Risiko- und Compliance-Management im Unternehmen

IBM Security Solutions ermöglicht neue Geschäftsmodelle und hilft bei der Einhaltung gesetzlicher Bestimmungen im gesamten Unternehmen

IBM

Inhalt

Kurzübersicht

In einer smarteren Arbeitswelt – die instrumentierter, vernetzter und intelligenter strukturiert ist – spielt die Sicherheit im Unternehmen eine entscheidende Rolle. Je mehr Daten und Informationen die Unternehmen ihren Zielkunden zur Verfügung stellen, umso größer werden die Risiken. Dadurch haben sich neue Anforderungen ergeben. Sicherheit muss über intelligente Sicherheitslösungen gewährleistet werden, die Vertrauen zwischen den Unternehmen und ihren Kunden, Geschäftspartnern, Mitarbeitern und anderen Beteiligten schaffen und darüber hinaus kritische Informationen, Anwendungen, Systeme und Services schützen. Aber das ist nur der Anfang.

Intelligente Sicherheitslösungen müssen Unternehmen auch die Möglichkeit bieten, neue und erfolgversprechende Modelle für ihre Geschäftstätigkeit optimal zu nutzen. Auf der Grundlage untereinander verknüpfter Geschäftsbeziehungen können Unternehmen zum Beispiel flexibler Informationen austauschen und im Rahmen einer umfassend vernetzten Umgebung zusammenarbeiten. Diese Verknüpfungen können enorme Herausforderungen mit sich bringen, denn je vernetzter in einem Unternehmen gearbeitet wird, desto anfälliger sind seine Systeme für Beeinträchtigungen. Intelligente Sicherheitslösungen werden auch im Hinblick auf neue Geschäftsmodelle benötigt, z. B. Cloud-Computing. Hierbei werden Ressourcen außerhalb der traditionellen Unternehmensgrenzen und der zugehörigen Sicherheitsinfrastrukturen verwaltet. Um die neuen Chancen in einer smarteren Arbeitswelt nutzen zu können, müssen Unternehmen die Gewissheit haben, dass alle kritischen Ressourcen sicher und geschützt sind, unabhängig davon, wer Zugriff auf die Ressourcen hat und wo diese sich befinden.

Durch neue Möglichkeiten bei der Durchführung der Geschäftstätigkeit ergibt sich eine stärkere Notwendigkeit, Unternehmen beim Risikomanagement in der gesamten Systemumgebung zu unterstützen. Regulierungsbehörden verlangen im heutigen Geschäftsumfeld die Einhaltung einer immer größeren Zahl von Standards, um den Datenschutz und die Integrität sensibler Daten zu gewährleisten. In Unternehmen müssen daher geeignete Sicherheitslösungen implementiert sein, um diese Anforderungen so kostengünstig wie möglich erfüllen zu können. Die Einhaltung dieser Standards garantiert allerdings noch keine sicheren Systeme. Die Unternehmen müssen darüber hinaus Risiken auf allen Systemen proaktiv analysieren und verwalten.

Geeignete Sicherheitskontrollen und bewährte Verfahren spielen dabei eine entscheidende Rolle, da sie dazu beitragen, dass Unternehmen komplexe Strukturen vereinfachen, Kosten senken und gesetzliche Bestimmungen einhalten können. Zur Verbesserung des Sicherheitsniveaus sollten Lösungen für das Risiko- und Compliance-Management daher im Rahmen eines Konzepts für ein integriertes Service-Management implementiert werden. Auf der Basis dieses Konzepts wird der Faktor Sicherheit zu einem integralen Bestandteil der Geschäftsprozesse, und nicht nur zu einer zusätzlichen Komponente. Unternehmen erreichen dadurch Transparenz, Kontrolle und Automatisierung für alle Business- und IT-Ressourcen.

Höhere Investitionen zur Erfüllung höherer Compliance-Anforderungen

Heutzutage gibt es Tausende von Bestimmungen, die in den unterschiedlichsten Unternehmen in den USA erfüllt werden müssen – und es werden immer mehr, insbesondere in stark regulierten Branchen wie dem Bankwesen und bei Finanzdienstleistungen. Im US-Haushalt sind für das Haushaltsjahr 2010 Ausgaben für Regulierungstätigkeiten in Höhe von 55,8 Mrd. US-Dollar vorgesehen, gegenüber 53,6 Mrd. US-Dollar aus dem vorherigen Haushaltsjahr. Viele Ausgaben werden vermutlich sogar noch höher ausfallen, als in der Haushaltsplanung vorgesehen. Es wird prognostiziert, dass die Regulierungstätigkeiten im Jahr 2010 um 4,2 Prozent gegenüber dem Vorjahr ansteigen. Die Haushaltsplanung sieht darüber hinaus vor, dass die Zahl der Mitarbeiter in staatlichen Regulierungsbehörden um 2,3 Prozent steigt. [1]

Während die US-Regierung die Ausgaben für Regulierungstätigkeiten erhöht, investieren private Unternehmen mehr in die Einhaltung gesetzlicher Bestimmungen. Laut einem Bericht werden die Ausgaben in amerikanischen Unternehmen für Governance-, Risiko- und Compliance-Management im Jahr 2010 auf 29,8 Mrd. US-Dollar steigen, d. h. um fast 4 Prozent im Vergleich zum Vorjahr[2] – die Ausgaben hierfür haben sich gegenüber den Prognosen für das Jahr 2005 fast verdoppelt.[3] Dabei ist noch nicht einmal berücksichtigt, wie hoch die Ausgaben weltweit für die Einhaltung gesetzlicher Bestimmungen aus den USA liegen. Unternehmen planen seit Jahren mit speziell festgelegten Budgets für die Einhaltung gesetzlicher Bestimmungen, und jedes Jahr steigt die Zahl der Mitarbeiter, die zur Einhaltung der immer größeren Anzahl an gesetzlichen Bestimmungen und branchenspezifischen Anforderungen benötigt wird.[4] Die gesetzlichen Bestimmungen sind die Folge realer und ernstzunehmender Risiken für Unternehmen und die privaten Daten von Einzelpersonen durch böswillige Personen und Unternehmen, die Missbrauch mit diesen Daten betreiben würden.

