Business Whitepaper

In vier Schritten Compliance-Prozesse automatisieren und Risiken minimieren

Automatisierte Compliance-Prozesse können Ihr Unternehmen vor enormen Kosten und den Konsequenzen von Compliance-Verletzungen bewahren

IT-Abteilungen tragen eine hohe Verantwortung bei der Einhaltung der für das Unternehmen geltenden Vorschriften, Normen, Richtlinien und Verfahren. Sie müssen jederzeit in der Lage sein, diese Regelkonformität auf Verlangen unter Beweis zu stellen. Durch Compliance-Management soll dabei sichergestellt werden, dass koordinierte Aktivitäten für alle Bereiche des Unternehmens – einschließlich Prozessen, Mitarbeitern, Partnern und Assets – festgeschriebene Anforderungen genau erfüllen. Im Wesentlichen gibt es drei Arten der Compliance - Compliance auf rechtlicher, geschäftlicher und unternehmensinterner Ebene.

- Compliance auf rechtlicher Ebene bezieht sich auf die Einhaltung brancheninterner und gesetzlicher Bestimmungen. Sie ist je nach den lokalen, regionalen und globalen Vorgaben häufig unterschiedlich ausgestaltet.
- Compliance auf geschäftlicher Ebene bezieht sich auf die Einhaltung von Lizenzbedingungen, Datenschutzrichtlinien und anderen Vereinbarungen mit Partnern, Händlern und Kunden.
- Compliance auf unternehmensinterner Ebene bezieht sich auf die Einhaltung interner Richtlinien wie Ethik-, Sicherheits- und Mitarbeiterrichtlinien.

Bei Compliance-Verletzungen steht viel auf dem Spiel. Sie können Zeit und Geld kosten und schlimmstenfalls juristische Strafen nach sich ziehen. Ein Beispiel: Erst kürzlich verstieß beispielsweise eine große Einzelhandelskette gegen die Datensicherheitsstandards der Kreditkartenbranche und setzte dadurch Millionen von Kundenkonten dem Risiko eines Hacker-Angriffs aus. Das Unternehmen zahlte eine Geldstrafe in Millionenhöhe. Als noch schlimmer erwiesen sich jedoch der Umsatzverlust und der Schaden für die Marke, als der Vorfall in ganz Nordamerika Schlagzeilen machte.

Das Compliance-Zeitalter

Unternehmen müssen heute eine überwältigende Flut von gesetzlichen Vorschriften und Richtlinien einhalten. Andernfalls drohen ihnen ernste Konsequenzen. Die folgende Auflistung ist nur ein Auszug der bekanntesten Gesetze, Richtlinien, Frameworks, Normen und Kontrollorgane, die die aktuelle Compliance-Landschaft prägen.

- Sarbanes-Oxley Act von 2002 (SOX)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- Federal Information Security Management Act of 2002 (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Vom Basler Ausschuss für Bankenaufsicht vorgeschlagene Eigenkapitalvorschriften für Banken (BASEL II)
- Payment Card Industry Security Standards Council (PCI)
- IT Infrastructure Library (ITIL)
- Control Objectives for Information and related Technology (COBIT)
- International Organization for Standardization (ISO)
- IT Governance Institute (ITGI)
- Center for Internet Security (CIS)

Compliance-Herausforderungen

Compliance-Management ist in modernen Großunternehmen ein komplizierter Prozess mit vielen Herausforderungen. Die meisten Unternehmen sind mit einer Vielzahl von Compliance-Standards aller drei Arten konfrontiert. Die Durchführung von Compliance-Audits und die Korrektur von Mängeln ist ein kostspieliger und langwieriger Prozess. Häufig sind die für Compliance-Prüfungen benötigten Informationen über IT-Silos verteilt und schwer zu finden und zu erfassen, da sich in der Regel mehrere Abteilungen die Zuständigkeit für Compliance-Fragen teilen. Diese Arbeitsteilung führt üblicherweise zu unvollständigen, inkonsistenten Berichten, die vor ihrer Fertigstellung bereits veraltet sind.

