Überwachung auf externe und interne Mainframebedrohungen für mehr Sicherheit und einfachere Einhaltung von Vorschriften

Tivoli® software

IBM Tivoli zSecure Alert

Highlights

- Überwachung sensibler Daten auf Missbrauch zur Verbesserung der Zugriffskontrolle
- Nutzung konfigurierbarer Benachrichtigungen zur Analyse und zur Verbesserung der Sicherheit
- Aufdeckung von Konfigurationsfehlern, bevor andere sie ausnutzen
- Senkung der Betriebskosten, die durch Reaktionen auf Störungen entstehen
- Einfaches Versenden kritischer Alerts an Prüf- und Überwachungssysteme (inkl. Compliance)
- Verfügbar für z/OS-Systeme mit RACF oder CA ACF2

Der Mainframe-Computer steht als Repository für wichtige Unternehmensdaten immer mehr im Zentrum des vernetzten Unternehmens. Mitarbeiter, Berater und Kunden sind auf die wichtigen Informationen auf dem Mainframe-Computer angewiesen, weshalb es von erheblicher Bedeutung ist, diese wichtige Ressource vor internen und externen Bedrohungen und unerwünschten Konfigurationsänderungen zu schützen. Gleichzeitig müssen Sie potenziellen Verletzungen von Vorschriften vorbeugen.

Idealerweise wäre die Überwachung des Mainframe-Computers ein Teil Ihrer allgemeinen Lösung zur Überwachung von Sicherheitsrisiken. IBM Tivoli zSecure Alert ist eine nahezu in Echtzeit arbeitende Überwachungslösung, die die effiziente Überwachung des Mainframe-Computers auf Eindringlinge und inkorrekte Konfigurationen ermöglicht und so dieses Ziel erreichbar macht. Mit Hilfe eines schnelleren Ereignismanagements und optimierter Prüfungsfunktionen kann Tivoli zSecure Alert Ihnen dabei helfen, Ihre sicherheitsrelevanten Aktivitäten auf dem Mainframe-Computer zu minimieren. Darüber hinaus verbessert die Lösung die Systemverfügbarkeit und und ergänzt die Funktionen zur Zugriffskontrolle.

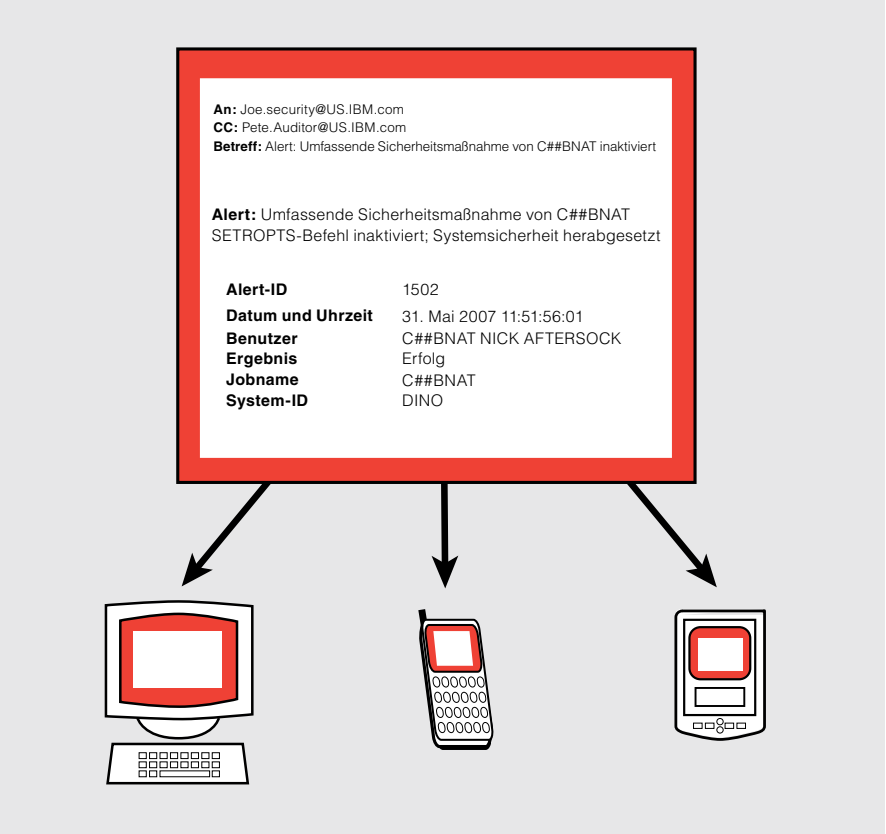
Überwachung kritischer Daten zur Unterstützung der Datenintegrität

