Presented by HIROC

privileged access management is a critical element of internal cyber security

The development of phishing scams and hackers using social engineering prove that it's essential we stay at the forefront of cyber security to keep our clients protected.

Continuing our series on cyber security, Cyber Underwriting Consultant Tim Hodgkins shares his thoughts on Privileged Access Management (PAM) and how it can be used to ensure businesses are protected from vulnerabilities that exist in the broader risk environment. His role in providing technical risk management advice and detailed insight into emerging cyber threats means he's well placed to share his thoughts on this vital component of cyber security.

What is privileged access?

Privileged access is classified differently across various organisations and government entities; however, NIST (National Institute of Standards and Technology) classifies it as:

A user that is authorised (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorised to perform.

From a threat actors' perspective, these are the user accounts that they will want to compromise the most. As a result of this, privileged access management tools exist.

What is privileged access management?

As the name suggests, it's the management of privileged accounts. If these accounts are misused, they can damage the security and integrity of an IT environment and the organisation. As a result, they need to be carefully managed.

To draw parallels with keeping valuable items safe in your home, any things that hold significant value, sentimental, financial, etc. may require additional protection, such as locking them away in a drawer or putting them in a safe. This would protect them from both internal threats such as pets, young children, leaking pipes, and external ones such as burglars and unwanted visitors.

The same principle applies to privileged accounts. They need to have additional protections on them to ensure only appropriate team members can log in and access them. Different forms of protection can include:

- Restricting access to the passwords/accounts to a subset of users
- Additional authentication steps based on something you are and something you have
- Password rotation after a credential is used
- Direct connection to the asset that is being accessed (instead of providing a user with a password)
- Logging and monitoring who is accessing the credential and what they are doing with it

continued

What are the benefits?

With each of the five features above, there are security benefits:

Feature	Security benefit
Restricting access	The fewer users that can access privileged accounts, the better. This reduces the attack surface.
Additional authentication	Additional authentication such as MFA combines something you have with something you are. For example, biometric data like a fingerprint is an additional layer of protection. This is virtually impossible for an external attacker to physically get their hands on.
Password rotation	Passwords can be automatically rotated after being checked back in by the user. This ensures that they cannot be reused by a user or attacker later. Another benefit is that if a password is compromised, this will no longer be valid on the target system.
Direct connection	When this feature is used, users can connect directly to an asset. This eradicates the need for a password as it is managed by the PAM tool.
Logging and monitoring	Advanced logging and monitoring give better visibility of what users are using their privileged credentials for. These can be configured to be sent to the Security Operations Centre.

What are the challenges?

Toolsets

There are several vendors in the PAM space, and choosing the correct tool for your organisation for the present and future is challenging. Different toolsets will be suited to different architectures and organisation sizes.

Scoping

The definition of what an organisation means by privileged is a common issue. This could be any user with the right privileges or just those with the ability to disrupt the organisation. Scoping of the accounts themselves should be driven by a business impact analysis. Which assets or services are the most critical for the organisation?

BAU impact

Where PAM tools have not been used previously and users have a high amount of standing access, there is often a cultural issue of changing how users carry out BAU tasks. Users often see tools as a way of preventing them from doing their jobs effectively.

How does a lack of PAM tooling leave an organisation exposed?

There are countless examples where careless storage/assignment of privileged credentials/ entitlements have left companies vulnerable.
They fall into two main categories:

1. Users have too much access to start with (access that far exceeds their day-to-day responsibilities)
2. Privileged credentials are stored in an insecure manner across the environment.

In the first instance, once an account with privileged access has been compromised, limited preventative controls can be relied upon to mitigate the risk of an attacker abusing this account. The attacker may have the ability to circumvent and turn off security controls such as EDR software and logging and monitoring tools. These types of attacks have been seen in the market, and once an attacker has this access, they can cause significant damage to the IT estate.

In the second case, the lack of a PAM tool or a process to manage privileged credentials can result in privileged credentials being stored insecurely, making them easily accessible to external attackers and insider threats. Insecure storage can come in various forms, some as basic as having credentials copied into a spreadsheet and stored on a company-wide network drive. This can result in an attacker escalating their privileges by using a standard account as an entry point.

According to cyber security experts Gartner, "…those who eliminate standing privileges will experience 80% fewer privileged breaches than those that don't."

This makes it clear that having appropriate PAM protocols in place is essential for the ongoing cyber security of a business.

Prepared for the road ahead

We hope this article has helped show you how PAM is an essential element of your client's cyber security. If you want to learn more about how Brit can help, read our cyber security page.