MANEWS Issue Number 27

the Mainframe Audit News

This newsletter tells you stuff you need to know to audit IBM mainframe computers running with z/OS and the MVS operating system. This issue we explore new mainframe developments, basic info to start a mainframe audit, and how to think about separation of duties.

Table of Contents

1) What's New in Mainframe Security?

Here are some new developments you'll want to be aware of:

- All three security software products have recently added new, more rigorous options for encrypting passwords. In RACF, it's called KDFAES and you can see whether it's implemented or not in the **SETR LIST** report. In ACF2, you can now have passwords encrypted with AES (Advanced Encryption Algorithm), which is stronger than the old DES algorithm. You can see whether this is implemented in the **SHOW ALL** report. For Topsecret, AES is also available to replace DES. You can see whether this is implemented in the **TSS MODIFY(STATUS)** report.

- MFA or Multi-Factor Authentication is the idea that you need to prove who you are in more that one way. Possible ways include: something you know (like a password), something you hold (like a token, key, or credit card), and something you are (like a fingerprint). The MVS operating system now provides support for MFA, as do all three security software products. When you think of all the breaches you've read about in the newspaper, you'll realize that almost all of them have to do with passwords. Many people believe that passwords alone can never be a reliable way of proving your identity, and they point to recent incidents to make their case. With MFA, if someone steals your password (or if you are careless with it), he still can't steal your identity unless he also steals your keychain, wallet,or thumb.

  Google, Facebook, and others are implementing MFA in a different fashion: they establish a secure handshake between their computers and your computers or smart phones. Once that handshake is established, any time you sign on to them, their computers recognize your computer or smart phone as one that is "trusted". If someone steals your password and tries to log onto your account from a different computer, these new authenticators recognize that the computer is not one they can trust, and so require further proof of who the user is. You'll see more of this in the future. Passwords may be completely obsolete within a matter of years.

- Policy-based encryption of data at rest is coming to the mainframe. We've all learned that if you want to protect something important, it's easier and more reliable if you have one, simple, comprehensive way of securing it. Any approach that relies on many people remembering to take precautions over and over is likely to fail.

Which is why we have policy based encryption over TCP/IP networks. With the Policy Agent software (which comes for free as part of z/OS), you can specify in one place, with absolute certainty, that certain ports and IP addresses will have encryption automatically. That place is the policy configuration file in Policy Agent.

Now IBM is about to add similar policy based encryption for data on disk and tape. This will let us specify in a single, reliable place (or policy), what disk and tape datasets are to be automatically encrypted. To prepare for this, we'll want to make sure we are already using the ICSF (Integrated Cryptographic Services Facility). ICSF is a program that serves as a central point for all encryption/decryption requests. You will want to have it in place as a stepping stone for both Policy Agent encryption over the network and policy based encryption for tape and disk.

2) How to Start Your First Mainframe z/OS Audit

There is a lot of data to collect about any mainframe data center to make your audits more effective. Gathering it all may seem like a lot of work, but it is data that belongs in your permanent workpapers. The effort to collect it will make your life much easier. Here are some suggested steps to get your first mainframe audit under way:

- Start your planning by getting the lay of the land. Request an inventory of all the mainframe computers, the LPARs (Logical Partitions similar to virtual machines), Sysplexes (networks of mainframes connected by fiber optic cable), and shared DASD (disk drives physically connected to more than one LPAR or computer). Each LPAR will have one image or instance of the MVS operating system. You will likely want to limit the scope of your first z/OS audit to a single MVS image. So find out which ones are for production and which are for test or development.

- Ask whether the security software is RACF, ACF2, or TopSecret. Learn how many security software database there are, and where they exist. Get the basic reports of security options for each security software database. (For RACF, these are SETR LIST and DSMON. For ACF2, SHOW ALL. For TSS, TSS MODIFY(STATUS)

- Get copies of risk assessments, policies, standards, procedures, naming conventions. Get an organization chart and from the policy statements, learn who is in charge of each area.

- Get an inventory of the network connections to the mainframe computers. You might want to exclude network issues from your scope at first, but you'll want to start understanding where the pieces are.

- If your audit will address security, decide whether it will address operating system security, security software implementation, application security, or some other aspect. It is almost always a mistake to attempt to audit more than one of these at once.

- Learn the financial auditors' control objectives, since they can empower you in the IS audit.

