SOA-Sicherheitslösungen
Zur Unterstützung Ihrer Geschäftsziele

Tivoli® software

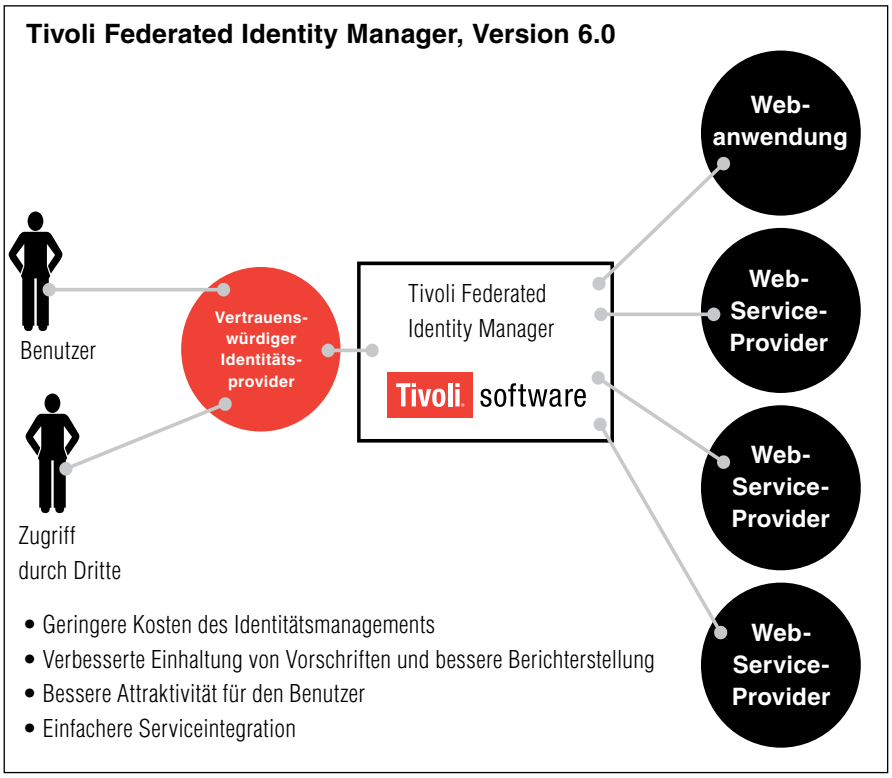
IBM

Sicherheit für Ihre SOA-Umgebungen

Nutzen Sie durch SOA neue Geschäftschancen

Unternehmen müssen heutzutage ebenso beweglich sein wie die Märkte, in denen sie aktiv sind. Globalisierung, wachsender E-Commerce, unerwartete Fusionen und Übernahmen, gestiegener Wettbewerb und neue gesetzliche Bestimmungen können eine Branche über Nacht ändern, da sie sich dramatisch auf Kostenstrukturen, Umsätze, Partnerschaften, Prozesse und Kundenbeziehungen auswirken.

Einige Unternehmen stellt diese Unbeständigkeit vor hohe, zuweilen bedrohliche Hürden. Für ein On Demand Business bedeutet jedoch jede Änderung eine neue Chance, rund um die Uhr und überall auf der Welt zusammenzuarbeiten, Innovationen durchzuführen und seine Märkte besser zu bedienen.



Um diese neuen Chancen zu nutzen, richtet ein On Demand Business die IT mithilfe einer serviceorientierten Architektur (SOA) an seinen strategischen Zielen aus. SOA wird bereits von Unternehmen aus einer Vielzahl von Branchen eingesetzt. Es handelt sich um eine unternehmensweite, standardisierte Integrationsumgebung, die die Unterschiede der Plattformen, Softwarearchitekturen, Sprachen und Netzprotokolle effektiv überwindet.

Mit SOA können Unternehmen die nahtlose Integration von Geschäftsprozessen, Anwendungen und Ressourcen innerhalb des Unternehmens und bei den Partnern unterstützen, um die Services zu verbessern, die Kosten zu senken und vorhandene Systeme wiederzuverwenden.