Die Einhaltung gesetzlicher Bestimmungen ist zudem nicht an einem bestimmten Punkt beendet, es handelt sich vielmehr um einen kontinuierlichen, zyklischen Prozess, der dauerhafte Sorgfalt und Aufmerksamkeit erfordert. Unglücklicherweise garantiert die Einhaltung der Bestimmungen nicht in allen Fällen sichere Systeme. Unternehmen müssen sich darüber im Klaren sein, wie sie Compliance-Anforderungen umsetzen, um in diesem Zusammenhang keine Zeit und kein Geld zu verschwenden. Durch eine Kombination aus proaktiven Risikoanalysen und der Eingrenzung von Risiken in der Systemumgebung sind Unternehmen in der Lage, Compliance-Anforderungen zu erfüllen und gleichzeitig die Grundlagen für neue Geschäftsmodelle zu schaffen, die Kosteneinsparungen und bessere Serviceleistungen ermöglichen sollen. Nach den Ergebnissen einer Studie erreichen Unternehmen, die umfassend von grundlegenden Ad-hoc-Prozessen auf eine allgemeine Optimierung umgestellt haben, höhere Umsätze, höhere Gewinne und eine stärkere Kundenbindung. Zudem liegen die jährlichen Ausgaben für die Einhaltung gesetzlicher Bestimmungen in diesen Unternehmen unter denen anderer Unternehmen, die sich noch in einer frühen Phase der Optimierung im Hinblick auf Compliance-Anforderungen befinden. [5]

Ermittlung intelligenter Lösungen zur Bewältigung dieser Herausforderungen

Risiken lassen sich in einem sich schnell verändernden regulatorischen und geschäftlichen Umfeld nur schwer eingrenzen. Hierfür sind intelligente Lösungen erforderlich, die neue, innovative Wege zur Ermittlung, Modellierung und Umsetzung risikobezogener Informationen ermöglichen. Bei einem intelligenten Risikomanagement geht es um die Sammlung aussagekräftigerer Informationen, deren schnellere und effektivere Nutzung und die Verringerung der Notwendigkeit von Benutzereingriffen in routinemäßige Abläufe. Derselbe Grad an Intelligenz und Vernetzung, der beim Risiko- und Compliance-Management eine so große Herausforderung darstellt, verspricht gleichzeitig den bestmöglichen Erfolg bei der Bewältigung der Herausforderungen:

- Smarte Unternehmen arbeiten instrumentiert und ermöglichen eine differenzierte Informationsverwaltung und -kontrolle. Die Unternehmen sind dadurch in der Lage, Risiken zu erkennen und schnell und präzise darauf zu reagieren.
- Die Systeme in smarten Unternehmen basieren auf miteinander vernetzten Daten, die Innovationen ermöglichen, direkt verarbeitet werden können und eine „Single Source of the Truth“ liefern.
- Smarte Unternehmen schaffen die Grundlagen für die schnelle, intelligente Analyse zahlreicher strukturierter und unstrukturierter Daten, um bessere Einblicke zu erhalten und fundierte Entscheidungen zu ermöglichen.

Um im heutigen Geschäftsumfeld in puncto Risiko- und Compliance-Management stets auf dem neuesten Stand zu bleiben, arbeiten smarte Unternehmen an der Verbesserung ihrer Fähigkeit, Risiken in allen Geschäftsbereichen weltweit und in Echtzeit erkennen und eingrenzen zu können.

Risiko- und Compliance-Management mit dem IBM Security Framework

Mit dem Aufbau von sicheren und dynamischen Infrastrukturen ergeben sich neue Notwendigkeiten, Sicherheitsrisiken über alle Sicherheitsbereiche hinweg einzugrenzen. Der Schlüssel zu einem erfolgreichen Risikomanagement in einer dynamischen Infrastruktur besteht in der Schaffung einer Grundlage aus Sicherheitsmaßnahmen, das die flexible und schnelle Bereitstellung von Serviceleistungen ermöglicht und gleichzeitig dazu beiträgt, die Kosten für Verwaltung und Betrieb der Sicherheitsinfrastruktur zu senken.

Hierfür hat IBM ein umfassendes Security Framework basierend auf folgenden Komponenten entwickelt:

- COBIT (Control Objectives for Information and related Technology), ein weltweit anerkanntes Governance-Framework auf der Grundlage von Branchenstandards und bewährten Verfahren.[6]
- Verhaltensrichtlinien für das Information Security Management (ISO/IEC 27002:2005), ein internationaler Standard, der Richtlinien und allgemeine Grundsätze für die Umsetzung, Verwaltung und Verbesserung des Information Security Management im Unternehmen etabliert.[7] Dieser Standard umfasst bewährte Verfahren für Zielsetzungen und Kontrollen in 11 Bereichen des Information Security Management.
- IT Infrastructure Library® (ITIL®), ein umfassendes, einheitliches und zusammenhängendes Framework mit bewährten Verfahren für das Management von IT-Services und die zugehörigen Prozesse.[8]

Aus sicherheitsspezifischer Sicht können Unternehmen durch die Integration dieser Prozesse und bewährten Verfahren sicherstellen, dass alle Abläufe innerhalb festgelegter Kontrollgrenzen funktionieren und die Serviceleistungen bereitgestellt werden, die in einem immer stärker vernetzten und immer komplexeren Umfeld erwartet werden oder erforderlich sind.