Zahllose IT-Abteilungen haben mit aufwändigen, zeitraubenden und teuren manuellen Prozessen versucht, dieser Komplexität Herr zu werden. Vielen liegen auf Papier verfasste Richtlinien zugrunde, die schwer zu verbreiten und zu aktualisieren, aber leicht zu ignorieren sind. Manuelle Korrekturprozesse sind arbeitsintensiv und lassen sich weder steuern noch überprüfen. Die Datenerfassung ist ineffizient, fehlerträchtig, nicht wiederholbar und auf Zeitpunkte beschränkt, die im Nu nicht mehr aktuell sind.

Es sieht so aus, als ob nachhaltige IT-Compliance kaum zu erreichen sei. Doch es gibt eine Lösung. Automatisierung ist der Schlüssel zum Schutz Ihres Unternehmens vor übermäßigen Compliance-Kosten und den Konsequenzen, die Ihnen drohen, wenn Sie Compliance-Anforderungen nicht erfüllen.

HP Ansatz zur Compliance-Automatisierung

IT-Abteilungen können durch Automatisierung ineffiziente und teure manuelle Compliance-Prozesse durch eine kontinuierliche, durchsetzbare Compliance, schnelle und effektive Mängelkorrekturen sowie aktuelle und genaue Berichte ersetzen. Außerdem lassen sich Richtlinien, Betriebsabläufe, Prozesse und die Berichterstellung gleichermaßen automatisieren, sodass Compliance-Anforderungen in der gesamten IT-Infrastruktur erfüllt werden.

Auf der Grundlage von HP Automatisierungslösungen haben wir einen vier Schritte umfassenden Prozess (Abbildung 1) zur Compliance-Automatisierung entwickelt. Er ermöglicht die Erstellung von Berichten zu allen drei Arten von Compliance-Anforderungen – auf rechtlicher, geschäftlicher und unternehmensinterner Ebene. IT-Komponenten wie Server, Datenbanken, Netzwerkeinheiten, Speicher und Clients unterstützen Prozesse zur Erfassung von Compliance-relevanten Informationen.

Abbildung 1
Mit dem HP Ansatz zur Compliance-Automatisierung kann Ihr IT-Team die Konformität mit Compliance-Anforderungen auf rechtlicher, geschäftlicher und unternehmensinterner Ebene für alle Server, Datenbanken, Netzwerkdienste, Speichereinheiten und Clients dokumentieren.

1. Definition von Richtlinien und Audits. **2.** Abruf von Live-Updates für Richtlinien. **3.** Erstellung genauer, aktueller und umfassender Reports. **4.** Korrektur durch automatisiertes Änderungsmanagement.

Definition von Richtlinien und Audits

Im ersten Schritt werden Compliance-, Sicherheits- und Best-Practice-Richtlinien für alle Infrastrukturelemente definiert und global zur Verfügung gestellt. Des Weiteren werden alle Aktionen in einem digital signierten Auditprotokoll erfasst.

Abruf von Richtlinien-Updates

Nach der Definition von Richtlinien und Audits wird im nächsten Schritt der Download von aktualisierten Regeln, Vorschriften und Richtlinien automatisiert. So ist Ihr Audit-Team stets über die jüngsten Änderungen informiert und kann sofort bestimmen, ob am Audit und den Korrekturrichtlinien Änderungen vorzunehmen sind. Wenn Sie diesen Schritt auslassen, laufen Sie Gefahr, das Audit nicht zu bestehen, weil Ihre Prozesse zwar effektiv, aber nicht mit den neuesten regulatorischen Details synchronisiert sind.

Erstellung von genauen, aktuellen und umfassenden Reports

Als Nächstes ist eine flexible und anpassbare Erstellung von Compliance-Reports erforderlich, die auf aktuellen und historischen Daten zu den verschiedenen Services basiert. Indem Sie Ihrer Konfigurationsmanagement-Datenbank den Zugriff auf zusammengeführte Compliance-Daten ermöglichen und den Weg für die Ad-hoc-Erstellung von Out-of-the-Box Compliance-Reports ebnen, die auf PCI, SOX, HIPAA, FISMA und andere Bestimmungen zugeschnitten sind, statten Sie Ihre Auditoren mit den erforderlichen Daten für Konformitätsprüfungen aus. Durch die Verfassung von Reports zur Regelkonformität von Änderungen gemäß Standard-Frameworks wie ITIL und COBIT, sind Sie gleichermaßen auf die Einhaltung unternehmensinterner Richtlinien vorbereitet.