Die Notwendigkeit erweiterter Sicherheit in einer SOA

Eine SOA-Umgebung integriert zuvor getrennt autorisierte und kontrollierte Domänen, zum Beispiel Geschäftsbereiche und Partner sowie Intranets und Extranets. Services werden in Mainframe-Computern und verteilten Systemen für verschiedene Anwendungen, verschiedene Sicherheitsmodelle und verschiedene Lieferanten bereitgestellt.

Aber gerade die Offenheit einer SOA bringt eine Reihe von Sicherheitsrisiken mit sich. Die „lose Anbindung“ von Anwendungen und IT-Ressourcen führt zuweilen zu Problemen bei der Verwaltung der Benutzerzugriffe, der Entdeckung von Sicherheitslücken der Ressourcen, der Durchsetzung von Sicherheitsrichtlinien und der Integration von Prüfberichten. Über eine SOA-Umgebung verteilte Services können Probleme mit sich bringen, was das Identitätsmanagement, die Nachrichtensicherheit und die Verwaltung der Sicherheitsberechtigungsnachweise betrifft. Darüber hinaus ist es für ein Unternehmen nicht nur kostspielig, sondern auch unpraktisch, die starke Zunahme von Identitäten und sicherheitsrelevanten Ereignissen auf verschiedenen Zugriffsebenen manuell zu verwalten.

Wenn Services über getrennte Unternehmensbereiche und geografische Grenzen verteilt sind, wird es nahezu unmöglich, die für die Einhaltung interner und externer Vorschriften erforderliche Sicherheitsstufe aufrechtzuerhalten. Eine ressourcenbezogene Sicherheit, die dem Schutz bestimmter Datenspeicher oder anderer IT-Ressourcen dient, ist zwar notwendig, aber für dynamische SOA-Umgebungen nicht länger angemessen.

Dementsprechend kommen Unternehmen heutzutage nicht umhin, über zwei wichtige Sicherheitsaspekte nachzudenken. Der erste Aspekt ist die Notwendigkeit, den Benutzer in den Mittelpunkt der Sicherheitsstrategie zu stellen. Der zweite Aspekt ist die Notwendigkeit, die Sicherheitsposition der Umgebung – Netze, Systeme und Anwendungen – aktiv und in Echtzeit zu überwachen und zu analysieren. Störungen müssen schnell und effizient entdeckt, untersucht und behoben werden, damit sie sich möglichst wenig auf die Services und die Kundeninformationen auswirken.

Einführung einer benutzerbezogenen Sicherheitsstrategie

Benutzerbezogene Sicherheit stellt sicher, dass die richtigen Personen im richtigen Kontext den richtigen Zugriff auf Daten und Services erhalten. Diese Strategie eignet sich für SOA-Umgebungen, deren Services ständig mit anderen Services kombiniert und wiederverwendet werden, wobei ein Service einer neuen Benutzergruppe zugänglich gemacht werden kann, für die er ursprünglich nicht vorgesehen war.

Benutzerbezogene Sicherheit bedeutet, dass jeder Benutzer individuell authentifiziert wird und dass seine oder ihre Berechtigung und die Zugriffsebene aufgrund interner Sicherheitsrichtlinien und externer gesetzlicher Bestimmungen verifiziert werden. Der Zugriff wird Benutzern und Anwendungen verweigert, die nicht authentifiziert und nicht autorisiert sind.

Der Schlüssel dazu liegt in einem unternehmensübergreifenden Identitätsmanagement

Benutzerbezogene Sicherheit ist allerdings nur der erste Schritt. In einer SOA-Umgebung können Unternehmen Services von anderen Unternehmen nutzen oder darauf zugreifen; kein Unternehmen möchte sich jedoch der mühseligen und kostspieligen Aufgabe unterziehen, Benutzer von anderen Unternehmen zu verwalten. Aufgrund der Struktur eines expandierenden Netzes wächst die Zahl der Benutzeridentitäten, die authentifiziert, autorisiert und verwaltet werden müssen, exponentiell, wenn der Umgebung weitere Services und Unternehmen hinzugefügt werden.

