System zur Identifizierung von Verstößen gegen Sicherheitsrichtlinien und potenziellen Sicherheitsschwachstellen

Tivoli® software

IBM Tivoli Security Compliance Manager

Highlights

- ***Senkung von Kosten- und Zeitaufwand durch Automatisierung von Sicherheitssuchläufen auf Server- und Desktopsystemen***
- ***Schnelle, einfache, proaktive und kosteneffiziente Lösung für den Schutz der IT-Infrastruktur im Unternehmen mit Funktionen zur präventiven Identifizierung von Sicherheitsschwachstellen***
- ***Integrierte Best Practices-Richtlinien und -Berichte für optimale Implementierung und Wertschöpfung***
- ***Effektive Lösung für die Bewertung und Überwachung der unternehmensweiten Einhaltung von Sicherheitsrichtlinien***

Die Notwendigkeit der Erweiterung und Überprüfung von Sicherheitslösungen

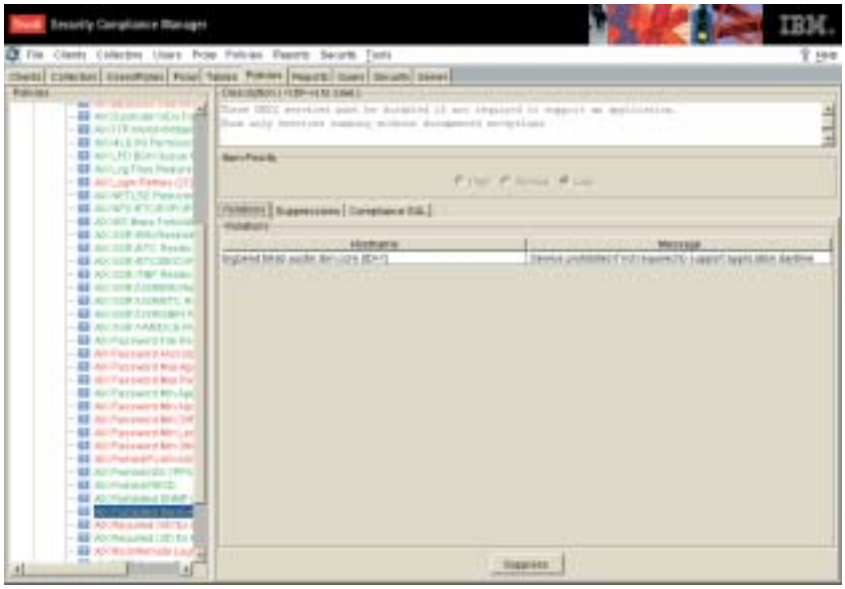
In den vergangenen Jahren sahen sich IT- und Sicherheitsadministratoren in zunehmendem Maß mit Angriffen durch Viren und Computerwürmer konfrontiert. Viele dieser Attacken kommen von außerhalb des Unternehmens. Andere wiederum werden innerhalb der Unternehmensgrenzen durch menschliche Fehler und Nachlässigkeiten hervorgerufen. Unabhängig von deren Herkunft kann das Eindringen in das Sicherheitssystem eines Unternehmens zu Zeitverlusten, beschädigten oder zerstörten Daten, Beeinträchtigungen der Glaubwürdigkeit, Rechtfertigungssituationen oder gar zu Rechtsstreitigkeiten führen.

90 Prozent aller Sicherheitsverstöße können durch Implementierung und Umsetzung konsistenter, unternehmensweiter Sicherheitsrichtlinien vermieden werden. IBM Tivoli Security Compliance Manager unterstützt in seiner Funktion als Frühwarnsystem kleine, mittlere und große Unternehmen bei der Erkennung von Verstößen gegen solche Sicherheitsrichtlinien und potenziellen Sicherheitsschwachstellen noch bevor es zu einer Sicherheitsverletzung kommt. Unternehmen steht damit eine schnelle, kosteneffiziente und proaktive Möglichkeit für die Erfassung und Verwaltung von Informationen zum aktuellen Stand der internen Sicherheits- und Diagnosesysteme zur Verfügung.

