

IBM z Systems

Sicherheit auf z Systems aus Auditor Perspektive

Martina von dem Bussche
IT Security Architect, CISM, CISA
tina.vondembussche@de.ibm.com

Manfred Gnirss
Senior IT Specialist
gnirss@de.ibm.com



Abstract

- Dieser Vortrag umfasst eine Einführung zu IT Audit-Themen, beispielsweise was genau und nach welchen Standards auditiert werden kann, welche Fragen ein Auditor stellt und was Ziel eines Audits ist. Außerdem werden die Unterschiede zwischen Status- und Event- basierendem Audit erklärt. Abschließend werden technische Möglichkeiten zur Unterstützung von Audits vorgestellt.

Agenda

- Begriffserklärung
- Richtlinien
 - bsi
 - PCI-DSS
- Auditoren
- Security vs. Compliance

- Umfrage

- Audit – technische Aspekte

Audit

- Untersuchung, ob Prozesse Anforderungen und Richtlinien erfüllen
- Werden von einem speziell hierfür geschulten Auditor durchgeführt
- In fast allen Bereichen von Unternehmen werden Audits durchgeführt:
 - Finanzwesen, Informationsmanagement, Datenschutz, Produktionsabläufe, Kundenmanagement, Qualitätsmanagement, Umwelt, Management bzw. Führung eines Unternehmens/Organisation, Arbeitszufriedenheit, etc.
- Vergleich der ursprünglichen Zielsetzung mit den tatsächlich erreichten Zielen
- Ziel: allgemeine Probleme / Verbesserungsbedarf feststellen



Audit

IT-Sicherheitsaudit oder Sicherheitsprüfung

- Maßnahmen zur Risiko- und Schwachstellenanalyse eines IT-Systems oder Computerprogramms
- Ziel: Reduzierung von Sicherheitslücken sowie Einführung von Best Practices

Compliance Audit

- Umfassende Überprüfung der Einhaltung von Regularien / Richtlinien
- Unabhängige Prüfer
- Ziel: Konformitätsnachweis

Security Monitoring

Status Monitoring

- z.B. Vergleich Ist-Zustand der Systemeinstellungen mit definiertem Soll-Zustand
- Anhand IT Security Policy, Complianceanforderungen, etc.
- In regelmäßigen Abständen

Event Monitoring

- Überwachung sicherheitsrelevanter Ereignisse
- Erfordert Logging, „Audit-Trail“
- In Echtzeit
- Herausforderung: Menge an Informationen, Interpretation
- Muss man einen erfolgreichen Log-in mitschreiben?

→ Security Information and Event Management (SIEM) Lösungen

Forensik

- Wissenschaftliche und technische Arbeitsgebiete, in denen z. B. kriminelle Handlungen systematisch untersucht werden

IT-Forensik / digitale Forensik

- Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen
- Feststellung des Tatbestandes und Täter durch Erfassung, Analyse und Auswertung digitaler Spuren
- Gerichtsfestigkeit der digitalen Beweismittel
- lückenlose und umfassende Dokumentation der Beweismittel und aller Analyseschritte bis zum Ergebnis

Audit-Trail / Logging

Generelle Empfehlung zur Nachvollziehbarkeit:

- Systemkritische Daten
 - Erfolgreiche und fehlgeschlagene Änderungen
- Sensitive Daten
 - Erfolgreiche und fehlgeschlagene Lese-Zugriffe

Richtlinien

Interne Security Richtlinien

- Generelle Richtlinie
- „Übersetzung“ pro IT-System (Windows, Linux, Hypervisor, ...)

Externe Regularien:

- Gesetzgebung:
 - Telekommunikationsgesetz
 - Bundesdatenschutzgesetz
- Standards:
 - bsi Grundschutz:
www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/inhalt_node.html
 - PCI-DSS: www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
 - SOX
 - HIPAA

bsi Grundschatzkatalog

M 4.212 Absicherung von Linux für zSeries

Absicherung von Linux unter z/VM

Für den Betrieb von Linux unter z/VM sollten zusätzlich folgende Empfehlungen berücksichtigt werden:

