Tivoli software

IBM Tivoli Security Operations Manager

Highlights

- Zentralisierung von Sicherheitsoperationen organisations-, technologie- und prozessübergreifend
- Ausrichtung der Sicherheitsoperationen an den IT-Operationen und Geschäftsprioritäten für eine deutlich verbesserte Service-Verfügbarkeit
- Einhaltung von Compliance-Vorgaben und Richtlinien für das Risikomanagement im Unternehmen
- Schnellere Erkennung und Behebung von Sicherheitsverstößen

Die Verfügbarkeit von Netzwerk und Ressourcen ist für die die Gewährleistung von Geschäftsprozessen und Services ein äußerst wichtiges Kriterium. Unternehmen, Behörden und Serviceanbieter laufen Gefahr, Jahr für Jahr Verluste in Millionenhöhe zu erleiden, weil Computerwürmer und andere Attacken Unternehmensressourcen und Kundenservice-Anwendungen zum Absturz bringen. Daher ist die Sicherheit von Informationen eine der wichtigsten Problemstellungen jedes IT-Verantwortlichen.

Um die Verfügbarkeit von Ressourcen und Services zu optimieren und Kundeninformationen ausreichend zu schützen, stehen die zuständigen Sicherheitsteams vor vielfältigen Aufgaben:

- *Schnelle Erkennung und Handhabung von Sicherheitsverstößen*
- *Umsetzung von Sicherheitsrichtlinien*
- *Unterstützung von Prüfungs- und Compliance-Initiativen*

Das Problem liegt darin, dass bei jeder dieser Aktivitäten Sicherheitsdaten ins Spiel kommen, die im ganzen Unternehmen verteilt sind. Unternehmen und Serviceanbieter müssen in der Lage sein, auf diese Daten zuzugreifen und sie schnellstmöglich zu analysieren. In den heutigen komplexen Umgebungen mit Komponenten unterschiedlicher Hersteller kann dieses Problem nur mit einer automatisierten und integrierten Lösung angegangen werden.

IBM Tivoli Security Operations Manager ist eine solche Lösung, die gezielt auf diese Herausforderungen eingeht. Diese SIEM-Plattform (Security Information and Event Management) ist so konzipiert, dass Effektivität, Effizienz und Transparenz von Sicherheitsabläufen und Risikomanagement deutlich verbessert werden. Tivoli Security Operations Manager zentralisiert und speichert Sicherheitsdaten aus der gesamten Technologieinfrastruktur, woraus sich zahlreiche Vorteile ergeben:

- *Automatisierung der Erfassung, Korrelation und Analyse von Protokollen*
- *Automatische Erkennung und Untersuchung von Ereignissen sowie Einleiten der entsprechenden Maßnahmen*
- *Optimierung der Verfolgung und Handhabung von Ereignissen*
- *Überwachung und Umsetzung von Richtlinien*
- *Umfassende Berichtsfunktionen zur Unterstützung von Compliance-Initiativen*

Mit Tivoli Security Operations Manager können viele sich wiederholende, zeitintensive Aktivitäten im Zusammenhang mit effektiven Sicherheitsoperationen automatisiert werden. Diese IBM Lösung ist folglich ein sehr effizienter und kostenwirksamer Ansatz für optimale Sicherheitsabläufe.