Die Gesamtgrundlage des IBM Security Framework setzt sich aus Elementen für die Sicherheitsgovernance, das Risikomanagement und die Compliance zusammen. Sie sorgen für Einheitlichkeit in Bezug auf Richtlinien, Ereignisverarbeitung und Berichterstellung. Zu den wichtigsten Komponenten des IBM Security Framework gehören folgende:

- Personen und IDs – dadurch ist sichergestellt, dass die richtigen Personen und Systemen zum richtigen Zeitpunkt Zugriff auf die richtigen Ressourcen haben
- Daten und Informationen – Schutz kritischer Daten bei der Übertragung und nach der Speicherung
- Anwendungen und Prozesse – dadurch sind die Verfügbarkeit und Sicherheit von Anwendungs- und Geschäftsservices gewährleistet
- Netzwerk, Server und Endpoint – dadurch werden neue Risiken für alle IT-Systemkomponenten rechtzeitig erkannt
- Physische Infrastruktur – Nutzung digitaler Steuerelemente zum Schutz von Abläufen in physischen Umgebungen

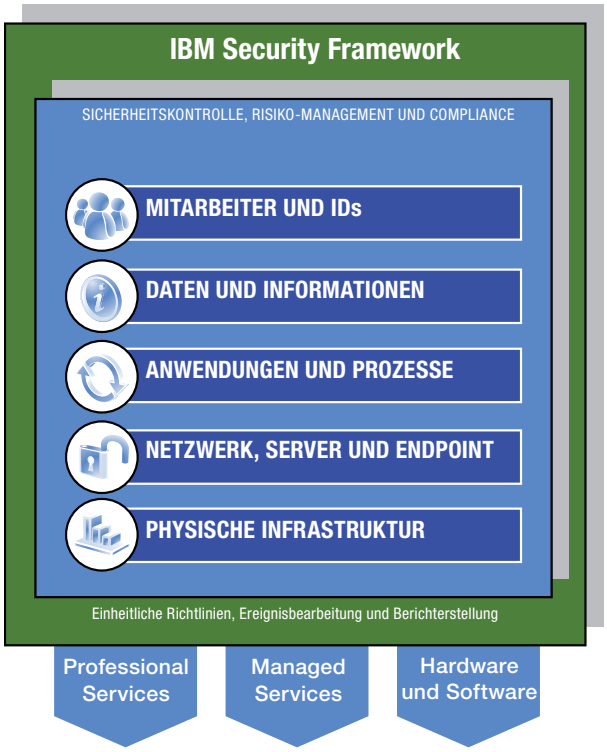

Abbildung 1: Das von IBM entwickelte Security Framework ist eine Grundlage für ein durchgängiges Risiko-Management für alle Sicherheitsdomänen im Unternehmen.

IBM bietet Unternehmen eine Kombination aus Hardware, Software und Serviceleistungen, um dieses Security Framework vollständig oder teilweise umsetzen zu können. Die IBM Lösungen für das Risiko- und Compliance-Management auf Unternehmensebene im Rahmen dieses Frameworks sind umfassend und flexibel einsetzbar. Sie können an die Anforderungen im jeweiligen Unternehmen in puncto geeignetes Risikomanagement und Nachweisbarkeit der Compliance für Regulierungsbehörden angepasst werden.

IBM Security Solutions für Risiko- und Compliance-Management im Unternehmen

IBM verfügt über ein umfassendes Produktportfolio mit Sicherheitslösungen für das Risiko- und Compliance-Management im Unternehmen, mit denen sich die Herausforderungen beim Schutz von Systemen in einem immer stärker instrumentierten, vernetzten und intelligenteren Geschäftsumfeld bewältigen lassen. Zu dieser Angebotspalette gehört ein großes Leistungsspektrum speziell zur Eingrenzung von Risiken im Zusammenhang mit Mitarbeitern, Prozessen und Informationen in Unternehmensumgebungen. Um sicherzustellen, dass die Systemumgebung ordnungsgemäß innerhalb festgelegter Kontrollgrenzen für alle Business- und IT-Ressourcen funktioniert, ist das richtige Maß an Transparenz, Kontrolle und Automatisierung erforderlich. Die Implementierung von Lösungen für das Risiko- und Compliance-Management im Rahmen eines Konzepts für ein integriertes Servicemanagement sorgen für ein höheres Sicherheitsniveau, da der Faktor Sicherheit als integraler Bestandteil der Geschäftsprozesse und nicht nur als zusätzliche Komponente integriert wird. IBM Security Solutions, die auf der Grundlage eines solchen Konzepts eingeführt werden, liefern das erforderliche Maß an Transparenz, Kontrolle und Automatisierung für ein Wachstum des Unternehmens in einer smarteren Welt.

IBM Lösungen für das Risiko- und Compliance-Management auf Unternehmensebene schützen das gesamte Unternehmen, d. h. alle IDs, Daten, Informationen, Anwendungen, Prozesse und Infrastrukturen. Jedes Angebot umfasst Funktionen für ein automatisiertes Risikomanagement, sodass Kontrolle und Verwaltung mit Prüfung und Compliance verknüpft werden. Durch das Etablieren integrierter Verfahren für das Compliance-Management bei allen Produktangeboten tragen IBM Lösungen zu einer einheitlichen Compliance auf allen Plattformen bei.

In diesem Dokument werden spezielle IBM Softwarelösungen für Risikoanalyse und -management im gesamten Unternehmen vorgestellt.

IBM Tivoli Security Management für z/OS: Mainframe-Security der nächsten Generation

Die immer komplexeren und umfassenderen Mainframeprozesse in Verbindung mit einem Mangel an qualifiziertem Personal speziell für Mainframesysteme stellen Unternehmen vor große Herausforderungen bei der Verwaltung ihrer sichersten Plattform. Die immer größeren Datenmengen, die Notwendigkeit zur gemeinsamen Nutzung der auf dem Mainframe abgelegten Daten und die Verpflichtung zur Überwachung der Zugriffskontrolle – selbst bei privilegierten Systembenutzern – können hohe Kosten und komplexe Sicherheitsprobleme nach sich ziehen. Unternehmen sind daher auf eine Mainframelösung angewiesen, mit der sich Prüf-, Benachrichtigungs- und Überwachungsfunktionen sicher automatisieren lassen und die Rolle des Mainframes als zentrale Komponente der Sicherheit im Unternehmen gestärkt wird.

