Rocket® software

How to Start a Mainframe Vulnerability Management Program

Introduction

The threats to cybersecurity are constantly evolving as new attacks emerge and older ones resurface to strike again. Cybercriminals target any organization with resources worth plundering, and security tools and strategies must constantly evolve to keep up with this complex reality.

To help, the National Institute of Standards and Technology (NIST) has updated its toolbox of safeguards that organizations can use as a guideline for protecting sensitive data. One of the organization's flagship risk management documents, NIST Draft Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, has undergone a significant update. It's part of a larger push by NIST to help organizations keep up with the evolving threat landscape by developing next generation security and privacy controls.

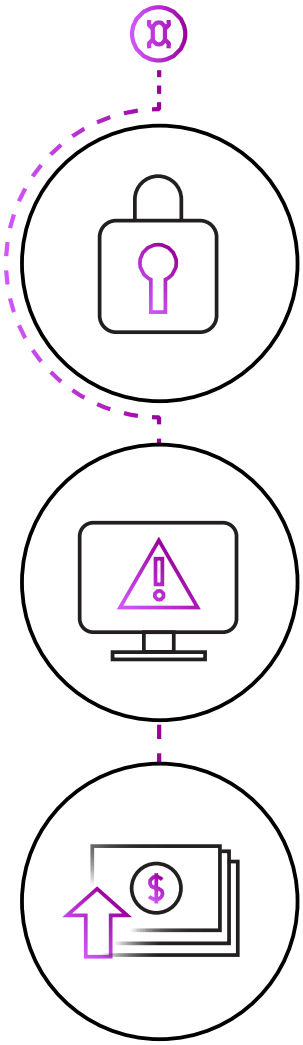
The revision improves on the security posture of the previous framework through a number of changes, from integrating privacy controls into the security framework to promoting alignment with different risk management and cybersecurity approaches and lexicons. This includes the NIST Cybersecurity and Privacy Frameworks. NIST is now recommending that companies scan all systems. Using these controls is mandatory for federal information systems, but even organizations not required to follow NIST's framework should take these changes into consideration.

Incorporating NIST's revised recommendations as guidelines for designing a stronger mainframe security strategy will help increase security and privacy. And now that NIST is calling for companies to scan all systems, including mainframes, it's more important than ever for organizations to implement mainframe vulnerability management programs. The first step to starting a mainframe vulnerability management program is awareness. So, let's take a step back and understand what mainframe vulnerabilities are, and why managing them is essential to ensuring system security and integrity.

> "Our objective is to make the information systems we depend on more resistant to cyberattacks. We want to limit the damage from those attacks when they occur, make the systems cyber-resilient, and at the same time protect the security and privacy of information."
>
> **RON ROSS,**
> One of the authors,
> NIST Draft Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations

What are mainframe vulnerabilities?

Mainframe vulnerabilities can arise from a variety of sources, including hardware configurations, IPL parameters, External Security Manager (ESM) configurations, and operating system programs. Businesses usually know that they need to scan applications for vulnerabilities. But, perhaps the most dangerous type of mainframe vulnerabilities is a category that's often overlooked: **code-based vulnerabilities.**



Code-based vulnerabilities are areas of flawed code that allow a program to bypass the security controls implemented by the operating system and organization. These vulnerabilities can appear any time a change is made to a mainframe operating system, such as an OS upgrade, standard maintenance, or the introduction of a new third-party software product. But they often slip through the cracks. For example, when vendors release a new product, they can't always simulate every client environment, so they aren't able to locate — and fix — all potential gaps.

If a hacker exploits a code-based vulnerability, they gain access to all the data, applications, and users on the entire mainframe. That's a huge amount of risk. If the hacker were to then gain system administrator privileges, it could be catastrophic for the entire organization. Hundreds of applications and thousands of users could be exposed, all from one code flaw.

This kind of breach could potentially bring a business to its knees, producing regulatory fines, consumer litigation, and a public relations nightmare. Globally, **the average cost of a breach is $3.86 million.** To protect against them, organizations need to secure the mainframe environment at every level and ensure operating system-level integrity is an essential part of their overall security strategy. Many organizations don't realize the severity of their exposures until they have completed a mainframe code-based vulnerability assessment.