Zentrale Protokollerfassung in komplexen Umgebungen

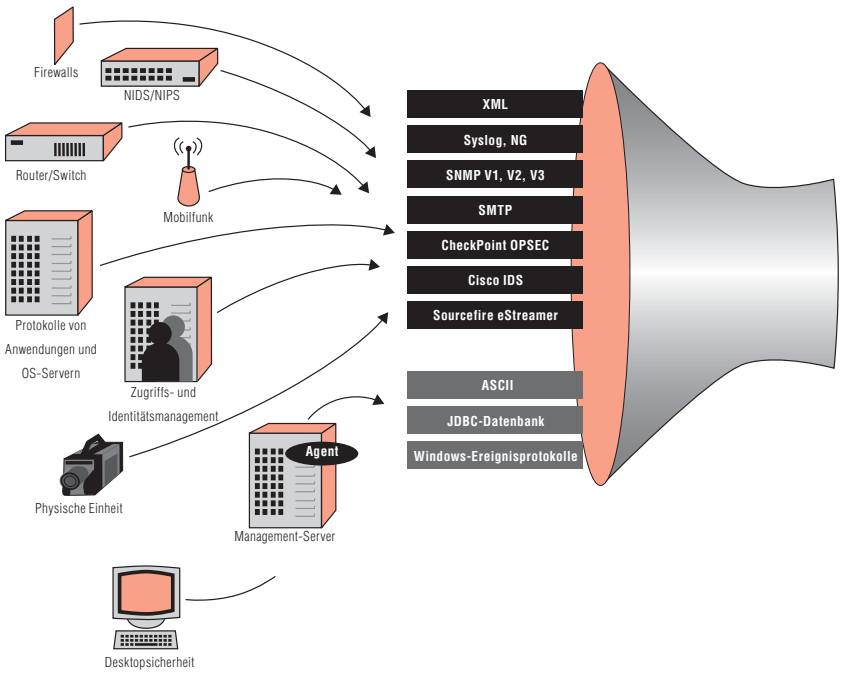
Um Attacken, Viren, potenziell gefährliche Fehlkonfigurationen und internen Missbrauch feststellen zu können, muss ein Sicherheitsteam eine Vielzahl von Ereignisdaten aus der gesamten Sicherheitsinfrastruktur analysieren. Dazu zählen:

- *Intrusion Detection-Systeme*
- *Firewalls*
- *Virtual Privat Networks (VPN)*
- *Antivirenprogramme*

Hinzu kommt, dass viele relevante Informationen von den Servern und Hosts typischer IT- oder Betriebsinfrastrukturen abgerufen werden müssen.

Häufig ist es so, dass die Datenmenge und die Anzahl der verteilten und unterschiedlichen Systeme in einem typischen Netzwerk die manuelle Analyse von Sicherheitsdaten nahezu unmöglich machen.

Folglich muss die Erfassung von Ereignissen aus unterschiedlichen Geräten und Systemen an einem zentralen Standort automatisiert werden. Dort werden die Daten korreliert, um die Reaktionen auf bestimmte Ereignisse und die damit verbundene Berichterstellung zu vereinfachen.



Tivoli Security Operations Manager stellt eine Plattform bereit, auf der Ihr Unternehmen Hostprotokolle, sicherheitsrelevante Ereignisse, Ressourcendaten und Verwundbarkeitsanalysen automatisch erfassen und für Analyse- und Korrelationszwecke heranziehen kann.

Die automatische Erfassung von Daten an einem zentralen Standort ist auch bei Compliance-Initiativen von besonderer Bedeutung. Viele Unternehmen speichern ihre Protokolldaten über lange Zeiträume hinweg, um bei Bedarf Protokollanalysen für diese Daten durchführen zu können.

Tivoli Security Operations Manager ist auch hierfür die ideale Plattform, über die Hostprotokolle, sicherheitsrelevante Ereignisse, Ressourcendaten und Daten zu Sicherheitslücken erfasst werden können. Dabei geben Sie selbst an, welche Datenmenge aus welchen Quellen von der Software herangezogen werden soll.

Tivoli Security Operations Manager erfasst dann die Daten mit Hilfe von Standard- und systemeigenen Protokollen wie Extensible Markup Language (XML), syslog, Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), CheckPoint OPSEC, Sourcefire eStreamer usw. Die Datenerfassung kann auch über den internen Universalagenten erfolgen. Tivoli Security Operations Manager erfasst bereits heute Ereignis- und Protokolldaten aus hunderten unterschiedlichen Einheiten ohne Vorbereitungs- oder Anpassungsaufwand. Darüber hinaus können kundenspezifische Programme und interne Anwendungen unterstützt werden.

Bessere Erkennung von Risiken durch geräteübergreifende Korrelation
Durch die Erfassung von Informationen aus der gesamten Infrastruktur unterstützt Tivoli Security Operations Manager bei der Erkennung von Attacken, Missbräuchen und Unregelmäßigkeiten. Die Software analysiert und priorisiert dabei Ereignisdaten mit Hilfe von vier zusätzlichen Korrelationsverfahren:

- *Regelbasierte Korrelation – erkennt bekannte Attacken und Richtlinienverstöße*
- *Korrelation von Sicherheitslücken – ordnet bekannte Attacken bekannten Sicherheitslücken im System zu*
- *Statistische Korrelation – erkennt Unregelmäßigkeiten durch erweiterte Analyse von Ereignissen und Hosts*
- *Anfälligkeitskorrelation – hilft bei der Ermittlung der Wahrscheinlichkeit von Sicherheitslücken bei Systemen*

Hinzu kommt, dass Tivoli Security Operations Manager anhand Ihrer Geschäftsprioritäten die Bedeutung von Ressourcen während des Korrelationsprozesses gewichten kann, um die Sicherheitsaktivitäten zu priorisieren. Wenn Sicherheitsanalysten also die Konsole benutzen, sehen sie keine endlose Liste mit sicherheitsrelevanten Ereignissen, sondern aussagekräftige Informationen, die entsprechend den vorgegebenen Zielsetzungen und Richtlinien priorisiert wurden.

Schnellere Risikominderung durch integrierte Untersuchungs- und Reaktionstools
Damit Sie den Zeitaufwand für die Handhabung von Attacken, Fehlkonfigurationen und Missbräuchen drastisch senken können, stehen Ihnen die integrierten Untersuchungs- und Reaktionstools von Tivoli Security Operations Manager zur Verfügung. Die IBM Software vereinfacht zudem den gesamten Eskalations- und Verfolgungsprozess. Zu den Untersuchungsfeatures gehören im Einzelnen:

- *Integrierte, einfach zu bedienende Untersuchungstools*
- *Automatische Reaktion auf Blockadegefahren und Close-the-Loop-Situationen*
- *Regionsübergreifende Verfolgung verdächtiger Aktivitäten*
- *Sicherheitsorientiertes Ticketsystem*

Mehr Effizienz durch Prozessintegration
Tivoli Security Operations Manager geht gezielt auf Ineffizienzen in den betrieblichen Abläufen ein, die durch isolierte IT-Abteilungen verursacht werden. Dabei wird der Fluss der Ereignisdaten zwischen den Teams des Sicherheits-, Netzwerk- und Systemmanagements vereinfacht. So kann Tivoli Security Operations Manager ganz eng in die Netzwerk- und Systemmanagementprodukte des Unternehmens wie Ereignismanager und Dashboards, in IBM Tivoli Enterprise Console und in Ticketsysteme im IT-Help-Desk-Bereich wie Remedy integriert werden. Dieser Integrationsansatz bringt viele Vorteile:

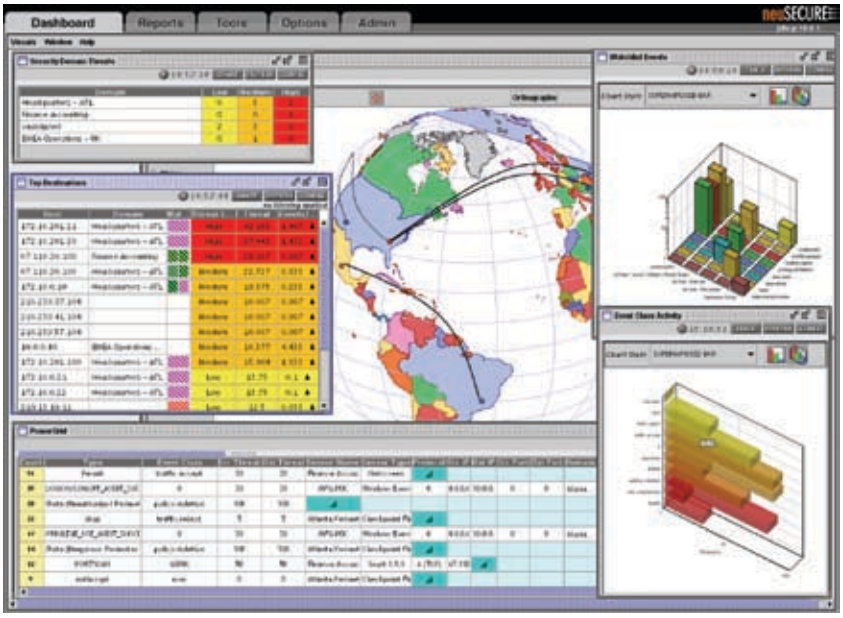
- *Unterstützung der Sicherheitsanforderungen von Geschäftsprozessen und Services*
- *Korrelation der Sicherheitsdaten mit Informationen aus der breiteren Betriebsumgebung*
- *Weitere Vereinfachung von Ereigniskorrekturen*

