Lösungen für Sicherheitsmanagement
zur Unterstützung Ihrer geschäftlichen Zielsetzungen

Tivoli software

IBM

Lösungen für Sicherheitsmanagement

Weniger Sicherheitslücken und mehr Effizienz durch zentrales Management und konsistente Ausführung von IT-Sicherheitsprozessen

ON DEMAND BUSINESS

Sicherheit ist eine Grundvoraussetzung – und bietet Geschäftschancen

Die Sicherheit von IT-Infrastrukturen war schon immer ein Thema von besonderer Bedeutung. Und mit jedem Tag wird dieser Aspekt für Unternehmen wichtiger, da erfolgreiche Unternehmen durch zunehmende globale Verbindungen die Effizienz ihrer Prozesse optimieren und sich zusätzliche Marktanteile sichern. Diese neue Dimension von weltweiten Verbindungen bringt jedoch auch ein wachsendes Potenzial an Bedrohungen und Risiken mit sich – und damit auch die Notwendigkeit einer klar strukturierten, auf Richtlinien basierenden Sicherheitslösung.

Typische Herausforderungen in Bezug auf die Sicherheit:

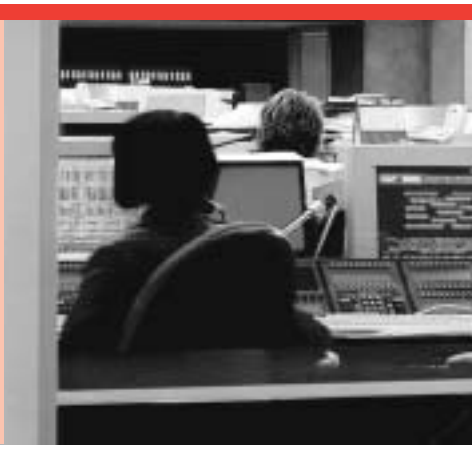
- *Die zunehmende Zahl an Benutzern belastet Administratoren, die diese Benutzer betreuen und verwalten müssen.*
- *Heterogene Systeme, Anwendungen und Speicherbereiche mit Benutzer-ID-Informationen, die nicht synchronisiert sind, können nicht vertrauenswürdige Daten enthalten.*
- *Externe und interne Sicherheitslücken bedrohen den Ruf und die Marke des Unternehmens.*
- *Compliance- und Auditanforderungen zwingen Unternehmen, konsistente Richtlinien für Unternehmensrevisionen und Datensicherung zu implementieren.*

In Anbetracht dieser komplexen Anforderungen stellt sich die Frage, wie man den Kosten und den Sicherheitslücken in Bezug auf die IT-Sicherheit begegnet. Die Antwort ist schnell gefunden: Sie brauchen eine effiziente Lösung, die Informationen, Personen, Know-how und Infrastruktur integriert – und zwar im gesamten Unternehmen. Gehen Sie daher das Thema Sicherheit mit einem zentralisierten, automatisierten Ansatz an. Dann werden Sie feststellen, dass Ihre Infrastruktur in der Lage sein wird, die unterschiedlichsten, wertschöpfenden Geschäftsinitiativen zu unterstützen.

Eine gemeinsame Sicherheitsstrategie trägt dazu bei, den wachsenden Anforderungen zur Einhaltung von Richtlinien gerecht zu werden. Da dieser Aspekt auch bei den täglichen IT-Abläufen immer wichtiger wird, müssen verständliche Sicherheitsrichtlinien implementiert, die Prozesse gemäß dieser Richtlinien ausgeführt und Auditfunktionen eingerichtet werden, mit deren Hilfe die Einhaltung dieser Richtlinien überwacht werden kann.

