Factsheet

DirX Access

Vertrauensvolle Zusammenarbeit

Schutz von Web-Anwendungen und -Diensten vor unberechtigtem Zugriff

Die Herausforderung

Unternehmen und Organisationen wie beispielsweise öffentliche Verwaltungen oder Anbieter von Finanzdienstleistungen oder von Diensten im Gesundheitswesen nutzen das Internet, um effizienter und kostengünstiger zu arbeiten und um Dienste preiswert anbieten zu können. Sie gehen Online-Partnerschaften ein, nutzen Informationen und Applikationen auf der Basis Service-orientierter Architekturen mit Web Services und bieten ihre Dienste auch privaten Verbrauchern an. Die Nutzung von Cloud- und SaaS-Anwendungen steigt rapide, da sich gezeigt hat, dass dies für viele Unternehmen und Organisationen durch die kostengünstigere und flexible Art, Anwendungen und Dienste zu nutzen, zu großen Einspareffekten führt. Da mehr und mehr sicherheitskritische Daten ihren Weg ins Internet finden, fordern Organisationen eine Web Access Management Lösung, um Daten gegen unbefugte Nutzung zu schützen und den richtigen Benutzern den richtigen Zugriff auf die richtigen Ressourcen zum richtigen Zeitpunkt zu ermöglichen, ohne die Sicherheit zu gefährden.

Der Aufbau eines agilen, virtuellen Unternehmens, das interne Anwendungen oder private oder öffentliche Cloud- oder Software-as-a-Service Angebote nutzt, führt zu einigen Herausforderungen, um in diesem Umfeld durchgehende Sicherheit zu gewährleisten.

Mit dem Aufkommen von Cloud, Mobile und Social Computing ist die Notwendigkeit für eine verstärkte Zugriffskontrolle stark gestiegen, um die Compliance mit den Authentisierungs- und Autorisierungsrichtlinien der Organisation sicherzustellen. Geschäftspartner müssen ihre Identitätsdaten austauschen oder integrieren, aber dieses muss geschehen, ohne versehentlich Sicherheitslücken zu erzeugen. Um die Benutzerfreundlichkeit zu verbessern, müssen Partner Single Sign-On Verfahren sowohl für interne als auch für externe Cloud-Anwendungen und -Dienste anbieten. Um schnellen Zugriff auf Cloud-Dienste für neue Benutzer bereitzustellen, müssen neue Benutzer schnell im System eingerichtet werden, so dass die aufwendige, manuelle Administration dieser Benutzer in jedem einzelnen Cloud- oder SaaS-Directory vermieden werden kann. Die Partner müssen zudem Sicherheitsmodelle für Online-Transaktionen der Nutzerdaten berücksichtigen, die die Sammlung und Kontrolle der Identitätsinformationen weg von den Online Service Providern in die Hände ihrer Benutzer verlagern und die Verwaltung dieser Informationen in die Hände von Identity Providern legen.

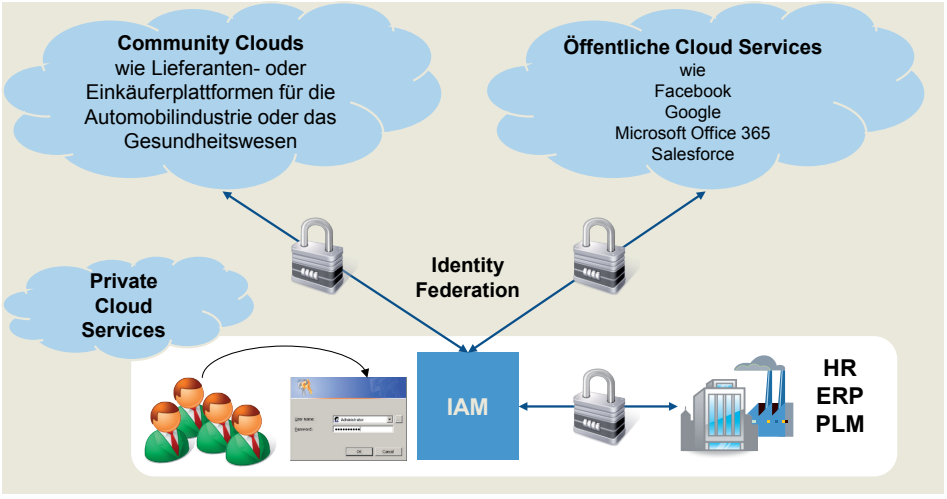
Die Möglichkeit, soziale Identitäten von Google, Facebook oder anderen Identity Providern zur Authentifizierung nutzen zu können, führt zu zusätzlichen Herausforderungen an die Sicherheit beim Zugriff auf Unternehmensanwendungen.

Organisationen, die verhindern wollen, dass Hacker unberechtigten Zugriff auf kritische Daten bekommen, haben die zusätzliche Anforderung, die erforderlichen Authentifizierungsmethoden anhand einer Risikobewertung auszuwählen.

Unsere Lösung

DirX Access ist darauf ausgerichtet, die genannten Herausforderungen zu meistern und ermöglicht den Schutz von Web-Applikationen und Web Services. Die aktuellsten Modelle für das Web Access Management sind bei DirX Access in einem einzigen Produkt implementiert: Authentifizierung, Autorisierung, Audit und Web Single Sign-On (SSO) zusammen mit Identity Federation basierend auf SAML, OAuth und OpenID Connect, sowie Just-in-Time Provisioning, Entitlement Management, die Durchsetzung von Sicherheits-Policies und sichere Web Services sind die wesentlichen Funktionen, um Web Ressourcen sowohl in der Cloud als auch intern im Unternehmen flexibel gegen unberechtigte Nutzung zu schützen.

