bmc

The Top Mainframe Security Threats of 2020

Real-world penetration and security assessments have uncovered the most common **risks to mainframe** security. What are they?

1 Too Many Users with Elevated Privileges

+ How does it happen?

The Superuser privilege is inappropriately used granting ALL users access to System Service and Order Management System resources and Data.

+ What's the risk?

Sensitive Data can be easily copied, deleted or held ransom.

2 Privilege Escalation Vulnerabilities

+ How does it happen?

Many enterprises grant excessive access to libraries and authorized datasets that leave Administrator and System level access unprotected.

+ What's the risk?

Bad actors can leverage this to elevate their privileges, read and write all data and memory.

3 Default Passwords and Weak Password Management

+ How does it happen?

Static passwords with no regular change intervals and default passwords that are used for months at a time.

+ What's the risk?

Unless manually changed, phishing or keylogger attacks could go undetected.

4 Access to Sensitive and Cryptographic Data

+ How does it happen?

Read access to the database allows it to be copied and downloaded. Data set profiles that are poorly configured allow read, update and control access.

+ What's the risk?

Data can be copied, updated or downloaded. Once downloaded, off-line password cracking tools can reveal passwords in the database.

5 "Faceless" Accounts

+ How does it happen?

Tasks that are system processes have poor or rarely changed passwords but system level privileges.

+ What's the risk?

A bad actor could have lengthy dwell times in addition to pervasive access to system resources to expand their attack.

Want to make sure your mainframe is secure?

Get an assessment or penetration test to uncover your vulnerabilities before an attacker can!