Umfassende Prüfberichte und Konformitätsanalysen zur Sicherheit von Großrechnern

Tivoli software

IBM Tivoli zSecure Audit

Highlights

- Senkung der Kosten für Ereigniserfassung und -analyse
- Identifizierung von Sicherheitsschwachstellen zur Minimierung der Risiken durch kostspielige Verstöße
- Nutzung angepasster Berichte zur Generierung grundlegender Sicherheits-prüfungen
- Protokollierung und Überwachung von Änderungen an den Basisdaten und an Bibliotheken
- Minimierung der Sicherheitsrisiken für RACF über dieselbe Schnittstelle
- Versionen für RACF, CA ACF2 und CA TSS verfügbar

Die Sicherheit ist eine wichtige Voraussetzung für die Kontrollstruktur jedes Unternehmens; vor allem in der vernetzten Wirtschaft von heute ist ein wirksamer Schutz vor IT-Sicherheitsrisiken unerlässlich. Die Folgen von Sicherheitsverstößen reichen von finanziellen Einbußen und unbefugtem Zugriff auf vertrauliche Informationen bis zu Diebstahl geistigen Eigentums und Schädigung des Ansehens. Zwar können Unternehmen diesen Problemen durch Prüfungen vorbeugen, die Beschaffung der dafür notwendigen Informationen kann jedoch ein mühsamer, zeitaufwendiger Prozess sein. Eine Möglichkeit, ein durch kurzfristige Prüfungen entstehendes Chaos zu vermeiden, besteht in der Implementierung eines automatisierten Routineprozesses für Prüfung und Berichterstellung.

IBM Tivoli zSecure Audit ist ein Prüfwerkzeug für Großrechner, mit dessen Hilfe Benutzer von IBM Resource Access Control Facility (RACF), CA ACF2 und CA Top Secret Security (TSS) die Mainframesicherheit und die Sicherheitsrichtlinien auf effiziente Art messen und deren Wirksamkeit überprüfen können. Mit Hilfe automatisch generierter Berichte, die in einem Standardformat angezeigt werden, können Sie schnell Probleme mit bestimmten Attributen im Umfeld einer bestimmten Ressource (zum Beispiel eines ungeschützten Datenbestandes) lokalisieren. Damit können Sie die Häufigkeit von Fehlern verringern und die Gesamtqualität der Services verbessern. Tivoli zSecure Audit wurde nicht nur ent-wickelt, damit RACF-, ACF2- und TSS-Benutzer ihre Aufgaben effizienter erfüllen können. Versierte Benutzer können mit diesem Werkzeug auch die Sicherheitsrichtlinien erweitern und besser durchsetzen und so die Sicherheit insgesamt deutlich erhöhen.

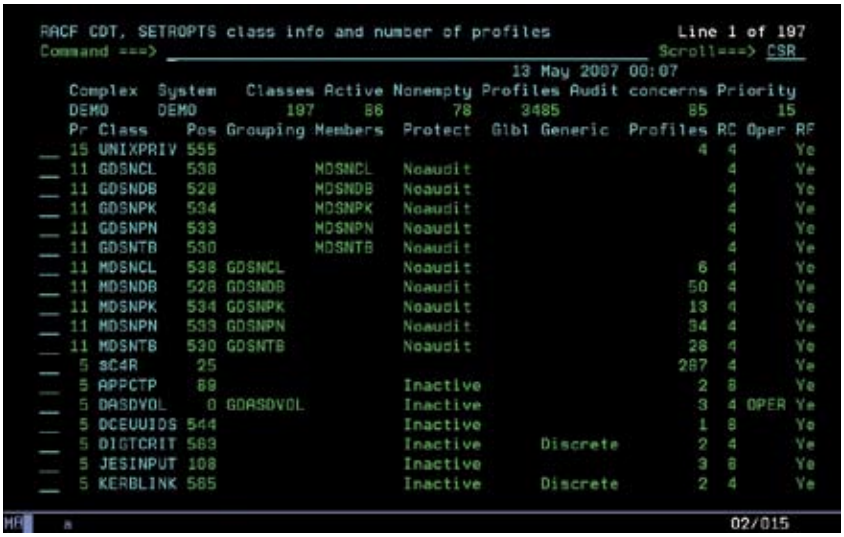
Effiziente Zusammenstellung und Analyse kritischer Informationen