- Für z/VM müssen die **aktuellen Patch-Stände** eingehalten werden. Es ist darauf zu achten, nicht mit veralteten Systemen zu arbeiten.
- Die Berechtigungen des z/VM Systemadministrators sind sehr hoch. Er kann unter z/VM weitere virtuelle Maschinen einrichten oder löschen. Dies beinhaltet eine Vertrauensstellung, in der dem **Administrator** bewusst sein muss, dass er für die **Sicherheit der Systeme mitverantwortlich** ist.
- Nach der Installation von z/VM müssen das **voreingestellte Login-Passwort** und das voreingestellte *Minidisk*-Passwort sofort geändert werden.
- Unter z/VM definierte virtuelle Maschinen sollten **nur die für die jeweiligen Aufgaben notwendigen Ressourcen erhalten**, beispielsweise *Minidisks*, Adressen usw. Die Zugriffe werden über z/VM kontrolliert. Die strenge **Trennung der virtuellen Maschinen** muss eingehalten werden.

bsi Grundschutzkatalog

M 4.212 Absicherung von Linux für zSeries

Absicherung von Linux unter z/VM

- Auch unter z/VM dürfen **nur die benötigten Dienste** gestartet werden. Nicht benötigte Dienste sind zu deaktivieren.
- Die **Sicherheitsadministration von z/VM muss über RACF für z/VM** erfolgen. *RACF für z/VM* dient als Security Manager und kann nur die Rechte der z/VM-Benutzer verwalten. Darüber hinaus sollten *Virtual Machines*, *Minidisks* und - falls gewünscht - auch *Terminals* über *RACF Resource Profile* geschützt werden. Zugriff auf diese Ressourcen dürfen nur diejenigen Anwender erhalten, die diese Rechte im Rahmen ihrer Tätigkeit benötigen. RACF kann jedoch nicht die Rechte der Linux-Benutzer und deren Zugriffe auf Systemressourcen innerhalb des Linux-Betriebssystems verwalten. Linux-Benutzer werden nach erfolgreichem Aktivieren des virtuellen Linux-Systems von den normalen Linux-Sicherheitsmechanismen kontrolliert. Sicherheitskritische System-Kommandos von z/VM (wie z. B. *CP DIAL*) sollten über RACF geschützt werden.

bsi Grundschutzkatalog

M 4.212 Absicherung von Linux für zSeries

Absicherung von Linux unter z/VM

- Zur [Verwaltung der Dateien und Verzeichnisse von z/VM](#) ist zu überlegen, das Utility *DIRMAINT* einzusetzen. Es erlaubt eine übersichtliche Verwaltung der Anwenderverzeichnisse und hilft dadurch bei der Vermeidung von Administrationsfehlern. *DIRMAINT*s Sicherheitsmechanismen sollten immer auf *RACF für z/VM* basieren. Kommandos und Nachrichten im Rahmen der *DIRMAINT*-Administration sollten unter Audit-Kontrolle stehen.
- Die [Journaling-Funktion von z/VM](#) und die [Audit-Funktionen von RACF](#) sollten für Audits eingesetzt werden.
- Es sollten die unter Unix bzw. Linux üblichen [Standardmechanismen zur Absicherung von TCP/IP-Anbindungen](#) eingesetzt werden. Darüber hinaus ist zu überlegen, ob zusätzlich die von Linux unterstützten *KERBEROS Authentication Services* oder *Secure SocketLayer* (SSL) eingesetzt werden sollen.
- Die Linux-Definitionen sollten so eingestellt sein, dass der [Aufruf rekursiver Funktionen](#) nicht zur Überlastung des Betriebssystems führen kann.

bsi Grundschutzkatalog

Prüffragen:

- Wird z/VM auf zSeries-Systemen immer auf dem aktuellen Patch-Stand gehalten?
- Wurden nach der Installation von z/VM auf zSeries-Systemen das voreingestellte Login-Passwort und das Minidisk-Passwort durch neue Passwörter ersetzt?
- Sind unter z/VM auf zSeries-Systemen alle nicht benötigten Dienste deaktiviert?
- Werden die Journaling-Funktion von z/VM und die Audit-Funktionen von RACF auf zSeries-Systemen für Audits eingesetzt?
- Erfolgt die Kommunikation von Betriebssystemen (z/OS oder Linux), die im LPAR - Mode oder unter z/VM auf derselben zSeries-Hardware installiert sind, über interne Kanäle?

PCI-DSS

- Payment Card Industry Data Security Standard (PCI DSS)
- Developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally
- PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data
- PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data and/or sensitive authentication data

PCI-DSS



Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Protect all systems against malware and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need to know8. Identify and authenticate access to system components9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for all personnel

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

- Protection methods such as [encryption](#), [truncation](#), [masking](#), and [hashing](#) are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include [not storing cardholder data unless absolutely necessary](#), [truncating cardholder data if full PAN is not needed](#), and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Protect Cardholder Data

PCI DSS Requirements

- **3.5** Document and implement procedures to **protect keys used to secure stored cardholder data** against disclosure and misuse:
- **Note:** *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*

Testing Procedures

- **3.5** Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:
 - **Access to keys is restricted** to the fewest number of custodians necessary.
 - Key-encrypting keys are at least **as strong as** the data-encrypting keys they protect.
 - Key-encrypting keys are **stored separately** from data-encrypting keys.
 - Keys are stored securely in the **fewest possible locations** and forms.