Wenn auf bestimmte, äußerst wichtige Daten zugegriffen wird – selbst wenn dies durch berechtigte Benutzer geschieht –, dann sollten Sie darüber Bescheid wissen. Die Möglichkeit zur erfolgreichen Überwachung von Daten ist umso wichtiger, wenn Ihr Compliancestatus möglicherweise gefährdet ist. Tivoli zSecure Alert befindet sich auf dem Mainframe-Computer und überwacht Subsysteme mit IBM z/OS, IBM Resource Access Control Facility (RACF), CA ACF2™ und UNIX®. Durch die Verbindung einer Wissensbasis zu den möglichen Bedrohungen mit den Parametern Ihrer aktiven Konfiguration kann die Lösung Ressourcen identifizieren, die eines besonderen Schutzes bedürfen, und relevante Angriffsmuster isolieren.

Im Gegensatz zu anderen Produkten, die Angriffe nur auf der Grundlage von Informationen erkennen können, die von IBM System Management Facility (SMF) bereitgestellt werden, kann Tivoli zSecure Alert schädliche Aktivitäten auch dann aufdecken, wenn diese nicht im Ereignisprotokoll (SFM-Record) aufgezeichnet sind. Und durch die Fähigkeit, Echtzeitaktivitäten mit aktuellen Mustern zu vergleichen, trägt Tivoli zSecure Alert zur Erkennung weiterer Bedrohungen bei.

Mit seiner breiten Palette von Überwachungsfunktionen kann Tivoli zSecure Alert Ihnen helfen, zahlreiche Arten von Angriffen und Konfigurationsrisiken zu erkennen:

- *Unerwünschte Anmeldungen und Anmeldeversuche:*
  - *Anmeldung durch unbekannte Benutzer*
  - *Anmeldung mit der Notfall-Benutzer-ID*
  - *Anmeldung durch privilegierte UNIX-Benutzer*
- *Änderungen, die Sicherheitsrichtlinien verletzen:*
  - *Hinzufügen oder Entfernen von Systemberechtigungen*
  - *Widerruf von Produktions-Benutzer-IDs*
  - *Übermäßige Gewährung umfassenden Zugriffs*
  - *Inaktivierung von Optionen für die Systemsicherheit (SETROPTS, GSO)*
  - *Inaktivierung des Prüfprotokolls*
- *Verdächtige Aktivitäten im UNIX-Subsystem:*
  - *Verstöße gegen Regeln zum Dateizugriff*
  - *Durch Authorized Program Facility (APF) oder anderweitig kontrollierte Programmzuweisung*
  - *Globale Schreib- oder Lesespezifikation*



Tivoli zSecure Alert bietet zeitnahe Benachrichtigungen, damit Sie effizienter auf Störungen reagieren können. Konfigurierbare Benachrichtigungen können per E-Mail, Mobiltelefon und auf Papier sowie an zentrale Sicherheits- und Netzmanagementkonsolen versendet werden.

Darüber hinaus kann Tivoli zSecure Alert feststellen, ob Ihre zentralen Systemressourcen durch das Auftreten eines oder mehrerer bestimmter Ereignisse gefährdet sind:

- *Aktualisierung eines Systemdatensatzes*
- *Dynamische Hinzufügung eines APF-Datensatzes*
- *Volle SMF-Puffer, mit der Gefahr von Datenverlust*
- *Mit nicht spezifizierter Berechtigung gestartete Tasks*

Schnelle, flexible Benachrichtigungen zur Vermeidung kostspieliger Schäden

Zeitnahe Benachrichtigungen sind ein entscheidender Bestandteil des Überwachungsprozesses, da sie Ihnen ermöglichen, schnell zu reagieren, um weitere Schäden zu verhindern. So möchten Sie beispielsweise erkannte Konfigurationsfehler beheben, bevor andere sie ausnutzen können. Tivoli zSecure Alert bietet leistungsfähige Benachrichtigungsfunktionen, damit relevante Mitarbeiter schnell über Änderungen, inkorrekte Zugriffe und Sicherheitslücken informiert werden. Die Benachrichtigungen sind in der benutzerfreundlichen Consul Auditing and Reporting Language (CARLa) geschrieben und können zur Versendung per E-Mail, Mobiltelefon und Pager sowie als Textnachricht angepasst werden. Die Auswahl und das Layout können auch von einer ISPF-Anwendung aus dynamisch rekonfiguriert werden.