*„Innerhalb der nächsten zehn Jahre wird sich der Schwerpunkt der Tätigkeit des Sicherheitsverantwortlichen vom Management der IT-Sicherheitsprojekte und -mitarbeiter hin zur Unterstützung der Business-Manager verlagern, um mehr Effizienz und Effektivität zu erreichen. Des Weiteren werden die Vereinfachung der Einhaltung von Richtlinien und Standards, sowie die Steigerung der Wertschöpfung von Geschäftsanwendungen zu seinem Aufgabenbereich gehören.“**

Forrester Research



Security Management-Lösungen von IBM ermöglichen eine unternehmensweite Sicht dieser Thematik und tragen dazu bei, die Sicherheitsprobleme in Ihrem Unternehmen zu lösen und Geschäftschancen optimal zu nutzen.

- *Optimierung von Leistung und Verfügbarkeit geschäftskritischer Anwendungen durch unternehmensweiten Schutz von IT-Ressourcen*
- *Freisetzung von IT-Mitarbeitern, Ressourcen und Budgets für Initiativen mit hohem geschäftlichen Nutzen durch zentrales, automatisches und unkompliziertes Sicherheitsmanagement*
- *Aufbau stabiler Geschäftsbeziehungen zu Kunden und Geschäftspartnern durch effiziente Bereitstellung von Identitäten und Datenzugriffsmöglichkeiten*
- *Optimierung der Reaktionsfähigkeit auf Endbenutzeranforderungen durch Möglichkeiten für Single Sign-On (SSO) und Self-Service-Funktionalität*
- *Schnelle und effektive Konzentration von Ausgaben und Ressourcen auf sich bietende Geschäftschancen anstelle wiederkehrender Routineprozesse bei Sicherheitscodings und Verwaltungsaufgaben*
- *Vereinfachung der Einhaltung von Unternehmens- und behördlichen Richtlinien durch Integration des Identitäts- und Zugriffsmanagements*

Letztendlich helfen Ihnen IBM Security Management-Lösungen beim Wandel zum On Demand Unternehmen, einem Unternehmen, dessen Geschäftsprozesse – integrierte End-to-End-Prozesse im gesamten Unternehmen und mit wichtigen Partnern, Lieferanten und Kunden – kurzfristig und schnell auf alle Kundenanforderungen, Marktchancen oder externe Bedrohungen reagieren können.

Prozessinterne und -übergreifende Umsetzung von Best Practices

IBM bietet ein breites Spektrum an Lösungen für das Sicherheitsmanagement in Ihrem Unternehmen, mit denen Sie Sicherheitsressourcen und Prozesse überwachen, anpassen und verwalten können. Somit sind Sie in der Lage, schnell auf die kontinuierlichen Veränderungen bei den Anforderungen an Ihr Unternehmen zu reagieren.

Mit IBM Lösungen können Sie Automatisierungs- und Integrationsbestrebungen sowohl innerhalb von IT-Prozessen als auch darüber hinaus umsetzen. Gestalten Sie Ihre Prozesse noch effizienter und nahezu fehlerfrei. Entscheiden Sie sich für eine durchgängige Transparenz in Ihrem Unternehmen, um Probleme und Geschäftschancen präzise identifizieren und schnell mit den entsprechenden Maßnahmen darauf reagieren zu können.

Lösungen sind dann besonders hilfreich, wenn sie flexibel für aktuelle und auch zukünftige Prozesse eingesetzt werden können. IBM bietet Unterstützung bei der Implementierung von Best Practices für Automatisierungsansätze bei folgenden Prozessen:

- COBIT (Control Objectives for Information and related Technology)
- COSO (Committee of Sponsoring Organizations of the Treadway Commission)
- ITIL (Information Technology Infrastructure Library)
- Eigene, spezielle Prozesse

Sowohl beim Sicherheitsmanagement als auch in anderen Bereichen des Infrastrukturmanagements können Sie mit Unterstützung von IBM Lösungen Ihre Best Practices ermitteln und konsistent umsetzen. Hierzu gehören:

- *Definition von Richtlinien (IT- und Unternehmensrichtlinien)*
- *Definition von Prozessen zur Implementierung und Realisierung dieser Richtlinien*
- *Identifizierung von Workflows – Angabe der Aufgaben, die zur Ausführung eines Prozesses automatisiert werden*
- *Gemeinsame Datennutzung, damit Prozesse nahtlos miteinander kommunizieren können*
- *Automatische Ausführung von Workflows und Datenaustausch*