Auditoren

- Checklisten abarbeiten
- Genau überprüfen

Sicherheit vs. Compliance

- Compliance ist eine Teilmenge von Sicherheit
- Compliant oder „Audit bestanden“ heißt nicht automatisch „sicher“

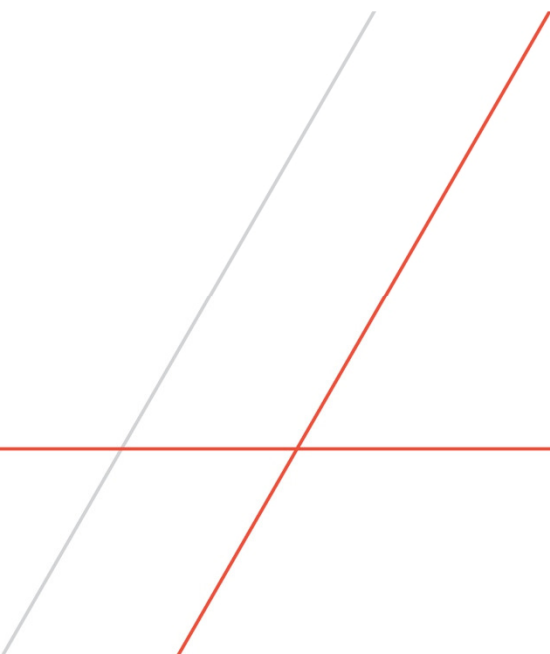
Chancen beim Audit

- Ein Audit kann helfen benötigte Gelder und / oder Ressourcen zu bekommen
- Aufmerksamkeit auf Themen, die bisher verborgen geblieben sind



Audit – technische Aspekte

Manfred Gnirss
IBM Client Center, Böblingen
gnirss@de.ibm.com



Audit – z/OS Aspekte

•Challenge

Protection of sensitive corporate data can be technically overwhelming and prohibitively costly. A balance must be found between unreasonably rigid access controls and too generous access to data by business users. Additionally, you must monitor and audit your privileged user community, the systems administrators.

•Implementation of Mainframe security:

External Security Manager (ESM) like RACF or vendor products

•Day to day management of ESM can be complex

Changes in the regulatory landscape have made it harder to meet audit requirements, and increased the frequency with which your organization faces these audits. The activity to answer the audit requirements usually takes time

•“automated tools” to simplify work and to provide an intelligent analysis of the real risks

IBM Security zSecure Suite delivers an integrated solution that addresses these security challenges. Or vendor products

•More Information

IBM z/OS Mainframe Security and Audit Management Using the IBM Security zSecure Suite, RedBooks SG24-7633-01. <http://www.redbooks.ibm.com/abstracts/sg247633.html>



Audit – z/VSE Aspekte

•z/VSE Basic Security Manager (BSM)

BSM introduced with z/VSE V2R4 together with the CICS Transaction Server for VSE. It got many improvements since z/VSE V2R4. The latest BSM enhancement was delivered with z/VSE V5R2: Allow separation the auditor from the administration functions. For that purpose you can now use the new user type AUDITOR.

•Auditing for resources defined in BSM control file

Enable (audit) or disable (noaudit) dynamically is possible to meet requirements

Always logged: Use of BSTADMIN cmd PERFORM with keywords AUDIT,SETOPT, PASSWORD

Never logged: ... LIST, LISTG, LISTU, PERFORM with keyword DATASPACE, STATUS

Optionally logged: other events

•Auditing resources defined in DTSECTAB

In past, Access Control Logging and Reporting (ACLR) was used to audit DTSECTAB resources. Starting with z/VSE V4R3 you can use Data Management Facility (DMF) for auditing. Access violations and administrative DTSECTAB are always logged. If DMF is not active, no audit records from the logger program

•BSM report writer (BSTRWPWTR)

To create a BSM report, use DFHDFOU to select SMF 80 records

•Additional Security Functionality via ESM

External Security Manager (ESM) from independent software vendor (ISV)



•More Information

Security on IBM z/VSE, RedBooks, SG24-7691-02, <http://www.redbooks.ibm.com/abstracts/sg247691.html>
z/VSE Administration book, <http://www.ibm.com/systems/z/os/zvse/documentation/index.html#vse>

Audit – z/VM Aspekte

•z/VM Security Policy

Most important: You need also a security policy for z/VM. you must monitor and audit your privileged user community, the systems administrators.

