THE SILENT SECURITY THREAT TO FINANCIAL SERVICES COMPANIES



Some of the most security-minded people I've met are CIOs, CISOs, or Security Operations people in the Financial Services industry. Some even border on paranoia as the high-profile breaches and bad press banks receive drive their CEOs to put more pressure on their Security Operations Centers to report and demonstrate security and compliance.

The sad reality is that there is a danger lurking in the back corners of many of these companies that is decades in the making – the mainframe. The supposedly inherently secure box that processes millions of bank transfers, ATM transactions, and payments every hour can be hacked in a few minutes with open-source tools. With just a few scripts an attacker can escalate their privileges to super user status and a motivated person will have complete control of the machine and can do pretty much whatever they want. While many think accessing the mainframe is limited, the reality is any threat actor inside the network can make their way to the mainframe and the mainframe is accessed remotely in financial transactions all the time. It happens at your local bank every day.

Hopefully by now you're scratching your head and asking, "Okay, so if I believe what you're saying, what is the answer? How do I secure the mainframe like all my other endpoints?" The answer is visibility, integration, and mainframe hardening. Real-time monitoring that is integrated with your existing SIEM allows you to set alerts when scenarios like those above happen. Someone's privileges mysteriously changed? Someone suddenly accessed data they shouldn't on the mainframe? Now you'll know the minute it happens.

What if you'd rather lock down your mainframe before that happens? This is where mainframe hardening comes into play. The mainframe can (and should) be penetration-tested (pentested) like the rest of your environment. The results will tell you exactly where you are vulnerable and how to change your policies to harden the mainframe from those vulnerabilities. Don't have the expertise in-house to do that? Consider leveraging a professional or managed service provider with the expertise to perform the pentest for you. But be aware that not all auditing and pentesting resources are the same. Some lack expertise specific to the risks Financial Services firms are facing while others are concerned only with helping you check a compliance box and not uncovering your risks. It's a good idea to learn more about the types of customers they service and how extensive their testing is.

If you want to learn more about the mainframe security risks facing Financial Services organizations, take a look at this infographic "Why Mainframe Security Matters for Financial Services Firms"

Related reading

- Modern Infrastructure Requires a Connected View
- FinTech: Redefining Possibility by Connecting Talent and Tech
- Does a More Resilient You Mean a More Resilient Customer?
- Stay Ahead of Cyber Threats in Financial Services
- Can Your Biggest Disruption Drive Your Greatest Innovation?