Daher wird eine zentrale, unternehmensübergreifende (föderierte) Identitätsmanagementlösung benötigt, in der jede Identität nur einmal verwaltet wird. Eine föderierte Identität ist eine eindeutige Benutzeridentität – eine Art von „digitalem Pass“ –, die von vertrauenswürdigen Vertragspartnern anerkannt und akzeptiert wird.

Dadurch kann ein Benutzer von einem Föderationspartner aus auf sichere und vertrauenswürdige Weise auf Ressourcen eines anderen Partners zugreifen – auf verschiedene Mainframe-Computer und verteilte Umgebungen, auf verschiedene Sicherheitsmodelle und verteilte Services.

Insofern kann föderiertes Identitätsmanagement die Kosten des Identitätsmanagements erheblich reduzieren. Es unterstützt den Einsatz von SOA-Anwendungen, da es Identitäten auf mehreren Plattformen, Anwendungen und Services bereitstellt. Außerdem erhöht es die SOA-Sicherheit, da es sicherstellt, dass die Sicherheitsrichtlinien bei den föderierten Partnern konsistent angewandt werden.

Darüber hinaus ermöglicht föderiertes Identitätsmanagement einem Unternehmen, Identitätsdaten über seine Benutzer an vertrauenswürdige Partner weiterzugeben. Durch gemeinsame Nutzung von Identitätsdaten kann ein Partnerunternehmen Informationen über eine fremde Identität (zum Beispiel eines Kunden, Lieferanten oder Mitarbeiters) vom Unternehmen dieses Benutzers beziehen.

Föderiertes Identitätsmanagement befähigt eine SOA-Umgebung, den folgenden Sicherheitsanforderungen gerecht zu werden:

- ***Authentifizierung –*** *Eine einheitliche Identitätsmanagementlösung für die gesamte Infrastruktur kann Benutzeridentitäten auf kosteneffiziente Weise ordnungsgemäß authentifizieren und verwalten.*
- ***Autorisierung –*** *Ein automatisiertes System für Zugriffe und Berechtigungen kann den Benutzer einmal identifizieren und anschließend die Identität des Benutzers automatisch mehreren Systemen, Services und Infrastrukturkomponenten zuordnen. Dies trägt zur Wahrung der Vertraulichkeit, der Integrität und der Verfügbarkeit von Daten und Datenquellen bei.*
- ***Prüfung und Einhaltung von Vorschriften –*** *Die ordnungsgemäße Einhaltung von Vorschriften und Richtlinien bezieht alle Probleme mit ein, die durch Authentifizierung und Autorisierung entstehen. Sicherheitskontrollen sowie Berichts- und Prüffunktionen bilden einen integralen Bestandteil einer SOA-Umgebung, was die Administration und die Richtlinienverwaltung betrifft.*

Höhere Attraktivität für den Benutzer

Föderiertes Identitätsmanagement kann auch den Komfort für Onlinebenutzer deutlich steigern: Die Benutzer können einfach und sicher mit Single Sign-on (SSO) und transparenter Kennwort- und Identitätsüberprüfung in SOA-Umgebungen navigieren.

Beispielsweise besucht eine Kundin die Website ihrer Bank und meldet sich an. Nachdem ihre Identität authentifiziert worden ist, kann sie ihren Kontostand überprüfen, eine Onlineüberweisung tätigen, bei einem anderen Anbieter einen Kredit beantragen und ihre Courtagekonten prüfen – alles zur selben Zeit ohne weitere Anmeldungen.

