Solution Brief

BROADCOM
MAINFRAME SOFTWARE

Mainframe Cyber Resiliency and Cyberattack Prevention

Overview

Preventing ransomware attacks has become one of the top cybersecurity priorities for organizations. Mainframes are not immune to ransomware or any other cyberattack. Yes, the most secure platform on the planet that runs mission-critical applications and holds approximately 80% of the world's most sensitive data requires the same focus and priority as the distributed and cloud platforms (The FutureScape of IT).

A system programmer connecting from an unsecured home network can bring risk to the mainframe by opening a simple phishing email, or through compromised credentials, ransomware gangs can enter into the environment!

Targeted Ransomware are planned attacks where hackers target the highest value data and information. The mainframe holds your organization's most crucial assets! No one can deny that the topmost cybersecurity priority is protecting the mainframe.

Preventing Attacks and Protecting Mainframe from Insider Threat, Bad Actors, or even Ransomware

First, know what mainframe assets are crucial for your business, where they are, and most importantly, who has access to them. This helps prioritize preparedness activities and know the impact in case of an attack.

Second, continuously learn about cyber threats, perform the risk assessment for your mainframe environment, and ensure you have implemented continuous security monitoring on the mainframe.

Best Practices to Help Prevent Cyberattacks

Typically, ransomware breaches begin through one of the following methods:

- Phishing email
- Remote desktop protocol compromise
- Malware ends up installed directly on servers or desktops

The first line of defense is increasing cybersecurity awareness through mandatory training to your employees and users about your organization's cybersecurity strategy and user-level best practices.

Colonial Pipeline paid a $4.4 million ransom, JBS (global meat producer) paid $11.0 million, and global insurance provider CNA Financial, paid $40.0 million…

These figures do not reflect the additional costs of an attack, including paying third parties, such as legal, PR, and negotiation firms, or the opportunity costs of having executives and specialized teams turn away from their day-to-day roles for weeks or months to deal with an attack and its aftermath, or the lost revenue that results.

– McKinsey & Company

"It seems clear that targeted ransomware attacks will be a key threat that large enterprise organizations will continue to face this year, and likely beyond. This is why it is important for all organizations to have an effective cyber-security strategy in place in order to protect themselves and mitigate the dangers of targeted ransomware attacks."

– The Ransomware Threat Landscape: What to Expect in 2022 from Symantec® by Broadcom® Software

Basic Hygiene Practices for Mainframe

Strong, Complex Passwords and Passphrases
In the past, some mainframe applications only supported up to eight-character passwords. However, modern mainframe security solutions fully support complex passwords and long passphrases. Review the published Security Technical Implementation Guides for password/passphrase complexity and ensure standards are enforced within ACF2™, TSS, and RACF. Do not allow simple passwords that can be cracked easily.

Multi-factor Authentication (MFA)
Cyberattacks that leverage compromised credentials are dangerous. MFA shields from such attacks. Implement MFA for all mission-critical applications and privileged users on the mainframe. For more information, see Advanced Authentication Mainframe.

Privileged Access Management
Privileged access should be limited to when the user requires such access and not be granted as permanent 24x7x365 access. To reduce the risk, elevate the user privileges for the time when they are performing the task, then return the user to normal access state. This practice reduces the organizational risk drastically. For more information, see Trusted Access Management for Z.

Restrict Access, and Move to the Least Privilege Access Model
Continuously monitor entitlements and users, track what access has been used and what has not been used. Provide automated reporting and cleanup of unused entitlements based on organizational frequency. This practice will reduce corporate risk by removing users and entitlements no longer required. For more information, see Cleanup.

Block Unused Ports and Protocols
Please find the unused or unsecured ports to the mainframe and fix them. Keep track of the open ports, review, and continuously monitor how the ports are protected. For more information, check NetMaster® Network Intelligence.

Every application, system, and software change should be reviewed by teams, including the cybersecurity or IT security team. The organization must assess changes for possible security impacts and ensure that any new security requirements or required security controls are implemented.

Implement mainframe security continuous monitoring to ensure that critical security and system controls are monitored with real-time alerting. Create an organization mainframe security continuous monitoring playbook with what to monitor, whom to notify, and what actions should be taken by whom for all items to be monitored. Once implemented at the mainframe system level, consider the critical areas of the applications, what should be monitored, and have real-time alerting set up. For more information, see Compliance Event Manager.

Software Updates
Software vulnerabilities are another common avenue for hackers, and software vendors often release security patches or product updates containing security fixes. Apply the patches and upgrade to the most current software version. This practice helps to fix the known vulnerabilities, and most importantly, you get vendor support. Always ensure that you are using currently supported software, especially for cybersecurity or operating system software.

Lastly, ensure that you have tested your backup and recovery procedures for your business critical applications and data—and be prepared for unexpected events.

Where is your personal data stored? Why should we not all work together to ensure that the data, digital assets, and personal data are as secure as possible?

Perhaps the next steps forward would be to ask for a mainframe security assessment or set up a meeting with our mainframe cybersecurity experts to discuss the current Top 10 cybersecurity challenges that involve the mainframe.

MF-CYRES-SB100 June 20, 2022