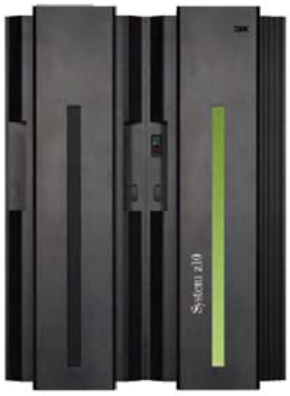
Whitepaper

11 Guidelines for Minimizing Vulnerability for IBM z/OS while Improving Compliance

Presented by CorreLog
www.correlog.com

CORRELOG®

The mainframe is perhaps the most critical asset in a data center because the stakes are higher in a breach – credit card and identity data, health records, government records, etc.



Your organization's potential for a mainframe breach

Google "mainframe security breach" and your browser will return some 168,000 entries. The same search for "Linux security breach" and "Windows security breach" yields 1.1 million and 3.05 million entries respectively. Every week we hear and read about attacks on high profile companies or government entities yet comparatively, the mainframe security breach is just not written about that much.

There are several possibilities for the 168,000 versus 3,050,000 numbers, the most obvious being that the mainframe just doesn't get hacked. Or, quite possibly because of the nature of data managed by mainframes and its link to government and industry standards such as HIPAA, PCI DSS, SOX and others, we just don't hear about it, so not much is written about it, so Google can't find much of it.

Anyone who attended the recent RSA InfoSec conference in San Francisco heard the vendor battle cry that "you are going to get breached, so let us help you minimize the damage." Sure, much of the hype is vendor-generated but with the recent breaches at high profile brands such as Target, Neiman Marcus, Sally Beauty Supply, and the University of Maryland, there is a great deal of merit to the "you are going to get breached" message we heard at RSA.

Include IT industry research consultancies like Gartner and the Federal Bureau of Investigation to the list of thought leaders telling the world "you are going to get breached." In January 2014, the FBI issued a confidential, three-page report to retailers warning of "memory parsing" malware that infects point-of-sale (POS) systems.[i] The FBI report describes how Target and Neiman Marcus could have been breached through "RAM scraping." RAM scraping extracts text files from the live memory location in POS terminals, before they are encrypted and sent to the credit card processor. And because sophisticated hacker code has made it difficult to detect, RAM scraping can go on for days before the retailer can identify the breach. The holiday-season Target breach of 2013 went 19 days before it was detected; 40 million credit and debit cards were stolen and 70 million Target customers had their personal information compromised.

A perusal of topics from research and webinars on Gartner's "Insight" web page fuels the you-are-going-to-get-breached hype:

- "NIST Framework Establishes Risk Basics for Critical Infrastructure"
- "Long-Range Planning Guidance for Information Security and Risk Management: Gartner's Security 2020 Scenario"
- "Advanced targeted attacks make prevention-centric strategies obsolete. Securing enterprises in 2020 will require a shift to information- and people-centric security strategies, combined with pervasive internal monitoring and sharing of security intelligence."
- "Seven Steps to Creating an Effective Computer Security Incident Response Team"
- "Security Management Strategy Planning Best Practices"

If you are saying to yourselves "so what does this have to do with mainframe breaches?" consider this: Seventy percent of the business and transactional systems around the world run on COBOL and 90 percent of global financial transactions are processed in COBOL.[ii] A large percentage of these transactions go through COBOL in an IBM mainframe.

If money makes the hackers of the world go 'round, they will follow the transactions linked to credit card data and those transactions will undoubtedly lead them to a mainframe.

Mainframes do not operate in a vacuum anymore

Mainframes have been an integral part of government and industry for nearly 50 years and have for the most part, resided in isolation from the outside world during that time. The mainframe environment of 2014 is quite different because of the proliferation of HTTP protocol. HTTP is request/response-based communication over TCP/IP and does not care if the request comes from Windows, Linux, UNIX or mainframe. As long as there is a TCP connection and an HTTP POST request, a response will be delivered. And because mainframes communicate via TCP and process Internet requests via CICS and WebSphere, they are exponentially more interoperable today than ever before.

Fifteen years ago the mainframe effectively operated in a vacuum and perimeter cyber defense centered mostly on insider threat via distributed systems. In a quest to simplify IT, CIOs have attempted to provide a "single pane of glass" for the performance, availability and security of entire NOCs, connecting distributed and mainframe systems to a single console. The theory is sound, yet the ability to execute is fleeting; there is just too much IT complexity to bring everything together in real time.

However, there has been fruit from their labor – interoperability. In more progressive IT shops, systems are now interconnected and data can be generated from just about every asset in a data center. The good news is the connectivity and we are making strides towards the single version of IT health truth. The bad news is also that everything is connected yet we continue to "manage" mainframe security as if it were the year 1980 – "our mainframe is isolated and locked down."

