

# Zu den Vorteilen eines vorgelagerten Authentisierungsservers Authentisierung ist keine Nebensache!

von Marc Bütikofer

Für Unternehmen und Behörden wird es immer wichtiger, dass sie ihren Kunden, Lieferanten, Partnern oder Mitarbeitern sicheren Zugang über das Internet zu Daten und Anwendungen ihrer Organisation bieten können. In vielen Fällen geht dies allerdings mit einer Vielzahl unterschiedlicher Authentisierungs- und Autorisierungsverfahren einher. Eine Möglichkeit, diesen Wildwuchs einzudämmen und gleichzeitig die Sicherheitsrisiken sowie die Kosten zu senken, ist der Einsatz eines vorgelagerten Authentisierungsservers.

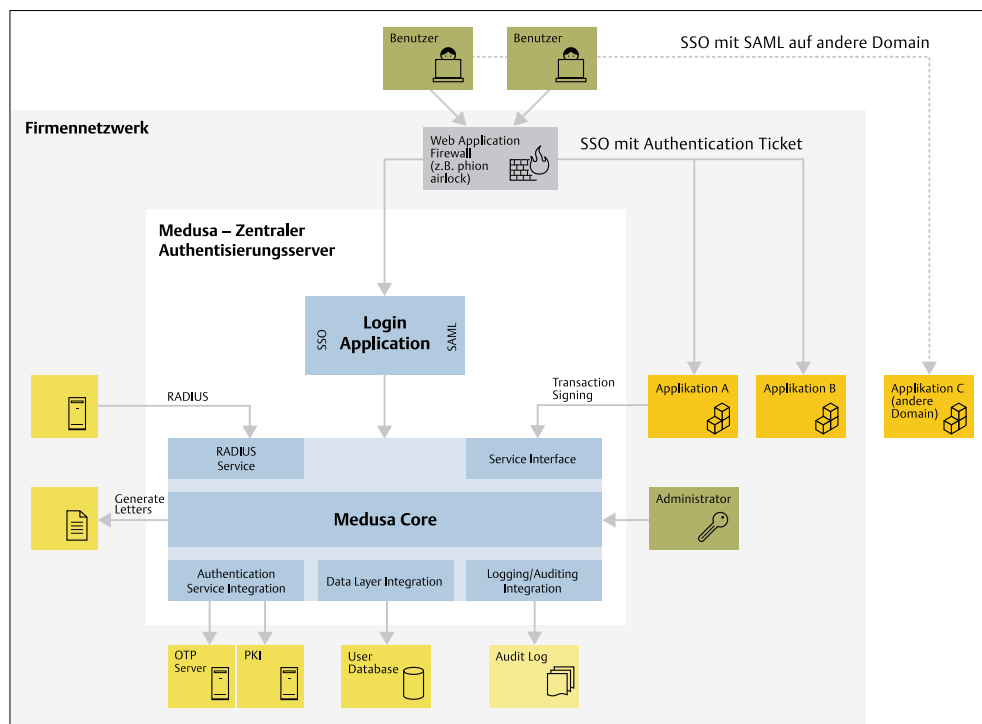


Marc Bütikofer, Senior Krypto- und Sicherheits-experte bei Ergon Informatik AG

Immer mehr Unternehmen ermöglichen immer mehr Personenkreisen den Zugriff auf Teile ihrer IT-Infrastruktur über das Internet beziehungsweise Intranet. Weil es sich dabei oftmals um geschäftskritische Systeme handelt, müssen diese entsprechend abgesichert werden. Dazu gehört ein adäquates Authentisierungsverfahren. Bei den meisten Firmen wird die Entscheidung für die Art der Authentisierung auf der Grundlage ökonomischer und betrieblicher Überlegungen gefällt. In vielen Fällen gibt es nicht nur eine einzige Form der Authentisierung, sondern verschiedene – also zum Beispiel starke Authentisierung für den Zugriff von ausserhalb, 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.

Um die Aufgabe der zuverlässigen Authentisierung effizient und nachhaltig zu lösen, bietet sich der Einsatz eines zentralen Authentisierungsservers an, der sich optimal in eine bereits bestehende Infrastruktur integriert und mit den steigenden Anforderungen eines Unternehmens wachsen kann. Um dieses Ziel zu erreichen, ist es wichtig, dass die Lösung über eine offene und flexible Architektur verfügt. Ebenso zentral ist es, dass das eingesetzte Produkt einfach zu konfigurieren und rasch in verschiedenste IT-Umgebungen integriert werden kann. Auf diese Art



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 Authentisierungsserver 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).

und Weise können gleich zwei Ziele erreicht werden: Kosteneffizienz und Passgenauigkeit.

### **Modularität und Erweiterbarkeit als wichtige Kriterien**

Modularität und Erweiterbarkeit sind demzufolge grundlegende Entscheidungskriterien bei der Wahl eines Authentisierungsservers. Er sollte eine schnelle und kundenspezifische Umsetzung von sicheren Authentisierungsapplikationen ermöglichen. Genauso einfach sollte die unabhängige Anbindung und einfache Integration von verschiedenen Authentisierungsdiensten, Entry-Servern und Web-Applikationen möglich sein, ebenso wie der Datenaustausch mit Directories oder Datenbanken.

Ein leistungsfähiger Authentisierungsserver bietet zudem 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 beschreiben und zu übertragen), was eine einmalige Authentisierung für alle ange-

bundenen Dienste erlaubt. Ausserdem automatisiert er die Verwaltung von Berechtigungsnachweisen (Credentials) und ist auf allen gängigen Plattformen lauffähig. Des Weiteren vereint und verdichtet er unterschiedliche Authentisierungsarten wie Passwort, PIN, Transaktionsnummern (TAN), indizierte TAN oder Matrixkarten, mobile oder SMS-TAN, Token sowie Verfahren wie zum Beispiel Challenge-Response und PKI (Client-Zertifikate) und stellt diese in einer einheitlichen Schnittstelle zur Verfügung.

### **Klare Trennung der Authentisierung von den Applikationen**

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 deutlich und höchste Sicherheit ist garantiert. Gleichzeitig gewinnen Unternehmen die Flexibilität, die Art der Authentisierung jederzeit abhängig von den Benutzergruppen, den Anwendungseigenschaften 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 mühelos und ohne aufwändige Anpassungen in den Applikationen realisieren.

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. Die Sicherheit von Login-Applikationen ist deshalb zentral für die Sicherheit von Web-Applikationssystemen. Dieser Tatsache muss jeder Authentifizierungsserver gebührend Rechnung tragen. ■

Ergon Informatik AG ist vom 12.-15. Mai 2009 an der Orbit in Zürich zu Gast. Besuchen Sie den Autor Marc Bütikofer am Ergon-Stand im IT Security Park.