Im Gegensatz zu Angeboten, die ihre Berichte nur anhand einer Datenbankkopie erstellen, ermöglicht Tivoli zSecure Audit den Zugriff auf die aktuellen Großrechnerdaten unter IBM z/OS mit RACF, ACF2 oder TSS und gewährleistet damit die Richtigkeit der Prüfungen bis zur letzten Minute. Die Analyse der aktiven Steuerblöcke des z/OS-Systems ermöglicht die schnelle Erkennung der folgenden Elemente:

- *RACF-Profile, ACF2-Anmelde-IDs/ACF2-Regeln, TSS Accessor IDs (ACIDs)/TSS-Genehmigungen*
- *Fragwürdige Definitionen*
- *Einträge in RACF-Zugriffslisten und ACF2-Regeln*
- *Systemoptionen*
- *Fehlerhafte Einstellungen*
- *Ausnahmen, zum Beispiel Änderungen an den Parametern, Profilen und Optionen, System- und Benutzerbibliotheken und angepassten, installationsspezifischen Elementen von z/OS*

Nach der Prüfung und Analyse des Betriebssystems z/OS vergibt Tivoli zSecure Audit Prioritäten und markiert Sicherheitsprobleme. In den bereitgestellten Ansichten werden Definitionen, Tabellen, Exits und weitere wichtige Informationen zu z/OS angezeigt. Gleichzeitig wird angegeben, wo Probleme festgestellt wurden. Die Probleme werden nach Prüfpriorität gewichtet und mit einer Nummer versehen, an der die relative Auswirkung eines Problems zu erkennen ist.

Tivoli zSecure Audit kann auch Prüf- und Analysefunktionen außerhalb von z/OS-Systemen bereitstellen. Dazu gehört die Möglichkeit, Sicherheitsdefinitionen von UNIX® auf dem Großrechner zu prüfen und Probleme in den Sicherheitsdefinitionen der UNIX-Subsysteme automatisch zu lokalisieren. Darüber hinaus unterstützt Tivoli zSecure Audit IBM DB2-Prüfereignisse, so dass die Aktivität innerhalb der DB2-Systeme auf dem Großrechner angezeigt werden kann.



Diese Ansicht zeigt die für ein bestimmtes RACF-System definierten Klassen, nach Prüfpriorität sortiert, so dass Probleme schnell lokalisiert werden können. Wenn Sie die gewünschte Klasse vergrößern, erhalten Sie eine Anzeige mit den relevanten Details.

Angepasste Berichte für spezielle Anforderungen

Tivoli zSecure Audit kann so konfiguriert werden, dass täglich per E-Mail Berichte bereitgestellt werden, wenn bestimmte Ereignisse eintreten oder ein Sicherheitsverstoß registriert wird. Zu den umfangreichen Möglichkeiten der Erstellung von Berichten gehören auch die folgenden Funktionen:

- *Generierung von Berichten im XML-Format.*
- *Import der Berichtsdaten in Datenbanken und Berichtswerkzeuge.*
- *Anzeige der Daten mit Microsoft® Internet Explorer*
- *oder Microsoft Excel.*
- *Möglichkeit für die Manager, Prüfberichte anzuzeigen, zu sortieren und zu kommentieren.*
- *Zentrale Erstellung der Berichte zur automatischen Verteilung an dezentral organisierte Gruppen.*
- *Zusammenfassung mehrerer Berichte zu einem Paket für die automatische Verteilung.*
- *Direkte Speicherung der Berichte auf dem Web-Server, wodurch die Berichte über das Intranet zugänglich werden.*
- *Erstellung maschinenlesbarer Berichte, damit diese in Nachbearbeitungsprogrammen auf z/OS oder anderen Plattformen weiterbearbeitet werden können.*