Come clean America, and let us help

By default, the war against the recurring information security (InfoSec) breaches we read about every week has been left up to the software vendor community. There are some excellent organizations like SHARE.org and MIS Training Institute aiding the cause, but these organizations are driven in large part by vendor dollars and vendor solutions to InfoSec issues. The software vendor community is putting up the good fight, but the war will never swing our way until government and industry come clean about cyber breaches. We know Target, Neiman Marcus, the University of Maryland were all breached and we know that last year Lockheed Martin had millions (maybe billions) stolen in intellectual property, but that's about all we know. We cannot cure what we don't know about and unfortunately, the black eye is too embarrassing for boards of directors to open the kimono to the public and say "okay vendors, help us find a solution."

The key to locking down your data center is to make it hard for the bad guys to breach it. There are some best practices that you can employ to make your organization a difficult target to hack. We are always going to have ambitious hackers who want to breach the most hardened environment and we are never going to have hack-free data centers. But if we make it difficult for the bad guys and steer clear of reactive InfoSec practices, chances are you won't endure the same fate the CIO of Target just experienced.

Here are 11 guidelines to keep your z/OS mainframe a soft target for a malicious hacker:

1. Collect all event logs in real time. Remediation and forensics for cyber breaches are immediate and nightly or weekly batch processing is too late.
2. Have a log management process and policy for collecting event log data across both distributed and mainframe environments
    a. Event log data is the window to user and system activity but you don't need to collect every event log that is generated; you would quickly run into a storage problem.
    b. You will need some mechanism like the CorreLog Agent for IBM z/OS to convert your z/OS SMF records to RFC 3164-compliant Syslog messages for your security operations center.
    c. You need to understand what event logs are most important to tell the story of the security of your data so that you can…

3. Correlate your data.
    a. Correlation is the process of combining multiple event logs to determine user or system behavioral patterns. Most of the time, these patterns are consistently repetitive and banal, but sometimes an anomaly will present itself and will need further investigation to rule out potential threat.
        i. Bob has logged onto the mainframe the past four days at 9:00 a.m. from Florida IP address 69.247.41.221. Today he logged in at 3:00 a.m. from the same IP address, but we know he is at a conference in Seattle. This needs further investigation.
4. Monitor all administrator access
    a. Invalid access attempts (DB2 IFCID 140) must be sent to your security operations center in real time.
    b. This is a PCI DSS requirement.
5. Have an audit trail for DB2.
    a. Know who accessed the repository and when; this is a critical component for correlation.
    b. DB2 audit trail is also a requirement for PCI DSS, HIPAA, SOX, FISMA, NERC and others
6. Additionally, you need to collect mainframe events and audit trails from security subsystems.
    a. RACF®, ACF2, and CA Top Secret
7. Track all TSO logons/logoffs and invalid access attempts.
    a. This is also a PCI DSS requirement.
8. Monitor all access to credit cardholder data by user privilege.
    a. You must be able to audit table reads/writes from DB2 IFCID 361, DB2 IFCID 143, DB2 IFCID 144.
    b. This is also a PCI DSS requirement.
9. Monitor system-level object creates and deletes.
    a. This is tracked through DB2 IFCID 97 and is also a PCI DSS requirement.
10. Audit FTP use in real time.
    a. Arguably FTP is the #1 mainframe vulnerability.
11. Audit TCP/IP access in real time
    a. You need immediate log details for login, telnet and other TCP-based events.

12. In a recent Enterprise Systems Journal article, software industry veteran and mainframe expert Phil Smith was asked the question: "What is the biggest z/OS security threat?"[iii]

Smith replied that mainframes have been generally more secure than other platforms and this has created a sense of complacency with securing the platform. But with increased Internet connectivity and the inability to lock down open source software packages in use in mainframe environments, the security threat to mainframe is very real. The practice we have experienced to great success with clients is to: 1) collect the right event data in real time to industry standards such as PCI DSS, 2) correlate all event data across all platforms, and 3) have an alerts-based ticketing system for immediate notifications of potential breach. The practice requires solid CISO leadership that understands that InfoSec does not take place exclusively on distributed platforms.

Mainframe computing is an integral IT asset that is always connected. This makes the mainframe perhaps the most critical asset in your data center because the stakes are higher in a breach – credit card and identity data, health records, government records, etc. – even if mainframe breaches aren't talked about when they happen.

---

[i] http://www.reuters.com/article/2014/01/23/us-target-databreach-fbi-idUSBREA0M1UF20140123
[ii] http://cis.hfcc.edu/faq/cobol
[iii] http://esj.com/articles/2011/11/28/best-practices-zos-security.aspx

CorreLog, Inc.
1004 Collier Center Way, Suite 103 • Naples, Florida 34110
1-877-CorreLog • (239) 514-3331 • info@correlog.com

CORRELOG®
www.correlog.com