Ein Thema, das zunehmend an Bedeutung gewinnt, ist die Einhaltung von Unternehmensrichtlinien, die als Antwort auf die wachsende Anzahl von gesetzlichen Regelungen in Bezug auf Datenschutz und Datenintegrität ins Leben gerufen werden. Deshalb sollte ein entsprechendes System eingesetzt werden, das die Einhaltung der Unternehmensrichtlinien überprüft.

Automationslösungen zur Optimierung zeitaufwendiger Routineprozesse

Manuelle Prüfprozesse zur Einhaltung von Sicherheitsrichtlinien können zeit- und kostenaufwendig sein und oft Tage dauern. Leider sind sie auch anfällig für menschliche Fehler und Inkonsistenzen. Tivoli Security Compliance Manager basiert auf dem On Demand Automationsansatz, dem zentralen Element der Softwarestrategien von IBM. Zentrale und automatisierte Checks zur Einhaltung von Sicherheitsrichtlinien können in der Regel innerhalb von Minuten durchgeführt werden. Sie befreien Administratoren von zeitaufwendigen Routineaufgaben, wodurch sich wiederum mehr Effizienz, Kosteneinsparungen und eine Senkung der Risiken durch menschliche Fehler erzielen lassen.



Tivoli Security Compliance Manager stellt für den schnellen Einstieg Sicherheitsrichtlinien als standardisierte Templates zur Verfügung. Diese kann der Kunde nach seinen Vorstellungen ändern oder neu erstellen, um den Anforderungen des Unternehmens gerecht zu werden.

Best Practices-Richtlinien – Bestandteil des Tivoli Security Compliance Manager-Pakets

Zum Lieferumfang des Tivoli Security Compliance Manager gehören sofort einsatzfähige Best Practices-Sicherheitsrichtlinien und vorgefertigte Berichte. Aufbauend auf einer flexiblen und skalierbaren Java™-Struktur können mit diesem Produkt die vorhandenen Templates individuell angepasst und daraus optimierte und sinnvolle Sicherheitsrichtlinien erstellt werden. Mit Hilfe der GUI-Schnittstelle können Sicherheitsadministratoren auf effiziente Weise anhand so genannter „Richtliniensnapshots“ die Einhaltung der vorgegebenen Richtlinien unternehmensweit ermitteln, die Verstöße gegen Sicherheitsrichtlinien aufdecken, Benutzer auf die Nichteinhaltung der Richtlinien hinweisen und Ratschläge zur Behebung solcher Situationen geben. Die Software gibt Warnungen bei einem festgestellten Verstoß in den Ampelfarben rot, gelb und grün aus. Der Administrator weiß damit sofort, bei welchen Systemen im Unternehmen Kennwörter falsch definiert wurden, abgelaufene Antiviren-Signaturdateien oder Betriebssystem-Hotfixes, gefährliche oder nicht erforderliche Services usw. vorhanden sind. Folgeprüfungen zur Einhaltung von Sicherheitsrichtlinien führen zu einem vollständigen Bild, das aufzeigt, wie und wo Sicherheitsverstöße behoben wurden und ob die bestehenden Richtlinien eingehalten werden.

Reduzierung komplexer, kostspieliger Prozesse bei gleichzeitiger Produktivitätsoptimierung

Die als Templates gelieferten Sicherheitsrichtlinien tragen dazu bei, die komplexen, zeitaufwendigen und kostspieligen Prozesse für die Einhaltung von Richtlinien zu reduzieren. Diese sofort einsatzbereiten Sicherheitsrichtlinien bilden den Rahmen für Sicherheitsadministratoren, auf dem diese aufsetzen können, ohne bei Projektbeginn immer wieder alles von Anfang an neu aufbauen zu müssen.

