Trap Doors, Storage Alteration, and System Instability vulnerabilities are several of the many you need to be aware of that can impact the integrity of your mainframe. The mainframe is the most enduring IT system, well-regarded for its processing speed and high degree of security. But just because the mainframe is secure, doesn’t mean it’s impervious. The myth of the mainframe as a secure powerhouse has meant that the system is often overlooked or ignored in corporate IT security strategy.

A critical piece of your mainframe security strategy is mainframe vulnerability management. Application and network scanning alone isn’t enough – you must scan for Integrity Vulnerabilities in operating system (OS) layer code and continuously assess security configurations – and it’s necessary to be aware of the mainframe vulnerability categories that could severely impact the security of your mainframe.

Leverage a Security Architect for the mainframe that understands the organization’s mission, objectives, stakeholders, and activities, and understands the policies, procedures, and processes required to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements.

Include the mainframe in your Vulnerability Management Program. Install a vulnerability scanner like Rocket® z/Assure® Vulnerability Analysis Program, for proactive monitoring, and scan all software before going to production. This enables you to identify vulnerabilities, perform forensics analysis, prioritize risks, and report the location of the exploitable code for ease of remediation.

As a suggested first step, we recommend you:

Learn more about z/Assure® Vulnerability Analysis Program

1. 91% of all cyber attacks begin with phishing emails to unexpected victims. Deloitte Malaysia, Risk Advisory, Press releases.