Bessere Sicherheitsüberwachung zur Verbesserung der Serviceverfügbarkeit

Die Offenheit und die höhere Komplexität der Infrastrukturbeziehungen in SOA-Umgebungen können die Zahl der Sicherheitslücken innerhalb von Anwendungen und der zugrunde liegenden Infrastruktur erhöhen. Außerdem sind SOA-Umgebungen in höherem Maße anfällig für XML-basierte Attacken, die zu Unterbrechungen und Ausfällen führen können. Diese Faktoren erhöhen den Bedarf an einer Echtzeitüberwachung und Analyse auf sicherheitsrelevante Ereignisse bezogener Daten, damit Sicherheitsrisiken und Störungen rasch erkannt werden können, bevor sie die Services beeinträchtigen.

Der Schlüssel ist zentrales, heterogenes Management sicherheitsrelevanter Ereignisse

Eine heterogene, echtzeitorientierte Lösung für die Verwaltung der Sicherheitsoperationen kann eine zentrale Konsole bereitstellen, über die Sie diese Sicherheitsrisiken in Ihrer SOA aufspüren, untersuchen und verwalten können. Sie muss Sicherheitsdaten aus verschiedenen Bereichen korrelieren und analysieren:

- *Geschäftsanwendungen*
- *Anwendungsserver und Datenbanken*
- *Netzinfrastruktur*
- *Hostprotokolle*
- *Sicherheitskomponenten*
- *Identitäts- und Zugriffsmanager*

Eine zentrale Plattform zur Verwaltung sicherheitsrelevanter Ereignisse sichert nicht nur die Serviceverfügbarkeit, sondern vereinfacht auch die Behebung von Problemen bei der Überprüfung und der Einhaltung von Vorschriften. Dazu dienen die Speicherung der Protokolle, die Überwachung der Richtlinien, die Verfolgung von Störfällen und die Erstellung von Langzeitberichten.

Prüfen Sie IBM Tivoli-Lösungen für SOA-Sicherheit und -Verwaltung

IBM stellt ein umfassendes Portfolio von Lösungen bereit, mit deren Hilfe Sie maximale Sicherheit, Benutzerfreundlichkeit und überlegene Leistung für SOA-Umgebungen sicherstellen können. IBM SOA-Sicherheitsprodukte bieten folgen Vorteile:

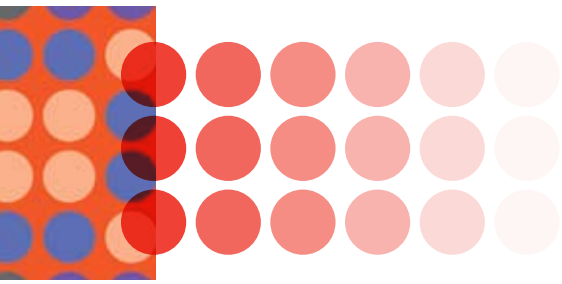
- *Kontextbezogene Sicherheit für Personen, Prozesse, Informationen und Technologien*
- *Reduzierung der Kosten des Identitätsmanagements und der Sicherheitsoperationen*
- *Höhere Attraktivität für den Benutzer und höhere Serviceverfügbarkeit*
- *Aufbau sicherer Business-Communitys durch einfachere Integration mit Partnern*
- *Maximale Rentabilität für Ihr Unternehmen und Ihre Partner*
- *Rationalisierung der Prüf- und Konformitätsprozesse in einer heterogenen Umgebung*

IBM Tivoli Federated Identity Manager unterstützt die Verwaltung föderierter Identitäten und den Zugriff auf SOA-basierte Web-Services, die mehrere Sicherheitsdomänen abdecken, darunter Mainframe-Computer und verteilte Umgebungen. Das Produkt ist in der Lage, auf effiziente Weise Identitäten zu verwalten und den Benutzern auf Vertrauensbeziehungen basierenden Zugriff auf Informationen und Services zu ermöglichen. Unternehmen, die SOA- und Web-Services einsetzen, bietet Tivoli Federated Identity Manager auf Richtlinien basierendes, integriertes Sicherheitsmanagement für föderierte Web-Services.

