RSM PARTNERS
Z MAINFRAME

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 practise 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, RSM continues to find significant failings, making the possibility of data breach, worryingly high.

RSM specialise in IBM's mainframe platform and are an acknowledged world authority on security considerations. Offering a range of consulting services, RSM's 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.

Countering the myth of mainframes being inherently secure, we're listing here a number of examples we've encountered recently:

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.

RSM were engaged to perform a detailed review of:

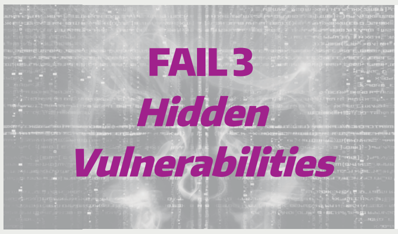
- Operating system (z/OS) and security (RACF) Controls
- Security related processes and procedures
- Cryptography

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 ?

RSM was engaged to perform a penetration test of another major banking client's mainframe systems. Using a standard non-privileged developer user ID, RSM 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.

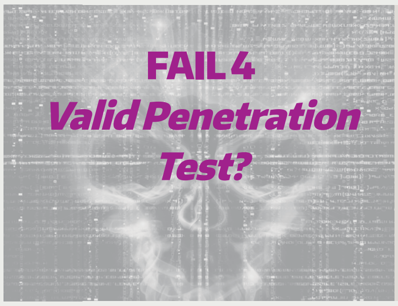
The Myth of Mainframe Security



FAIL 3 *Hidden Vulnerabilities*

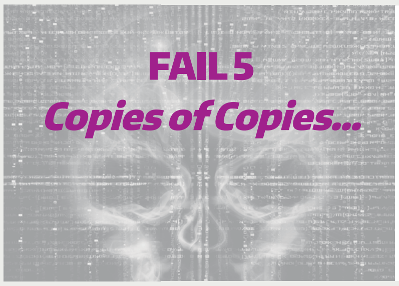
RSM sees many of our clients investing in scanning their enterprise software environment for vulnerabilities – but not the mainframe environment.

Where RSM 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?*

RSM sees the majority of organisations engaging with external specialists to undertake penetration tests in order to both identify and prioritise 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...*

RSM sees many instances where organisations 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/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*

RSM was engaged by another blue chip client to perform a penetration test of their mainframe systems, using a standard non-privileged developer user ID. Whilst performing various standard tests, we discovered an Administrator privilege that was not properly secured. This allowed us to take a dump of ANY dataset on the system (Production, Development or System), read the output file, download it to our desktop and email the file off site.

So ... 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.

Business Partner IBM

Business Partner IBM
Ready for
Security Intelligence

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

To find out more about these and other RSM Partners services, call **+44 (0) 1527 837767** or visit **www.rsmpartners.com**

T +44 (0) 1527 837767 | **E** info@rsmpartners.com | **www.rsmpartners.com**

RSM PARTNERS
MAINFRAME