

Umfassende, kosteneffiziente Sicherheitslösungen, die Onlinezusammenarbeit und Unternehmenswachstum ermöglichen



Highlights

- ***Umfassende, leistungsfähige Sicherheitslösungen für plattformübergreifende Sicherheit im ganzen Unternehmen***
- ***Schnellere Implementierung von Anwendungen und Services durch ein starkes Fundament aus Sicherheitstechnologien***
- ***Kein unbefugter Zugriff auf vertrauliche Daten oder Verwendung solcher Daten, wenn dies eine Verletzung der Datensicherheit oder einen Verstoß gegen geltende Vorschriften zur Folge haben könnte***
- ***Schutz des Unternehmens vor internen und externen Bedrohungen durch den Einsatz leistungsfähiger und flexibler Sicherheitsmaßnahmen***
- ***Senkung der Gesamtkosten bei gleichzeitiger Berücksichtigung effizienter Compliance-Initiativen***
- ***Verwaltung von Benutzeridentitäten und Zugriffsrechten während des gesamten Benutzerlebenszyklus***
- ***Einfachere und sicherere Onlinezusammenarbeit zwischen Interessengruppen***
- ***Beseitigen sicherheitsbedingter Hürden, die den Ausbau der Geschäftstätigkeit behindern können***



Für Unternehmen wird es zunehmend schwieriger, mit den steigenden Kundenerwartungen und dem schnellen Wandel Schritt zu halten. Durch die wachsende Anzahl digitalisierter Geräte wie Karten, Ausweisen und Telefonen rücken die reale und die digitale Welt immer enger zusammen. Steigende Transaktionsvolumen, um Zugang zu Geld, Privilegien und geschützten Daten zu erhalten, stetig zunehmende Benutzerzahlen, darunter Mitarbeiter, Geschäftspartner, Patienten, Bürger und Verbraucher, und immer mehr Dienstleistungen, die es notwendig machen, dass Menschen sicher auf ihre Daten zugreifen können – durch diese Anforderungen werden IT-Prozesse und -Infrastrukturen immer stärker belastet. Solche Entwicklungen bewirken zwar einerseits neue Chancen für ein Unternehmen, andererseits führen neue Technologien wie Virtualisierung und Cloud-Computing jedoch auch zu mehr Komplexität und neuen Sicherheitsrisiken.

Insbesondere die Bereiche Identity und Access Management sowie Anwendungs-, Infrastruktur- und Informationssicherheit, die bei nicht ausreichender Berücksichtigung Wettbewerbsfähigkeit und Wachstum erheblich beeinträchtigen können, stellen IT-Abteilungen im Hinblick auf Sicherheits- und Compliancefragen vor immer größere Herausforderungen. Idealerweise sollten Unternehmen auf Infrastrukturen zurückgreifen können, die sie bei der Nutzung innovativer Geschäftschancen unterstützen und nicht behindern.

Mit dem Aufbau von Infrastrukturen, die zur Kostensenkung beitragen und die intelligent, sicher und genauso dynamisch wie das moderne Wirtschaftsleben sind, geht unmittelbar die Notwendigkeit einher, Sicherheitsrisiken strategisch und über alle Sicherheitsbereiche hinweg zu betrachten und zu kontrollieren. Der Schlüssel zum erfolgreichen Risikomanagement in einer dynamischen Infrastruktur besteht in der Schaffung eines Fundaments aus Sicherheitsmaßnahmen, das Ihnen die flexible und schnelle Bereitstellung leistungsfähiger Geschäfts- und IT-Services ermöglicht und gleichzeitig dazu beiträgt, die Kosten für Management, Administration und Betrieb der Sicherheitsinfrastruktur zu senken.

