MAINFRAME SECURITY: DEBUNKING MYTHS AND FACING TRUTHS

Today's mainframe is well positioned to support ever-evolving digital business environments, however one important piece of the puzzle can sometimes be overlooked—security. IT leaders must confront certain myths about mainframe security head on to develop the proper security posture for today's digital transformation. Can you answer the following questions confidently? How secure is my mainframe? Would you know if you had security vulnerabilities? Would we pass a compliance audit?

The idea that mainframes are impenetrable is based largely on myth and urban lore. In fact, mainframes can potentially make attractive prey for hackers and those with malicious intent because:

- Mainframes have IP addresses and are exposed to classic cyber threats
- Enterprises often are not aware they have been hacked because they are not receiving real-time notifications
- Hackers are very good at covering their tracks and their presence can go undetected for months
- Stolen passwords provide easy access to your most business-critical data
- Defending against hackers injecting malware is extremely difficult

There are many myths about mainframe security, but the truth is, solid, proven methodologies exist to secure your mainframe. I hope the following helps you to separate fact from

fiction

Myths - Mainframes Are Not Hackable and Are Not at Risk

Mainframes sometimes fall off enterprise security radar and IT security professionals think they are not at serious risk because of the inherent security built into the systems, but that is a false belief.

IT complexity adds to the risk of security gaps. The fact is we deal with multiple IT worlds and multi-faceted environments with vastly different operating systems and programs. They speak different languages, and fewer and fewer professionals are fluent in all of them. Since it takes approximately 200 days to detect a breach, mainframe professionals must be even more vigilant, even as it gets harder to do so.

Data breach. Two chilling words no security professional wants to ever hear. Unfortunately, mainframe data might be among the most vulnerable, because of the sensitive and attractive nature of the data. Think of stock trades in finance or money transfers in manufacturing or government. The money trails and IP addresses lead to mainframes, so enterprise security postures must include that platform. The odds of a future data breach have increased, and average total costs have grown to nearly $4 million per lost or stolen record. It is not only hard to recover from financial losses like that, it can be excruciatingly difficult to recover from a tarnished brand.

The Truth – The Mainframe is the Most Securable Platform

It is more important now than ever to fortify the critical business data that resides on your mainframe. With the right tools, IT security professionals can capture operational data and build useful 360-degree mainframe views that alert in real-time. You can identify and correct for risky circumstances and prove compliance for both national and international security regulations and compliance mandates. Look for out-of-the-box capabilities and audit scorecards that help you meet requirements set forth by PCI DSS, HIPAA, GDPR and other standards.

Companies want and need to secure their data, but achieving that goal can be onerous for stretched IT teams. Fortunately, technology and services have risen to the challenge. For the mainframe to remain viable, it must be simple and straightforward for IT to maintain and enhance innovative technology, that includes automation, correlation, and security. At BMC, we have taken important steps to help our mainframe clients bolster their security posture with our AMI for Security offerings and our built-in industry-leading mainframe SIEM technology.

Now that you know more about distracting myths and correlating truths, you have the knowledge to debunk mainframe security myths and embrace the truths with a mature security posture. It is imperative for you to take the right steps and prepare for your enterprise-wide security. BMC is here to help. Discover more about BMC Automated Mainframe Intelligence (AMI) here.