Tivoli Security Operations Manager kann auch problemlos in IBM Tivoli Identity Manager und IBM Tivoli Access Manager for e-business integriert werden, um IDs und Zugriffsrichtlinien beim Kunden verwalten und überwachen zu können. Dies erfolgt beispielweise durch die Einhaltung von Richtlinien und die schnelle Erkennung und Behebung möglicher Missbrauchsversuche.

Fundiertes Verständnis durch umfassende, aussagekräftige Berichte
Die Tivoli Security Operations Manager-Funktionen für Data-Mining, Erstellung von Langzeitberichten, Selbstüberwachung und Verfolgung während des Betriebs sind wichtige Komponenten, um Sicherheitstrends verstehen zu können. Hinzu kommt, dass diese Berichte den IT-Mitarbeitern helfen, relevante Sicherheitsinformationen an andere Zielgruppen wie Management und Prüfteams weiterzuleiten.

Die Features im Einzelnen:

- *Standard- und anpassbare Berichtsvorlagen*
- *Automatisch ablaufender Berichtsplaner*
- *Export von Diagrammen und Tabellen aus HTML, PDF und XML*
- *Selbstprüfung und Verfolgung aller Sicherheitsaktivitäten*



Dashboard von Tivoli Security Operations Manager.

Tivoli Security Operations Manager greift auf Informationen einer Datenbank für sicherheitsrelevante Ereignisse zu, um bedarfsgerecht die Erstellung von Langzeitberichten und die Ermittlung von Trends zu ermöglichen.

Wahlmöglichkeit zwischen mehreren Implementierungsoptionen für Ihre Umgebung

Die modulare Architektur von Tivoli Security Operations Manager kann problemlos an die Sicherheitsinfrastruktur im Unternehmen angepasst werden und mit ihr wachsen. Jede einzelne Komponente – das Event Aggregation-Modul, das Daten erfasst und normalisiert, der Central Management Server, der erweiterte Analysen und Korrelationen durchführt, und die Datenbank mit den Protokolldaten – kann auf verschiedene Hardwarekomponenten verteilt werden, oder alle Komponenten können zusammen implementiert werden.

Zudem können mehrere Event Aggregation-Module im Unternehmen implementiert werden, um größere Mengen an Ereignisdaten verarbeiten zu können oder die geografische Verteilung von Systemressourcen zu vereinfachen. Das folgende Beispiel soll dies verdeutlichen: Ein Kunde verwendet zwölf Event Aggregation-Module für seine geografisch verteilten Standorte, wodurch das Unternehmen die Erfassung und Verarbeitung der Daten verteilt organisieren kann.

Alle Event Aggregation-Module können zudem Daten an ein und denselben Central Management-Server senden. Die IBM Lösung bietet Unternehmen auch die Möglichkeit, mehrere Server einzusetzen, um die Verfügbarkeit weiter zu optimieren. Ist ein Server für ein Event Aggregation-Modul nicht verfügbar, wird das Ereignis an einen zweiten Central Management Server weitergeleitet.

Plattform für Managed Security Services

Neben seiner Funktion als kritische IT-Sicherheitsplattform für mittelständische und Großunternehmen kann Tivoli Security Operations Manager auch als stabile, bewährte Basislösung für den äußerst profitablen Bereich Managed Security Services eingesetzt werden. Dieselben Implementierungsoptionen, die Tivoli Security Operations Manager seine hohe Skalierbarkeit und Zuverlässigkeit verleihen, machen die IBM Lösung auch zum geeigneten Instrument für die Anforderungen von Umgebungen mit verteilten Services.

