Protect Db2 for z/OS Data: Security and Compliance

Bob Tilkes, IBM

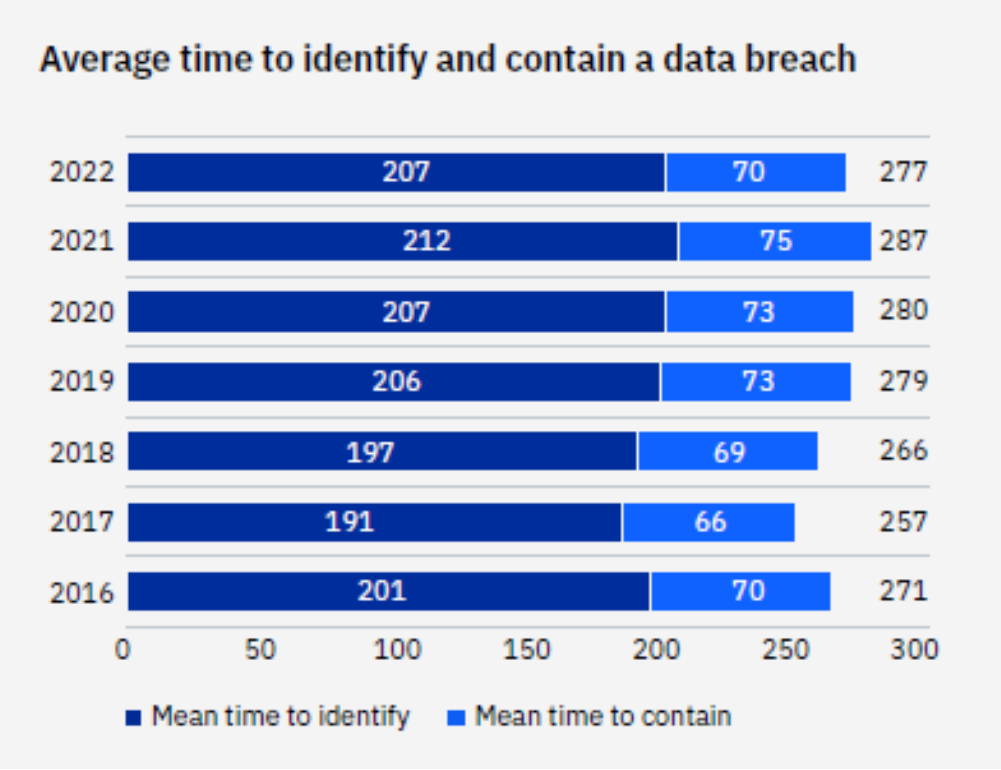
New England Db2 Users Group
March 23, 2023

- Why is Security and Compliance Important?
- Security Vulnerability/Patch Management
- Privileged ID Authentication
- Pervasive Encryption for Db2 Data sets
- Db2 System Parameters
- Restricting Connection Types on Packages
- Mainframe Security
- Db2 Security
- Access Reviews

Why is Security and Compliance Important?

Data beaches and Ransomware attacks are getting more sophisticated and occurring at a greater frequency

- According to IBM Security – Cost of a Data Breach Report 2022
  - Average Cost of a Data Breach is $4.35 million
    - Untied States being the highest at $9.44 million
  - Average Cost of a Ransomware Attack $4.54 million
    (this does not include the cost of the ransom itself)
    - Healthcare being the highest at $10.10 million
- Examples of some past mainframe data breaches
  - Bangladesh Central Back
  - Large US Banking Institution
- Unnamed bank victim of mainframe ransomware
  - Spear phishing attack against a system programmer
  - Keylogger to get mainframe credentials
  - Submitted job through FTP to scan for sensitive data sets
  - Submitted second job thru FTP to encrypt data sets



Security Vulnerability/Patch Management

Gain insights to Security vulnerabilities in your Db2 for z/OS environment

- Best Practice
  - Order/receive the current maintenance and ++HOLDDATA
  - From the IBM Security Portal download the latest security vulnerability ++HOLDDATA
    - How to register for IBM Z and LinuxONE Security Portal
      - ✓ IBM Z & LinuxONE Security Portal frequently asked questions (FAQs)
  - Receive the ++HOLDDATA from the IBM Security Portal to assign the SECINT source ID
  - Run the REPORT ERRORSYSMODS *(See Appendix for sample JCL)*
    - The report will now include PTFs that have been identified by IBM as Security Vulnerabilities and are assigned a CVSS Score

