immer!) erweiterte, teilweise dynamische Zugriffsschutzmechanismen, die die wesentlichen Anforderungen des Datenschutzes zu erfüllen vermögen. Die Zugriffsberechtigung auf Datenelemente kann abhängig sein von:

- den Daten selbst: Die Daten erlauben einen Entscheid, ob ein Zugriff erlaubt wird (z. B. Datenowner, Sachbearbeiter, Status eines Dossiers…);
- von einem Workflow-System: Dem Bearbeiter wird ein elektronisches Dossier mit einem Workflow-System zugewiesen. Nur während der Bearbeitung des Workflow-Schrittes hat der Mitarbeiter Zugriff auf die Daten;
- vom Arbeitsplatz: Auf bestimmte Daten kann nur von bestimmten Arbeitsplatzrechnern zugegriffen werden;
- von der Rolle eines Mitarbeiters: Die Applikation «weiss», in welcher Rolle ein Mitarbeiter auf Daten zugreift;
- von der Zeit: Ein Mitarbeiter kann nur auf die Daten zugreifen, wenn er gemäss Einsatzplan in einer bestimmten Rolle tätig ist.

Der Entscheid, ob ein Zugriff auf Daten erlaubt ist, ist damit nicht nur von der Identität des Benutzers, sondern von weiteren, sich ständig ändernden Informationen abhängig. Damit kann aber erst unmittelbar vor dem Zugriff auf die Daten entschieden werden, ob dies zulässig ist.

Viele Applikationen in der Praxis arbeiten mit solchen dynamischen Zugriffsberechtigungen, die auch einer engen Auslegung des Datenschutzgesetzes standhalten können. Wo liegen also die Probleme?

Die Probleme

Untersuchungen in einem Forschungsprojekt zeigten die folgenden Probleme auf:

- Komplexe Zugriffschutzregeln werden in der Applikation häufig mittels Programmierung implementiert. Dies kann zu einer festen «Verdrahtung» des Zugriffschutzes führen, bei der die Administrierbarkeit eingeschränkt ist. Bei Änderungen der internen Prozesse und/oder der Organisationsform kann der Zugriffschutz nicht angepasst werden. Dies kann Umgehungslösungen erzwingen, die das ursprünglich gute Zugriffschutzkonzept aufweichen.
- Durch die Implementierung des Zugriffschutzes im Programmcode wird dieser nicht mehr auditierbar. In komplexen Fällen wird ohne eine Konsultation des Source-Codes keine gesicherte Aussage darüber möglich sein, wer nun genau in welchen Fällen Zugriff auf bestimmte Daten hat.
- Vielfach sind einzelne sensitive Datenelemente redundant in unterschiedlichen IT-Systemen abgelegt. So kann beispielsweise eine Kern-Applikation einen perfekten Schutz auf die Daten implementieren, aber Auszüge dieser Daten können für den organisationsübergreifenden Datenaustausch auch in Form von Office-Dokumenten auf einem Datei-System abgelegt sein. Dateisysteme bieten heute in der Regel nur statische Zugriffschutzmechanismen an.

Einige Gedanken

Man kann sich grundsätzlich fragen, ob der heute zumeist gewählte Ansatz, komplexe Zugriffschutzanforderungen im Programmcode zu

implementieren, korrekt ist. Beim Identity Management hat in den letzten 10 Jahren ein Umdenken stattgefunden. Während ältere Applikationen fast durchwegs eine eigene Benutzerverwaltung implementierten, greifen moderne Applikationen auf Directory-Systeme zu, um die Identität (Authentizität) und die Rolle (Berechtigungsgruppe) des Benutzers festzustellen.

Lösungsansätze

Es gibt heute verschiedene Initiativen, nicht nur die Identitäten, sondern auch die Zugriffschutzanforderungen applikationsübergreifend an einem zentralen Ort zu verwalten. Zusätzlich zum Authentisierungsdienst (z. B. Active Directory) wird ein Autorisierungsdienst implementiert. Applikationen greifen für die Zugriffsentscheide auf diesen Dienst zu.

Verschiedene grosse Firmen (CA, IBM, Oracle Corporation, Sun Microsystems und weitere) arbeiten am OASIS-Standard XACML. XACML ist eine auf XML basierende Beschreibungssprache, die es erlaubt, applikationsunabhängig Regeln aufzustellen. Diese beschreiben, wer in welcher Art und Weise auf Daten (allgemeiner: Ressourcen) zugreifen darf. Definitionen in dieser Beschreibungssprache werden von einem Autorisierungsdienst interpretiert. Applikationen, die mit diesem Autorisierungsdienst arbeiten, fragen vor jeder Operation diesen Autorisierungsdienst an, ob die konkrete Operation zulässig ist. XACML-basierte Autorisierungsdienste befinden sich gegenwärtig noch in einer experimentellen Phase, könnten aber schon bald eine wichtige Rolle in grösseren Organisationen spielen.

In reinen Microsoft-Umgebungen kann mit Hilfe des Autorisierungsmanagers eine zentrale Verwaltung der Autorisierung in einer einzigen Verwaltungskonsole applikationsübergreifend durchgeführt werden. Der Autorisierungsmanager generiert eine XML-Datei, die über den Verzeichnisdienst an verschiedene Applikationen verteilt wird. Eine in die Applikation eingebundene Library führt die Zugriffsschutzentscheide durch.

Ausblick

Es kann damit gerechnet werden, dass in den nächsten Jahren zentrale Autorisierungsdienste in vielen grösseren IT-Umgebungen eine wichtige Rolle spielen werden. Die Hersteller von Applikationen können damit die Applikationen schlanker gestalten. Die Auslagerung von komplexen Autorisierungsmechanismen erleichtert zudem die Erstellung von Standard-Software, da die kundenspezifischen Zugriffschutzanforderungen erst im Rahmen der Einführung festgelegt und implementiert werden können. Mit solchen Autorisierungsdiensten können Zugriffschutzberechtigungen flexibel implementiert werden und es wird auch Nichtinformatikern möglich sein, die implementierten Mechanismen zu verstehen und zu überprüfen. ■

FACHHOCHSCHULE
ZENTRALSCHWEIZ

HTA
HOCHSCHULE FÜR
TECHNIK+ARCHITEKTUR
LUZERN

Literatur, weiterführende Links

- Sun Microsystem: A Brief Introduction to XACML; http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html
- Microsoft: Authorize it: http://msdn.microsoft.com/msdnmag/issues/03/11/AuthorizationManager/