Without operating system integrity, there can be no system security

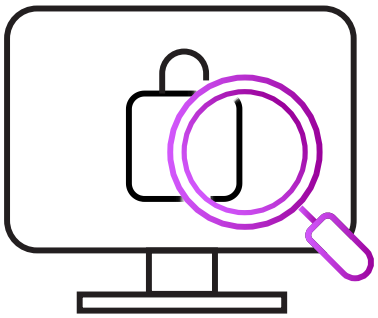
Code-based vulnerabilities occur when one of the authorized programs on a company's z/OS® system violates the IBM® z/OS Statement of Integrity, which says:

> **IBM's commitment includes design and development practices intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security – that is, to prevent them from gaining access, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless allowed by the installation. Specifically, z/OS "System Integrity" is defined as the inability of any program not authorized by a mechanism under the installation's control to circumvent, disable, store or fetch protection; access a resource protected by the z/OS Security Server (RACF®), or obtain control in an authorized state — that is, in a supervisor state, with a protection key less than eight (8) or an Authorized Program Facility (APF). If an IBM System Integrity problem is reported to IBM, IBM will always take action to resolve it in the specified operating environment for releases that have not reached their announced End of Support 1 dates.**

It's important to note that IBM doesn't promise that z/OS won't have system integrity issues. IBM only says that if system integrity issues are reported, they'll take action to resolve it. But, this means that organizations that rely on z/OS need to be looking for system integrity issues, which involves scanning for vulnerabilities.

System integrity is a critical component of z/OS — all the major ESMs depend upon system integrity to function properly. Just one code-based vulnerability could compromise the integrity of the entire mainframe, and mainframe integrity breaches can undermine your security systems. You can't have system security without operating system integrity.

What it takes to scan for mainframe vulnerabilities



Many companies rely on third-party security solutions like RACF, CA Top Secret, and ACF2 to ensure mainframe security. But these tools alone aren't enough. While they can provide some important security functions, like helping to establish permissions (authentication) and access control (authorization), these kinds of tools simply aren't capable of ensuring integrity since they don't secure the mainframe at every level.

Instead, companies need to invest in a comprehensive mainframe security strategy, starting with a mainframe vulnerability management program that provides ongoing testing and evaluation to uncover known and zero-day vulnerabilities.

Starting a mainframe vulnerability management program

The deep-seated nature of code-based vulnerabilities means that they can be difficult to find — and fix. To ensure the integrity of a z/OS system, companies need to scan all of their authorized programs to determine if any code-based vulnerabilities have been introduced. Subsequently, organizations can move forward on a path to remediation before those vulnerabilities are exploited by a bad actor. **A successful mainframe vulnerability management program includes these components:**

Vulnerability Scanning Software:

Scanning programs manually is both costly and impractical. Code-based and configuration-based software can perform automated scanning on an ongoing, scheduled basis, helping to ensure system integrity.

Standardized Risk Ratings:

Assigning risk ratings to vulnerabilities helps companies clarify the necessary course of action. Systems like the Common Vulnerability Scoring System (CVSS) from the National Vulnerability Database provide a common language to get everyone on the same page for the remediation plan.

Policies and Procedures:

Develop and implement processes around vulnerability mitigation. How will you keep key stakeholders throughout the business informed of mainframe security risks? What happens when a vulnerability is found? Who on your internal team needs to know about the vulnerability, and who will report the vulnerability to the vendor? What steps will you take to address the gap quickly?

Now that you've identified the key components of a successful mainframe vulnerability management program, learn more about the vulnerability categories you need to be aware of when adopting this program — or, speak to one of our mainframe security experts for additional guidance.

About Rocket Software

Rocket Software partners with the largest Fortune 1000 organizations to solve their most complex IT challenges across Applications, Data and Infrastructure. Rocket Software brings customers from where they are in their modernization journey to where they want to be by architecting innovative solutions that deliver next-generation experiences. Over 10 million global IT and business professionals trust Rocket Software to deliver solutions that improve responsiveness to change and optimize workloads. Rocket Software enables organizations to modernize in place with a hybrid cloud strategy to protect investment, decrease risk and reduce time to value. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located throughout North America, Europe, Asia and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and Twitter.

Ready to learn about the **categories of mainframe vulnerabilities?**

Read the blog post or **Talk to an expert**

Visit RocketSoftware.com ›

Rocket software

MAR-8052_WhitePaper_MFvulnerabilityMgtProgram_V5