WHY PRIVILEGED ACCESS MANAGEMENT IS A MUST-HAVE FOR MAINFRAME SECURITY



The mainframe has been around a while. Mainframe security came a little later, but to put it into context, IBM® RACF® (Resource Access Control Facility) was introduced in 1976. What else happened in 1976? Jimmy Carter won the U.S. presidential election, Concorde took its first commercial flight, and VHS video tapes were launched to compete against Sony's Betamax. So, what does RACF, which pre-dates most high-end tech companies, have to do with a security risk? The short answer is potential technical debt. Technical debt—accrued by delaying necessary work in the name of expediency—is part of working in IT, but when it comes to security, it can lead to vulnerabilities. Without due process, housekeeping, and continual service improvement there is the potential for decades worth of mismanagement in privileged access being given to users.

What is privileged access management (PAM) and why should it be part of your security strategy?

PAM is also termed "elevated access" and "breakglass," among other names. PAM does exactly what it says—it manages privileged access. Applying PAM to your enterprise means removing all permanent access to anything considered privileged and instead implementing a process around granting privileged access to users on a temporary basis. This can be as simple as an email approval from a manager and an administrator manually giving and revoking access; users requesting access through a web portal which triggers a managerial approval request; or having your ITSM call a piece

of software that grants and removes access. PAM should be part of your security strategy because it implements a least-privileged approach and works toward zero trust, resulting in fewer accidental changes due to permanent privileged access being removed and providing an audited approval trail of privileged access usage.

Defining privileged access in your organization

The National Institute of Standards and Technology (NIST) defines a privileged user as "A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform." Would it therefore be fair to assume that any access that is classified as a security-relevant function should be controlled via PAM and the job is done? Maybe, but mainframe controls are very granular, so we can therefore go a bit further.

First, each role needs to be approached differently. For example, your database administrator cannot have the same criteria as the security engineer. A good rule of thumb is that any access that can risk the integrity of business data or any access that can risk business operational continuity should be considered privileged. One thing to keep in mind when segregating privileged and non-privileged access is that a lot of breaches and outages happen entirely accidentally by non-malicious employees who simply have privileged access, which makes mistakes catastrophic.

Implementation

There are two notable parts to implementing PAM in the enterprise. One is very obviously the technical, but not to be overlooked is the political. You are going to be changing the way potentially thousands of people work and may have done so for decades. There can be pushback around the idea of lack of trust and productivity. Ultimately, the message is simple: Follow best practices and PAM should not be a hindrance. As for the technical part, the roles identified with a lot of privileged access make the most sense to bring under PAM first. The organization must decide how they will action PAM requests, whether manually or through a software-based solution. Before any access is moved under PAM, it is imperative that comprehensive training is done to roll out on the sandpit system and pre-production it before going live.

Periodic reviews and access reduction

Once PAM has been implemented and is live for a suitable period, it is time to begin regular reviews. If anyone has not elevated their ID using PAM for a period deemed appropriate by the site, then they should no longer have the right to request it as it is evidently not required by them. The access given when the user selects privileged access should also be reviewed—if the sysprog's privileged group is not using certain access over a set period, then it can be deemed not used and removed. Caution should be exercised here, as there can be caveats.

Joiners, movers, and leavers

Using privileged access is part of many roles on the mainframe, and one often-overlooked aspect is implementing it into the joiners, movers, and leavers (JML) process of the organization. If a role requires privileged access, anything that is required in order to request it should be actioned at the point of user creation and again when the user changes roles or leaves an organization.

Summary

To conclude, PAM should be part of your least-privileged strategy while you constantly work towards zero trust. As access becomes much harder to abuse, it is a very quick and effective way to flush out malicious behavior because PAM can help identify it by quickly checking whether the events are being actioned while elevated and cross-refencing the approval to understand the work being carried out. A PAM solution can also help keep a system compliant while simplifying the audit process around access controls.