Tivoli Security Operations Manager unterstützt Anbieter von Managed Security Services wie folgt:

- *Senkung der Betriebskosten durch einen hohen Grad an Prozessautomatisierung*
- *Kürzere Realisierungszeiten durch schnellere Implementierung und sofort einsatzfähige Funktionen*
- *Abbildung der Service-Levels und Nutzen für den Kunden durch umfassende Berichtsfunktionen*

Fazit

Sicherheitsverstöße können gravierende, messbare Folgen nach sich ziehen: Umsatzeinbußen, Ausfallzeiten, Imageschäden, Beschädigung von IT-Ressourcen, Diebstahl von eigenen oder Kundendaten, hohe Bereinigungs- und Wiederherstellungskosten oder sogar Prozesskosten. Um diese Risiken weitestgehend auszuschließen, müssen sicherheitsbewusste Unternehmen in der Lage sein, Attacken schnell zu erkennen und darauf zu reagieren.

Tivoli Security Operations Manager bietet Ihnen eine ganzheitliche Sicht Ihrer Sicherheitsaufstellung und der verschiedenen Möglichkeiten, Detailabfragen/-analysen zu Attacken schnellstmöglich durchzuführen. Unternehmen steht damit ein nützliches und hilfreiches Tool zur Vermeidung von unbefugten Zugriffen und zur Optimierung der Sicherheit im Unternehmen zur Verfügung.

Tivoli Software von IBM

Tivoli Software unterstützt Unternehmen bei der effizienten Verwaltung von IT-Ressourcen, -Aufgaben und -Prozessen, um den sich ständig ändernden geschäftlichen Anforderungen gerecht zu werden, eine flexible und reaktionsschnelle Verwaltung von IT-Services zu ermöglichen und gleichzeitig die Kosten zu senken. Das IBM Tivoli Portfolio umfasst Softwarelösungen für die Bereiche Sicherheit, Compliance, Speicher, Leistung, Verfügbarkeit, Konfiguration, Prozesse und IT-Lebenszyklusverwaltung. Gestützt wird dies durch die weltweit erstklassigen IBM Leistungen in den Bereichen Service, Support und Forschung.

Tivoli Security Operations Manager auf einen Blick

Empfohlene Systemvoraussetzungen für den Central Management Server:

- Red Hat Enterprise Linux® ES 3.0-Plattform mit:
  - Dual Intel Pentium® IV-Prozessor mit 3,0 GHz oder höher
  - Min. 4 GB RAM
  - Min. 120-GB-Festplattenlaufwerk (der Speicherbedarf hängt in erster Linie von der Systemereignisrate sowie den Archivierungs- und Berichterstellungsaktivitäten ab)
- Sun Solaris 9-Plattform mit:
  - SunFire V440 Dual UltraSparc-Prozessor mit 1,5 GHz oder höher
  - Min. 4 GB RAM
  - Min. 146-GB-Festplattenlaufwerk

Empfohlene Systemvoraussetzungen für das Event Aggregation Module:

- Red Hat Enterprise Linux ES 3.0-Plattform mit:
  - Pentium IV-Prozessor mit 3,0 GHz oder höher
  - Min. 2 GB RAM
  - Min. 36-GB-Festplattenlaufwerk
- Sun Solaris 9-Plattform mit:
  - SunFire V240 Dual UltraSparc-Prozessor mit 1,5 GHz oder höher
  - Min. 2 GB RAM
  - Min.
  - 73-GB-Festplattenlaufwerk

Unterstützte Browser für die Clientkomponente:

- Microsoft® Internet Explorer 6.x oder höher
- Mozilla Firefox 1.7 oder höher
- Sun Java™ 1.4.2_08 oder höher

Unterstützte Datenbanken:

- MySQL 4.1
- Oracle Enterprise Edition 9i

Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie Tivoli Security Operations Manager Sie bei der zentralen Verwaltung und Überwachung von Sicherheitsoperationen unterstützt, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner – oder besuchen Sie uns unter:

ibm.com/tivoli

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 eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern.

Tivoli und Tivoli Enterprise Console sind Marken der IBM Corporation in den USA und/oder anderen Ländern.

Intel, Intel Inside (Logo), MMX und Pentium sind Marken der Intel Corporation in den USA und/oder anderen Ländern.

Java und alle Java-basierenden Marken und Logos sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft ist eine Marke von Microsoft Corporation in den USA und/oder anderen Ländern.

Andere Namen von Unternehmen, Produkten und Services können Marken oder Servicemarken anderer Unternehmen sein.

Hergestellt in den USA
06-06

© Copyright IBM Corporation 2006
Alle Rechte vorbehalten.

GC28-8415-00-GE