Tivoli Security Compliance Manager setzt den Ansatz der On Demand Automation in die Realität um, indem statt kostspieliger und aufwendiger manueller Sicherheitsprüfungen automatische Richtlinienprüfprozesse zum Einsatz kommen. Die Automatisierung dieser Vorgänge trägt dazu bei, den Zeitaufwand für die Verwaltung von Sicherheitsrichtlinien oder Konformitäts- und Sicherheitsprotokollen zu reduzieren. Weiteres

Einsparpotenzial ergibt sich aus der Tatsache heraus, dass potenzielle Sicherheitsrisiken auf Systemen wie IBM AIX, Solaris, HP-UX, Microsoft® Windows®, Linux und Linux on zSeries frühzeitig erkannt werden, bevor es zu einer Sicherheitsverletzung kommt.

Tivoli Security Compliance Manager ist zudem mit verschiedenen Autonomic-Funktionen ausgestattet. Hierzu gehört u. a. eine „Heartbeat"-Funktion, die automatisch in regelmäßigen Abständen Impulse von den verwalteten Endpunkten zum zentralen Server sendet. Dadurch wird dem System mitgeteilt, dass die Systeme auf dem aktuellen Stand sind und fehlerfrei laufen. Über diese Autonomic-Funktion kann die Software relevante, Java-basierte Endpunkte selbst verwalten und automatisch aktualisieren. Als Teil der On Demand Initiative von IBM umfasst dieser Automationsansatz in Bezug auf die Einhaltung von Sicherheitsrichtlinien auch Supportleistungen für unsere Kunden, die ihr Unternehmen gegen drohende Gefahren widerstandsfähiger und anpassungsfähiger machen wollen.

Integration in IBM Tivoli-Produkte für automatisches Sicherheitsmanagement

Tivoli Security Compliance Manager sendet Informationen zu Sicherheitsverstößen oder zur Nichteinhaltung von Richtlinien direkt an die verschiedenen Tivoli-Tools für automatisches Sicherheitsmanagement, wodurch Verstöße gegen Sicherheitsrichtlinien und damit verbundene Risiken unmittelbar sichtbar werden. Durch die Integration in und die Nutzung von anderen Tivoli-Softwareprodukten wie IBM Tivoli Risk Manager, IBM Tivoli Enterprise Console und IBM Tivoli Configuration Manager können Unternehmen selbst aktiv werden, wenn es darum geht, Schaden vom Unternehmen abzuwenden und Sicherheitsverstöße zu beheben. Durch die Koppelung von Tivoli Security Compliance Manager mit diesen Tivoli-Lösungen entfallen nicht benötigte Services, Änderungen von Berechtigungen, Software-Upgrades oder die Implementierung von Patches.

Weitere Informationen

Wenn Sie mehr über Tivoli Security Compliance Manager und integrierte Lösungen von IBM erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner, oder besuchen Sie uns unter ibm.com/tivoli/products/security-compliance-mgr

Tivoli Software von IBM

Als integraler Bestandteil der umfassenden IBM On Demand Infrastrukturlösungen hilft Tivoli Management-Software traditionellen Unternehmen, On Demand Unternehmen und Internetunternehmen weltweit bei der Maximierung ihrer getätigten und kommenden IT-Investitionen. Mit Unterstützung erstklassiger IBM Service-, Support- und Forschungsleistungen bietet Tivoli-Software eine nahtlos integrierte und flexible On Demand Lösung für Infrastrukturmanagement, die, aufbauend auf widerstandsfähigen Sicherheitsfunktionen, Mitarbeiter, Geschäftspartner und Kunden miteinander verbindet.

Hardwarevoraussetzungen

Prozessor- und Speichervoraussetzungen für Tivoli Security Compliance Manager-Server

Tivoli Security Compliance Manager-Implementierung	Prozessor	Speicherbedarf
Kleinunternehmen (1-500 Clients)	1	512 MB RAM
Mittleres Unternehmen (501-2.500 Clients)	2	512 MB RAM
Großunternehmen (2.501-10.000 Clients)	2-4	2-4 GB RAM