- Get an inventory of the applications (such as Order Entry, General Ledger, or Inventory). Consider selecting one, significant, production application to be the focus of your first mainframe audit. Use your knowledge of the financial auditors' control objectives to select your first application.

- Decide the aspect you are auditing: security, compliance, cost-efficiency, user satisfaction, other. Your audit will go much faster if before it starts you have narrowed it to one aspect of one significant production application that is important to the financial audit.

- Collect information about that one application. What programs and batch jobs does it execute? What datasets does it use? What inputs feed it and where to do they come from? What outputs does it produce and where to do they go? What middleware does it use (such as DB2, CICS, or MQ series?)

- If the application is online, get a list of the transaction names and what each one does.

- Get copies of the dataset rules and resource rules in the security software that protect the application's datasets and resources. Get copies of the written approvals or re-certifications for the accesses permitted by the rules.

This may seem like a lot of work for you to request, and for the data center staff to prepare. But this is all information that they should have easily available already.

It is difficult to manage any operation if you don't know what's in it (the inventories).

It's difficult to maintain an application program if you don't have documentation on how it works and what updates have been made to it.

It is difficult for a manager to say that he has provided adequate controls over his operation if he has not conducted a risk assessment first.

If data center staff is not able to produce the basic documentation described above, consider how you would address in this in your Tests of Design. The information listed above is a basic part of essential management controls for any well-run data center.

3) Separation of Duties Question

We often find that auditors would like clearer understanding of separation of dutes for mainframe security administration. You might be interested in a question one auditor asked a friend, and the answer that came back. Here is the question:

"***Our RACF Administrator recently left the company and they decided rather than to restaff the position or train someone else to handle his duties, they moved the duties (to configure RACF and administer user***

rights) to the System Programmers responsible for managing the MVS.

I feel like there is a Separation of Duties concern here but I can't seem to put my finger on it, assuming that they continue to document RACF settings and maintain controls over changes to RACF to properly segregate the Approval, Execution and Reviewing of the change.

Is there anything else that conflicts with their System Programmer access or duties?"

(You have probably already recognized that the three functions to be separated are the approval, execution, and review of the granting of any access or privileges)

Here is one possible answer:

"I think you may have legitimate concerns, but they may be trumped by reality. Imagine that you are auditing a small payroll application on a small UNIX box in the payroll department that had only two programmer/sysadmins, both with UID(0), that is, root. You might have separation of authorities questions, but with only two IT staff members, it's hard to improve the situation.

That said, I find that a good test whenever I think I have an audit finding, but I'm not sure what it is, I go back to auditing 101 and ask "What's the risk?" To put that into technical terms, what is the possibility of:

- Improper use of the system
- Improper copying or modifying data

- Loss of ability to process transactions
- Inaccurate or corrupted data

And then I try to match that to financial, operational, or business risk, or to financial auditor control objectives:

- Are the financial statements reliable (complete, accurate, timely, authorized...)?
- Are the company's assets protected (info and info processing assets)?
- Are we complying with laws and regulations?
- Do we expect to be in business next year (going concern)?

And then I ask what control mechanisms we might have in place, for example change control over application programs and over system software updates... These often depend on separation of authorities: someone approves, someone else makes the change, someone else reviews that all changes have matching approvals. And some mechanism like RACF, ACF2, TSS prevents changes without authorization. This is what mean by “a control architecture”.

We've all seen shops with lots of compliance forms and a lot of energy and time and paper spent demonstrating that "we're in compliance" even when the security isn't anywhere near sufficient. "But we're in compliance!"

So you want to concentrate on real risk. I think you can demonstrate it from the above, something along the lines of “there are xx sysprogs who can change, copy, sell our data, destroy our system and ability to process transactions and run their own service bureau companies on our company's computers, all without being detected. This could happen accidently or deliberately. Their manager does or does nor ensure that everything they do is supervised, approved, and reviewed. They do or do not have good change control and recovery procedures if someone should accidently install software with a bug in it. Here are the business applications which run on this computer: GL, AP, order entry...”

But the risk may be less significant if there's only a small number of people who can do this, and you have some reason to trust them (long term employees who live in our town with conservative life styles, not North Korean contractors driving Corvettes), and maybe some other detective controls.