Security Vulnerability/Patch Management …

Example of REPORT ERRORSYSMODS with SECINT

- How do I assess risk using the CVSS Score?
  - Base Metrics
  - Temporal Metrics
  - Environmental Metrics

Qualitative Severity Rating Scale	
Rating	**CVSS Score**
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

EXCEPTION SYSMOD REPORT FOR ZONE TARGET

HOLD FMID	SYSMOD NAME	APAR NUMBER	---RESOLVING SYSMOD---- NAME	STATUS	RECEIVED	HOLD CLASS	HOLD SYMPTOMS
HDBCC10	HDBCC10	AH45816	UI81201	GOOD	YES	HIPER	FUL,PRV
		[redacted]	[redacted]	GOOD	YES	SECINT	B5.6,T5.4
		AH46287	UI80832	GOOD	YES	HIPER	FUL
		AH46368	UI81246	GOOD	YES	HIPER	FUL
		AH46446	UI82645	GOOD	YES	HIPER	PRF
		[redacted]	[redacted]	HELD	YES	SECINT	B5.0,T4.8
		AH48261	UI82887	GOOD	YES	HIPER	DAL
		AH48289	UI83868	GOOD	YES	HIPER	IPL
		AH48375	UI82467	GOOD	YES	HIPER	FUL
		AH49442	UI82901	GOOD	YES	HIPER	FUL
			UI83688	GOOD	YES		
		AH49479	***NONE			HIPER	FUL,PRV
		AH49619	UI83368	GOOD	YES	HIPER	DAL
		AH49674	UI83388	GOOD	YES	HIPER	DAL
		AH51086	***NONE			HIPER	IPL
		AH51108	UI83921	GOOD	YES	HIPER	FUL
	UI74469	AH45719	UI80599	GOOD	YES	PE	
	UI79458	AH47264	UI81719	GOOD	YES	PE	
HIR2230	HIR2230	CH42898	UI78782	GOOD	YES	HIPER	IPL
			UI83449	GOOD	YES		
		[redacted]	[redacted]	GOOD	YES	SECINT	B5.3,T5.1
		CH47973	UI81867	GOOD	YES	HIPER	IPL
		CH48700	UI82760	GOOD	YES	HIPER	FUL
	UI79859	CH47973	UI81867	GOOD	YES	PE	
HIZCC10	HIZCC10	[redacted]	[redacted]	GOOD	YES	SECINT	B3.8,T3.7

Privileged ID Authentication

- **Fire Call / Break Glass**

Privileged ID Authentication …

- **Multi-Factor Authentication**

Pervasive Encryption for Db2 Data Sets

Db2 z/OS –

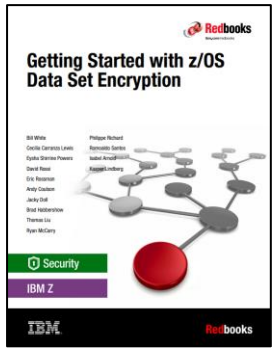
- Underlying VSAM files
  - Catalog & Directory
  - System Databases (Vendor Tooling, IVPs.etc)
  - Application Databases
- Active & Archive Log Data Sets

Db2 Knowledge Center Link

- Encrypting your data with z/OS DFSMS data set encryption

Redbooks

- Introducing IBM z/OS Data Set Encryption



Sample Policy Requirement	Category	Covered by IBM Z Pervasive Encryption	Encryption of Data at Rest
All sensitive data must be encrypted during transmission	Data in-flight	Yes	No
All sensitive data residing on DASD (Disk) and Tape must be encrypted	Data at rest	Yes	Yes
Where sensitive data resides on disk, but whole disk encryption is not required, dataset or file level encryption must be applied	Data at rest	Yes	Yes
Sensitive data flowing through the z/OS Coupling Facility must be encrypted	Data in-flight	Yes	No
Sensitive data flowing from application to application must be encrypted	Data in-flight	Yes	No

New Db2 v 13

Ability to Delete an Active Log Data Set while Db2 is Running

Db2 for z/OS System Parameters

- AUTHEXIT_CACHEREFRESH = ALL
- MFA_AUTHCACHE_UNUSED_TIME = 0, 120-7200
- AUTH = YES
- EXTSEC = NO

> **Note:** This is a security-related parameter. When this parameter is set to YES, detailed reason codes are returned to the client when a DDF connection request fails because of security errors that might enable more malicious attacks. If this parameter is set to YES, RACF users can change their passwords by using the DRDA change password function.

- TCPALVER = SERVER_ENCRYPT

> **Attention:** |< This is a security-related parameter. A setting of YES or CLIENT provides minimal security. With YES or CLIENT, Db2 is subject to security attacks, because the identity of the user or process that is attempting to gain access is not verified. Specify these settings only if you have a highly secure network. >|

> **Recommendation:** Setting the parameter to SERVER_ENCRYPT provides the best security. Connections are accepted only if user credentials are provided to authenticate the user ID, and strong encryption is used to protect the user ID and credentials.

- DEFLTID = xxxxxxxx (ID should be something other than IBMUSER)

ZPARMS

Db2 for z/OS System Parameters …

- SEPARATE_SECURITY = YES
  - SECADM1
  - SECADM1_INPUT_STYLE
  - SECADM1_TYPE
  - SECADM2
  - SECADM2_INPUT_STYLE
  - SECADM2_TYPE

WARNING: *If both SECADM1/SECADM2 are set to roles and those roles have not been created, no one will be able to manage security objects. Must create the necessary trusted contexts and roles prior to setting SEPARATE_SECURITY to YES if using ROLE on the SECADMx_TYPE*

- SYSADM1
- SYSADM2

- SYSOPER1
- SYSOPER2

ZPARMS

Restricting Connection Types on Packages/Plans

ENABLE / DISABLE

Options -

- TSO
  - (BATCH)
- CICS
  - (CICS) / (CICS) CICS(*applid, …*)
- Call Attach Facility (CAF)
  - (DB2CALL
- IMS
  - (IMS) / (DLIBATCH) / (DLIBATCH) DLIBATCH (*connection-name*) / (IMSBMP) / (IMSBMP) IMSBMP (*imsid*, …) / (IMSMPP) / (IMSMPP) IMSMPP(*imsid, …*)
- Remote
  - (REMOTE)
- RRS Attachment Facility
  - (RRSAF)

➢ *Note – Minimize the usage of option (*) as it enables all connections*

Mainframe Security

- APF-Authorized Programs
- Started Task IDs
- Data Set Access
- RACF Classes

Mainframe Security

APF-Authorized Programs

- Db2 for z/OS APF-Authorized Libraries
  - Db2 has 5 libraries that are usually APF Authorized
    - xxxx.SDSNLINK
    - xxxx.SDSNLOAD
    - xxxx.SDSNLOD2
    - xxxx.SDSNEXIT
    - xxxx.RUNLIB.LOAD
  - Fully qualify the data set names with minimal use of wild cards for data set profiles for all APF Authorized data sets. (be very specific)
    - EX. DSNC10.DB??.SDSNLOAD
    - Ex. DSNC10.DBD1.RSU?????.SDSNLOAD
  - Restrict ALTER, CONTROL, or UPDATE Access to USERs based on Roles and Responsibilities
  - Remove UACC
  - Use ID(*) and Db2 Started Task IDs to Grant READ Access privilege to all users instead of UACC

Mainframe Security …

Db2 for z/OS Started Task IDs

- Recommendation:
  - Define IDs as Restricted IDs (Can be a Single ID for the Group, Member, or Individual Started Task IDs)
    - IDs do not have access to UACC or ID(*) Privileges
    - All Privileges must be explicitly permitted
  - If the IDs is placed in a GROUP, no privileges should be given to the group. This prevents a USER from being added to the group to gain access to privileges permitted to the group
  - Permit Privileges that are only needed by the ID to run the Db2 Started Tasks(Least Access Needed)

** Suggestion (consider doing this in a lower environment to reduce impact)

- Permit known privileges
- Place the ID in Warning Mode
- Review the output from SMF Type 80 records
- Permit needed privileges found
- Remove Warning Mode

Mainframe Security …

Data Set Access

Restrict Access to Db2 for z/OS Product data sets

- Recommendation: (Least Access Needed)
  - In Security software –
    - Provide the Db2 Started Tasks, READ Access
    - Restrict ALTER, CONTROL, or UPDATE to USERs based on Roles and Responsibilities
    - Restrict READ Access based on Roles and Responsibilities
    - Remove UACC
    - Use ID(*) and Db2 Started Task IDs to Grant READ Access privilege to all users instead of UACC

Mainframe Security …

Data Set Access …

Restrict Access to BSDS, Db2 Active Log, and Archive Log data sets

- Recommendation: (Least Access Needed)
  - Provide the Db2 Started Tasks, ALTER Access
  - Restrict ALTER, CONTROL, or UPDATE to USERs based on Roles and Responsibilities
  - Restrict READ Access based on Roles and Responsibilities
  - Remove UACC
  - Do not provide ID(*) to permit USERs READ Access

Mainframe Security …

Data Set Access …

Restrict Access to VSAM Data Sets Associated with Db2 Objects

- Recommendation: (Least Access Needed)
  - Provide the Db2 Started Tasks, ALTER Access
  - Restrict ALTER, CONTROL, or UPDATE to USERs based on Roles and Responsibilities
  - Restrict READ Access based on Roles and Responsibilities
  - Remove UACC
  - Do not provide ID(*) to permit USERs READ Access

hlq.DSNDBC.**
hlq.DSNDBD.**
Or
hlq.DSNDB?.**

***Note - can further qualify out to include database and space name if required*

Mainframe Security …

Data Set Access …

Restrict Access to Db2 Image Copy Data Sets

- Recommendation: (Least Access Needed)
  - Provide the Db2 Started Tasks, ALTER Access
  - Restrict ALTER, CONTROL, or UPDATE to USERs based on Roles and Responsibilities
  - Restrict READ Access based on Roles and Responsibilities
  - Remove UACC
  - Do not provide ID(*) to permit USERs READ Access

Mainframe Security …

RACF Classes

OPERCMDS - Controls who can issue operator commands.

Recommendation:

- Consider locking down CANCEL, MODIFY, START, and STOP on the Db2 Started tasks
  - This controls who has that privilege to the commands above.
  - Access should be based on roles and responsibilities
  - May need to provide access to Automation Tool Started task ID
  - Remove UACC
  - Remove ID(*)

Mainframe Security …

RACF Classes …

STARTED - Assigns an identity to a started task during the processing of an MVS START command.

Recommendation:

- Preferred
  - Explicitly list every started Task and assign it a started task ID.
    - ✓ Prevents unauthorized use of a started task ID for a new task
- Alternative (depends on organizations risk tolerance)
  - Use wildcard(s) in the started task name e.g., DBX?MSTR.** where X represents the group identifier and ? (wildcard) is the single digit member identifier
    - ✓ Creates flexibility allowing the possibility of easily adding and removing Db2 members
    - ✓ Requires either a single started task ID for the Group or Single ID for the xxxxMSTR for example for the group
    - ✓ Very limited use case
    - ✓ Reduces the number of entries required in RACF

Mainframe Security …

RACF Classes …

DSNR – (*ssid.environment)* Controls access to Db2 for z/OS subsystems

Environment -

- **MASS** for IMS (including MPP, BMP, Fast Path, and DL/I batch).
- **SASS** for CICS.
- **DIST** for DDF.
- **RRSAF** for Resource Recovery Services attachment facility. Stored procedures use RRSAF in WLM-established address spaces
- **REST** for Db2 REST services
- **ACCEL** for IBM Integrated Synchronization access by IBM Db2 Analytics Accelerator for z/OS® or by IBM® Db2 for z/OS Data Gate.
- **BATCH** for all others, including TSO, CAF, and utilities.