Kontinuierliche Optimierung und Stabilisierung Ihrer Prozesse
IBM Security Management-Lösungen unterstützen geschlossene Regelkreissysteme. Dabei implementieren Sie nicht nur die gewünschte Richtlinie oder Funktion, sondern versetzen Ihre Systeme auch in die Lage, Veränderungsbedarf zu erkennen, auf die sich ändernden Bedingungen zu reagieren und die Veränderungen für Auditzwecke zu verfolgen. Gleichzeitig identifizieren Sie weitere Möglichkeiten zur Maximierung der Sicherheit und Optimierung des Sicherheitsmanagements.

Das Leistungsspektrum, das Sie brauchen – heute und morgen
IBM verfügt bei den Sicherheitslösungen über das Spektrum und das fundierte Know-how, das Sie für Ihre geschäftlichen Herausforderungen brauchen. Das Tempo bestimmen Sie dabei selbst. So können Sie beispielsweise Ihre vorhandenen Sicherheitsprozesse bereits jetzt optimieren und zu einem späteren Zeitpunkt den Grad der Automatisierung nach Ihren Vorstellungen erhöhen.

Heutzutage ist das Sicherheitsmanagement kein integrierter Einzelprozess, sondern vielmehr eine Reihe lose gekoppelter Aktivitäten, die mehrere Prozesse umspannen. Mit dem verfügbaren IBM Portfolio können Sie alle Aspekte des Sicherheitsmanagements prozessübergreifend berücksichtigen. Hierzu gehören Prozesse in den von Analysten in der Regel festgelegten Kategorien:

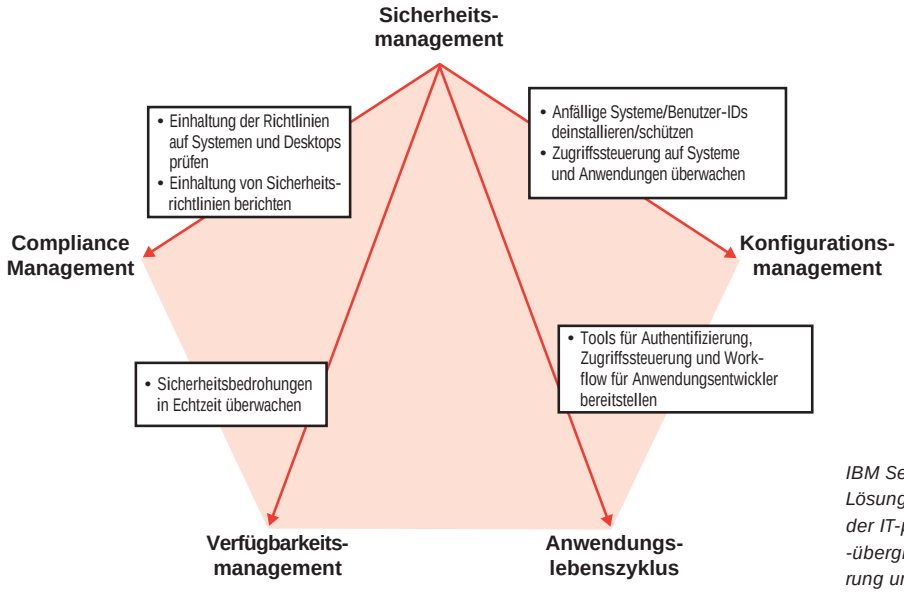
- *Identitäts- und Zugriffsmanagement*
- *Sicherheitslückenmanagement*
- *IT-Compliance-Management*

Das Diagramm zeigt die Schnittstellen des Sicherheitsmanagements mit Prozessen im gesamten Portfolio der IBM Tivoli-Software.

Management von Benutzer-IDs und Zugriffsregeln im gesamten Unternehmen
Mit Hilfe von IBM Software können Sie das Management von ID-Daten zentralisieren, das Management von ID-Änderungen vereinfachen und Zugriffsmöglichkeiten konsistent verwalten.

