

# The Myth of Mainframe Security

## CAUSE FOR CONCERN

Many users of the IBM® mainframe platform believe them to be inherently secure—a platform that cannot be hacked. While it's true that the platform is one of the most securable on the planet, in practice this is often found not to be the case. Site specific security configurations, often set up decades ago, are invariably found lacking—especially in today's much evolved, increasingly connected environments. In every recent client engagement, we have found significant failings, making the possibility of data breach worryingly high.

BMC Mainframe Services by RSM Partners specializes in IBM's mainframe platform and is an acknowledged world authority on security considerations. Offering a range of consulting services, BMC Mainframe Services by RSM Partners' penetration testing service quickly uncovers vulnerabilities which not only allow the possibility of data leakage, but also means that users could elevate their privileges without detection.

## FAIL 1

### Clean Audits?

A major banking client who had been receiving clean audit reviews from their external auditor for the past 10 years. Concern was raised about the quality and depth of the reviews being performed. BMC Mainframe Services by RSM Partners was engaged to perform a detailed review of:

- Operating system (IBM® z/OS®) and security (IBM® RACF®) controls
- Security related processes and procedures
- Cryptography

The resultant 100+ page report detailed over 50 issues, 25 of which were deemed both high risk and high probability.

## FAIL 2

### Exactly How Secure ?

BMC Mainframe Services by RSM Partners was engaged to perform a penetration test of another major banking client's mainframe systems. Using a standard non-privileged developer user ID, BMC Mainframe Services by RSM Partners was able to quickly demonstrate easy circumvention of security controls, allowing full edit access to production data, downloading it to a PC, formatting it using Excel, and loading onto a USB pen drive.

## WHY BMC MAINFRAME SERVICES BY RSM PARTNERS?

BMC Mainframe Services by RSM Partners is recognized worldwide as specialists in IBM® Z® skills: from consulting, security, project delivery and managed services, to extensive systems programming capabilities, ad hoc skills and resources for additional on-site or remote coverage, 24/7 incident support, mainframe capacity cost reduction programs, migrations, and more. Working with organizations large and small, no other partner offers the same depth of knowledge and experience. Clients know they can rely on BMC Mainframe Services by RSM Partners for quality, flexibility, and value.

### FAIL 3

#### Hidden Vulnerabilities

BMC Mainframe Services by RSM Partners sees many of our clients investing in scanning their enterprise software environment for vulnerabilities—but not the mainframe environment. Where BMC Mainframe Services by RSM Partners has been engaged to complete such a scan, we regularly find between 5 to 15 vulnerabilities, where the majority of the vulnerabilities could be easily exploited, leading to a significant control failure.

### FAIL 4

#### Valid Penetration Test?

BMC Mainframe Services by RSM Partners sees the majority of organizations engaging with external specialists to undertake penetration tests in order to both identify and prioritize necessary security remediation investment. However, these specialists invariably field a team that have little to no mainframe understanding, despite the robustness of the mainframe being key to the client. Time and again we see this resulting in dangerous oversight, giving rise to a similar situation as “Fail 1”.

### FAIL 5

#### Copies of Copies

BMC Mainframe Services by RSM Partners sees many instances where organizations feel their sensitive data is fully secured, but what is often overlooked is the data housed on the mainframe. On this platform, there are invariably a great many copies (taken over the years, for multiple purposes), now stored in a vast array of locations, in anonymous or not easily identifiable datasets. This scenario leaves the company at serious risk of both data leakage and non-compliance, either with internal company policy and/or regulatory compliance.

### FAIL 6

#### Data Leakage

BMC Mainframe Services by RSM Partners was engaged by another blue-chip client to perform a penetration test of their mainframe systems using a standard non-privileged developer user ID. While performing various standard tests, we discovered an administrator privilege that was not properly secured. This allowed us to take a dump of ANY dataset (production, development, or system), read the output file, download it to our desktop, and e-mail the file off-site.

### WHAT NEXT?

The question is, to what extent your own environment suffers from the above failings?

To decide whether action is warranted, clients invariably need some quantification of the issue as it pertains to their own particular environment.

### QUANTIFYING THE PROBLEM:

#### Either

A mini technical assessment, taking a quick look at your current mainframe security set up, producing a high level “security posture” document, highlighting the nature of any key issues identified.

#### Or

A mini penetration test, determining to what extent it would be possible for a potential “rogue element” to gain access to sensitive data or elevate their access privileges.



### FOR MORE INFORMATION

To learn more about The Myth of Mainframe Security, please visit [bmc.com](http://bmc.com)

#### About BMC

From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

**BMC—Run and Reinvent**

[www.bmc.com](http://www.bmc.com)



BMC, the BMC logo, and BMC's other product names are the exclusive properties of BMC Software, Inc. or its affiliates, are registered or pending registration with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other trademarks or registered trademarks are the property of their respective owners.  
© Copyright 2020 BMC Software, Inc.



\* 5 2 2 0 7 3 \*