➢ *Note – Minimize the usage of ssid.* as it enables all environments*

Mainframe Security …

RACF Classes …

DSNR – (*gpid.environment or*)Controls access to Db2 for z/OS subsystems…

Environment -

- **WLMENV.*wlm_environment* –** determine if users are allowed to create stored procedures in a WLM environment
- **WLM_REFRESH.*wlm_environment*** – authorizes users to use the WLM_REFRESH stored procedure

DSNR – (TRUSTEDCTX.*profile*) control the users who can be switched in a trusted connection by defining an external security profile

DSNR – (DSNAUDIT.*policy-name*) prevents any tamper-proof audit policy records from being modified or stopped

Db2 z/OS Security

- Public Access
- Restrict Elevated/Privilege Access
- Roles & Trusted Context
- Enabling At-TLS/Secure Ports for DRDA
- Audit Db2 Elevated Privileges

Db2 for z/OS Security

PUBLIC Access

- REVOKE PUBLIC Access to all DB2 Objects
  - Catalog and Directory Objects
    - SYS*AUTH Tables
    - SYSCONTROLS
    - ROLES and TRUSTED CONTEXT Tables
    - Audit Policies Table
    - Db2 Communication DB Tables
      - ✓ Consider using Db2 Stored Procedure DSNLEUSR to encrypt User ID and Password in USERNAMES table
  - Other Db2 Objects to consider
    - Profile Tables
    - Resource Limit Tables
    - DSNSERVICE (REST Services)
    - Application Objects
    - Plans/Packages/Stored Procedures/UDFs
    - System Level Privileges

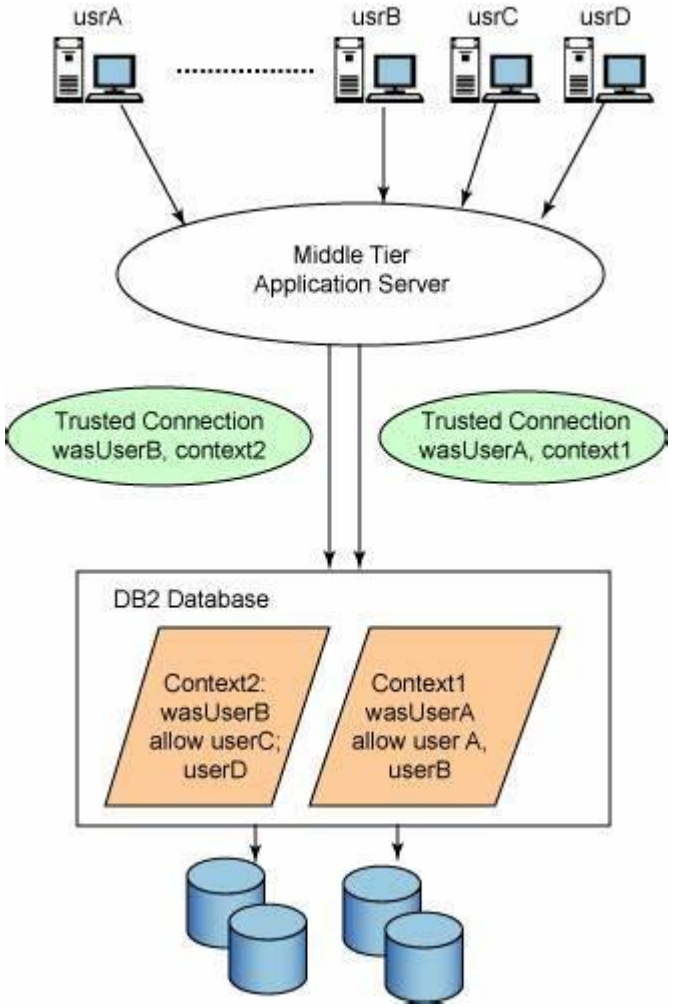
Db2 for z/OS Security …

Elevated Privileges

Db2 for z/OS Security …

Roles & Trusted Context

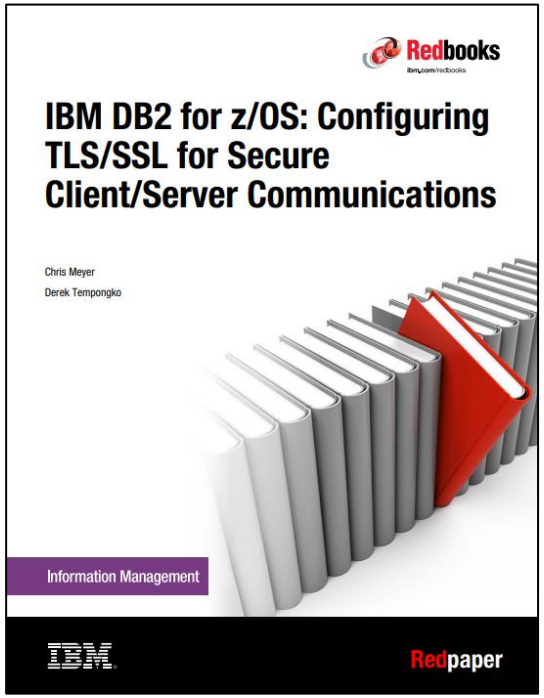
- Use Cases
  - Batch Scheduler IDs
  - Application Servers & IDs



