THINK LIKE A HACKER, ACT LIKE AN ENGINEER

System programmers can and should play a critical role in security and disaster planning and recovery, helping protect the mainframe from accidental and malicious acts in a complex and evolving cyberthreat landscape.

I was only 16 years old when I started working with mainframes. That was back in May 1980, a month that also saw the release of *The Empire Strikes Back* in the UK and USA. As I've written previously, in the intervening years, neither big iron nor the *Star Wars* universe have been very far away. In fact, both are proliferating today more than ever. It's a funny old world.

I was a system programmer for many years. I knew that world then and I still know it now. According to IBM®, "In a mainframe IT organization, the *system programmer* (or systems programmer) plays a central role." In practice, this means installing, customizing, and maintaining the operating system, and installing and upgrading products that run on the system.

IBM's definition then lists various tasks, including planning hardware and software system upgrades and changes in configuration, automating operations, capacity planning, integration testing, tuning, and so on.

So, what's missing?

What can system programmers *really* do, above and beyond that list? The missing part of the jigsaw puzzle is *security*.

The mainframe is probably the most securable platform on the planet, but it does not come secure

out of the box. And the mainframe has become mainstream. No longer existing in "splendid isolation," it's an interconnected system that, for many enterprises, is the hub for all major business applications. To the bad actors, internal or external, it's simply another server to be targeted. And like any part of modern technology or business, accidents can happen, compromising this critical platform.

The cyberthreat is real and we all have a part to play in keeping the mainframe secure. The world keeps changing and the goal posts keep shifting. When IBM decided to put containers on a mainframe, it perhaps didn't foresee that skilled security professionals would rapidly demonstrate the reality of escaping a container on a mainframe, breaking the IBM z/OS® Container Extensions (zCX) Docker environment in both directions.

The cybercriminals just need a way in. Spear phishing attacks are only one of many, many methods, meaning a data breach, ransomware, or malware attack may be just around the corner. So, given that backdrop, what's readily available to help system programmers with security, governance, and compliance issues?

From a hardware perspective, manufacturers like IBM and Dell EMC are working to combat cyberthreats. Hardware requirements need to focus on a number of capabilities, such as surgical and catastrophic recovery, forensic analysis, and data validation. IBM Z® Cyber Vault has reduced time-to-recovery from days to minutes. Similarly, Dell EMC Cyber Data Protection for mainframe data helps strengthen against attacks while reducing recovery time.

There are also software solutions available, including BMC AMI Datastream for real-time mainframe threat detection, which delivers mainframe access data to a distributed SIEM (security information and event management) system in real time, for a unified, multi-platform view of enterprise security events in a single console. Other examples include IBM solutions for security administration and reporting, MainTegrity solutions for file integrity monitoring (FIM) and KRI solutions for software vulnerability scanning.

Spanning hardware, software, planning and processes, you can also access external security consulting expertise, professional services, and managed services from a range of third parties (including BMC) - to better support your internal efforts. These providers can deliver everything from pen testing and security audits to staff augmentation and fully managed security solutions.

My basic point is that, in a world where hackers see the mainframe as just another computer, system programmers have to adapt and change, updating our thinking. We have to use all of the weapons at our disposal: assess the threats, weigh-up our options, then deploy the right solutions and approaches.

Today's landscape isn't only about the authorized program facility (APF) to identify system or user programs that may use sensitive functions, or about security privileges (Special, Operations, NON-CNCL, etc.) We also need to consider IBM z/OS® UNIX System Services (z/OS UNIX, aka USS), FTP with the mainframe, the Secure Shell (SSH) protocol on the mainframe, and the list goes on. What about containers on IBM Z® and Z for Linux®?

System programmers have to be more involved in security matters, taking ownership where it makes sense. In short, to prepare for the cybersecurity threats of today and tomorrow, we must *think like a hacker but act like an engineer*.

Note: this blog is a shortened version of a BMC white paper.