Kosten senken mit IBM Tivoli Identity Management-Software
Mit Hilfe des IBM Tivoli Identity Managers können Sie die Bereitstellung/Zurücknahme und das Management von Benutzer-IDs zentralisieren und automatisieren. Mit dieser Software können Sie IDs und erforderliche Änderungen durch Anpassungen an interne Sicherheitsrichtlinien problemlos verwalten:

- *Benutzerprüfung – Prüfung der Gültigkeit jedes Benutzerkontos auf jeder Ressource*
- *Benutzerbereitstellung – Richtige Konfiguration des Benutzerzugriffs für jede Ressource und schnelle Reaktion auf Änderungen*
- *Benutzerproduktivität – Einrichtung des effizienten Zugriffs für Benutzer auf gültige Ressourcen*



IBM Security Management-Lösungen unterstützen bei der IT-prozessinternen und -übergreifenden Automatisierung und Integration.

Einrichtung einer einheitlichen Sicht auf Benutzer-ID-Informationen mit einer offenen, flexiblen IBM Directory Synchronization-Lösung. IBM Tivoli Directory Integrator erlaubt die Integration von mehr als 70 Endpunkten, die ID-Daten aufweisen. Hierzu gehören:

- *Personalverzeichnisse*
- *CRM-Datenbanken*
- *E-Mail-Systeme und andere Anwendungen*
- *ID-Datenspeicher*
- *Verwaltete Systeme*

Anstatt einen komplett neuen, zentralen Datenspeicher zu erstellen, können Sie die Datenbestände in der gesamten IT-Infrastruktur korrelieren. Die Software dient dabei als flexible Synchronisationsschicht zwischen den ID-Datenquellen und der ID-Struktur Ihres Unternehmens.

Sicherer Austausch von Benutzer-Credentials mit Geschäftspartnern durch den IBM Tivoli Federated Identity Manager. Durch die gemeinsame Nutzung eines auf offenen Standards basierenden Authentifizierungsframeworks mit gesicherten Entitäten können Sie:

- *neue Benutzer schnell und mit nur minimalem Verwaltungsaufwand aktivieren*
- *E-Commerce-Aktivitäten mit Geschäftspartnern und Kunden vereinfachen*
- *diese Aktivitäten ohne Sicherheitsrisiken durchführen*

Prozesse für Benutzer einfach gestalten – und für Administratoren

IBM Tivoli Access Manager-Software unterstützt bei der Konsolidierung verschiedener Kombinationen aus Kennwörtern und Benutzer-IDs. So können Sie Benutzer besser betreuen und den Aufwand für Administratoren verringern.

Konsistente Umsetzung von Sicherheitsrichtlinien mit IBM Tivoli Access Manager-Software. Diese Lösung kann mit einer Vielzahl von Web- und Anwendungsressourcen integriert werden – dies sind z. B. geschäftskritische Anwendungen, Dateien, Betriebsumgebungen und Daten, die im gesamten Unternehmen verteilt sind. Die Lösung bietet u. a. folgende Funktionen:

- *Management von Wachstum und Komplexität*
- *Tools, die es erlauben, Zugriffe bei On Demand Anforderungen dynamisch an geänderte Bedingungen anzupassen*
- *Senkung des Zeit- und Kostenaufwands für Verschlüsselung und Verwaltung von Sicherheitsfunktionen innerhalb jeder Anwendung*
- *Bereitstellung von Single Sign-On (SSO) im Web für die Benutzer*

Identifizierung und Schließung von Sicherheitslücken
Die Integration von Tools für Sicherheitsmanagement und Systemmanagement hilft Ihnen bei der Handhabung von Sicherheitsrisiken wie fehlenden Programmkorrekturen und falsch konfigurierten Server- und Desktopsystemen. IBM Security Management-Lösungen wie IBM Tivoli Security Compliance Manager, IBM Tivoli Access Manager for Operating Systems und IBM Tivoli Risk Manager können unternehmensweit in Systemmanagement-Tools integriert werden. Dies erlaubt das zentrale Management aller Aspekte bei der kontinuierlichen Schließung vorhandener Sicherheitslücken:

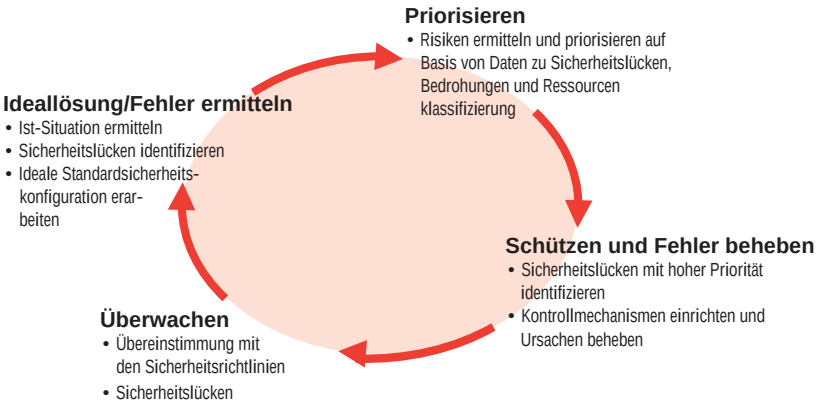
1. *Ermittlung und Dokumentation der IT-Sicherheitsrisiken in der Betriebsumgebung. Vergleich einer aktuellen mit einer idealen Sicherheitskonfiguration in allen Bereichen der IT-Infrastruktur.*
2. *Priorisierung der Risiken, die Sie beseitigen wollen. Nutzung von Daten über Sicherheitslücken – und Bedrohungen – hinsichtlich der verschiedenen Ressourcentypen.*
3. *Schutz der Infrastruktur gegen Sicherheitslücken mit hoher Priorität. Vereinfachung der automatischen, schnellen Schließung festgestellter Sicherheitslücken.*
4. *Überwachung der Systeme hinsichtlich der Einhaltung von Richtlinien, vorhandener Sicherheitslücken und Bedrohungen. Automatische Identifizierung von Abweichungen von der Standardsicherheitskonfiguration. Verwendung dieser Informationen zur Optimierung der Sicherheitskonfigurationen. Anpassung der Prioritäten der Risiken, die ausgeschlossen werden sollen, und Optimierung der Best Practices in Bezug auf die Reaktionen auf Probleme.*

Implementierung unternehmensweiter Sicherheitsrichtlinien
Unternehmen sehen sich durch die zunehmende Anzahl an behördlichen Vorgaben und Gesetzen gezwungen, für ausreichenden Datenschutz und die Identifizierung von Datenzugriffen zu sorgen. Folglich benötigen Unternehmen Lösungen, um IT-Kontrollmechanismen automatisieren, messen und umsetzen und die Einhaltung dieser Vorgaben handhaben zu können.

Mit IBM Security Management-Lösungen sind Sie in der Lage, die Einhaltung unternehmensweiter Richtlinien zu definieren, zu überwachen, umzusetzen und zu überprüfen. Bringen Sie mehr Transparenz in die Auflistung der exakten Anzahl der Benutzer, die auf Ihr Unternehmenssystem zugreifen, und deren Zugriffsberechtigungen. Auf diese Weise können Sie:

- *jeden Benutzer identifizieren, der auf Ihre Systeme zugreift,*
- *die erteilten Zugriffsberechtigungen an Ihren geschäftlichen Prioritäten und Anforderungen ausrichten,*
- *einheitliche Regeln zur Kontrolle der Offenlegung von Daten implementieren,*
- *die Prüfung von IT-Systemen automatisieren und zentralisieren, um eine konsistente Einhaltung der Sicherheitsrichtlinien zu gewährleisten.*

IBM Security Management-Lösungen helfen bei der automatischen Erfassung und dem zentralen Management der Sicherheitsdaten, die von Ihren IT-Steuerkomponenten verwendet werden. Dabei werden detaillierte Informationen zum Sicherheitsstatus aufgezeichnet, die Sie zur Identifizierung der Schritte heranziehen können, die für die Einhaltung der Richtlinien in bestimmten Systemen/Abteilungen erforderlich sind. Durch die präzise Aufzeichnung der Änderungen bei der Offenlegung und den Zugriffsrechten von Daten können Sie mit IBM Security Management-Lösungen schnell alle Auditfragen beantworten.