IBM Tivoli Federated Identity Manager for z/OS verfügt über ein einfaches, lose verbundenes Modell für z/OS-Umgebungen und ermöglicht die effiziente Verwaltung der Identitäten und des Zugriffs auf Ressourcen, die sich auf mehrere Unternehmen oder Sicherheitsdomänen erstrecken.

IBM Tivoli Federated Identity Manager Business Gateway ist ein schlankes Produkt mit geringem Speicherbedarf, das ohne großen Aufwand konfiguriert und bereitgestellt werden kann und die Integration mit Business Partnern und Lieferanten vereinfacht. Es ermöglicht Unternehmen, Daten sicher und wirtschaftlich gemeinsam mit Partnern zu nutzen, um sichere Business-Communitys zu schaffen.

IBM Tivoli Identity Manager ist eine sichere, automatisierte, auf Richtlinien basierende Benutzermanagementlösung, mit der Sie Identitäten, Kennwörter und den Zugriff auf SOA-Services sowie auf traditionelle Anwendungen effektiv verwalten können. Dadurch werden SOA-Implementierungen unterstützt, in denen die Zahl der zugriffsberechtigten Benutzer gestiegen ist und deren Services und Anwendungen zu modularen Anwendungen kombiniert worden sind. Zentrale Richtlinien in Tivoli Identity Manager dienen der Automatisierung von Workflows auf der Basis eindeutiger Geschäftsprozesse und ermöglichen ein sicheres Identitätsmanagement für SOA-Anwendungen.



Die Software unterstützt die schnelle Einrichtung neuer Benutzerkonten und Kennwörter für Mitarbeiter und Kunden; Benutzer können ihre eigenen Kennwörter zurücksetzen und synchronisieren. So können Unternehmen die Operationen ihres Sicherheitsmanagements transparenter gestalten und schnell Berichte für Sicherheitsprüfer erstellen.

IBM Tivoli Access Manager ist eine Familie integrierter Produkte, die dafür konzipiert sind, umfassende Sicherheit für SOA-Umgebungen sicherzustellen:

IBM Tivoli Access Manager for Business Integration ist eine plattformübergreifende Sicherheitsmanagementlösung für IBM WebSphere MQ, die die systemeigenen Sicherheitsservices von WebSphere MQ auf diejenigen von IBM WebSphere MQ Extended Security Edition aufrüstet. Es bietet Datenschutz auf Anwendungsebene für Anwendungen auf der Basis von WebSphere MQ, ohne dass diese modifiziert oder gar erneut kompiliert werden müssen.

IBM Tivoli Access Manager for e-Business ist eine vielseitige Lösung für Probleme der Authentifizierung und der Autorisierung. Tivoli Access Manager-Implementierungen, die in erster Linie auf Web-Anwendungen ausgerichtet sind, reichen von einfachem Single Sign-on bis zu komplexeren Sicherheitsinfrastrukturen. Damit kontrollieren Sie das Wachstum und die Komplexität, behalten eskalierende Verwaltungskosten im Griff und bewältigen die Probleme, die mit der Implementierung von Sicherheitsrichtlinien für eine Vielzahl von Web- und Anwendungsressourcen einhergehen.

IBM Tivoli Access Manager for Enterprise Single Sign-On ist eine auf Unternehmen abgestimmte Single Sign-on-Lösung auf der Basis von Passlogix-Technologie – ein integraler Bestandteil des IBM Security Identity Management-Portfolios. Die Lösung enthält eine einfache Authentifizierungsfunktion für Microsoft® Windows®, Web, Java™, UNIX® Telnet, unternehmensintern entwickelte Anwendungen und hostgestützte Mainframeanwendungen. Sie arbeitet mit Tivoli Access Manager for e-Business und Tivoli Identity Manager zusammen und bietet leistungsfähige Funktionen, die sich des Durcheinanders der Kennwörter innerhalb des Unternehmens annehmen.