In den großen Unternehmen von heute befinden sich viele geschäftskritische Anwendungen auf einem IBM Mainframesystem. IBM schafft die Grundlagen dafür, dass der Mainframe als Sicherheitshub im Unternehmen eingesetzt wird, und hat eine durchgängige Sicherheitslösung für den Mainframe entwickelt, die Funktionen zur Umsetzung von Sicherheitsrichtlinien, eine effektive Benutzerverwaltung, die Überwachung von Sicherheitsrisiken sowie andere Funktionen im Zusammenhang mit dem Risiko- und Compliance-Management bietet.

IBM trägt durch die Definition und Umsetzung von Sicherheitsrichtlinien basierend auf den Sicherheitsanforderungen des jeweiligen Unternehmens zu einem besseren Risikomanagement und zur Einhaltung gesetzlicher Bestimmungen bei. Unternehmen können über RACF (Resource Access Control Facility) die Einhaltung von Sicherheitsrichtlinien proaktiv erzwingen, interne Sicherheitsfehler vermeiden, nicht konforme Sicherheitsbefehle identifizieren und Benachrichtigungen ausgeben lassen, wenn es sich um riskante Befehle handelt.

Tivoli Security Management für z/OS ermöglicht eine effektivere Benutzerverwaltung und eine einfachere Verwaltung von Sicherheitsfunktionen. Dadurch erhöht sich die Effizienz und verringert sich die Zahl der Fehler bei Aufgaben im Zusammenhang mit dem Risiko- und Compliance-Management. Administratoren können z. B. Änderungen an der Sicherheitskonfiguration ohne Auswirkungen auf die Produktion testen, potenzielle Konflikte zwischen mehreren RACF-Datenbanken ermitteln und Benutzer, Gruppen, Aufgabenbereiche, Berechtigungen und Richtlinien über eine zentrale Schnittstelle verwalten.

Dank der umfassenden, kontinuierlichen Überwachung auf potenzielle Sicherheitsrisiken können mit Tivoli Security Management für z/OS Änderungen an festgelegten Referenzkonfigurationen und der Missbrauch von Berechtigungen erkannt werden, sodass sich das Risiko von Bedrohungen durch Insidern verringern lässt. Die IBM Lösung ermöglicht darüber hinaus die plattformübergreifende Sammlung von Protokollen, leistungsfähige Datenanalysen und vordefinierte Berichtsfunktionen für alle Betriebssysteme, Anwendungen und Datenbanken. Dadurch lässt sich die Einhaltung staatlicher und branchenspezifischer Bestimmungen und Standards auf einfachere Weise belegen.

Tivoli Security Management für z/OS kann mit allen derzeit unterstützten Versionen des Betriebssystems IBM z/OS und allen Subsystemen (z. B. CICS) eingesetzt werden, die für Unternehmen von entscheidender Bedeutung sind. So verringert sich der Aufwand bei Upgrades auf ein neues Release von z/OS, und das unterbrechungsfreie Risiko- und Compliance-Management wird einfacher.

Auf der Grundlage der kombinierten Sicherheitsmerkmale der IBM Lösung – RACF, auf Mainframesysteme zugeschnittene Sicherheitsfunktionen von System z und andere IBM Sicherheitslösungen für Unternehmen – lässt sich ein Sicherheitshub im Unternehmen einrichten, mit dem das Sicherheitsmanagement und Sicherheitsrichtlinien im gesamten Unternehmen zentralisiert und standardisiert werden können. Über diesen Hub stehen Funktionen für das Risiko- und Compliance-Management zur Verfügung, z. B. Identity Management für den gesamten Benutzerlebenszyklus, Richtlinien für die Zugriffssteuerung, systemübergreifendes Identity Management sowie Funktionen für Compliance-Überwachung und Berichterstellung.

Tivoli Security Management für z/OS gehört zur zSecure-Produktfamilie, die Angebote mit zusätzlichen Funktionen für Prüfung und Risikomanagement für CA TopSecret, CA ACF/2 und RACF enthält.

IBM Lösungen für das Management privilegierter IDs: Schutz vor internen Risiken

Der Schutz von IT-Systemen vor externen Bedrohungen ist natürlich äußerst wichtig, insbesondere, wenn sich traditionelle Grenzen aufgrund der Notwendigkeit zur gemeinsamen Benutzung von Informationen und zur Zusammenarbeit mit anderen Unternehmen verschieben. Dennoch gilt es zu beachten, dass sich auch innerhalb des Unternehmens Risiken durch privilegierte Benutzer ergeben können. Es handelt sich hierbei um Personen, die IT-Systeme, Anwendungen und Daten nutzen, um ihre täglichen Aufgaben zu erfüllen, die Zugriff auf sensible Informationen und Ressourcen haben und die häufig umfassend qualifiziert sind. Aufgrund ihrer umfangreichen Zugriffsrechte auf IT-Systeme stellen diese Personen möglicherweise das größte Risiko für die Datenintegrität und den Datenschutz im Unternehmen dar. Nach den Ergebnissen einer Studie aus dem Jahr 2007 sind Mitarbeiter oder frühere Mitarbeiter die Ursache für etwa 69 Prozent aller Sicherheitsverstöße.[9] Diese Verstöße können schwerwiegende Beeinträchtigungen nach sich ziehen, unabhängig davon, ob sie absichtlich und böswillig oder nur versehentlich verursacht wurden. Unternehmen müssen sich in jedem Fall sorgfältig dagegen schützen.

Die Einschränkung von Zugriffsrechten ist sicherlich keine sinnvolle Maßnahme zur Eingrenzung von Risiken durch privilegierte Benutzer, denn Administratoren, LOB-Manager und andere Personen sind auf umfangreiche Zugriffsrechte angewiesen. Sinnvoller wäre es, ein angemessenes Maß an Transparenz bei deren Tätigkeiten sicherzustellen, und Richtlinien und Prozesse zu etablieren, um schnell auf Probleme und potenzielle Probleme reagieren zu können. IBM Security Solutions kann zu einem derartigen Schutz im Unternehmen beitragen – mit Funktionen für die Verwaltung von Zugriffen auf Systeme und Anwendungen durch die Umsetzung von Benutzerberechtigungen, mit der Überwachung von Verhaltensmustern in Echtzeit zur Identifizierung von Problemen und mit Benachrichtigungen in Echtzeit, um Risiken schnell beheben zu können.