Mit der IBM Tivoli-Software steht Ihnen ein umfassendes Portfolio mit Lösungen für Security, Risk und Compliance Management zur Verfügung, die Ihnen helfen, die notwendige Sicherheit für eine dynamische Infrastruktur umzusetzen. Diese Sicherheitslösungen beinhalten die ganze Bandbreite an Sicherheitsfunktionalität, die notwendig ist, um Personen, Prozesse und Informationsrisiken in einer Umgebung zu berücksichtigen und gleichzeitig die Servicebereitstellung zu verbessern und Kosten zu senken:

- *IBM Tivoli Identity and Access Assurance – Ermöglicht berechtigten Personen zur richtigen Zeit den effizienten und regelkonformen Zugriff auf die richtigen Ressourcen*
- *IBM Tivoli Data and Application Security – Schützt die Integrität und Vertraulichkeit von Unternehmensdaten und Transaktionen vom Browser bis zur Festplatte*
- *IBM Tivoli Security Management for z/OS – Schutz und Überprüfung kritischer Services auf der zuverlässigsten und widerstandsfähigsten Plattform*

Diese Lösungen bieten umfassende Sicherheit über alle Identitäten, Daten und Informationen, Anwendungen, Prozesse und Infrastrukturen hinweg. Jedes Angebot stellt Funktionalität für automatisiertes Compliance Management bereit, sodass Sicherheitsmaßnahmen, Security Management, Prüfung und Compliance einen geschlossenen Kreislauf bilden. Durch Integration eines Compliance Management-Mechanismus in alle Produktangebote ergeben sich Synergieeffekte, die dazu beitragen, die konsistente Einhaltung von Vorschriften plattformübergreifend sicherzustellen und den Nutzen für die Kunden zu steigern.

„Bei der diesjährigen RSA-Konferenz war Tivoli mit seinen Identity Management-orientierten Angeboten, die immer enger mit dem Produktportfolio für Compliance Management verknüpft sind, ganz eindeutig wegweisend. Diese Kombination aus Richtlinien- und Identifikationstechnologien und Lösungen zur Aktivitätsüberwachung bietet einen ganzheitlicheren Ansatz ...“

Merv Adrian, IT Market Strategy

Mit IBM Tivoli-Lösungen für Security, Risk und Compliance Management können Unternehmen in Bezug auf die IT-Sicherheit auf Produkte eines einzigen Anbieters zurückgreifen, wodurch sich die Komplexität verringern und die Gesamtbetriebskosten reduzieren lassen. IBM kann als anerkannter Anbieter auf langjährige Erfahrung in der Entwicklung und Implementierung umfassender Sicherheitslösungen für Unternehmen auf der ganzen Welt zurückblicken. Mit Lösungen von IBM können Sie ein Sicherheitskonzept entwickeln, das Ihre Ziele besser unterstützt – ein Konzept, das die sichere Zusammenarbeit zwischen wichtigen Interessengruppen erleichtert und die sicherheitsbedingten Hürden beseitigt, die das Unternehmenswachstum behindern können.

IBM Tivoli Identity and Access Assurance

Angesichts einer steigenden Anzahl an Benutzern, Anwendungen und Zugriffspunkten stehen Unternehmen vor der Herausforderung, Identitäten während des gesamten Benutzerlebenszyklus verwalten zu müssen. Ziel ist, den bequemen Zugriff auf eine Vielzahl an Anwendungen zu ermöglichen, während gleichzeitig ein hohes Maß an Sicherheit und die Einhaltung entsprechender Vorschriften sichergestellt ist. Mit dem Funktionsspektrum von IBM Tivoli Identity and Access Assurance für Bereiche wie Identity Management, Access Management und Complianceprüfung für Benutzer können Unternehmen sicherstellen, dass die richtigen Benutzer zeitgerecht auf die richtigen Informationen zugreifen können. Die Lösung zentralisiert und automatisiert das Benutzermanagement und ergänzt Identity und Access Management zu einem



geschlossenen Kreislauf; leistungsfähige Funktionalität wird nicht nur für das Zuweisen und Durchsetzen von Benutzerzugriffsrechten, sondern auch für die Überwachung von Benutzeraktivitäten und zum Erkennen und Beheben von Sicherheitsverletzungen bereitgestellt.