Die in Tivoli zSecure Audit verwendete Consul Auditing and Reporting Language (CARLa) ermöglicht Ihnen die Anpassung der Ansichten und Berichte und den Aufbau installationsspezifischer System-, RACF-, ACF2-, TSS- und SMF-Berichte (System Management Facility, Systemverwaltungsfunktion). Mit dem Befehl DEFINE können Sie Tivoli zSecure Audit um eigene Variablen ergänzen, um installationsspezifische Informationen abzubilden und diese in Auswahl- und Ausgabefunktionen zu verwenden.

Die Berichte können in IBM Interactive System Productivity Facility (ISPF) oder im Stapelbetrieb für eine beliebige RACF- oder ACF2-Datenbank, für aktuelle oder extrahierte SMF-Datenbestände oder für nicht geladene Daten ausgeführt werden – ohne die CARLa-Programme ändern zu müssen. In den Berichten kann auch das HTTP-Zugriffs- und -Fehlerprotokoll analysiert werden, um festzustellen, wer über das Internet auf Daten in der internen IT-Umgebung zugreift oder sie verwendet.

Tivoli zSecure Audit ermöglicht auch das Senden von SNMP-Nachrichten (Simple Network Management Protocol) an eine unternehmensweite Managementkonsole bei Nichteinhaltungen von Sicherheitsrichtlinien oder bei Ausnahmen, die auf einen Sicherheitsverstoß oder eine Schwachstelle hindeuten.

Schnelle Reaktionen durch Analyse von RACF-Profilen und ACF2-Einträgen

Tivoli zSecure Audit verwendet zur Analyse der definierten Profile/Einträge zu Benutzer, Gruppe, Datei und Ressource die aktive oder externe RACF-Datenbank oder ACF2-Datenbank. Auf Anforderung werden die ausgewählten Datensätze mit Detailinformationen in einer ISPF-Ansicht mit Scrollfunktion oder in einem druckbaren Bericht ausgegeben. Für alle Felder in den Profilen können Sie über Suchfunktionen Fragen beantworten, zum Beispiel „Wer hat Zugriff auf diese Datei?“ und „Erstelle eine Liste aller Systembenutzer, die ihre Kennwörter nicht geändert haben.“ Diese Berichte können Sie im Dialogbetrieb unter ISPF anzeigen oder automatisch im Stapelbetrieb ausführen.

Analyse von SMF-Protokolldateien zur Erstellung eines umfassenden Prüfprotokolls

Tivoli zSecure Audit analysiert SMF anhand der aktuellen SMF-Dateien oder anhand extrahierter SMF-Daten auf Band oder Platte. Die SMF-Analysekomponente unterstützt mehr als 40 Standardtypen von z/OS-SMF-Datensätzen und beinhaltet spezielle Prüffunktionen für RACF, ACF2, TSS, DB2 und UNIX, um grobe und detaillierte Berichte zur System- und Benutzeraktivität aus SMF-Protokolldateien zu generieren. In z/OS-Systemen mit TSS kann auch Audit Tracking File verwendet werden.

Da aktuelle Datenbestände verwendet werden, können die Informationen aus dem aktiven System sofort nach Eintritt eines Ereignisses angezeigt werden. Tivoli zSecure Audit erkennt für jede Sitzung mit IBM Time Sharing Option (TSO), für jeden Stapeljob und für jede gestartete Task nach dem Auffinden in SMF die zugehörige RACF-Benutzer-ID. Anschließend werden die SMF-Datensätze aus derselben Task mit dieser Information gekennzeichnet. Dies ermöglicht Ihnen die Erstellung eines umfassenden Prüfprotokolls für eine bestimmte Benutzer-ID aus SMF, einschließlich der Ereignisse aus SMF-Datensätzen, die keine RACF-Informationen enthalten, und der Ereignisse aus Stapeljobs mit beliebigen Namen.