Ein weiterer wesentlicher Vorteil der IBM Lösungen für das Management privilegierter Benutzer besteht darin, die Kontrolle und Verantwortlichkeit privilegierter Benutzer auch dann sicherstellen zu können, wenn weitere virtuelle Maschinen hinzukommen, die Konsolidierung im Rechenzentrum vorangetrieben wird und ausgereiftere Cloud-Computing-Lösungen zum Einsatz kommen.

Mithilfe der Lösungen aus der IBM Tivoli Access Manager-Produktfamilie können Unternehmen ein effektives, automatisiertes System zur Verwaltung der Zugriffsrechte privilegierter Benutzer auf Betriebssysteme, e-Business Anwendungen und andere kritische Systeme einrichten. Sobald dieses System eingerichtet ist, lassen sich z. B. mit dem Tivoli Security Information and Event Manager Verhaltensweisen von Benutzern automatisch überwachen, Probleme identifizieren und Benachrichtigungen zu Benutzeraktivitäten verschicken. Dadurch stehen verlässliche Informationen zur Überwachung von Benutzeraktivitäten zur Verfügung, insbesondere im Hinblick auf den Nachweis der Compliance mithilfe interner Richtlinien und gesetzlicher Bestimmungen im Zusammenhang mit Sicherheitsrisiken durch privilegierte Benutzer. Tivoli Security Information and Event Manager hat zudem Funktionen zur Benachrichtigung nahezu in Echtzeit. Informationen über verdächtige Aktivitäten können zur weiteren Analyse und für weitere Maßnahmen an eine Korrelationsengine weitergeleitet werden.

IBM Tivoli Security Information and Event Manager: Optimierte Compliance

Mithilfe von SIEM (Security Information and Event Management) verringern sich Aufwände im Zusammenhang mit der Sicherheit und Compliance. Hierbei werden Funktionen für das Echtzeit-Management mit denjenigen für Überwachung und Berichterstellung kombiniert. IBM Tivoli Security Information and Event Manager umfasst die beiden wichtigsten Aspekte von SIEM: ein Dashboard für das Echtzeit-Management vom Incident Management und ein Dashboard für Informationsanalysen der Beurteilungen zur Einhaltung von Richtlinien. Damit ist eine zuverlässige Grundlage für das Risiko- und Compliance-Management gewährleistet. Durch die gemeinsame Verwendung beider Funktionen können Unternehmen die Sammlung von Protokollen und die Ereigniskorrelation im gesamten Unternehmen zentralisieren. Sie profitieren zudem von einem hochentwickelten Compliance-Dashboard, über das Ereignisse und Verhaltensweisen von Benutzern mit unternehmensweiten Richtlinien verknüpft werden können.

Das zuverlässige, unternehmensweite Audit-Dashboard, das über Tivoli Security Information and Event Manager zur Verfügung steht, liefert Sicherheitsbeauftragten und Auditoren eine zentrale Sicht auf alle relevanten Aktivitäten im Unternehmen. Sie sehen damit auf einen Blick, wie viele Aktivitäten protokolliert wurden und können Benutzerprofile mit den aufgerufenen Informationen vergleichen. Mit dem Audit-Dashboard können auch Verstöße gegen Richtlinien angezeigt und Protokolldatenbanken eingesetzt werden, um verschiedene Anforderungen an Berichterstellung und Compliance zu erfüllen.

Im Hinblick auf die Einhaltung spezieller Bestimmungen beinhaltet die IBM Lösung außerdem eine Reihe von Managementmodulen, die jeweils folgende äußerst detaillierte Informationen liefern:

- Eine Vorlage zur Ressourcenklassifizierung, in der die betroffenen Informationen, Mitarbeiter und Ressourcen angezeigt werden. Hierbei wird die in gesetzlichen Bestimmungen übliche Terminologie verwendet.
- Eine Richtlinienvorlage, mit der Ereignisdaten anhand einer individuellen Richtlinie beurteilt werden, über die festgelegt ist, wer auf welche regulierten Informationen zugreifen und welche Vorgänge damit durchführen darf.
- Ein Report Center, das auf der Ressourcenklassifizierung und den Richtlinienvorlagen basiert und Dutzende relevanter Compliance-Berichte zu speziellen Bestimmungen oder bewährten Verfahren liefert.

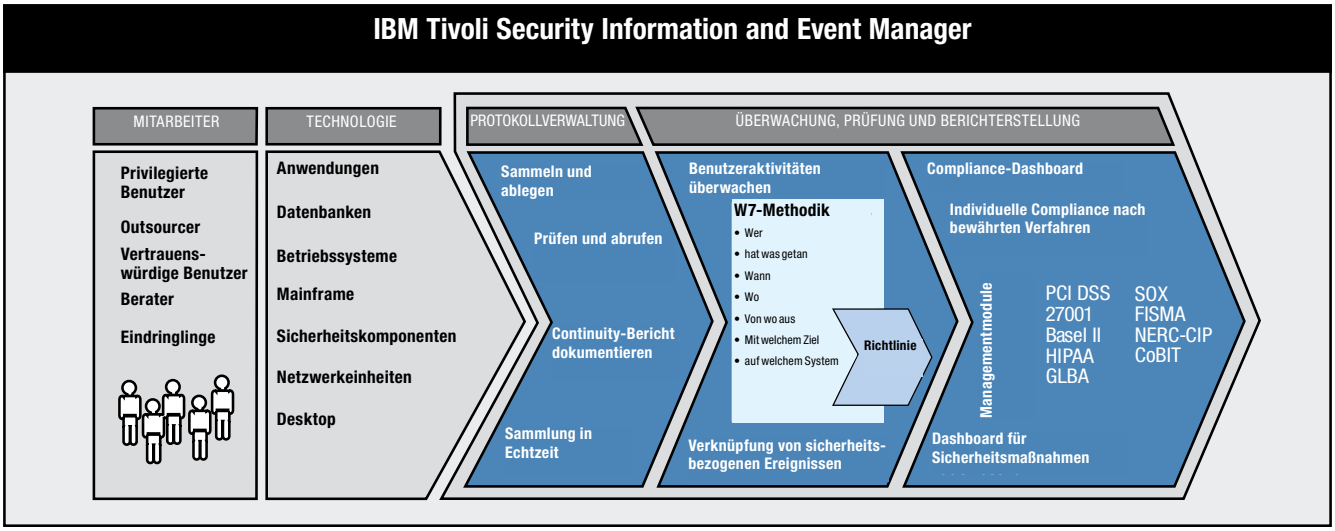

Abbildung 2: IBM Tivoli Security Information and Event Manager ist eine umfassende Grundlage zur Erfüllung von SIEM-Anforderungen.