So there may be some limited amount of risk, but also maybe not much you can do about it. You don't want to be all harum scarum without practical recommendations. But I think you do have a responsibility to report at least to the financial auditors "Here is this risk. It's this small or big. Here's how it might affect the financial control objectives. Here's the sum of what's possible to mitigate this risk. Here's my recommendation. I hope you have ways to audit around any computer-related risk". Of course, never let your boss be surprised.

Appendices: Seminar Information and Miscellanea

Appendix A) >>>>Seminar Information

Henderson Group seminars are available for in-house as well as public sessions. For more info, please visit www.stuhenderson.com/XAUDTTXT.HTM

The Henderson Group offers these "How to Audit..." courses :

- How to Audit **z/OS Applications** (June 15-16, 2017 in Bethesda, MD)
- How to Audit **z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (February 28-March 3, 2017 in Clearwater, FL and Sept. 25-28, 2017, in Chicago)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (June 12-14, 2017 in Bethesda, MD), a logical follow-on to the previous course
- How to Audit **UNIX and Windows Security** (October 24-27, 2017 in Bethesda, MD)

Appendix B) >>>>This Issue's Proverb of the Day

“*Some people think they can and others think they can’t, and they’re probably both right.*” — Henry Ford

Appendix C) >>>>Useful Information

Here are more useful information sources to help you audit more effectively:

1. Articles on Mainframe Security
http://www.stuhenderson.com/Articles-Archive.html

New Era offers free webinars by top speakers, and free books to help you audit mainframes better. You can see the seminar schedule and get handouts from previous sessions at
http://www.newera-info.com/The-z-Exchange.html

2. The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes
https://web.nvd.nist.gov/view/ncp/repository

3. Useful guidelines for knowing that your InfoSec is comprehensive (Note especially Publication 800-53):
http://csrc.nist.gov/publications/PubsSPs.html#800-53

4. The current release of z/OS is 2.2. The previous releases are z/OS 1.13 and z/OS 2.1. The end of support for z/OS 1.13 is September 30, 2016. You can monitor end of support dates for IBM software at
http://www.ibm.com/software/support/lifecycle/index_z.html

5. An additional source of free, practical information on mainframe security and auditing, from a variety of sources:
http://www.stuhenderson.com/XINFOTXT.HTM

6. IBM z/OS manuals (including Healthchecker under “z/OS System-Level:)
http://www-03.ibm.com/systems/z/os/zos/library/bkserv/v2r2pdf/

7. IBM Multi-Factor Authentication Manual
http://publibz.boulder.ibm.com/epubs/pdf/azfug100.pdf

Interesting Products

MIS Training Institute (MISTI) is the international leader in audit, IT audit and information security training delivering a wide range of seminars, eLearning courses, in-house training and conferences. In addition to an unparalleled course curriculum, MISTI also publishes five weekly newsletters to help keep you up-to-date on trends and analysis in the industry. Please visit www.misti.com to view our upcoming events or to select the newsletter that’s right for you. You can also connect with MISTI on Twitter and LinkedIn.

www.misti.com/index.php?option=com_content&view=article&id=234

www.twitter.com/mis_training

www.linkedin.com/company/32813?trk=tyah&trkInfo=clickedVertical%3Acompany%2CclickedEntityId%3A32813%2Cidx%3A2-1-3%2CtarId%3A1466421830896%2Ctas%3Amisti

Appendix D) >>>>About the Mainframe Audit News; Subscribe/Unsubscribe

The MA News is a free, email, newsletter for auditors who need (or suspect that they will need) to be auditing IBM mainframe systems (primarily **MVS**, **z/OS**, and the system software associated with them). This software includes: **CICS**, **DB2**, **JES**, **VTAM**, **MQSeries**, **TSO**, **USS** (UNIX System Services), **TCP/IP**, and others.

It also includes the **httpd daemon** software which connects a mainframe to the Internet. (Note, we expand each of these acronyms and explain how the software works in past and future issues.) The MA News is for auditors who are new to IBM mainframes, and also for experienced MVS auditors who want to keep up to date with the latest developments. We will not make the list of subscribers available to anyone else for any reason.

To Subscribe or Unsubscribe Click on http://www.stuhenderson.com/subscribe.html .

To see Back Issues: www.stuhenderson.com/Newsletters-Archive.html

Feel free to contact us at (301) 229-7187 or stu@stuhenderson.com.