Vanguard Security Assessments

According to Gartner, "The IBM z/OS mainframe continues to be an important platform for many enterprises, hosting about 90% of their mission-critical applications... [Yet] the incidence of high-risk vulnerabilities is astonishingly high."[1]

The mainframe's reputation for top-notch security is what has lulled many organizations into a false sense that this critical asset is protected. Many companies still rely on mainframe security best practices and auditing procedures that were developed years ago when only a small number of tightly controlled users accessed mainframes over secure corporate networks.

Mainframes have become a key part of cloud, big data and other initiatives, and more users than ever before are accessing IBM® System z® mainframes over the Web and via cloud-based services. This expanded use, combined with outdated security configurations and practices, is increasing mainframe security vulnerabilities and putting many organizations at risk.

Today's mainframe is just another box in the data center, accessible internally and externally like every Windows, Unix, Linux or other server. Not only are System z environments vulnerable to internal malicious users, but also to external hacktivists, criminals and competitors. To ensure critical assets are properly protected, organizations should perform regular mainframe security assessments.

Vanguard's Professional Services team members conduct Vanguard Security Assessments to discover high-risk mainframe vulnerabilities.

Vanguard Security Assessments help to:

- Prevent security breaches and other risks.
- Protect critical customer and corporate data and applications.
- Reduce risk by ensuring that security policies and procedures meet current regulatory and industry standards.
- Increase efficiencies in managing and auditing mainframe systems.
- Enhance productivity by avoiding downtime and better aligning security resources.

Reduce Risk, Avoid Breaches and Business Disruptions

Vanguard Security Assessments quickly identify and prioritize mainframe penetration risks, determine whether the System z implementation reflects best practices for security and integrity, and evaluate the potential impact and exposure of any findings on an organization's operations and reputation, e.g., failing audits, losing revenue or violating privacy protections.

In more than 120 assessments the Vanguard security team has recently conducted, it has discovered on average more than three severe and high security risks that need immediate remediation, and more than 20 total findings that need to be addressed.

- Identify and prioritize mainframe security risks that impact critical information assets
- Review and update company security policies and procedures to meet industry security standards and regulatory requirements on the mainframe
- Develop remediation plans to improve the System z security environment and help achieve broader business objectives
- Transfer knowledge to security staff to ensure mainframe security and compliance

VANGUARD
INTEGRITY PROFESSIONALS
INFORMATION SECURITY EXPERTS

Assessments include a rigorous review of security policies, procedures and more than 170 security configuration controls (each of which has tens of thousands or hundreds of thousands of instances in a System z environment). More specifically, Vanguard Security Assessments evaluate the following:

- Integrity and security of System z implementations including key security elements in place for the z/OS® operating system and RACF® system-wide options, database datasets, general resource class profiles, group structures and access, exits, and recovery procedures.
- Documented security policies for users and the protection of information assets and procedures for provisioning and administration.
- Security-related procedures for operations, help desk and support departments.

Vanguard regularly updates its assessment process to ensure it supports the latest industry and regulatory standards (see sidebar for supported standards). The findings from Vanguard Security Assessments are documented in a comprehensive report that provides:

- Details on specific areas where mainframe security policies, procedures and systems are creating risk.
- Rankings, from low to severe, of detected vulnerabilities.
- Instructions for remediating security problems and meeting industry standards and regulations.
- Guidance about how to prevent erosion of the mainframe environment once it is secure and compliant.

Vanguard Security Assessments help organizations create and maintain a secure and compliant mainframe environment to maximize their investments and provide a solid base for ongoing operational improvements and new initiatives.

About Vanguard Integrity Professionals

Vanguard Integrity Professionals provides enterprise security software and services that solve complex security and regulatory compliance challenges and deliver a rapid return on investment. With automated solutions for identity and access management, and governance, risk and compliance, Vanguard enables government agencies and corporations around the world to ensure continuous monitoring of mainframes, safeguard cloud computing secure domains, and protect critical data and applications from cybersecurity threats.

For More Information

To find out more about how Vanguard Security Assessments can help your organization, email sales@go2vanguard.com or call (702) 794-0014.

Vanguard Security Assessments Support

- Basel II and III
- Centers for Medicare & Medicaid Services (CMS)
- Control Objectives for Information and Related Technology (COBIT)
- Defense Information Systems Administration (DISA) STIG
- Federal Financial Institutions Examination Council (FFIEC)
- Federal Information System Controls Audit Manual (FISCAM)
- Gramm-Leach-Bliley (GLB)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)
- National Institute of Standards and Technology (NIST)
- Payment Card Industry Data Security Standards (PCI DSS)
- Sarbanes-Oxley (SOX)

[1] “Why Your IBM z/OS Mainframe May Not Be as Secure as You Think It Is and What You Can Do About It,” 2010 Gartner RAS Core Research Note

VSAPS-101