AUDIT COMPLIANCE WILL NOT STOP A MAINFRAME HACKER

If your company uses big iron to power your IT infrastructure, then you have sensitive data which will require you to pass an external audit. These auditors are taking their cues from the government organizations which have been drafting legislation to protect their constituents personally identifiable information (PII) whether it is the Payment Card Industry (PCI) Data Security Standard (DSS), Health Insurance Portability and Accountability Act (HIPPA), Europe's General Data Protection Regulation, or dozens of others. These robust regulations specify dozens of requirements like encryption, password complexity, audit logging, and many more that companies have to adhere to in order to safely secure their user's data. Since these detailed regulations specify how to protect our mainframes then we should be secure from cyber attacks if we are in adherence, right?

The best way to answer this question is to understand how to handle security incidents. For that we should use the National Institute of Standards and Technology (NIST) cybersecurity model which is a voluntary Framework consisting of standards, guidelines, and best practices for managing cybersecurity-related risk.[1] This framework is notably different that the regulations listed above because it focuses holistically on managing cyber security incidents throughout the lifecycle of the event. It breaks this lifecycle down into five key functions:

1. Identify – In this first step it is key to identify the key stakeholders for security. Some shops may have their mainframe directly integrated into their Security Operations Center where the same security analysts who are protecting the distributed systems assets are responsible for the mainframe. Many others have their mainframes separated and managed entirely under a mainframe

manager. Either way your company decides to task organize, the responsibility for ensuring the security of the mainframe needs to be established because too many organizations are putting security and the mainframe in separate bins and are finding themselves years behind their peers at capably handling the rest of these functions.

2. Protect – This second step is the most familiar and easiest to understand. Mainframe shops are comfortable using their External Security Management (ESM) systems like IBM's RACF to establish authorities. They are also used to passing their compliance regulatory requirements and ensure they are using encryption, logging data at some regular interval, setting password requirements, and ensuring global permissions match whichever audit they are required to meet. Mainframe teams have been doing this for decades and are usually quite competent. Unfortunately, many organizations tend to stop focusing on security at this point because they have a false sense of it thanks to passing their audit requirements. This myth leaves companies with a major unknown risk because of two critical reasons:

a. Nothing done in this section will effectively stop an insider threat which more than 69% of enterprise security executives reported experiencing.[2]
b. Hackers and penetration testers continue to prove remarkably successful at bypassing the controls that defenders put in place.

3. Detect – Step three is where the NIST framework really diverges from a technical list of regulations found in audits and begins to demonstrate how to fully handle security incidents. It starts with the basic fact – given enough time and resources a hacker can break into any system. We have seen real world cases of viruses taking down a nuclear power plant, so it should be no surprise that hackers can gain access to the mainframe which is, truly, just another connected computer on your IT infrastructure.[3] So how do we handle this? With a robust detection capability designed to catch hackers in the act.

There are many software solutions that attempt to assist companies with detecting malicious and anomalous behavior on their mainframe, yet few truly enhance an organization's ability to detect a breach in real time. To be effective, your security solution needs to do two things:

a. **Real-Time Visibility** – The first step of detecting breaches in real time is to be able to view mainframe activity in real time. This is generally achieved by getting mainframe events transported directly to a Security Information and Event Management (SIEM) solution like Splunk, Arcsight, or Qradar. The ability to view events in real time can give you a key advantage for viewing abnormal behavior for your privileged users, a restricted user who has somehow escalated their privileges, sensitive dataset access attempts, login attacks, and many more. If you do not have the ability to see your mainframe in real time, you are at risk to have a breach that goes undetected for weeks to months.[4]

a. **Indicators of Compromise (IOC)** – The next vital step is to be able to automate and correlate the data you are collecting in the real time scenario above. Getting mainframe dashboard views in your SIEM is a great first start but we need to be candid and understand that most Security Operations Centers are overworked and unable to monitor dashboards all day. To be truly effective, you must leverage automation in this step to derive actionable intelligence from the data. To do this, you need to conduct multi-variate analysis on your mainframe data to

determine which action(s) by a user are suspicious enough to warrant raising an alert for a security analyst to investigate. When mainframe hackers sit down and build correlation threads based on their penetration testing experience you can derive highly accurate and effective Indicators of Compromise (IOCs) that automate your detection and enable you to immediately respond to malicious threats.Building these IOC's are hard because they require legitimate security expertise and a background with bypassing all the controls established in the protect phase. If your security solution is alerting you on configuration changes that would upset an auditor, and not actions a hacker would actually take, then you are still only in protect and will fail at detecting Advanced Persistent Threats (APT).

4. Respond– When your automated defense spots an IOC or your malicious threat's actions have caused enough damage that you take notice to their behavior, you should have an incident response playbook detailing how to respond. To be effective in this phase you should have deliberate plan of action detailed in this runbook which can be tested periodically to ensure both the mainframe system programmers and security analysts each know their roles and reporting procedures. Really mature shops are starting to adopt Security Orchestration and Automation Response (SOAR) software which automates the flowchart response to minimize the threat's availability on the system. Packaged together, distributed systems often run software labelled Endpoint Detection and Response (EDR) which runs on each individual endpoint to provide automatic detection and response to IOCs and provides security teams the ability to quickly conduct incident response to determine the scope of the threat. This capability significantly raises the bar hackers would need to bypass the systems innate protection and this functionality is something most mainframe shops are lacking on the biggest and most important computer in the company.

5. Recover– The final stage is remediation and this comes after you have effectively responded to and removed the threat. Fortunately, most mainframe shops tend to be prepared here thanks to the ultimate importance of the platform which can go down for reasons outside of cyber-attacks. Being prepared to back up from tape in the case of ransomware or fail over to additional LPARs to quarantine a malicious user may save a company millions of dollars in lost data and downtime.

When you read through the lifecycle of the NIST cybersecurity framework it illustrates each core function that a company needs to be able to conduct in order to minimize the damage of a security incident. For most mainframe shops, their biggest risk comes from a false sense of security in protection from passing an audit and the corresponding failure to adequately address detection and response. If you believe your mainframe shops are perfectly protected, I challenge you to a true mainframe penetration test led by a real ethical hacker, not an auditor.

To assist with closing this gap, BMC is dedicated to working with world's leading mainframe hackers and penetration testers on developing state of the art Indicators of Compromise. We're building them into BMC AMI Security, which is the only mainframe Endpoint Detection and Response solution on the market that provides real-time visibility and actionable intelligence to protect the most important asset in your infrastructure. If you'd like to hear more or see a demonstration, please contactChristopher_perry@bmc.com.

---

[1] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[2] https://www.darkreading.com/vulnerabilities---threats/8-surprising-statistics-about-insider-threats/d/d-id/1326653?image_numbe

r=2

[3] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[4] https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack