MANEWS Issue Number 22

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 an actual break-in to a mainframe computer over the Internet and what we can learn from it.

.

Table of Contents

1) Lessons From a Real Mainframe Break-In Over the Internet

This break-in occurred in a mainframe data center in a northern European country in 2012. The details below are from an extract of the official inquiry into what happened, and how the break-in was possible. (At least some of the hackers have been caught and are being prosecuted.)

- This was a true break-in, a deliberate, successful, criminal attack on a service bureau's mainframes over the Internet. It was not stealing a tape off a truck or tricking someone into giving out his password. It was a RACF shop, but everything here would have applied if it were ACF2 or TopSecret.

  Conclusion: Mainframes can be hacked if the security is not properly configured. Hackers are starting to get interested in them. Because many mainframes are connected to the Internet, there are additional security and audit issues. Auditors need to consider whether their audit plans adequately address Mainframe / Internet security.

- The break-in took place over several months. It was finally discovered as the result of an investigation into high CPU usage. Shades of "*The Cuckoo's Egg*" by Cliff Stoll

  Conclusion: Security breaches are being discovered months late and from usage monitoring and chargeback systems, instead of from security reviews and monitoring. We should be doing a better job of providing detection. Auditors need to address how effectively controls function to identify breaches quickly.

- These hackers broke in over several different paths. The first known penetration was by means of FTP using a client batch userid. Eventually the hackers used FTP to download the RACF database and to crack all the userids and passwords. (People seem to think that because passwords are encrypted, they can't be read. But brute force cracker programs will do the job. In a couple of days they cracked the passwords for 30,000 userids.)

  Conclusion: FTP on the mainframe, while very securable, has features beyond other FTPs, including uploading and downloading of MVS files, access to print files, access to DB2, and submission of batch jobs. This can all be secured with existing tools, but often is not. Mainframe auditors need to evaluate the risks and controls for every path into the system.

- As soon as management became aware of the break-in, they notified the State Police, who responded rapidly. The State Police also asked "By the way, is this the data center where we keep our State Police records?" The answer was "YES", after which the Police responded even more rapidly.

  Conclusion: We need to be prepared to assist authorities in forensic analysis if we are ever penetrated. We need to be prepared to know what to say and how to say it. One control often overlooked in audits is getting advice in advance from from the Legal, Public Relations and other departments on how to react in the case of a break-in.

- The hackers also broke into distributed computers that were front-ends (between the mainframe and the Internet).

  Conclusion: Having UNIX or Windows firewalls between our mainframes and the Internet is not a guarantee of adequate protection, especially if the the mainframe and distributed security administrators don't work together. If our mainframe is connected to the Internet, it is difficult to opine on mainframe security unless we understand the network security. If we do not know whether our mainframe is connected to the Internet, we need to find out.

- The hackers installed outbound programs onto the mainframes. These programs called out over the Internet, making it easier for the hackers to bypass firewalls and other protections.

  Conclusion: We can often benefit by re-visiting our assumptions about what makes our controls effective. Controlling outbound pathways is almost as important as controlling inbound.

- All of the security holes the hackers used were the result of mis-configuration, not weaknesses in mainframe security or RACF.

  Conclusion: The issues in protecting mainframe security are more often organizational issues than technical. Audits can, and should, address questions such as

  - "Who is Responsible (If anyone)?"
  - "Who Has the Knowledge?"
  - "Who Makes the Decision?" (If anyone)
  - 'How Do We Measure Degree of Protection?"
  - Do our audits direct sufficient attention to TCP/IP networks and Internet connections?

==

2) How to Conduct Your Own Self-Test

This break-in should have many readers asking themselves “Does our IS audit program address mainframe-Internet security sufficiently?” Here’s a simple test: Issue (or have someone issue for you) the TSO command NETSTAT.

