KEY RESOURCES
The Key to zSystems Integrity

CASE STUDY

A Tale of Two Worlds: Integrating Mainframe Scanning with a Global Bank's Penetration Testers

CHALLENGE

- Shift mainframe vulnerability scanning tasks to the penetration testing team.
- Educate penetration testers on mainframe language, scheduling and scanning.

SOLUTIONS

- Recruited systems programmers within the company to become in-house vulnerability scanning advocates.
- Provided mainframe education to penetration testers.
- Mainframe vulnerability reports provided in standardized CVSS scoring methodology.

BENEFITS

- Penetration testers now adept at mainframe vulnerability scanning, capable of analyzing vulnerability reports, working with vendors to mitigate the vulnerabilities, and running automated checks
- Mainframe operations team no longer responsible for vulnerabilities and other security challenges outside of their purview.

The relationship between the mainframe security, operations, and penetration testing teams at many global enterprises can be a tricky one. Increasingly, mainframe teams at large organizations are looking to shift the responsibility for overseeing mainframe vulnerability management to the penetration testing side. But, oftentimes, the penetration testing teams don't have any mainframe experience, and being tasked with overseeing mainframe vulnerability management appears daunting.

Key Resources, Inc. has experience supporting enterprises through these challenges. We've fielded many requests on how to integrate mainframe scanning with penetration testing, including from one global banking firm.

A Lack of Mainframe Experience

Key Resources had been performing mainframe vulnerability assessments for this bank for four years, when their mainframe operations director said that his team did not feel comfortable being held responsible for vulnerability scanning and the resulting reporting, reasoning that it should lie with their penetration testing team instead. The problem: everybody on the penetration team only knew network and PC scanning methodologies; no one had any experience with the mainframe.

"We never even thought we could have vulnerabilities on the mainframe," said the bank's chief information security officer (CISO).

But, both teams came to agree that mainframe scanning responsibilities were better off centralized with the penetration testing team. They met with the bank's CISO to determine the challenges and frictions in migrating these responsibilities from one team to the next, and identify what they needed in order to build out a mainframe education program for the penetration testers.

That's where Key Resources stepped in.

"Getting our penetration testers up to speed on the mainframe seemed like a tall task at the beginning, but it was well worth the time and effort we put into this integration," said the bank. "And, our company is much more secure to show for it."

Achieving 100 Percent Accuracy

The first step in integrating the mainframe and penetration testing methodologies together was to find mainframe systems programmers who could work and train the penetration team members. Training would cover both mainframe operating system fundamentals, as well as specific vulnerability testing procedures and mitigation processes.

> "Getting our penetration testers up to speed on the mainframe seemed like a tall task at the beginning, but it was well worth the time and effort we put into this integration. And, our company is much more secure to show for it."
>
> CIO

The bank located two veteran systems programmers to assume this role, and Key Resources oversaw a six-month training program. Because the penetration testers were accustomed to PCs, where you don't schedule jobs the way you would on a mainframe, they had to learn the mainframe scheduling language. The programmers-turned-mainframe-advocates in the bank were able to offer hands-on training, with Key Resources continuing to provide outside support in the event a critical question arises.

After picking up these basics, testers learned how to set up automatic vulnerability scanning schedules within z/Assure® Vulnerability Assessment Program (VAP), a Key Resources solution. Today, they're able to re-test and perform mitigation assessments that don't require re-running an entire set of schemes.

"Thanks to this assistance, the results of our mitigation efforts have been 100 percent accurate," the bank said.

Fully Integrated

Despite their PC-based background, the bank's network penetration testing team is now capable of running automatic mainframe vulnerability checks on z/Assure® VAP, fully assuming responsibility for scanning of the firm's mainframe systems for vulnerabilities.

They're now well-versed in mainframe operating system fundamentals, from analyzing vulnerability reports that detail specific classes of vulnerabilities to running autonomous checks across the bank's multiple data centers around the world.

"The integration process was even easier than we originally thought," said the bank. "There were some bumps along the way, but overall it proceeded very smoothly."