Db2 for z/OS Security …

Enabling AT-TLS/Secure Ports for DRDA

- Encrypts Data in Motion
- Transparent to Db2 z/OS
- Minimizes the need for changes to application servers
- Recommend Best Practice for all DDF connections
  - Especially Db2 Native Rest Services



Redpaper

- IBM Db2 for z/OS: Configuring TLS/SSL for Secure Client/Server Communications

Db2 for z/OS Security …

Audit Db2 Elevated Privileges

- Install SYSADM
- SYSADM
- System DBADM
- DBADM
- SECADM
- Etc…

Tamper-Proof Audit Policies

Access Reviews

RACF Access Reviews

- ID – Recertification
- Generic IDs (Started Task, Application, or System IDs)
- Groups
- Data Sets
- Classes

Db2 Access Reviews

- Roles and Trusted Context
- Elevated Privilege Access
- System Privileges
- Object access should be reviewed by Data Owners

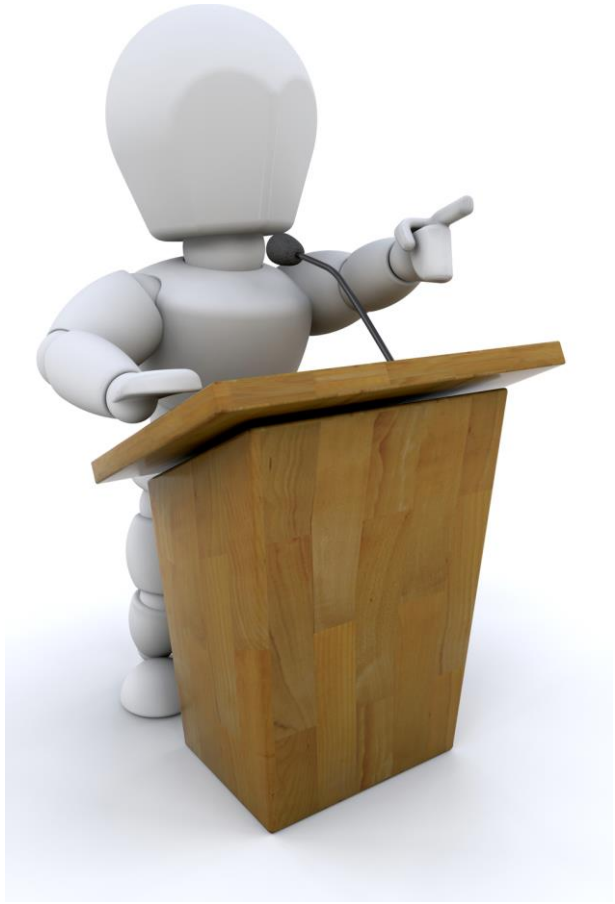
Additional Areas to Consider

- Restricting Db2 z/OS USS file system access
  - File System Privileges
  - RACF UNIXPRIV profiles
- Secure & Real-Time Monitor/Audit – FTP, SSH, & HTTP connections
- Using RACF SERVAUTH to protect from unauthorized access to Db2
  - Consider contacting your z/OS Network Team/Staff for better understand
  - Provides the ability to control the access to Db2 from a range of IP addresses defined as a security zone
    - When the controls are enabled Db2 requires that the z/OS user ID of each Db2 client be permitted access to the resource that represent the network security zone
    - If the user ID is not permitted, then logon with fail
- Network Job Entry(NJE) – RACF NODES profiles (*Responsibility may vary by installation*)
  - Whether jobs are allowed to enter the system from other JES2 nodes
  - Whether jobs that enter the system from other nodes must pass user identification and password verification checks
    - Understanding NODES profiles