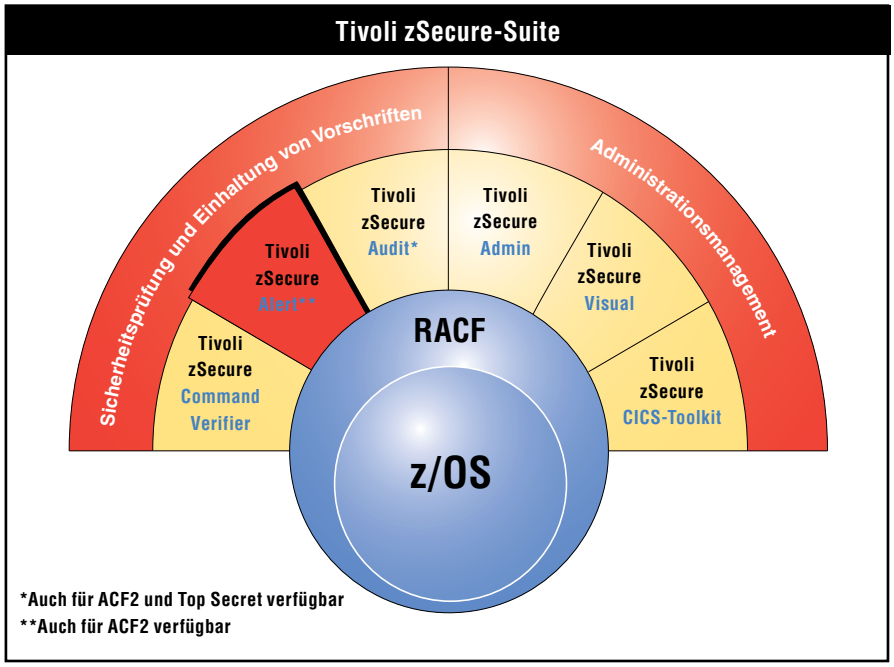
Tivoli zSecure Alert kann mit anderen Werkzeugen integriert werden. So können Sie relevante Benachrichtigungen an Ihre zentrale Sicherheits- oder Netzmanagementkonsole schicken. Sie können beispielsweise Benachrichtigungen im Simple Network Management Protocol (SNMP) bei Verletzungen von Sicherheitsrichtlinien an das IBM Tivoli Compliance Insight Manager-Dashboard, für die Echtzeitkorrelation und die Überwachung von Bedrohungen an den IBM Tivoli Security Operations Manager, an die IBM Tivoli Enterprise Console und an viele weitere Ziele senden.

Treffen Sie effektive Gegenmaßnahmen

Tivoli zSecure Alert geht über herkömmliche Lösungen zur Erkennung von Angriffen hinaus und hilft Ihnen festzulegen, welche Gegenmaßnahmen Sie treffen sollten, wenn eine Bedrohung erkannt wird. So können Sie zum Beispiel eine Maßnahme, etwa den sofortigen Widerruf von Zugangsberechtigungen für einen Benutzer oder das Beenden einer Anwendung, vordefinieren und anpassen, wenn ein sicherheitsrelevantes Ereignis auftritt. Darüber hinaus können Sie „WTO“ -Nachrichten senden, um automatisierte Operationen auszulösen oder um RACF-Befehle autonom auszugeben.

Weitere Informationen

Tivoli zSecure Alert basiert auf jahrzehntelanger Erfahrung, gewonnen durch Tests auf Mainframe-Computersystemen und zusammengefasst in einer Wissensbasis zu möglichen Bedrohungen, die Sie schnell auf verdächtige Aktivitäten aufmerksam macht. Tivoli zSecure Alert kann nahtlos mit der gesamten Tivoli zSecure-Suite von Verwaltungs- und Prüfungslösungen für die unternehmensweite Sicherheit integriert werden und bietet so eine umfassende und durchgängige Arbeitsumgebung für das RACF-Sicherheitsmanagement.



Wenn Sie mehr darüber erfahren möchten, wie Tivoli zSecure Alert Ihrem Unternehmen helfen kann, potenzielle Sicherheitsverstöße zu erkennen, um in effektiver Weise Audit- und Sicherheitsprobleme zu lösen, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter:

ibm.com/tivoli

Tivoli zSecure Alert auf einen Blick

Systemvoraussetzungen:

- z/OS oder z/OS.e

Unterstützte Verwaltungsplattformen:

- RACF
- CA ACF2

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

Gedruckt in den USA
06-07

TAKE BACK CONTROL WITH Tivoli®

TID10370-DEDE-00