Tivoli Identity and Access Assurance bietet die folgenden Hauptmerkmale:

- *Identity Management – Angefangen beim Anlegen neuer Benutzer und Zuweisen geeigneter Zugriffsrechte über das Ändern von Benutzerrollen und Berechtigungen bis hin zum Aufheben von Benutzerzugriffsrechten am Ende des Benutzerlebenszyklus*
- *Access Management – Sichere Authentifizierung von Benutzern, einschließlich Single Sign-on, und Durchsetzen von Benutzerzugriffsrichtlinien, nachdem ein Benutzer authentifiziert wurde*
- *Complianceprüfung für Benutzer – Überwachung, Prüfung und Meldung der Benutzeraktivitäten, um die Einhaltung organisationsbezogener Richtlinien und behördlicher Vorschriften zu unterstützen und das Risiko interner Sicherheitsbedrohungen zu reduzieren, indem Benutzer im Hinblick auf regelwidriges Verhalten überwacht werden*

Tivoli Identity and Access Assurance ist eine umfassende und benutzerfreundliche Lösung für Identity und Access Management, die sich sehr leicht implementieren lässt. Sie kann in Kombination mit einer großen Auswahl an Identitätsrepositorys verwendet und problemlos für die Verwaltung großer Benutzergruppen eingesetzt werden. Darüber hinaus ermöglicht sie die Automatisierung von Prozessworkflows, wodurch die Verwaltungseffizienz erhöht und kostspielige Fehler weitestgehend vermieden werden. Durch das von Tivoli Identity and Access Assurance unterstützte Compliance Management werden Identity und Access Management ergänzt und zu einem geschlossenen Kreislauf vervollständigt. Benutzerzugriffsaktivitäten werden automatisch erfasst und zentral abgeglichen, um dann in einem Dashboard für die Einhaltung von Sicherheitsbestimmungen zusammenfassend dargestellt zu werden. Anhand von Überwachungsberichten können Sie feststellen, ob Benutzeraktivitäten mit den Berechtigungen und Richtlinien Ihres Unternehmens im Einklang stehen. Mithilfe des Dashboards und der Berichtsfunktion werden außerdem nicht richtlinienkonforme Aktivitäten hervorgehoben, sodass entsprechende Maßnahmen zu ihrer Beseitigung ergriffen werden können.

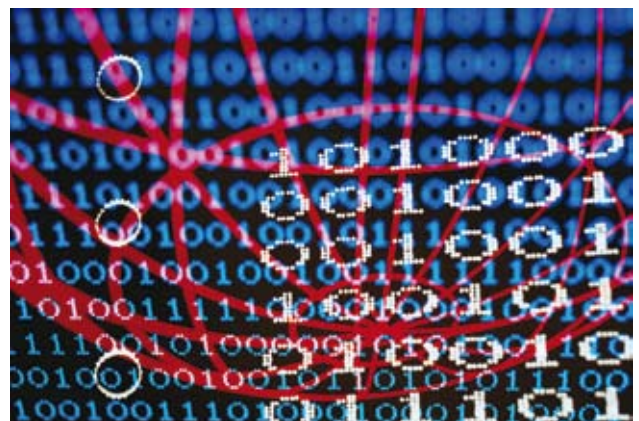
Mit Tivoli Identity and Access Assurance stellt IBM die besten Leistungsmerkmale und Tools des IBM Identity und Access Management-Portfolios in einer einzigen Lösung bereit, die den gesamten Benutzerlebenszyklus berücksichtigt. Mithilfe dieser Lösungen können Unternehmen ihr Serviceangebot verbessern, da sie die Zusammenarbeit über rollenbasierte Portale ermöglicht, den schnellen Rollout neuer Services erleichtert und Single Sign-on unterstützt. Mit Tivoli Identity and Access Assurance können Unternehmen die Kosten für die Verwaltung von Konten, Gruppen, Richtlinien, Identifikationsdaten und Zugriffsrechten während des gesamten Benutzerlebenszyklus senken, da sie eine integrierte Lösung eines einzigen Anbieters nutzen können. Hierdurch können die Gesamtkosten und die Komplexität der Lösung minimiert und den Benutzern gleichzeitig der schnelle Zugriff auf benötigte Ressourcen ermöglicht werden. Durch die integrierte Unterstützung von Compliance-Initiativen, einschließlich der zentralen und automatisierten Funktionalität für Complianceprüfberichte, der zuverlässigen Überwachung von Benutzeraktivitäten und den Funktionen zum Durchsetzen strikter Kennwortrichtlinien, können Unternehmen Risiken besser handhaben.