IBM Tivoli Access Manager for Operating Systems ist ein komfortables, leistungsfähiges Sicherheitssystem, das geschäftskritische Anwendungen, Dateien und Betriebsumgebungen sicher einschließt, um unbefugten Zugriff zu verhindern. Diese Sicherheitsfunktion hindert Personen innerhalb und außerhalb des Unternehmens, unbefugt auf wertvolle Daten von Kunden, Mitarbeitern und Business Partnern zuzugreifen.

IBM Tivoli Security Operations Manager bietet eine zentrale Plattform und ein Dashboard für die Überwachung, Korrelation, Analyse und Untersuchung von Sicherheits- und Richtlinienverstößen. Die Plattform analysiert und korreliert sicherheitsrelevante Ereignisse bei Anwendungen, Geräten und Systemen überall in der verteilten IT-Umgebung. Damit können Unternehmen, die SOA eingeführt haben, die Sicherheit erhöhen, ohne das Sicherheitspersonal oder die Sicherheitsausrüstung aufzustocken. Das Produkt verbessert nicht nur die Sicherheitsoperationen, sondern kann auch die Zeit für die Behebung von Sicherheitsverstößen reduzieren, die die Serviceverfügbarkeit beeinträchtigen. Es stellt eine zentrale Plattform bereit, um Berichte über die Sicherheitslage des Unternehmens an Prüfungs- und Konformitätsinitiativen zu senden.

Profitieren Sie von einer sicheren SOA-Umgebung

IBM Tivoli-Produkte stellen vielseitige, integrierte Lösungen bereit, die Ihrem Unternehmen folgende Vorteile bieten:

- *Einfachere Integration von Systemen und Anwendungen*
- *Unterstützung von Sicherheits- und Konformitätsinitiativen*
- *Höhere Attraktivität für den Benutzer*
- *Größere Betriebszeit und Verfügbarkeit*
- *Schaffung umsatzgenerierender Verkaufschancen*
- *Verringerung des Verwaltungsaufwands*
- *Senkung der Betriebskosten*

Weitere Informationen

Wenn Sie mehr über Tivoli-Lösungen erfahren möchten und wissen möchten, wie Sie für ordnungsgemäße SOA-Sicherheit sorgen können, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter:

ibm.com/tivoli

Tivoli-Software von IBM

Tivoli-Software stellt ein umfassendes Paket von Angeboten und Funktionen zur Unterstützung von IBM Service Management zur Verfügung – ein skalierbares, modulares Verfahren, das Ihrem Unternehmen effizientere und effektivere Services bereitstellt. Tivoli deckt den Bedarf für Unternehmen jeder Größe und ermöglicht es Ihnen, durch Integration und Automatisierung von Prozessen, Arbeitsabläufen und Aufgaben hervorragende Services für die Unterstützung Ihrer Geschäftsziele bereitzustellen. Die sichere, auf offenen Standards basierende Tivoli Service-Management-Plattform wird ergänzt durch proaktive Lösungen für operatives Management mit durchgängiger Transparenz und Kontrolle. Sie wird außerdem gestützt durch den hervorragenden IBM Kundendienst, die IBM Unterstützungsfunktion und ein aktives Geschäftsumfeld von IBM Business Partnern. Des Weiteren können Tivoli-Kunden und -Partner gegenseitig ihre bewährten Verfahren nutzen, indem sie an unabhängigen IBM Tivoli-Benutzergruppen auf der ganzen Welt teilnehmen. Besuchen Sie:

www.tivoli-ug.org

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

IBM, das IBM Logo und ibm.com sind eingetragene Marken der IBM Corporation.

Tivoli, WebSphere und z/OS sind Marken der IBM Corporation in den USA und/oder anderen Ländern.

Java und alle Java-basierenden Marken und Logos sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Microsoft ist eine Marke von Microsoft Corporation in den USA und/oder anderen Ländern.

UNIX ist eine Marke von The Open Group in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Hergestellt in den USA
10-06

© Copyright IBM Corporation 2007
Alle Rechte vorbehalten.

TAKE BACK CONTROL WITH Tivoli®

TIB10253-DEDE-00