MANEWS Issue Number 23

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 describe the new version of z/OS, suggestions for comprehensiveness, protection of residual data on disk, and mainframe TCP/IP security.
.

Table of Contents

1) New Release of z/OS: 2.2

This Fall IBM will be announcing the latest release (version) of the z/OS software package (including the MVS operating system). There will also be a new release of RACF for z/OS, also called release 2.2. ACF2 and TopSecret will be unveiling their newest releases (ACF2 16 and TopSecret 16) at about the same time. This all affects mainframe audits in several ways:

a. You likely want to verify that the system software is being kept up to date. (z/OS 1.12 is already off IBM support. z/OS 1.13 goes off support in September 2016. The next release 2.1 has not yet had the off support date announced. See http://www-03.ibm.com/systems/z/os/zos/support/zos_eos_dates.html to tell when a given release loses support.)

b. New password options will be possible (see the section on Passwords below)

c. Further security options will be announced by the Fall

We intend to provide more details in the next issue. Note that IBM plans on a new release of z/OS every two years or so.

==

2) How to Tell All the Inputs and Outputs

We know of an audit of a General Ledger application that was delayed because an IS auditor discovered at the last minute an input to the application that no one had known about. The input turned out to be a large number of records which had been created on personal computers using spreadsheets. No one had evaluated the controls over the quality of this data, since no one had been aware that it was a feed into the General Ledger. Review of the data quality revealed serious problems which eventually led to revision of some of the financial statements.

It's important for any application audit that we identify all the inputs and outputs, and that we assess the controls for each to support data integrity. There are several sources to identify the input and output files: the application documentation, the JCL (Job Control Language), and the SMF (System Management Facility) log data.

Application documentation should include a complete description of all the files used by the application. Without such documentation, there is the risk of not being able to maintain the application or of maintenance being applied incompletely. We learned with the Y2K brouhaha why proper application documentation matters.

JCL is the scripting language for batch jobs which says "run this program with these files and then this other program with these other files". (Note "***file***" and "***dataset***" mean the same thing.) Each unit of work is represented by one "job" or set of JCL script. Each file in the JCL is described with a DD (Data Definition) statement. DD statements describing tape or disk files will have a **DSN=** (DSNAME or DATASETNAME =) specification to tell you the dataset's name. If the DD statement specifies **SYSOUT=,** it is almost always a print file. If the DD statement specfies **DD ***, then the data that constitutes that dataset follows immediately after that statement.

The SMF data can record each time a dataset is opened, along with the information describing the job and the program which opened it. You can request a report listing all the datasets accessed by a given application’s jobs.

Once you know the inputs and outputs, you can evaluate where the inputs come from and what controls exist to ensure that their data is: complete, accurate, timely, not duplicated, authorized, and other aspects of data quality.

===

3) Addressing Passwords in the Audit

We often address password restrictions such as minimum length and content in our audits. Beyond that, we need to assess the overall risk instead of just checking one or two constraints. Here are some ways to think about this.

A recent CBS Sunday morning television show interviewed a white hat hacker, asking him out of any list of say 100 companies, how many did he think he could break into. Without hesitation, he answered “100". Asked to describe how, he described a Google search for one target company which uncovered a press release from a router company stating that the target company used that company’s routers. A further search led to the installation manual for the routers, which revealed the vendor supplied userid and password. The hacker tried them out on the target company’s routers, and was able to make the first step of his attack by taking over the routers.

We understand that part of what made the recent hacking of Sony computers was the fact that the administrative userid password was the same for all the computers.

You may be chuckling at this, but would your last audit have identified these situations? Did you check the minimum password length settings? Did you ask whether standards required vendor supplied passwords to be changed? Did you determine whether the standards were followed? Did you verify that passwords must be changed every so many days? It’s easy to check the items on the checklist, but don’t forget to evaluate the overall risk.

You will want to see the hilarious Jimmy Kimmel video on password strength. It's at

https://www.youtube.com/watch?feature=player_embedded&v=opRMrEfAIiIFeb%2023,%202015

Bruce Wells of IBM has provided us a comprehensive description of how to address password security, including new password options with RACF for z/OS 2.2. In addition, he has developed software to let you set almost any password options at all, including the ability to demonstrate to auditors that your password rules are STIG-compliant. You can get his handout at www.stuhenderson.com/Handouts/NyRUG2015TakingTheSwordOutOfPassword.pdf

==

4) New Details on Protecting Residual Data

Residual data is of course the data that still exists on a disk drive after you erase a dataset. When disk datasets are erased, it's actually the pointer to the data that is erased, not the data itself. So when another program allocates a new dataset on that part of the disk drive, that other program can read the data. If it's sensitive data, we have an exposure. IBM states that this is a real problem, and does not require specialized knowledge or tools to abuse.

And IBM gives us a solution: a feature in the security software that obliterates the data in disk datasets when they are erased. RACF calls this feature EOS (Erase-On-Scratch). ACF2 and TopSecret call it AutoErase. You can see how it is set in (respectively): SETR LIST, SHOW ALL, and TSS MODIFY(STATUS).

When this feature was first introduced, it had terrible performance problems, often described as "bringing the system to its knees". It was difficult to write an audit finding when the only easy solution had unacceptable performance problems. And no one seemed to have hard measurements on how serious the problems were.

But IBM then made major changes in disk drive hardware and software that almost completely eliminated the performance problem. We still had no hard measurements, but several installations started using this feature for selected datasets. (For those interested in the technology, the improvements include a new CCW that frees up the channel and control unit while obliterating the data, and which uses all the Read/Write heads at once.)

And now, IBM has pretty much eliminated the performance problem altogether, and we have hard measurements to back this. Apparently the system software didn't take full advantage of these performance improvements until z/OS 2.1.

Cheryl Watson and Frank Kyne have shown with hard measurements that EOS is much, much faster with z/OS 2.1 than z/OS 1.13. See details in the last three slides of www.stuhenderson.com/Handouts/DontKnow.pdf . They comment that the measurements show such stunning performance improvements that any installation not using EOS or AutoErase should re-visit the issue, once you get to z/OS 2.1. If your audit of mainframe security software hasn't addressed this yet, here is a fine reason to do so.

5) Mainframe Firewall

Mainframes come with full support for TCP/IP networks, including the Internet. Most installations with mainframes have at least one mainframe connected to the Internet. It is not uncommon for audits to uncover TCP/IP connections that do not provide encryption for passwords and other sensitive information. Another finding from some TCP/IP audits is the existence of open ports which could be used to provide unauthorized access to the system. It is difficult to claim that mainframe audits are comprehensive if they don't address TCP/IP security. We have two tools to help us address this.

First, the **NETSTAT** command in TSO lists all the TCP/IP connections on a computer, including what programs are involved and the to and from IP addresses and ports. You can use this in your audit planning to determine whether your audit should include TCP/IP.

The second tool is a free firewall-like tool that IBM provides with z/OS. It is called **Policy Agent**, or **PAGENT** for short. Depending on how it is configured, it can provide for encryption, logging, blocking of ports, intrusion detection, VPNs and IPSEC, packet filtering, and more.

All these options are specified in configuration files. To start collecting information about PAGENT, ask whether it is being used, and request copies of all its configuration files.

You can learn more about PAGENT and how to read its configuration files from a free webinar presented by the z/OS Exchange on May 28: http://www.newera-info.com/Webcast.html

6) What We’re Doing Isn’t Working

With all the time, money, and effort being put into IS audits, we still see headlines and surveys telling us that serious security breaches occur far too often in organizations which have been audited both internally and externally. Stepping back to look at why this might be suggests the following: we often follow our checklists and guidelines without making sure that we understand all the risks and all the controls. When we audit without an overall understanding of the risks (starting with an inventory of hardware, software, applications, data, and networks), we are bound to miss important areas. An interesting exercise is to review your organization’s audit planning documents, audit reports, and post mortems. Is it clear that your organization understands its IT risks? Do IS audits provide an overall answer to the question “Are we adequately protected against computer break-ins?”? If what we’re doing isn’t working (and it isn’t), then maybe it’s time for us to try something else. The starting point for this will likely be your audit planning and scoping.

Appendices: Seminar Information and Miscellanea

Appendix A) >>>>Seminar Information

Henderson Group seminars are available for in-house as well as public sessions.

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

- How to Audit **z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (September 21-24, 2015 in Chicago)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (November 10-12, 2015 in Bethesda, MD), a logical follow-on to the previous course
- How to Audit **UNIX and Windows Security** (October 26-29, 2015 in Raleigh,NC)

To learn more about them, please go to

http://www.stuhenderson.com/XAUDTTXT.HTM

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

"*Don't waste my time telling me you checked the lock on the front door when you've haven't checked the back door lock, and you don't know how many windows and side doors there are. Tell me you've looked at all the risk and looked at the controls and concluded that we are reasonably safe.*" — Attributed to a board of directors member

"*If you conclude that the general controls can't be relied upon, there's no point in spending a lot of time evaluating the application controls*." — an IS auditor

Appendix C) >>>>Useful Information

Here are two useful sets of guidelines to help you think about info security more widely:

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

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

Here's a source of free, practical information on mainframe security and auditing, from a variety of sources: http://www.stuhenderson.com/XINFOTXT.HTM Topics include:

- Glossary of Mainframe Terms
- How to Get z/OS Basic Skills and IBM z/OS Manuals in pdf Format
- Integrity Statements from CA Technologies and IBM
- z/OS Configuration Info: Documents, Audit Guides from NewEra
- Back Issues of z/Journal Magazine and Mainframe Executive Magazine
- IBM Presentation Handouts on Security and RACF from SHARE and GSE
- Free Articles on Mainframe Security and Auditing

Appendix D) >>>>About the Mainframe Audit News; How to 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 meant for auditors who are new to IBM mainframes, as well as for experienced MVS auditors who want to keep up to date with the latest developments from IBM. 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.