IBM Tivoli Data and Application Security

Störungen, bei denen es zu Datenverlusten kommt, sind heutzutage keine Seltenheit. Sie können dramatische Auswirkungen auf das Geschäftsergebnis eines Unternehmens haben. Insbesondere Angriffe auf persönliche und vertrauliche Daten haben zahlreiche Kontrollbehörden und Normungsorganisationen dazu veranlasst, weiter gefasste und strengere Sicherheitsmaßnahmen für Daten (archivierte ebenso wie aktuell verwendete Daten), einzufordern. Darüber hinaus verdoppelt sich die Menge der verfügbaren Daten alle 18 Monate, was die Bemühungen, für eine sichere interne und ausgelagerte Speicherung der Daten zu sorgen, zusätzlich erschwert.²

Anwendungen gehören mittlerweile zu den Hauptangriffspunkten bei Verletzungen der Datensicherheit, wobei 75 Prozent der Angriffe auf der Ebene von Webanwendungen stattfinden.¹ Die steigende Komplexität moderner Anwendungen zusammen mit dem steten Bemühen, den Zugriff auf Anwendungen für die Benutzer zu vereinfachen, die Informationen gemeinsam nutzen müssen, hat zur Folge, dass die Anwendungen eines Unternehmens anfälliger als je zuvor sind.

IBM Tivoli Data and Application Security ist eine umfassende Lösung, die Unternehmen beim Schutz von Daten und Anwendungen unterstützt, indem überprüfbare Zugriffskontrollen bereitgestellt, die differenziertere Steuerung von Benutzerberechtigungen ermöglicht und die Verwaltung von Schlüsseln für die Datenverschlüsselung zentralisiert wird. Diese leistungsfähige Lösung erlaubt den umfassenden Schutz sensibler Daten in unternehmensinternen Speichersystemen und innerhalb kritischer Anwendungen. Hierdurch ist es Unternehmen möglich, Vorgaben und behördliche Vorschriften einzuhalten und die Zuverlässigkeit von Daten und Anwendungen zu erhöhen.



Tivoli Data and Application Security bietet die folgenden Hauptmerkmale:

- *Differenziertere Verwaltung von Benutzerberechtigungen, angefangen bei der Anwendungsbis hin zur Betriebssystemebene*
- *Zentrale Verwaltung und Durchsetzung von Nutzungsrechten und Sicherheitsrichtlinien, die eine differenziertere Berechtigungsprüfung und die Zugriffssteuerung auf Datenebene ermöglicht*
- *Zentrale Verwaltung von Verschlüsselungsschlüsseln sowohl für Band- als auch für Plattenspeichersysteme*
- *Umfassende und automatisierte Überwachung und Berichterstellung für Benutzeraktivitäten*
- *Zentrale, automatisierte Erstellung von Complianceberichten und Management von Protokollen, die im Hinblick auf eine Vielzahl an Verordnungen und Branchenstandards wie PCI DSS, Basel II und ISO 17799 angepasst ist*

Mit Tivoli Data and Application Security stellt IBM eine integrierte Lösung leistungsfähiger Sicherheitsfunktionen aus dem Tivoli-Softwareportfolio bereit, die einer breiten Palette an Anforderungen im Bereich Daten- und Anwendungssicherheit Rechnung trägt.

Mit Tivoli Data and Application Security können Unternehmen ihren Service verbessern, indem die sichere gemeinsame Nutzung von Daten durch interne und externe Benutzer vereinfacht wird, was auch webbasierte Services einschließt. Dank der Unterstützung des zentralen Security Managements können Unternehmen die mit isolierten Sicherheitsmaßnahmen verbundenen Kosten senken: Verwaltungsaufgaben werden vereinfacht und zentralisiert, redundante Sicherheitssysteme werden vermieden. Zudem können die Vorzüge einer integrierten Plattform im Hinblick auf eine optimierte Verwaltung und Durchsetzung von Richtlinien genutzt werden. Außerdem kann die Lösung dazu beitragen, den unbefugten Zugriff auf sensible Daten und ihre Verwendung zu verhindern und somit Verletzungen der Datensicherheit und die Nichteinhaltung von Vorschriften zu vermeiden.