5 MB Plattenplatz für die Installation des Serverpakets erforderlich.

Plattenplatz- und Speicherbedarf für Client und Collectors

Plattenplatz- und Speicherbedarf für Tivoli Security Compliance Manager-Client

Clientplattform	Plattenplatzbedarf für Installationsverzeichnis	Plattenplatzbedarf für temp. Verzeichnis	Speicherbedarf
AIX	64 MB	45 MB	75 MB RAM
HP-UX	64 MB	6 MB	75 MB RAM
Linux	64 MB	46 MB	75 MB RAM
Solaris	64 MB	65 MB	75 MB RAM
Windows	64 MB	44 MB	75 MB RAM

Hinweis: Die Angaben für die Plattform HP-UX sind niedriger als die Angaben für die anderen Plattformen, weil Java Runtime Environment nicht im HP-UX-Clientpaket enthalten ist.

Plattenplatz- und Speicherbedarf für Verwaltungstools

Plattenplatz- und Speicherbedarf für die Tivoli Security Compliance Manager-Administrationskonsole

Administrationskonsole (Plattform)	Plattenplatzbedarf für Installationsverzeichnis	Plattenplatzbedarf für temp. Verzeichnis	Speicherbedarf
Windows	64 MB	42 MB	128 MB RAM (Minimum) 256 MB RAM (empfohlen)

Softwarevoraussetzungen

Voraussetzungen für Tivoli Security Compliance Manager:
IBM DB2 Universal Database, Version 7.2 oder 8.1 (Tivoli Security Compliance Manager 5.1 beinhaltet DB2 Universal Database, Version 8.1.)

Unterstützte Betriebssysteme
In der folgenden Tabelle sind die unterstützten Betriebssysteme für Tivoli Security Compliance Manager-Server, -Client und Administrationskonsole aufgeführt.

Tivoli Security Compliance Manager-Server

Betriebssystem	Level	Patch/Programmfix
AIX	5.1, 5.2	Kein Fixpack erforderlich
Windows 2000	Server	Aktuelles Fixpack
Solaris	2.8, 2.9	Aktuelles Fixpack
SUSE Linux Enterprise Server	8	Aktuelles Fixpack

Tivoli Security Compliance Manager-Client

Betriebssystem	Level	Patch/Programmfix
AIX	5.1, 5.2	Akt. kumulative Patches
HP-UX	11.0, 11i	Akt. kumulative Patches
Red Hat Linux	6.2, 7.0, 7.1, 7.2, 7.3, 8.0, 9.0	Akt. kumulative Patches
Solaris	2.6, 2.7, 2.8. 2.9	Akt. kumulative Patches
Windows NT®	4.0 Server, 4.0 Workstation	Akt. Servicepack und Security Roll Up Package
Windows 2000	Server, Advanced Server, Professional	Akt. Servicepack und Security Roll Up Package
Windows XP	Professional	Akt. Servicepack und Security Roll Up Package
Windows 2003	Server Standard Edition, Enterprise Edition	Akt. kumulative Patches
Red Hat Enterprise Linux	2.1	Akt. kumulative Patches
Red Hat Enterprise Linux Advanced Server	3.0	Akt. kumulative Patches
Red Hat Enterprise Linux for zSeries	3.0	Akt. kumulative Patches
Red Hat Enterprise Linux for iSeries oder pSeries	3.0	Akt. kumulative Patches
Red Hat Enterprise Linux for zSeries	7.2	Akt. kumulative Patches
Red Hat Enterprise Linux Advanced Server	2.1	Akt. kumulative Patches
SUSE Linux	7.0	Akt. kumulative Patches
SUSE Linux Enterprise Server	8	Akt. kumulative Patches
SUSE Linux Enterprise Server for zSeries	8	Akt. kumulative Patches
SUSE Linux Enterprise Server for iSeries oder pSeries	8	Akt. kumulative Patches

Tivoli Security Compliance Manager-Administrationskonsole

Betriebssystem	Level	Patch/Programmfix
Windows 2000	Professional	Akt. Servicepack und Security Roll Up Package
Windows XP	Professional	Akt. Servicepack und Security Roll Up Package

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

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

IBM Schweiz
Bändliweg 21, Postfach
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

ON DEMAND BUSINESS

G507-1072-01-GE