Nutzung vielseitig verwendbarer Berichte durch Unterstützung externer Dateien

Tivoli zSecure Audit kann auch externe Dateien mit vorhandenen Daten verwenden. Ergänzende Informationen aus vorhandenen Datenbanken und unternehmensweiten Anwendungen (wie Bereichs-, Abteilungs- und Personaldaten) können gefiltert und gemeinsam mit den technischen Daten aus z/OS, RACF, ACF2 und TSS in automatisch generierten Berichten dargestellt werden.

So können zum Beispiel bei einer Ausnahme von einer Richtlinie, wie einer Anmeldung nach der Arbeitszeit, die Informationen zum Benutzer (Name, entsprechende Benutzer-ID, Abteilung, E-Mail-Adresse und Telefonnummer) aus der Personaldatenbank abgerufen werden.

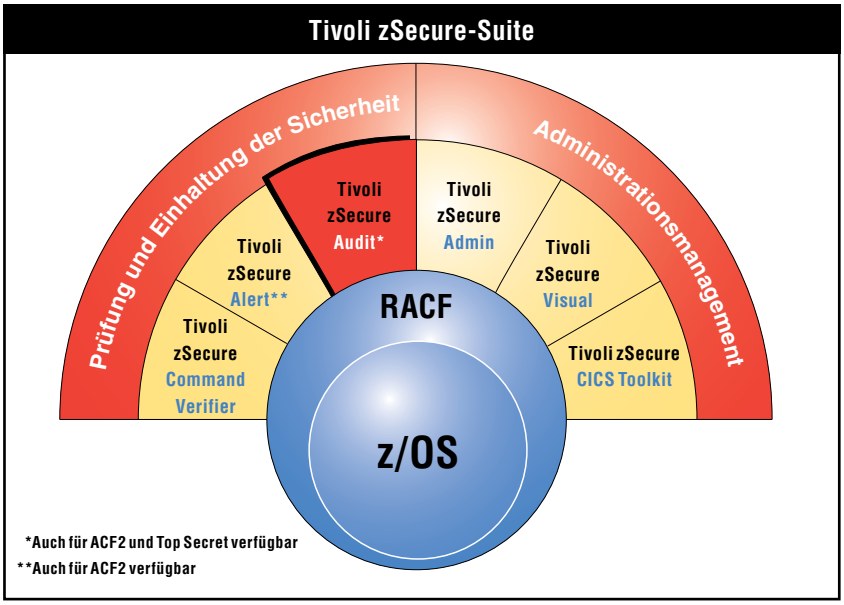
Erkennung von Systemänderungen zur Minimierung der Sicherheitsrisiken

Tivoli zSecure Audit kann Änderungen in den Einträgen partitionierter Datenbestände erkennen. Dazu werden digitale Signaturen für die einzelnen Einträge der überwachten Bibliotheken verwendet. Tivoli zSecure Audit erkennt, wenn ein Eintrag hinzugefügt, gelöscht oder geändert wurde. Bei Lademodulen erkennt Tivoli zSecure Audit auch die angewendeten vorläufigen Programmkorrekturen (PTFs) und ZAP-Instruktionen und meldet anschließend die Unterschiede zwischen zwei oder mehreren PTFs.

Tivoli zSecure Audit kann identische Einträge in derselben oder in verschiedenen Bibliotheken, gleichnamige Einträge mit unterschiedlichem Inhalt und von PTFs und ZAP-Instruktionen betroffene Lademoduleinträge erkennen. Tivoli zSecure Audit stellt eine Erstausstattung mit Vorlagen für tägliche Berichte über automatisch erkannte Änderungen und mit ISPF-Dialogen für die Überprüfung Ihres Systems bereit.