IBM Tivoli Security Management for z/OS

Der IBM Mainframe setzte lange Zeit Maßstäbe im Hinblick auf die Bereitstellung geschäftskritischer Sicherungstechnik. Mit IBM Tivoli Security Management for z/OS wird die wegweisende Sicherheitstechnologie der IBM z/OS-Plattform verbessert, indem integrierte, automatisierte und vereinfachte Sicherheitsfunktionalität für Mainframes bereitgestellt wird. In dieser umfassenden Lösung werden die wichtigsten Funktionen aus dem Portfolio der IBM System z-Sicherheitssoftware zusammengeführt, um Organisationen bei der automatisierten Erstellung von Complianceberichten, der Prozessoptimierung und der Reduzierung von Kosten und Risiken zu unterstützen.



Tivoli Security Management for z/OS bietet die folgenden Hauptmerkmale:

- *Verbessertes Risk Management und bessere Richtlinien-compliance für IBM System z durch Definition und Durchsetzung von Sicherheitsrichtlinien basierend auf den spezifischen Sicherheitsanforderungen des jeweiligen Unternehmens. Unternehmen können über Resource Access Control Facility (RACF) die Einhaltung von Sicherheitsrichtlinien proaktiv erzwingen, interne Sicherheitsfehler vermeiden, nicht konforme Sicherheitsbefehle identifizieren und Benachrichtigungen ausgeben lassen, wenn es sich um riskante Befehle handelt.*
- *Vereinfachte Verwaltung von Sicherheitsfunktionen und wirkungsvolleres User Management, was zur Erhöhung der Effizienz und Reduzierung von Fehlern beitragen kann. Mit Tivoli Security Management for z/OS kann die Produktivität sowohl von Administratoren als auch von Prüfern erhöht werden, indem eine wirkungsvollere gruppen- und rollenbezogene Aufgabenverwaltung unterstützt wird. Änderungen an der Sicherheitskonfiguration können ohne Beeinträchtigung der Produktion getestet und potenzielle Konflikte zwischen mehreren unternehmensinternen RACF-Datenbanken proaktiv identifiziert werden.*
- *Umfassende Überwachung im Hinblick auf Sicherheitsbedrohungen, Änderungen an der Prüfkfiguration und die Ressourcennutzung. Mit Tivoli Security Management for z/OS können Änderungen an festgelegten Referenzkonfigurationen sowie der Missbrauch von Berechtigungen erkannt werden, wodurch sich das Risiko von Insiderbedrohungen reduzieren lässt.*
- *Umfassende Compliancefunktionen mit plattformübergreifender Protokollsammlung, leistungsfähiger Datenanalyse und vordefinierten Berichtsfunktionen, die in Ihrem Unternehmen betriebssystem-, anwendungs- und datenbankübergreifend nutzbar sind. Diese Funktionalität ermöglicht das Aufzeigen der Einhaltung von Branchenvorschriften, behördlichen Bestimmungen und Standards wie PCI, SOX, GLBA, HIPAA, FISMA und BASEL II. Protokollierung und Berichterstellung können an die individuellen Anforderungen jeder IT-Abteilung angepasst werden.*

Die Kombination der Sicherheitsfunktionalität von Mainframes, RACF, Tivoli Security Management for z/OS und anderen Tivoli-Sicherheitsprodukten für Mainframe-Computer ermöglicht einem Unternehmen den Aufbau einer Sicherheitszentrale, in der Security Management und Sicherheitsrichtlinien für eine dezentral organisierte Unternehmensumgebung zentralisiert und standardisiert werden können. Diese Zentrale unterstützt das Identity Management für den gesamten Benutzerlebenszyklus, Richtlinien für die Zugriffssteuerung, föderiertes Identity Management, Encryption Key Management und Complianceüberwachung und -berichterstellung.

Mit Tivoli Security Management for z/OS können Unternehmen ihr Serviceangebot verbessern, indem Sicherheitsmaßnahmen zusammengeführt und somit die sichere Zusammenarbeit und ein höheres Maß an Zuverlässigkeit ermöglicht werden. Durch eine automatisierte und vereinfachte Verwaltung trägt die Lösung zur Kostensenkung im Unternehmen bei, indem die Produktivität gesteigert und der komplexe und aufwändige Betrieb von Mainframe-Computern vereinfacht wird. Die Lösung bietet außerdem leistungsfähige Sicherheitsmechanismen und Funktionen für die Erstellung von Complianceberichten, die das Risk Management im Unternehmen unterstützen, indem Identifikation und Abwehr interner und externer Sicherheitsbedrohungen für den Mainframe und das erweiterte Unternehmensnetz ermöglicht werden.