This will tell you every TCP/IP connection that is active on that mainframe. It will include the to- and from- IP addresses and ports and the associated programs. The programs may include: FTP, CICS, TN3270 (remote log-in program, like telnet), MQ Series, DB2, the httpd daemon, and others. Then ask yourself whether your audit planning risk assessment includes these programs and network connections.

==

3) Matching Audit Resources to the Risk

These basic audit planing steps are well-known, but often get by-passed in the rush of real life. Here’s a review list of the steps to remind us how to stay balanced:

A. List all our platforms (computers) and the applications and data on each.

B. List all the networks they are connected to, and which apps use which networks

C. Rank the platforms and networks according to the business risk related to their apps and data. Involve the financial auditors in this step. A clear measure of your audit planning effectiveness is whether you actually have this ranked list in writing.

D. Assess how well the allocation of your audit resources matches this risk ranking. Adjust as needed.

==

4) This Issue's Featured Standards Document.

We're always looking for useful standards to use in our mainframe audits. This one is useful, even if the auditees don't accept it as an official standard. You can always use the outline it provides as a guideline. For any items you choose to include in your audit, it's fairly easy to provide backing with a quick risk assessment. This document provides a structured approach with the flexibility to adopt to a given organization's requirements.

The document is "***Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations*** " It's available from the Federal government for free at: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

It's organized into 18 control families, including Access Control, Awareness and Training, and Security Assessment and Authorization. This organization makes it easier to narrow your scope when the budget is insufficient. It also make it easier to find a specific detailed topic.

The 800-53 document provides a series of baseline controls which can be adjusted to meet the sensitivity and security requirements of a given organization. A **baseline** is defined as "*minimum set of security controls for the information system*."

To make your audit more efficient, you can request before the audit starts copies of any baseline documents the IT organizations uses for mainframe security. This gives you a standard to audit against if it exists. If it doesn't exist, your audit report can explore the risks of not having a minimum set of security controls in writing, possibly along with the dependence on the knowledge of a single individual.

This document sensibly assumes that adequate control depends upon: understanding of the risk, specification by responsible managers of what controls are to be in place, and independent evaluation of the how effective those controls are. Your job as an auditor can be to determine if the first two exist, and then to perform the evaluation of the specified controls. If you find either of the first two missing, this may lead you to an audit finding.

An Example of the Flexibiity 800-53 Provides:

One of the controls this document addresses is Control AC-11, the automatic locking of terminals after a specified number of minute of inactivity. It states clearly that each organization is to decide on the number of minutes of inactivity, and whether the control is needed or not. In this way, 800-53 provides flexibility for each organization. By explicitly stating that the control is to be determined in writing by the organization, (and not by a single individual), 800-53 reminds you to consider the control, and insists that the organization consider whether and how to implement it.

==

5) How Snowden Got Access

If you’ve been wondering how Edward Snowden got access to the classified information he later leaked, here’s one way: According to the Washington Post (February 14, 2014, page A2), quoting a Reuters report, Snowden “may have persuaded between 20 and 25 fellow workers to give him their log-ins and passwords by telling them they were needed for him to do his job as a computer systems administrator.” and, quoting an NSA memo, “[an employee] allowed Snowden to use [the employee’s credentials] to gain access to classified information on NSANet, the agency’s intranet, ‘access that he knew had been denied to Mr. Snowden.’ “

This raises the audit question of whether mainframe system programmers should be granted access to all data on the system solely on their statement that they need it to do their job. If no one else is responsible for approving such access, we might want to address the issues of IT governance and separation of duties. How do you deal with this in your audits?

==

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** (March 3-6, 2014 in Clearwater, FL; Fall session dates and location to be announced)

- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (November 18-20, 2014 in Bethesda, MD), a logical follow-on to the previous course

- How to Audit **TCP/IP Security** (December 1, 2014 in Bethesda, MD)

To learn more about them, please go to

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

_

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

“*Don’t expect what you don’t inspect*” — Chinese Proverb

Appendix C) >>>>Useful Information

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.