IBM Publishes Security Benchmarks

Center for Internet Security

- IBM Z SYSTEM
  - CIS IBM z/OS V2R5 with RACF Benchmark v1.0.0
  - **CIS IBM Db2 13 for z/OS Benchmark v1.0.0**
  - CIS IBM CICS Transaction Server 6.1 Benchmark v1.0.0
  - CIC RHEL8 on IBM Z Linux Benchmark v1.0.0



Summary

- Security Vulnerability/Patch Management
- Privileged ID Authentication
- Pervasive Encryption for Db2 Data Sets
- Db2 System Parameters
- Restricting Connection Types on Packages
- Mainframe Security
- Db2 Security
- Access Reviews

Speaker: Bob Tilkes

Company: IBM

Email Address: robert.tilkes@ibm.com

Appendix

- Acknowledgements
- References
- SMP/e REPORT ERRORSYSMODS sample JCL

Acknowledgements:

- Share Presentation - Anatomy of a Mainframe Hack
- Top 6 ways a hacker will gain access to your mainframe
- Top 10 Privilege Escalation Hacks For The Mainframe
- Ransomware Put Mainframe Security in the Spotlight, but There's More to Learn
- 11 Guideline for Minimizing Vulnerability for IBM z/OS While Improving Compliance
- Confused About Encrypting Data at Rest vs Pervasive Encryption?
- Center for Internet Security (CIS) Downloads - CIS IBM Db2 13 for z/OS Benchmark
- IBM Security – Cost of a Data Breach Report 2022

References

Security Vulnerability Management

- Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards
- Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology (nist.gov)
- IBM Z & LinuxONE Security Portal frequently asked questions (FAQs)
- zSystem-Integrity.pdf

Pervasive Encryption for Db2 System data sets

- Encrypting your data with z/OS DFSMS data set encryption
- What is pervasive encryption for IBM Z?
- Redbook - Introducing IBM z/OS Data Set Encryption

ENABLE / DISABLE Bind Options

- ENABLE and DISABLE Package/Plan bind options

PLANMGMT Bind Options

- PLANMGMT bind option

DSNR Class

- Naming protected access profiles
- Defining external security profiles
- Managing authorizations for creation of stored procedures in WLM environments

References …

Elevated Db2 Privileges

- Administrative authorities

Roles and Trusted Context

- Roles in a trusted context
- Managing access through trusted contexts

Enabling AT-TLS/Secure Ports for DRDA

- Rebook - Db2 for z/OS: Configuring TLS/SSL for Secure Client/Server Communications

Audit Policies

- Db2 for z/OS Audit Policy
- SYSAUDITPOLICIES Catalog Table
- Updating tamper-proof audit policies

zPARMS

- Directory of subsystem parameters, panel fields, and application default values

SMP/e REPORT ERRORSYSMODS sample JCL

```
//<jobcard>
//*
//* WILL NEED TO PROVIDE/UPDATE THE FOLLOWING PRIOR TO SUBMITTING JCL:
//*       <jobcard> - REPLACE WITH A VAILD JOB CARD
//*       <hlq> - HIGH LEVEL QUALIFIER FOR THE SMP/E GLOBAL ZONE
//*             <<<NOTE THIS MAYBE SEVERAL QUALIFIERS>>>
//*       <target_zone> - SMP/e TARGET ZONE THE REPORT ERRORSYSMODS
//*                   IS GOING TO EXECUTE ON.
//*
//*       SMP ZONE-RELATED FILES ARE DYNAMICALLY ALLOCATED,
//*       THIS INCLUDES THE SMPPTS, SMPLOG, AND SMPTLIB DATA SETS,
//*       IF APPLICABLE.
//*
//JSTRGT01 EXEC PGM=GIMSMP,
//        PARM='PROCESS=WAIT',
//        DYNAMNBR=120
//SMPCSI   DD DISP=SHR,DSN=<hlq>.GLOBAL.CSI
//SMPPUNCH DD SYSOUT=*
//SMPCNTL  DD *
 SET    BOUNDARY (GLOBAL)
            .
 REPORT
       ERRSYSMODS
       ZONES(
            <target_zone>
           )
            .
/*
//
```