Korrektur durch automatisiertes Änderungsmanagement

Schließlich müssen Sie Korrekturen an den Systemen und Geräten vornehmen, die Compliance-Anforderungen nicht erfüllen. Automatisierung strafft den Änderungsprozess durch koordinierte Abläufe und Übergänge zwischen Teams, Abteilungen und Kompetenzbereichen. Standardisierte Änderungsmanagementprozesse für Ihre physischen und virtuellen IT-Assets mindern die Fehleranfälligkeit und das Ausfallrisiko.

HP Automatisierungslösungen

Mit einer einheitlichen Compliance-Strategie für Ihre gesamte IT-Infrastruktur legen Sie den Grundstein für Kontinuität im Compliance-Management, für schnelle und effektive Korrekturen sowie für ein sorgfältiges Reporting, sodass Sie Compliance-Herausforderungen in traditionellen und virtuellen IT-Infrastrukturen genauso meistern wie in der Cloud. HP unterstützt diesen Ansatz mit einer Fülle von Automatisierungslösungen (Abbildung 2).

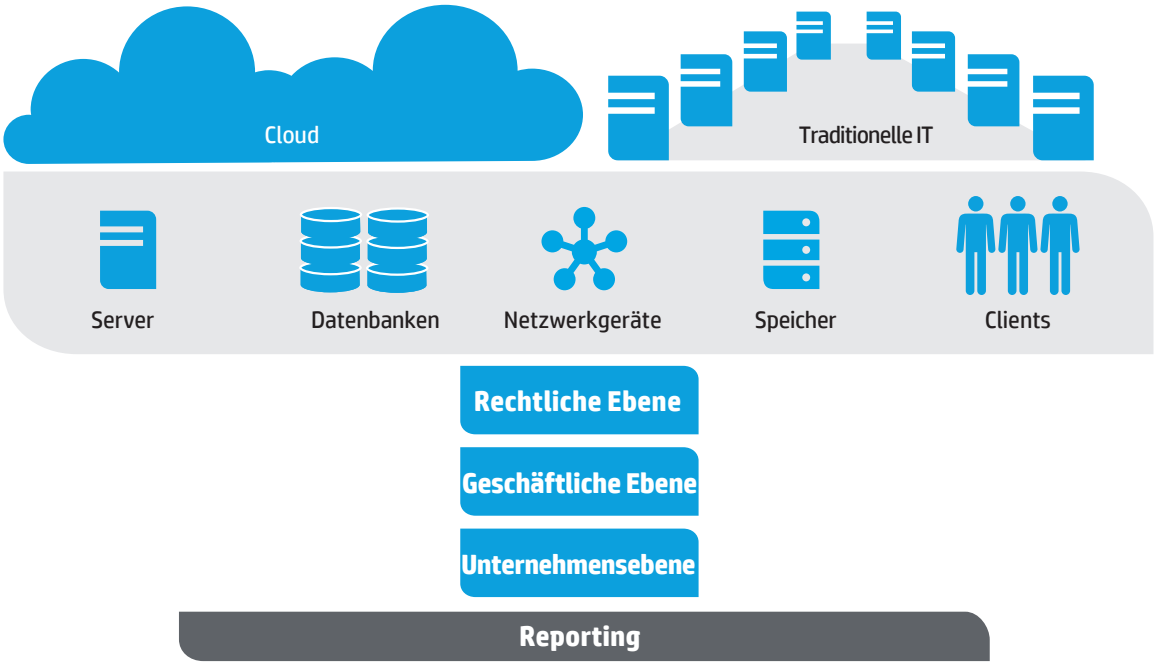
HP Software wie Server Automation, Network Automation, Client Automation, Storage Essentials und Database and Middleware Automation ist das Fundament für die Festlegung und Umsetzung von Unternehmensrichtlinien. Diese Tools bilden den Rahmen für die Definition Ihrer Compliance-Richtlinien und -Audits.