Ganzheitliches Security Management

Die Tatsache, dass IBM im Bereich der Sicherheitstechnologien führend ist, ist eine Folge unseres breit angelegten Lösungsportfolios, unseres riesigen Netzes aus Servicespezialisten und unserer dynamischen Business Partner-Community. Bei der Entwicklung und Unterstützung offener Standards ist IBM wegweisend. Unsere Sicherheitslösungen bieten daher eine breite Plattformunterstützung.

Diese IBM Tivoli-Lösungen für Security, Risk und Compliance Management vereinigen in sich die Leistungsfähigkeit und Zuverlässigkeit, die unsere Kunden brauchen und erwarten, was Merv Adrian von IT Market Strategy zu folgender Feststellung veranlasste: „Bei der diesjährigen RSA-Konferenz war Tivoli mit seinen Identity Management-orientierten Angeboten, die immer enger mit dem Produktportfolio für Compliance Management verknüpft sind, ganz eindeutig wegweisend. Diese Kombination aus Richtlinien- und Identifikationstechnologien und Lösungen zur Aktivitätsüberwachung bietet einen ganzheitlicheren Ansatz ...“³



Unsere umfassenden Lösungen ermöglichen Unternehmen den Aufbau eines breiten Sicherheitsfundaments, das den Schutz von Benutzern, Daten, Anwendungen und Plattformen unternehmensweit unterstützt. Mit den Lösungen von IBM kann sich Ihr Unternehmen unsere langjährige Erfahrung zunutze machen, um eine bessere Servicequalität zu ermöglichen und gleichzeitig Kosten zu senken und Risiken zu minimieren.

Weitere Informationen

Weitere Informationen zu IBM Tivoli-Softwarelösungen für Security, Risk und Compliance Management erhalten Sie bei Ihrem IBM Ansprechpartner, bei Ihrem IBM Business Partner oder auf der folgenden Website:

ibm.com/tivoli/solutions/security

IBM Deutschland GmbH
Pascalstrasse 100
70569 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, ibm.com, RACF, System z, Tivoli und z/OS sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese oder weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter:

ibm.com/legal/copytrade.shtml

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

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

Diese Veröffentlichung darf ohne schriftliche Genehmigung der IBM Corporation weder vervielfältigt noch übertragen werden.

Die Produktdaten wurden zum Datum ihrer ersten Veröffentlichung auf ihre Korrektheit überprüft. Die Produktdaten können von IBM jederzeit ohne vorherige Mitteilung geändert werden. Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele von IBM.

Jeder Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. Es obliegt allein dem Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Einhaltung aller relevanten Gesetze und gesetzlichen Bestimmungen beraten zu lassen, die sich auf seine Geschäftstätigkeit und alle Maßnahmen auswirken können, die er im Hinblick auf die Einhaltung solcher Bestimmungen durchführen muss. IBM erteilt keine Rechtsberatung und gibt keine Garantie bezüglich der Compliance von IBM Produkten oder Services mit jeglichen relevanten Gesetzen und Verordnungen.

- 1 Stasiak, Ken, „Web Application Security“, *Information Systems Control Journal*, 6. Jahrgang, ISACA, 2002. www.isaca.org/Content/ContentGroups/Journal1/20023/Web_Application_Security.html
- 2 „Data Volume is Becoming Unmanageable, Say Executives“, *Government Technology News Report*, 5. August 2008. www.govtech.com/gt/articles/385068
- 3 Adrian, Merv, „IBM Touts Software's Role in Infrastructure Efficiency“, *Market Strategies for IT Suppliers*, 19. Juni 2009. <http://mervadrian.wordpress.com/2009/06/19/ibm-touts-software-role-in-infrastructure-efficiency>

© Copyright IBM Corporation 2009
Alle Rechte vorbehalten.

TIB14008-DEDE-00



Recyclebar, bitte recyceln!