HOW TO START THE MAINFRAME SECURITY HARDENING PROCESS



What is security hardening?

Security hardening is the business process of reducing vulnerability to an internal or external attack by examining all vectors. This should be a continuous process that falls under the scope of attack surface management (ASM), but organizations have neglected the process on the mainframe for so long that they're in need of a starting point.

Where to start?

Let's say you have just started your new job as the mainframe security team lead and have been informed there is an audit coming up. Your first question is probably, "Could I see the results of the last pentest (a.k.a. penetration test), please?" All too often the answer is, "What pentest? The mainframe is out of scope."

Let's clarify one thing—the mainframe is not out of scope and should never be deemed as such. The organization's most valuable data is stored on the mainframe and security of the platform should be a top-tier priority.

To kick off your new security hardening program, you'll first need to assess your landscape and understand the current state of the system. This means having a third party perform a full-detail

security assessment, which is the quickest way to understand the state of your system and includes the operating system, network, Unix system services (USS), external security manager (ESM), and all subsystems. While a pentest will confirm whether it's possible to breach your system, an assessment is more valuable, providing an industry-scored vulnerability rating that can be indexed to help guide your priorities as you begin hardening the mainframe.

It's important to note that the assessment should be performed by an external organization. Conducted with automated tooling and a bigger view of the ecosystem, it will be far more in-depth than an internally performed review.

Next steps

Now that you have your assessment, it's time to analyze the report and work with the organization that performed the assessment to help build a remediation plan:

- At the top of your list should be any easily exploitable high-impact assets, such as un-protected authorized program facility (APF) libraries. Yes, there is a risk in making changes, however the threat here is more likely to be human and, based on job role, you can quickly identify who should have access to these datasets. If the risk team is blocking changes, another quick win is to use a privileged access manager and put the access behind a manager-approved auditable change record.
- Next, organize all other remediation tasks into a continuous service improvement plan, which is a rolling process. If ten years' worth of manpower is required to carry out this work, your organization needs to adopt a pragmatic approach. This may mean expanding the team, but at the bare minimum, every vulnerability should be logged in a risk register and shared, with sign-off from the compliance team.
- Now it's time to breathe. The dust has settled, you know where the vulnerabilities are and have an approved plan to remediate them. Sadly, for any security professional, the bad actors are also aware of this, and the mainframe is still vulnerable to a never-ending list of complex attack vectors.

An agile and ASM approach to mainframe security that ensures the mainframe adheres to the National Institute of Standards and Technology (NIST) cybersecurity framework is essential to addressing the continuously evolving attack landscape. While this approach will include software solutions, you can still start your security hardening immediately with a rolling security assessment that will validate remediation and a pentest that will confirm it.

In Summary

Mainframes need to be secure—there is no debate. The good news is that, with a focused approach and organizational investment, there is no reason this can't be achieved. Once the storm has calmed and you've begun the hardening process, it's important to start thinking more laterally, and with 95% of breaches being human error, you should never underestimate in the value of education.

It may seem difficult to find a starting point in the process, but by following the above steps, you can begin a continuous process of hardening the mainframe and protecting your organization from costly and damaging breaches.