Dieselbe Technologie zur digitalen Identifizierung kann verwendet werden, um die Authentizität von Protokolldateien zu prüfen und nachzuweisen, dass Protokolle nicht manipuliert wurden – was sowohl für Sicherheits- als auch für Konformitätsinitiativen von großer Bedeutung ist.

Zur weiteren Risikominderung können Sie IBM Tivoli zSecure Command Verifier implementieren. Dieses Modul überprüft jeden RACF-Befehl auf Übereinstimmung mit Ihrer Sicherheitsrichtlinie und unterbindet bei Nichtübereinstimmung dessen Ausführung – bevor er Schaden anrichten kann.



Protokollierung und Überwachung von Änderungen an den Basisdaten für RACF und ACF2

Tivoli zSecure Audit unterstützt Sie bei der Definition einer Basis für RACF- und ACF2-Sicherheitsparameter sowie bei der Ermittlung von Indikatoren, wie zum Beispiel Profilen und Parametern, die von der Basis abweichen. Änderungen an den Indikatoren können zur Aktualisierung der Basis verwendet oder für Folgemaßnahmen gekennzeichnet werden. Sie können der Basis auch installations- und anwendungsspezifische Indikatoren hinzufügen, wie zum Beispiel Profile für Anwendungsdatenbestände, die obligatorische Inaktivität von Notfall-Benutzer-IDs oder Profile, die nur für bestimmte Benutzer zugänglich sind.

Erkennung von Verletzungen der Integrität

Tivoli zSecure Audit enthält eine leistungsfähige Funktion zur Analyse der Systemintegrität, mit deren Hilfe Verletzungen der Systemintegrität und weitere Unregelmäßigkeiten erkannt werden können. Auf der Grundlage einer intelligenten Analyse werden in den Berichten Sicherheitslücken und potenzielle Sicherheitsrisiken gemeldet. Da die Sicherheitsrisiken in den Berichten nach Dringlichkeit geordnet werden, können Sie leichter die Art der notwendigen Korrekturmaßnahme ermitteln.

Tivoli zSecure Audit auf einen Blick

Systemvoraussetzungen:

- z/OS oder z/OS.e

Unterstützte Administrations-plattformen:

- RACF
- CA ACF2
- CA Top Secret Security

Tivoli zSecure Audit kann problemlos mit IBM Tivoli zSecure Admin integriert werden, was eine lückenlose Überwachung und Korrektur ermöglicht. Die nahtlose Integration mit Tivoli zSecure Admin versetzt Administratoren in die Lage, schnell zur Diagnose und Beseitigung von Störungen und Sicherheitsrisiken überzugehen.

Tivoli zSecure Audit kann auch mit IBM Tivoli Compliance Insight Manager integriert werden und ermöglicht damit die Einspeisung von Mainframe-sicherheitsinformationen in eine unternehmensweite Prüfungs- und Konformitätslösung.

Weitere Informationen

Auf der Basis über zwanzigjähriger Erfahrung in den Bereichen Sicherheitsprüfung und Konformitätsmanagement bietet Tivoli zSecure Audit eine branchenweit führende Lösung, mit deren Hilfe Unternehmen ihren Aufwand für Prüfungsvorbereitung und Analyse senken können. Durch nahtlose Integration in die Tivoli zSecure-Suite aus unternehmensweiten Lösungen für die Sicherheitsprüfung stellt Tivoli zSecure Audit eine umfassende, durchgängige Arbeitsumgebung für das RACF-Sicherheitsmanagement bereit.

Wenn Sie mehr darüber erfahren möchten, wie die Suite Tivoli zSecure Ihr Unternehmen dabei unterstützen kann, den Anforderungen einer Prüfung zu entsprechen, 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

Hergestellt in den USA.
06-07

TAKE BACK CONTROL WITH Tivoli®

TID10368-DEDE-00