Guardium-Software von IBM: Risiko- und Compliance-Management für Datenbanken

Das Interesse an kostengünstigen, unternehmensweiten Lösungen für das Risiko- und Compliance-Management mit Echtzeit-Sicherheitsfunktionen und differenzierten Prüffunktionen hat sich inzwischen auch auf Datenbankumgebungen ausgeweitet, in denen Standalone-Geräte zur Umsetzung von Richtlinien ohne wesentliche Leistungseinbußen eingesetzt werden können.

Mit der Guardium-Software für die Überwachung von Datenbanken in Echtzeit und Sicherheitsfunktionen für unternehmensweite Anwendungen können Unternehmen kritische Daten schützen, indem sie nicht autorisierte Datenbankaktivitäten proaktiv ermitteln. Hierzu gehören auch Prüf- und Compliance-Funktionen zur Vereinfachung von Prozessen in Bezug auf Compliance und Datenschutz. Im Gegensatz zu vielen Lösungen für die Datenbank-Auditierung kann die Guardium-Software auch auf der Betriebssystemplattform z/OS eingesetzt werden und eignet sich damit für nahezu alle Datenbanken. Die Software liefert differenzierte Prüfprotokolle, ohne dass es hierbei zu Einbußen bei Leistungsmerkmalen und Stabilität kommt, vereinheitlicht die Überwachung mehrerer Plattformen und gewährleistet die Aufteilung von Aufgabenbereichen, da sie außerhalb der Datenbank als unabhängige Netzwerkeinheit arbeitet.

Zu den Funktionen der Guardium-Software für die Datenbanküberwachung und -sicherheit gehört eine Anwendung zur Workflow-Automatisierung, die Compliance-Workflowprozesse optimiert. Mit dieser Anwendung lässt sich das Lifecycle-Management zur Datenbanksicherheit von einer fehleranfälligen, zeitaufwändigen und unregelmäßigen Aktivität in einen kontinuierlichen, automatisierten Prozess umwandeln, der die Zielsetzungen beim Risiko- und Compliance-Management effizient unterstützt. Die Software bietet folgende Vorteile:

- Zentrale Richtlinien und Berichte für die gesamte Infrastruktur, ohne jeden Datenbankserver konfigurieren oder neue Software installieren zu müssen
- Speicherung des Prüfprotokolls und der Ergebnisse in einem Repository, das auch von privilegierten Benutzern nicht geändert werden kann
- Protokollierung der Ergebnisse elektronischer Sign-offs und Eskalationen
- Verwaltung der regelmäßigen Verteilung von Compliance-Berichten im gesamten Unternehmen
- Proaktive Antworten in Echtzeit zu Sicherheits- und Richtlinienverstößen anstelle ausschließlich nachträglicher Analysen statischer Protokolldaten
- Automatische Compliance-Berichte und Workflow-Automatisierung zur Reduzierung von IT-Workloads

Die Guardium-Software kann auch zur Automatisierung sich wiederholender Tätigkeiten verwendet werden. Sie können z. B. regelmäßige Prüfungen so planen, dass sensible Objekte automatisch erkannt werden, die möglicherweise hinzugekommen sind oder von bisherigen Positionen verschoben wurden. Die daraus resultierenden Informationen können anschließend zur automatischen Aktualisierung aller geeigneten Richtliniengruppen für diese Objekte verwendet werden.

IBM Tivoli Data and Application Security: Durchgängiger Schutz von Unternehmensdaten

Da die Datenmengen immer größer werden und die gemeinsame Nutzung von Daten ein wesentlicher Bestandteil bei der Durchführung von Geschäftstätigkeiten bleibt, müssen Unternehmen im heutigen Geschäftsumfeld immer größere Risiken im Zusammenhang mit Datenverlusten bewältigen. Die Datenmenge verdoppelt sich jeweils innerhalb von 18 bis 24 Monaten, sodass Maßnahmen zur Bereitstellung sicherer Speicherlösungen für Unternehmensdaten immer komplexer werden.[10] Anwendungen sind bei Verstößen gegen die Datensicherheit darüber hinaus zum wichtigsten Ziel geworden. Angesichts der immer größeren Komplexität moderner Anwendungen und den kontinuierlichen Bemühungen, den Zugriff auf Anwendungen für die Benutzer zu vereinfachen, die Informationen gemeinsam nutzen müssen, sind die Anwendungen eines Unternehmens anfälliger als je zuvor. Datenverluste können dramatische Auswirkungen auf das Unternehmen haben. Die Folgen reichen von einer einfach nachvollziehbaren Verschlechterung des Geschäftsergebnisses bis hin zu schlecht messbaren, aber gleichermaßen schädlichen Auswirkungen, z. B. Imageverlusten.

IBM Tivoli Data and Application Security unterstützt Unternehmen beim Schutz von Daten und Anwendungen, indem überprüfbare Zugriffskontrollen bereitgestellt, die differenziertere Steuerung von Benutzerberechtigungen ermöglicht und die Verwaltung von Schlüsseln für die Datenverschlüsselung zentralisiert werden. Die Lösung sorgt für den umfassenden Schutz sensibler Daten in unternehmensinternen Speichersystemen, Datenbanken und kritischen Anwendungen. Dadurch sind Unternehmen in der Lage, gesetzliche Bestimmungen einzuhalten und die Zuverlässigkeit von Daten und Anwendungen zu erhöhen.