DirX Access ermöglicht die konsistente Durchsetzung von Sicherheitsrichtlinien sowohl intern im Unternehmen als auch in der Cloud, und bietet dazu zentrale, Policy-basierte Authentifizierungs- und Autorisierungs-Services. Basierend auf seinen Audit-Funktionen unterstützt DirX Access die Compliance mit amtlichen und internen Vorschriften.



Eine Identity Federation Lösung mit DirX Access schafft die Basis für den effizienten und sicheren Zugriff auf Cloud Services

Bull
atos technologies

Die neuesten Sicherheitsmodelle in einem einzigen Produkt

Wesentliche Stärken

- **Vielfältige Authentifizierungsmöglichkeiten und Web Single Sign-On**

  Ermöglicht sicheren und bequemen Zugriff auf Web-Anwendungen und -Ressourcen mit einer einzigen Authentifizierung und stellt eine breite Palette von Authentifizierungsmethoden inklusive Multi-Faktor-Authentifizierung zur Verfügung.
- **Zentrale, Policy-basierte Autorisierung**

  Unterstützt die zentrale und konsistente Durchsetzung von Sicherheitsrichtlinien für den Zugriff auf Web-Anwendungen und -Ressourcen.
- **Standard-basiertes Policy Management**

  Enthält Funktionen zur Verwaltung von Autorisierungs- und Authentifizierungs-Policies basierend auf dem XACML-Standard.
- **Identity Federation**

  Unterstützt Industrie-Standards für Federation wie SAML, OAuth und OpenID Connect und kann sowohl als Identity Provider als auch als Service Provider eingesetzt werden.
- **Authentifizierung mit Identitäten von sozialen Medien**

  Vereinfacht den Authentifizierungsprozess für die Benutzer beim Zugriff auf weniger kritische Ressourcen durch Nutzung von Identitätsprovidern wie Facebook oder Google und daraus resultierender Vermeidung zusätzlicher Logins.
- **Risiko-basierte Authentifizierung**

  Bietet Step-Up-Authentifizierung durch Bewertung des Risiko-Profils der Login-Aktivität.
- **Cloud-Unterstützung**

  Unterstützt standardmäßig Identity Federation mit bekannten Cloud- und SaaS-Providern.
- **Microsoft SharePoint Unterstützung**

  Ermöglicht Identity Federation mit Microsoft SharePoint mittels Claims-basierter Authentifizierung.
- **Zentrale Verwaltung von Sessions**

  Verwaltet Security Sessions mit den relevanten Benutzerinformationen, die in Autorisierungsentscheidungen genutzt werden können.
- **Web Services Security für SOA**

  Ermöglicht die zentrale und konsistente Durchsetzung von Sicherheitsrichtlinien für Web Services in Service-orientierten Architekturen.
- **Administration und Benutzerverwaltung**

  Nutzt LDAP Directory Server zur Benutzerverwaltung und zum Speichern von Konfigurations- und Policy-Daten; jeder Standard LDAP Directory Server kann als Benutzerdatenhaltung dienen.
- **Ausfallsicherheit, Hochverfügbarkeit und Skalierbarkeit**

  Unterstützt Active-Active-Szenarien, um maximale Verfügbarkeit und Ausfallsicherheit sowie Skalierbarkeit und Lastverteilung zu ermöglichen.
- **Unterschiedliche Einsatzmöglichkeiten**

  Integriert sich mit den Applikationen, die geschützt werden sollen, mittels Policy Enforcement Points, die als Plugins in Web Servern oder Application Servern oder anderen Anwendungen eingesetzt werden und unterstützt auch Reverse-Proxy-Konfigurationen.
- **Audit**

  Zeichnet automatisch die Ergebnisse von Authentifizierungs-, Autorisierungs- und anderen sicherheitsrelevanten Ereignissen auf und speichert diese Daten für nachfolgende Analysen.

Ihre Vorteile

- Liefert durchgängige und kostengünstige Sicherheit für die Unternehmens-übergreifende Zusammenarbeit.
- Verbessert in hohem Maße die Benutzerfreundlichkeit und senkt die Kosten für Compliance.
- Ermöglicht den nahtlosen, sicheren und komfortablen Zugriff von Kunden und Geschäftspartnern auf Web-Applikationen und -Ressourcen ohne die Notwendigkeit, deren Identitäten und Passwörter zu verwalten oder die Benutzerverzeichnisse zu synchronisieren.
- Ermöglicht die feingranulare Verwaltung von Berechtigungen für mehrere Anwendungen und Services.
- Ermöglicht, Identitäten sozialer Medien zu nutzen, um Anmeldevorgänge zu vermeiden, wenn Benutzer bereits bei Identity Providern sozialer Medien registriert sind.
- Reduziert das Risiko betrügerischer Aktivitäten durch Stärkung der Authentifizierungsprozesse.
- Ist darauf ausgelegt, sowohl die Anforderungen an hohe Verfügbarkeit und hohe Skalierbarkeit zu unterstützen.
- Unterstützt Millionen von Benutzern in großen und geschäftskritischen Infrastrukturen.
- Nahtlose Integration mit Microsoft Produkten.
- Liefert mittels seiner Audit-Services den Nachweis von Aktivitäten, um die Einhaltung von Vorschriften für den Geschäftsverkehr und von Datenschutzbestimmungen nachzuweisen.
- Eng mit allen anderen DirX-Produkten integriert.

Für weitere Informationen: security@atos.net oder www.atos.net/identity

atos.net

Diese Broschüre wurde auf Papier in Kombination aus 40% Öko-zertifizierten Fasern aus nachhaltig verwalteter Forstwirtschaft und 60% recycelten Fasern gedruckt, welches den aktuellen Umweltstandards (ISO 14001) entspricht. IMPRIM'VERT®

F-Dirx acces-de1