IBM Security Management-Lösungen helfen beim Management des gesamten Regelkreisprozesses bei der Handhabung von Sicherheitslücken.

IBM Security Management-Lösungen sind Teil des Portfolios an IBM Infrastructure Management-Lösungen

Neben den Integrationsmöglichkeiten untereinander für die IT-prozessinterne und -übergreifende Automatisierung und Integration bieten IBM Security Management-Lösungen auch Interoperabilität zu anderen IBM Infrastructure Management-Lösungen. Hierzu gehören beispielsweise:

- *IBM IT Service Management-Lösungen mit ihren branchenführenden Tools für Verfügbarkeits-, Konfigurations-, Service-Level-, Anwendungs- und Workload-Management. Diese können einzeln oder im Verbund mit anderen Tools genutzt werden und tragen so zu einer optimalen Leistungsfähigkeit der IT bei, um die gesetzten Service-Level-Ziele auch in einem sich ständig ändernden Geschäftsumfeld zu erreichen.*
- *IBM Storage Management-Lösungen für die Vereinfachung und Automatisierung des Speicherinfrastrukturmanagements, um Anwendungsverfügbarkeit, Nutzung von Speicherressourcen und Produktivität der Mitarbeiter zu verbessern.*

Alle IBM Infrastructure Management-Lösungen ermöglichen den Einsatz verschiedener Best Practices für die interne und übergreifende Automatisierung und Integration bei aktuellen und auch zukünftigen IT-Prozessen – einschließlich der ITIL-Prozesse.

Zusammenfassung

Das breite Angebotsspektrum von IBM Security Management-Lösungen umfasst branchenführende Tools, mit deren Hilfe Sie ein zentrales, automatisches und auf Richtlinien basierendes Sicherheitsmanagement im gesamten Unternehmen implementieren können.

Weitere Informationen

Wenn Sie mehr über IBM Security Management-Lösungen und integrierte Lösungen von IBM erfahren möchten, wenden Sie sich an Ihren zuständigen IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter:
ibm.com/software/de/tivoli
ibm.com/software/info/inframgmt/de

Die Vorteile von IBM Security Management-Lösungen

- ✓ Einrichtung einer zentralen Plattform für das konsistente Management von Benutzer-IDs und des Zugriffs auf IT-Ressourcen und Geschäftsdaten im Unternehmen.
- ✓ Aufbau stabiler Geschäftsbeziehungen zu Kunden und Geschäftspartnern mit Hilfe von Funktionen für Single Sign-On (SSO) und Identitätsmanagement im Verbund.
- ✓ Senkung der Kosten für das Sicherheitsmanagement sowie für die Entwicklung von Umsatz generierenden Anwendungen.
- ✓ Implementierung eines effizienten Regelkreisprozesses für die Identifizierung und Schließung von Sicherheitslücken gemäß den definierten Prioritäten.
- ✓ Definition, Überwachung, Umsetzung und Optimierung von unternehmensweiten Sicherheitsrichtlinien mit automatischen Tools, mit deren Hilfe Sie schnell auf Fragen zur Einhaltung von Richtlinien bei Auditprüfungen reagieren können.

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 Marken der IBM Corporation. On Demand Business, das On Demand Business Logo und Tivoli sind Marken der IBM Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Unternehmen sein

* Steve Hunt et al. Forrester Research. *Securing the Enterprise: Best Practices in Operational Excellence, Regulatory Compliance, and Infrastructure Security.* 26. Oktober 2004.

Hergestellt in den USA
03-05

© Copyright IBM Corporation 2005
Alle Rechte vorbehalten.

G507-1104-00-GE