IBM Tivoli Data and Application Security bietet folgende wesentlichen Features:

- Differenziertere Verwaltung von Benutzerberechtigungen – von der Anwendungs- bis zur Betriebssystemebene
- Zentrale Verwaltung und Umsetzung von Berechtigungen und Sicherheitsrichtlinien im Hinblick auf eine differenziertere Autorisierung und Zugriffssteuerung auf Datenebene
- Zentrale Verwaltung von Verschlüsselungsschlüsseln für Band- und Plattenspeichersysteme
- Umfassende und automatisierte Überwachung und Berichterstellung zu Benutzeraktivitäten
- Zentrale, automatisierte Compliance-Berichte und Protokollverwaltung im Hinblick auf zahlreiche Bestimmungen und Branchenstandards, z. B. Payment Card Industry Data Security Standard (PCI DSS), Basel II, Sarbanes-Oxley (SOX) und ISO 27002.

Außerdem kann die Lösung dazu beitragen, den unbefugten Zugriff auf sensible Daten und deren Verwendung zu verhindern und somit Verstöße gegen die Datensicherheit und die Nichteinhaltung von Vorschriften zu vermeiden. Gleichzeitig sorgt sie für eine Vereinfachung der gemeinsamen Nutzung von Daten durch interne und externe Benutzer, z. B. über webbasierte Services.

IBM Rational AppScan Enterprise Edition: Tests auf Schwachstellen in Webanwendungen

Tests und Berichte zur Sicherheit von Webanwendungen sind ein immer wichtigerer Bestandteil des Risiko- und Compliance-Managements in allen Unternehmen, die im e-Business tätig sein. Die Herausforderung für viele Unternehmen besteht hierbei darin, die Überprüfung von Anwendungen auf das gesamte Unternehmen auszuweiten und dennoch die zentrale Kontrolle von Daten über Schwachstellen aufrechtzuerhalten. IBM bietet hierfür die IBM Rational AppScan Enterprise Edition an. Es handelt sich hierbei um eine webbasierte Lösung zur Anwendungssicherheit für Testteams mit mehreren Benutzern, die zentrale Schwachstellentests durchführen müssen. Zu den Leistungsmerkmalen dieser Software gehören hochentwickelte Funktionen zur Anwendungsprüfung, Korrekturfunktionen, Kennzahlen und Dashboards zur Sicherheit sowie wichtige Compliance-Berichte.

Die IBM Rational AppScan Enterprise Edition enthält eine erweiterbare Unternehmensarchitektur, die eine zentrale Überprüfung mehrerer Anwendungen gleichzeitig ermöglicht. Dabei wird eine Webanwendung durchsucht, analysiert und auf Sicherheits- und Compliance-Verstöße getestet. Anschließend werden aussagekräftige Berichte generiert. Die Software erkennt integrierte Malware und Links zu böswilligen oder unerwünschten Websites in Webanwendungen. Dadurch verringert sich das Risiko, dass die Websites eines Unternehmens die Systeme von Besuchern der Websites infizieren oder diese zu risikobehafteten Onlineadressen umleiten. Sobald während des Prüfprozesses eine Sicherheitslücke identifiziert wird, liefert die Software intelligente Empfehlungen zur Fehlerbehebung, um den Korrekturprozess zu vereinfachen. Zudem werden eine kontinuierliche Überwachung und Sammlung von Kenndaten durchgeführt, damit die langfristige Fehlerbehebung und Verbesserungen gewährleistet sind. Hochentwickelte Dashboards und flexibel einsetzbare Berichtsansichten sorgen für die unternehmensweite Transparenz in Bezug auf Risiken und Fortschritte bei der Fehlerbehebung. Durch die nahtlose Integration mit Testtools zur Qualitätssicherung und Einheiten zur Codeprüfung werden Sicherheitstests und die Fehlerbehebung durch Mitarbeiter der Qualitätssicherung und Entwicklung vereinfacht.

Um nachweisen zu können, dass die Systeme im Unternehmen alle Sicherheitsvorschriften erfüllen, sind im Lieferumfang der Software über 40 direkt einsetzbare Compliance-Sicherheitsberichte enthalten. Hierzu gehören z. B. Berichte für die Sicherheitsstandards PCI DSS, ISO 27001 und ISO 27002 und für branchenspezifische Bestimmungen, wie den Health Insurance Portability and Accountability Act (HIPAA), den Gramm-Leach-Bliley Act (GLBA) und Basel II.

IBM Security Services: Ein umfassendes Konzept für ein durchgängiges Risikomanagement

IBM Security Services bietet das branchenweit umfassendste und innovativste Angebot an Sicherheitsservices, die dem Kunden ein effektives Risikomanagement bei gleichzeitig optimaler Nutzung von Investitionen in Sicherheitslösungen ermöglichen. Auf der Grundlage einer Vielzahl von Services für alle Bereiche des IBM Security Framework (Risiko- und Compliance-Management, Daten und Informationen, Anwendungen und Prozesse, Netzwerk, Server, Endpoints, physische Infrastruktur) sorgen die IBM Security Services für eine bessere Integration, kürzere Zeiträume für die Markteinführung und schnellere Wertschöpfung für Unternehmen.

Zum IBM Security Services-Produktportfolio gehört Folgendes: Professional Security Services für die Analyse, Planung und Implementierung von Sicherheitslösungen, Managed Security Services (z. B. Managed Firewall Services), über die IBM Sicherheitsfunktionen für Unternehmen über eine Cloud verwaltet, und Cloud Security Services, z. B. Filterung von Web-URLs oder Protokollverwaltung sicherheitsrelevanter Ereignisse.

