5 Myths That Can Put Your Mainframe At Risk

Rui Miguel Feio
Security Lead
RSM Partners
Agenda

• Introduction
• Myth #1 – The mainframe is dead
• Myth #2 – No one hacks the mainframe
• Myth #3 – The mainframe is isolated from the rest of the world
• Myth #4 – “We don’t use Unix System Services”
• Myth #5 – Outsourcing will solve all the problems
• Questions
Introduction

• Rui Miguel Feio

  – Security lead at RSM Partners (UK)

  – I am a mainframe technician specialising in mainframe security

  – Experience in other platforms as well

  – I have been working with mainframes for the past 16 years

  – Happy to take questions as we go
Myth #1
The mainframe is dead
Myth #1

• Since the advent of the PC in the 1980’s the mainframe has been set for extinction.

• “The PC is now as powerful as a mainframe!”

• Only ‘old’ people know about mainframes.
Myth #1 – Some Facts

- IBM keeps bringing out new mainframes:
  - z13 – Jan 2015
  - zEnterprise BC12 (zBC12) – Jul 2013
  - zEnterprise EC12 (zEC12) – Aug 2012
  - zEnterprise 114 (z114) – Jul 2011
  - zEnterprise 196 (z196) – Jul 2010
  - z10 Enterprise Class (EC) – Feb 2008
  - z9 Enterprise Class (EC) – Sep 2005
  - z890 – Apr 2004
  - z990 – May 2003
  - ...

Myth #1 – Some Facts

- Mainframe as a whole contributes to 25% of IBM’s revenue and 35% of its operating profit*

- 96 of the world’s top 100 banks and 90% of the world’s largest insurance companies still use mainframes

- 85% of all mission-critical applications run on COBOL and the mainframe**

*Toni Sacconaghi of Bernstein Research
**Microfocus
Myth #1 – Some Facts

• Keeping in sync with the new technologies:
  – Enterprise Linux Server:
    • http://www-03.ibm.com/systems/z/os/linux/els.html
  – Enterprise Cloud Computing:
    • http://www-03.ibm.com/systems/uk/z/solutions/cloud/
  – Enterprise Mobility:
    • http://www-03.ibm.com/systems/z/solutions/mobile.html
  – Enterprise Security:
    • http://www-03.ibm.com/systems/z/solutions/security.html
  – Business Analytics and Big Data:
    • http://www-03.ibm.com/systems/z/solutions/data.html
Myth #1 – Leads to Risks

• Lack of understanding:
  – What the mainframe is and what it can do

• Lack of investment:
  – New solutions for the mainframe
  – Training

• Lack of resources:
  – Not hiring new resources
  – Replacing existing resources
Myth #2

No one hacks the mainframe
Myth #2

• “The mainframe is the most secure platform in the world”

• “Who’s gonna hack the mainframe?!?”

• “You need to be a mainframer to be able to use the mainframe”
Myth #2 – Some Facts

• Although highly securable, the mainframe is not secure by default
  • Like any platform, the mainframe needs to adapt and security needs to be constantly reviewed

• People with no mainframe background are getting interested...
  • http://soldieroffortran.org
  • http://mainframed767.tumblr.com
Myth #2 – Some Facts

• Guess what? The mainframe can be hacked!

  – Cyber attack on up to 100 banks - estimated $1bn (£648m) in losses (2015)

  – Swedish Nordea bank – personal data, money (2013)

  – IT firm Logica – more than 10,000 social security numbers (2012)
Myth #2 – Some Facts

• Have you considered the ‘inside threat’?
  – Recent case in the UK
  – Senior Applications developer
  – Detailed knowledge of the application
  – Exploited a known security control
  – Defrauded his employer of over £2,000,000!
Myth #2 – Leads to Risks

- Lack of investment
- Lack of training
- Lack of resources
- Lack of understanding
- Too much confidence

Security Risks & Exposures
Myth #3
The mainframe is isolated from the rest of the world
Myth #3

• There is still this idea that the mainframe is independent of everything else.

• In a meeting discussing security aspects with a director of the company we’ve mentioned their mainframe. His reaction was:
  – “Mainframe? What mainframe?”
Myth #3 – Some Facts

Guess what? The mainframe is only a piece of the big picture!
Myth #3 – Leads to Risks

• The mainframe is not isolated!
  – Hackers can target the mainframe directly
  – Hackers can target other devices in the network to get to the mainframe
  – Beware of IoT and BYOD

• If you don’t know you have a mainframe then you have a BIG problem!!
Myth #4

“We don’t use Unix System Services”
Myth #4

- Again, and again we hear clients saying:
  - “We don’t use Unix System Services”
  - “We don’t need to know Unix System Services”
  - “We don’t need to deal with Unix System Services”
  - “I’m a mainframer! I only deal with MVS!”
Myth #4 – Some Facts

- Unix System Services is part of z/OS whether you like it or not

- You may not know Unix System Services but you need Unix System Services!
Myth #4 – Some Facts

- Unix System Services (USS) is used by:
  - TCP/IP
  - DB2
  - CICS
  - IMS
  - Websphere MQ
  - Oracle Web Server
  - ...

- There’s no point in ignoring Unix System Services!!
Myth #4 – Leads to Risks

- Ignoring USS doesn’t it make it go away

- If not properly dealt with USS can be a major security risk

- Hackers have a deep understanding of Unix. Where do you think they will start at when trying to hack the mainframe?
Myth #5
Outsourcing will solve all the problems
Myth #5

• Companies see outsourcing as a way to save money

• On the other hand outsourcers want to make money

• Can you see a problem here?
Myth #5 – Some Facts

• ‘Blinded’ with the idea of saving money most of the time a company:
  
  – Assumes everything will be covered by the outsource
  – Doesn’t read the documentation provided
  – Does not review their own documents (processes, procedures, etc)
  – Does not ask pertaining questions
  – Fails to assume responsibility (IT infrastructure has a direct impact in the business)
Myth #5 – Some Facts

• Most of the times the outsourcer will:
  
  – Provide technical and non-technical documentation constructed with a greater emphasis in legal terms
  
  – Technical documentation does not describe how things are done (processes and procedures)
  
  – Allocate the same technical resource to more than one client
  
  – Charge for every piece of work not covered by the agreement (remember the lack of processes?)
Myth #5 – Leads to Risks

• In order to make money the outsourcer will:

  - Save money on training
  - Save money on the technical team:
    - Technical resources shared amongst different clients
    - Reduce the number of technical individuals
    - Replace experienced members by cheaper inexperienced personnel
  - Only cover the minimum contracted services
  - Charge for any extra service including security
Myth #5 – Leads to Risks

• The company itself still wanting to save money:
  
  – Will only address and pay for what is really required – typically audit findings
  – Will not review processes (internal and from the outsourcer)
  – Will not review reports with the attention they deserve (e.g. monitoring, alerting, access)
  – Risk wise – “We have a mainframe. No one hacks the mainframe.”
Conclusion
Conclusion

- The mainframe is going nowhere!

- The mainframe can and has already been hacked!!

- The mainframe is just another platform of the company’s ecosystem.

- Unix System Services is part and in use by the mainframe. Get used to it!!

- Outsourcing can be helpful but beware of the pitfalls!
Questions
References & Sources

- Bernstein Research - https://www.bernsteinresearch.com
- The Economist - http://www.economist.com
- Bloomberg - http://www.bloomberg.com
- Microfocus - http://online.microfocus.com/
- My own blog – http://www.ruifeio.com/
Contact

Rui Miguel Feio
RSM Partners
ruif@rsmpartners.com
mobile: +44 (0) 7570 911459
www.rsmpartners.com