•CP Basic Security

Built-in security to protect system (itself and guests including all resources and guarantee integrity

•External Security Manager (ESM)

Configure a system according Common Criteria with OSPP you need a ESM (like RACF or vendor product). ESP delivers a finer granularity for protection of resources and audit capabilities.

•Audit points

System Config, IPL parameters, LOADPARM in activation profile, directory, subsystem config files, RACF database, RACF audit logs

•Separation of duties

If no separation of duties by person, LOGON RACAUDIT BY MANFRED to do audit tasks instead of LOGON MAINT BY MANFRED

•“automated tools” to simplify work and to provide an intelligent analysis of the real risks

IBM Security zSecure Suite delivers an integrated solution. Or vendor products

•More Information

IBM z/VM Secure Configuration Guide, SC24-6230-5, <http://www.vm.ibm.com/library/zvm/pdf.html>

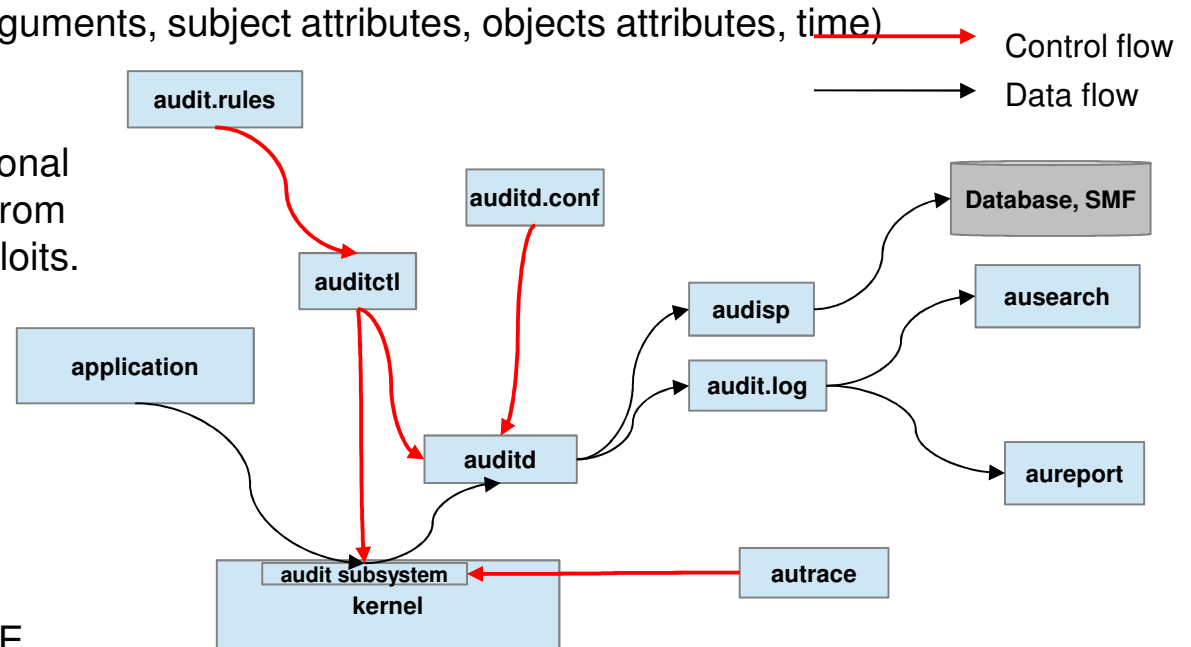
Audit – Linux on z Systems Aspekte

Common Criteria Certification

Linux on z Systems distributions (RHEL, SLES) reached Common Criteria certification EAL 4+ using Operating System Protection Profile (OSPP). Audit capability is part of it.

Linux audit Framework

- Collect information regarding events occurring on a running system and helps to make system more secure (Kernel events (system calls) and user events (audit-enabled programs))
- Form and log a record describing each event using information collected from that event (syscalls arguments, subject attributes, objects attributes, time)
- Analyze the log of records
 - Analyze what is happening
 - However, it does not provide additional security by itself. It does not protect from code malfunctions or any kind of exploits.
 - But it useful for tracking these issues and helps you take additional security measures to prevent the issues from happening or being repeated.



More Information

Documentation from RedHat or SUSE