In puncto Risiko- und Compliance-Management bieten die Angebote von IBM Security Services Unternehmen die Möglichkeit, folgende wesentlichen geschäftlichen Herausforderungen zu bewältigen: Einhaltung gesetzlicher Bestimmungen, Erkennung und Eingrenzung von Risiken und die Umsetzung geeigneter Richtlinien und Kontrollen. Zu den Serviceleistungen zur Bewältigung dieser Herausforderungen gehören folgende:

- Planung und Entwicklung von Sicherheitsrichtlinien
- Analysen von Sicherheitsrisiken
- Security Health Checks
- Security Workshops
- Entwicklung eines Frameworks zur Informationssicherheit
- Entwicklung einer unternehmensweiten Sicherheitsarchitektur
- Datenschutzservices
- Analysen zur PC-Sicherheit

Diese Angebote bieten Unternehmen Vorteile in mehrfacher Hinsicht: Hilfe bei der Schaffung von Grundlagen für die Einhaltung gesetzlicher Bestimmungen durch die Analyse von Compliance-Fehlern anhand führender Bestimmungen und Branchenstandards, Entwicklung eines geeigneten und effektiven Frameworks für das Risiko- und Compliance-Management. IBM Security Services greift auf erstklassige Produkte von IBM und anderen Anbietern von Sicherheitslösungen zurück, die IBM Select Partner sind.

Warum IBM?

Als führender Anbieter von Sicherheitslösungen arbeitet IBM mit dem Kunden bei der Bereitstellung von Sicherheitsprodukten und -services als vertrauenswürdiger Partner zusammen. In diese Zusammenarbeit fließt unser Know-how aus den Bereichen Forschung, herausragende Technologien, Beratung, Implementierung und erstklassiger Support für IT-Sicherheitslösungen ein und wird miteinander verknüpft. Dadurch ergibt sich ein hohes Sicherheitsniveau im Design Ihrer IT-Serviceumgebung. Wir unterstützen unsere Kunden dabei, komplexe Strukturen zu vereinfachen, Kosten zu senken und Compliance-Probleme zu beseitigen und sorgen so für Sicherheit in einer smarteren Arbeitswelt. IBM ist ausgezeichnet positioniert, um die Sicherheitsanforderungen unserer Kunden zu analysieren, Lösungen bereitzustellen und sicherzustellen, dass diese Lösungen erfolgreich eingeführt werden:

- Wir haben das Fachwissen – IBM hat X-Force, um Risiken zu erkennen und zu beseitigen, sowie Tausende von Forschern, Entwicklern, Beratern und Fachleuten für Sicherheitsinitiativen.
- Wir haben das Know-how – Wir haben Tausende von Sicherheitsprojekten beratend begleitet und implementiert und haben die erforderliche praktische Erfahrung mit bewährten Verfahren, Prozessen und Return-on-Investments. Außerdem sind wird am geschäftlichen Erfolg unserer Kunden interessiert.
- Wir haben den Gesamtüberblick – IBM bietet durchgängige Lösungen, von der Sicherheitsstrategie und -Governance bis zur Sicherheit für Mainframes, Desktopsysteme, Netzwerke, Pervasive Computing und vieles mehr.
- Wir sind mit den Branchen unserer Kunden vertraut – IBM hat umfassende branchenspezifische Erfahrung und kann Sicherheitslösungen an vertikale Herausforderungen der jeweiligen Branchen anpassen, z. B. den Schutz von Geschäftsprozessen.
- Wir arbeiten selbst auf dieser Grundlage – Wir sorgen für die Sicherheit und den Datenschutz für weltweit 400.000 Mitarbeiter, und unsere Service-Teams verwalten täglich über 7 Mrd. sicherheitsrelevante Ereignisse für unsere Kunden.
- Wir können es belegen – IBM stellt seit über 30 Jahren IT-Sicherheitslösungen zur Verfügung. Wir können auf über 200 Kundenreferenzen im Sicherheitsbereich und auf über 50 veröffentlichte Fallstudien verweisen.
- Wir haben ein Netzwerk aus Geschäftspartnern – IBM hat eine große Business Partner-Community, die unsere Lösungen ergänzt und implementiert.
- Wir helfen Ihnen bei der Auswahl – Berater von IBM Security Services können eine Liste mit Produkten von IBM und anderen Anbietern zur Verfügung stellen, damit der Kunde die bestmögliche Lösung für seine Systemumgebung zusammenstellen kann.

Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie IBM bei der Entwicklung einer Sicherheitslösung unterstützen kann, die dank eines effektiven Risiko- und Compliance-Managements besser auf Ihre Geschäftsziele abgestimmt ist, wenden Sie sich an den zuständigen IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter: **ibm.com**/security

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
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

1 deRugy, Veronique, und Melinda Warren, “Regulators’ Budget Report: Expansion of Regulatory Budgets and Staffing Continues in the New Administration,” Mercatus Center, George Mason University, Oktober 2009. http://mercatus.org/publication/regulators-budget-report

2 Tucci, Linda, “Governance, risk and compliance spending to grow in 2010,” SearchCompliance.com, 1. Dezember 2010. http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html

3 D’Antoni, Helen, “Security Conforms to Regulatory Compliance,” Information Week, 29. August 2005. www.informationweek.com/news/securityshowArticles.jhmtl?articleID=170100825

4 “64% of Companies Have Dedicated Regulatory Compliance Budgets, According to META Group Study,” Business Wire, 26. Juli 2004. www.thefreelibrary.com/64%25+of+Companies+Have+Dedicated+Regulatory+Compliance+Budgets,...-a0119745130

5 Greiner, Lynn, “Compliance spending offers benefits besides security,” Network World, 12. August 2008. www.networkworld.com/news/2008/081108-compliance-spending-offers-benefits-besides.html

6 Weitere Informationen über COBIT finden Sie unter www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

7 Weitere Informationen über ISO/IEC 27002:2005 finden Sie unter www.iso.org/iso/catalogue_detail.htm?csnumber=50297

8 Weitere Informationen über ITIL finden Sie unter www.itil-officialsite.com/home/home.asp

9 The Global State of Information Security 2007, ein gemeinsames Forschungsprojekt von CIO und CSO in Zusammenarbeit mit PricewaterhouseCoopers. www.pwc.com/en_BE/be/publications/state-of-infsecurity-pwc-07.pdf

10 “Data Volume is Becoming Unmanageable, Say Executives,” Government Technology News Report, 5. August 2008. www.govtech.com/gt/articles/385068

Bitte der Wiederverwertung zuführen

TIW14052-DEDE-00