

Authentisierung ist keine Nebensache!

Für Unternehmen wird es immer wichtiger, ihren Kunden oder Mitarbeitern sicheren Zugang über das Internet zu Daten und Anwendungen ihrer Organisation zu bieten. In vielen Fällen führt dies allerdings zu einer Vielzahl unterschiedlicher Authentisierungs- und Autorisierungsverfahren. Eine Möglichkeit, diesen Wildwuchs einzudämmen und gleichzeitig die Sicherheitsrisiken und Kosten zu senken, ist der Einsatz eines vorgelagerten SAML-fähigen Authentisierungsservers.



Marc Bütikofer

Senior Krypto- und Sicherheitsexperte bei Ergon Informatik AG

Immer mehr Unternehmen ermöglichen verschiedensten Personenkreisen den Zugriff auf Teile ihrer IT-Infrastruktur über das Internet und Intranet. Weil es sich dabei meist um geschäftskritische Systeme handelt, müssen diese entsprechend abgesichert werden. Dazu gehört ein adäquates Authentisierungsverfahren. Meist wird die Entscheidung für die Art der Authentisierung auf Grund ökonomischer und sicherheitstechnischer Überlegungen gefällt. Es gibt verschiedene Formen der Authentisierung: Zum Beispiel starke Authentisierung für den Zugriff übers Internet, mittlere Authentisierung für den internen Zugriff oder eine separate Variante für den B2B-Kanal. Das hat zur Folge, dass man in der Praxis häufig mehrere Benutzerverzeichnisse mit verschiedenen Authentisierungsarten und teils überlappenden Benutzergruppen findet.

Ein zentraler Authentisierungsserver

Um die Authentisierung zuverlässigen effizient und nachhaltig zu lösen, bietet sich der Einsatz eines zentralen Authentisierungsservers an, der sich in

eine bereits bestehende Infrastruktur integriert und mit den steigenden Anforderungen eines Unternehmens wachsen kann. Die Vorteile eines vorgelagerten Authentisierungsservers liegen auf der Hand: Zum einen trennt er die Authentisierungslogik konsequent von den umgebenden Komponenten.

Dadurch reduziert sich die Komplexität. Gleichzeitig gewinnen Unternehmen die Flexibilität, die Art der Authentisierung jederzeit abhängig von den Anwendungen, den Benutzergruppen oder anderen Kriterien frei zu wählen. Eine Umstellung des Authentisierungsverfahrens oder die Einführung einer neuen Authentisierung – wie beispielsweise Zertifikatsauthentisierung für speziell sichere Zugriffe – lassen sich so einfach und ohne aufwändige Anpassungen in den Applikationen realisieren.

Modularität und Erweiterbarkeit als wichtige Kriterien

Es ist äusserst wichtig, dass die Authentisierungslösung über eine offene und flexible Architektur verfügt, einfach konfiguriert und rasch in verschiedens-

te IT-Umgebungen integriert werden kann. Auf diese Weise können gleich drei Ziele erreicht werden: Kosteneffizienz, Passgenauigkeit und erhöhte Sicherheit.

Authentisierung ist Bestandteil der Sicherheitsinfrastruktur – und nicht der einzelnen Anwendungen

Die Erfahrung zeigt, dass die Umsetzung von Authentisierungslösung sehr viel mit integrativer Arbeit zu tun hat. Dies gilt speziell bei grösseren Unternehmen, da dort typischerweise schon verschiedene Benutzerverzeichnisse und Authentisierungsarten vorhanden sind. Ein modularer Authentisierungsserver hilft hier, Kosten zu sparen.

Modularität und Erweiterbarkeit sind demnach grundlegende Entscheidungskriterien bei der Wahl des Authentisierungsservers. Dadurch ermöglicht er eine schnelle und kundenspezifische Umsetzung von sicheren Authentisierungsapplikationen. Die unabhängige Anbindung und einfache Integration von verschiedenen Authentisierungsdiensten, Entry-Servern und Web-Applikationen ist sehr wichtig, ebenso der Datenaustausch mit Directories oder Datenbanken.

Single Sign-On mit SAML

Ein leistungsfähiger Authentisierungsserver bietet in Verbindung mit einem Entry-Server und Web-Applikationen Single Sign-On (SSO) auf der Basis von SAML (Security Assertion Markup Language: Stellt Funktionen bereit, um sicherheitsbezogene Informationen zu be-

schreiben und zu übertragen), was die einmalige Authentisierung für mehrere angebundene Dienste erlaubt.

Für die Übertragung authentischer Identitäten („Identity Propagation“) macht es aus mehreren Gründen Sinn, einen Standard wie SAML einzusetzen.

Neben Single Sign-On als Hauptanwendungsszenario ist SAML auch eine standardisierte Integrationschnittstelle für geschützte Webapplikationen: Unterstützt eine Webapplikation – oder der Web-Container in der sie betrieben wird – SAML, so ist deren Integration in eine SAML-fähige Authentisierungsinfrastruktur sehr einfach oder sogar häufig nur eine Angelegenheit der Konfiguration. Die Unterstützung von SAML in der Authentisierungslösung bietet also auch hier Sparpotential, selbst wenn gar kein Single Sign-On erreicht werden soll.

Dies gilt besonders auch bei heterogenen Applikationslandschaften, da SAML nicht nur in der Java-Welt sondern z.B. auch von .NET-Frameworks unterstützt wird.

Ein weiteres Argument ist die Sicherheit: Die Propagierung von Identitäten stellt eine delikate Angriffsfläche dar. Es macht deshalb Sinn, dazu anstelle einer Lösung der Marke „Eigenbau“ ein standardisiertes und geprüftes Verfahren einzusetzen (die korrekte Implementation von SAML wird vorausgesetzt).

Weitere Funktionen

Als andere wichtige Funktionen automatisiert ein Authentisierungsserver die Verwaltung von Berechtigungsnachweisen (Credentials) und ist auf allen gängigen Plattformen lauffähig. Er vereint und verdichtet unterschiedliche Authentisierungsar-

ten wie Passwort, PIN, indizierte TAN oder Matrixkarten, mobile oder SMS-TAN, Token sowie Verfahren wie zum Beispiel Challenge-Response und PKI (Client-Zertifikate).

Sicherheit und Stabilität

Eines gilt es bei der Anschaffung eines Authentisierungsservers in jedem Fall zu beachten: Authentisierungsapplikationen sind per se exponiert, weil sie grundsätzlich anonym erreichbar sind – nicht nur für zugelassene Benutzer, sondern auch für potenzielle Angreifer. Gleichzeitig sind Authentisierungsapplikationen auch sehr mächtig: Sie entscheiden, wer mit den geschützten Applikationen interagieren darf und wer nicht. Diese „explosive“ Mischung macht die Sicherheit und Stabilität von Login-Applikationen absolut zentral und wirkt sich direkt auf die die Sicherheit der damit geschützten Web-Applikationen aus. Dieser Tatsache muss jeder Authentifizierungsserver zwingend Rechnung tragen!