InformationWeek

TOP TIPS

10 Best Practices for Securing Your Mainframe Environment

Mainframes are a critical component of the IT infrastructure at a majority of large organizations. Despite years of predictions about their demise, mainframes continue to power business-critical applications and host more volumes of sensitive data than ever.

However, a growing shortage of skills and outdated notions about the impenetrability of Big Iron have put mainframe environments dangerously out of sync with the rest of the IT infrastructure and security teams. The following are some best practices for securing your mainframe environment and getting the most out of your investments.

Address Vulnerabilities with Proper Patching Practices

Key Points: Organizations are often reluctant to apply security patches and updates to their mainframe environments in a timely fashion because of downtime concerns. Another reason is that applying patches to mainframes can require more of a manual effort than applying updates to Windows and other IT environments. Mainframe vendors often do not have a scheduled patch release or formal patch announcement process, so organizations can miss important security updates. Failure to patch heightens breach risks.

Recommendations: Implement a formal security update/patch deployment process. Automate patching where possible and have a process for verifying the updates have been properly installed. Not all vulnerabilities that impact the mainframe environment are documented in the NIST National Vulnerability Database, so make sure to check for updates from your vendor. Regularly scan your environment for and address any missing patches and updates in the operating system and third-party software.

Implement Secure Configuration Management

Key Points: An overemphasis on availability can sometimes lead to configuration errors that put confidentiality and the integrity of the mainframe environment at risk.

Recommendations: Organizations should implement formal configuration management processes around identities, passwords, provisioning and deprovisioning of accounts, privileged account management, shared accounts, segregation of duties, and event monitoring.

Sponsored by

bmc

Manage Your Privileged Users

Key Points: Users and accounts with privileged access pose a risk to the security of the mainframe environment. Without proper controls, the accounts can be misused for everything from changing mainframe security configurations to compromising critical applications and data. Insiders who misuse privileged access pose one of the biggest threats to mainframe security.

Recommendations: Identify all users with privileged access and regularly review the entitlements they have to applications and data. Remove any accounts that are not being used or are not needed. Monitor, record, and audit privileged user access. Block or limit the ability of privileged and superusers to alter or reset critical controls on their own. Implement least privileged access and ensure proper segregation of duties. Require strong authentication for privileged users.

Have Strong Access Controls

Key Points: Users with overly permissive access to mainframe data, applications, and databases can undermine the security of the entire environment. Users these days can access the mainframe environment directly, via a web interface, through other applications, and other means.

Recommendations: Determine who needs access to your mainframe resources, what they need to access, and what kind of access they require. Limit the ability to read, update, or delete files, transactions, and databases or to execute commands and other actions to only those users who actually require it. Implement access controls to mainframe libraries, resources, and databases. Log and audit access to ensure access is happening only as defined.

Address Staffing and Skill Gaps

Key Points: An aging mainframe workforce — and a shortage of new skilled technicians to replace them — could soon impact the ability of organizations to get the most from their mainframe investments.

Recommendations: Look for ways to augment the workforce with managed services and automation where possible. Invest in training and education. Consider using programs and consulting services to train a junior staff member or a new college graduate. Use modern development tools and development methodologies, such as DevOps and continuous integration/continuous delivery (CI/CD), to attract fresh talent.

Sponsored by

bmc

Conduct Regular Penetration Tests

Key Points: Penetration tests can help organizations proactively uncover and protect against vulnerabilities in the mainframe environment. Pen tests are also useful from a regulatory compliance standpoint, especially for organizations in industries such as financial services, healthcare, and energy.

Recommendations: Conduct regular pen tests to identify potential vulnerabilities in your mainframe infrastructure, operating system, code from independent software vendors, and in internally developed code. In addition, use pen tests to identify weak passwords, weak access controls, and other potential configuration weaknesses that could enable privilege escalation and other misuse.

Don’t Let Backward Compatibility Hold You Back

Key Points: Organizations are so focused on backward compatibility that they sometimes fail to take advantage of new features and capabilities available with the new generation of mainframe software and hardware.

Recommendations: Emphasize efforts to learn new technologies. Managed service providers often provide specialized skills and training that can help you get started. Focus on trying to find ways to take advantage of the latest innovations around mainframe software and hardware, especially in areas such as encryption and cloud-native development. Many new features are disabled by default to ensure they don’t break production availability. Analyze and research these functions and study ways to enable them securely.

Avoid Vendor Lock-In

Key Points: The days of having to be locked into a single hardware or software vendor for your mainframe environment are long gone. Vendor lock-in can increase costs, reduce choice, and limit interoperability and portability.

Recommendations: Take advantage of alternative/third-party software and service providers where possible to cut down on costs and prevent vendor lock-in. Even though the mainframe environment offers fewer options than other technology segments, there are enough choices for you to be able to swap out existing products with potentially more modern, less expensive alternatives for just about all of your mainframe requirements.

Automate Where Possible

Key Points: Mainframe staffing is becoming a critical issue. People with mainframe skills are becoming harder to find. Automation can help reduce some of the dependencies as the next generation is staffed and trained.

Recommendations: Take advantage of available technologies to automate operations and testing where possible. Numerous tools are available that allow organizations to apply modern testing practices around development. Use intelligent automation to monitor privileged user activity, to get alerted on unauthorized access, and to protect, detect, and respond to other threats.

Integrate with Your SIEM

Key Points: When threat events happen on the mainframe (and they do), your security teams need to be notified in order to take action. However, security and infrastructure operations tend to operate in silos.

Recommendations: Leverage your existing security investments by integrating the mainframe with your enterprise security information and event management (SIEM) technology. Real-time alerts and reporting can surface actionable intelligence that close the opportunity for attackers to go undetected.

Learn more about how BMC can help you with your mainframe security and services requirements here.

Sponsored by

bmc