HP BSA Essentials Abonnementservices für Sicherheits- und Compliance-Anforderungen bauen auf diesem Software-Fundament auf und liefern vorkonfigurierte Compliance-Inhalte, die HP Server Automation, HP Network Automation und HP Client Automation die Umsetzung von Compliance-Richtlinien nach Industriestandard ermöglichen. Das Abonnement umfasst auch die Bereitstellung von aktuellen Hinweisen zu Sicherheitslücken, die in umsetzbare Richtlinien integriert werden.

Alle Softwarekomponenten – HP Server Automation, HP Network Automation, HP Client Automation, HP Storage Essentials und HP Database and Middleware Automation – bieten Funktionen zur Erstellung von Reports zu den von ihnen verwalteten Einheiten. HP Business Service Automation Essentials ermöglicht die Erstellung von Out-of-the-Box Compliance-Reports und bietet eine einfach zu bedienende Drag-and-Drop-Benutzeroberfläche für die Erstellung von angepassten Reports. Audit-Trails für die Überwachung und Protokollierung von ausgeführten Prozessen und Aufgaben liefern eine operative und zusammenfassende Sicht auf die Compliance-Historie.

HP Operations Orchestration Software dient zur Dokumentation und Durchführung von standardisierten Änderungsprozessen für die automatisierte Korrektur von Einheiten, die Compliance-Anforderungen nicht erfüllen. Dies erleichtert Ihnen, die Konformität mit externen Vorschriften, internen Richtlinien und Best-Practice-Frameworks wie ITIL sicherzustellen.

Abbildung 2
HP Compliance-Automatisierung ist eine Komplettlösung für das Compliance-Management in der gesamten IT-Infrastruktur



Erfolgreiche Compliance-Automatisierung - Beispiele aus der Praxis

- **Server:** Ein weltweit agierendes Technologieunternehmen hat Compliance-Prozesse auf 800 Servern automatisiert und dadurch den Zeitaufwand für Compliance-Prüfungen von 32 Wochen auf zwei Tage verkürzt.
- **Netzwerkgeräte:** Der Anbieter eines weltweiten Internet-Portals fiel regelmäßig bei Audits durch und konnte nur etwa 3 % der Compliance-Anforderungen für Netzwerkgeräte erfüllen. Durch die Automatisierung von Compliance-Prüfungen und Korrekturprozessen konnte das Unternehmen die Compliance-Anforderungen geräteübergreifend zu 100 % erfüllen.
- **Clients:** Eine US-amerikanische Wertpapierfirma benötigte zwei Monate für das Aufspielen von Patches auf allen Clientgeräten und konnte die Compliance-Anforderungen meistens nicht erfüllen. Das IT-Team automatisierte die Patching- und Compliance-Prozesse für die Clients, sodass die Patches in weniger als fünf Tagen auf allen Clientsystemen installiert waren und diese die Compliance-Anforderungen erfüllten.

Zusammenfassung

Ihr Unternehmen kann es sich nicht leisten, gegen Vorschriften, Gesetze, Lizenz- und Datenschutzvereinbarungen sowie interne Richtlinien zu verstoßen. Wenn Sie jedoch versuchen, den immer zahlreicheren Compliance-Anforderungen mit manuellen, isolierten Prozessen zu begegnen, ist ein Scheitern wahrscheinlich.

Compliance-Automatisierung, die auf branchenführenden, praxiserprobten HP Lösungen basiert, kann Ihnen dagegen die Gewissheit geben, dass Ihr Unternehmen gegen die Folgen von Compliance-Verletzungen abgesichert ist. Automatisierung kann auch zur Reduzierung Ihrer Betriebskosten beitragen und Ihren IT-Mitarbeitern mehr Freiraum für Innovationen eröffnen. Wenn Sie mehr über die Vorteile der Compliance-Automatisierung für Ihre IT-Abteilung und Ihr Unternehmen erfahren möchten, sollten Sie sich noch heute an Ihren HP Vertriebsbeauftragten wenden.

4AA2-9515DEE, erstellt Juni 2012