

Wider dem Wildwuchs

Ein vorgelagerter SAML-fähiger Authentisierungs-server löst die Authentisierung und Autorisierung einmal richtig, senkt Sicherheitsrisiken und Kosten und erhöht die Flexibilität.

Quelle: iStockphoto

MARC BÜTIKOFER

Für Unternehmen wird es immer wichtiger, verschiedensten Personenkreisen wie Kunden, Partnern, Lieferanten oder Mitarbeitenden den Zugriff auf Teile ihrer IT-Infrastruktur über das Internet und Intranet zu bieten. 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.

Verschiedene Formen

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. Dies hat zur Folge, dass man in der Praxis häufig mehrere Benutzerverzeichnisse mit verschiedenen Authentisierungsarten und teils überlappenden Benutzergruppen findet und eine Vielzahl unterschiedlicher Authentisierungs- und Autorisierungsverfahren im Einsatz sind.

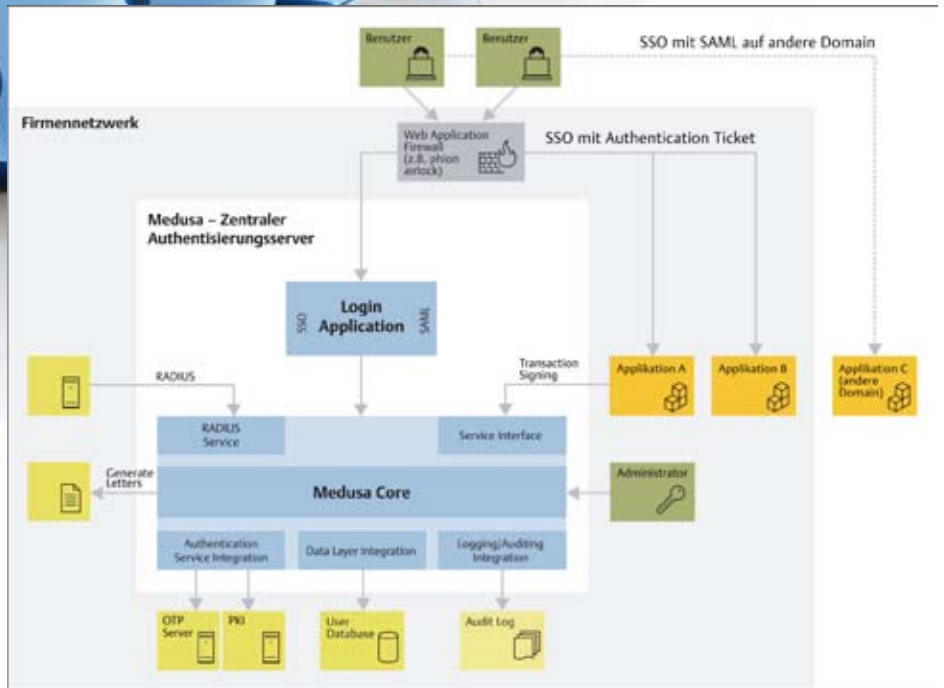
Ein zentraler Authentisierungsserver

Um die Authentisierung 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 umge-

benden Komponenten. Dadurch reduziert sich die Komplexität. Gleichzeitig gewinnen Unternehmen jene erwünschte 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 verschiedenste IT-



Die Grafik zeigt eine mögliche Systemübersicht für die vorgelagerte, zentrale Authentisierung auf der Basis der beiden Produkte phion airlock als Web Application Firewall und dem Medusa Authentifizierungsserver von Ergon. Der Benutzer meldet sich über den Browser für die Web Applikation A an. Die Web Application Firewall leitet den Benutzer beim ersten Zugriff an den Authentisierungsserver weiter, wo er sich je nach der Authentisierungsart ausweist. Der Authentisierungsserver prüft die Angaben und schaltet den Benutzer für die Applikation A frei. Wenn der Benutzer für Applikation B ebenfalls zugelassen ist, kann er darauf ohne weiteren Login zugreifen. Es ist sogar der Zugriff auf Applikation C in einer anderen Domain möglich (Cross Domain Single Sign-On mit SAML). Quelle: Ergon

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

Die Erfahrung zeigt, dass die Umsetzung von Authentisierungslösungen 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, was die einmalige Authentisierung für mehrere angebundene Dienste erlaubt. SAML steht für Security Assertion Markup Language und stellt Funktionen bereit,

um sicherheitsbezogene Informationen zu beschreiben und zu übertragen.

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

Standardisierte Integrationsschnittstelle

Neben Single Sign-On als Hauptanwendungsszenario ist SAML auch eine standardisierte Integrationsschnittstelle 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.

Weitere Funktionen

Als andere wichtige Funktionen automatisiert ein Authentisierungsserver die Verwaltung von Berechtigungsnachweisen (Credentials) und ist auf allen gängigen Plattformen lauffähig. Erweitert und verdichtet unterschiedliche Authentisierungsarten 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 erfordert höchste Sicherheit und Stabilität der Login-Applikation. Neben der richtigen Technologie ist auch die Wahl eines erfahrenen Partners für die professionelle Projektbegleitung entscheidend. ■

Der Autor: Marc Bütikofer ist als Senior Krypto- und Sicherheitsexperte bei Ergon Informatik AG tätig.