A Spotlight On... Privileged Access

Why be concerned about privileged access?

One of the most significant risks in cyber security is the misuse of **privileged user** accounts.

Some research suggests at least 80% of data breaches are linked to compromised privileged accounts. And the risk grows with each new application that organisations use.

Due to this high level of risk, both regulators and industry standards (NIST, SOX, PCI DSS) focus on policing access management.

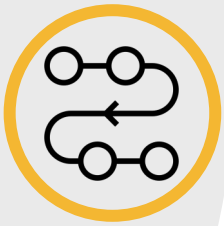
Why is privileged access so dangerous?

By their nature, these accounts hold greater privileges than for a standard user, e.g. IT administrator roles.

These accounts can access information far more widely, and also change systems without needing authorisation. This makes them a target for individuals looking to exploit an organisation and its data. Protecting such accounts is key to securing information and protecting brand reputation.

How can you manage the risk?

You need to understand what rights any privileged accounts have and their associated risks. Appropriate steps can be then be taken to reduce the security threat:



Step 1: Identify and onboard privileged accounts to a Privileged Access Management (PAM) solution.

- Enables organisations to understand their full privileged access usage.
- Ensures activity using privileged access is monitored.

Step 2: Limit the use of privileged accounts to those with a specific requirement.

- Restricts privileged access to the right people for a limited, authorised time period.
- Implements a process that ensures different levels of privilege go through the right approvals.

Step 3: Recertify access to privileged accounts.

- Ensures people have the correct access levels for their job roles.
- Identifies privileged access that should be removed.

Step 4: Remove redundant or inappropriate privileged accounts. Accept risks where systems block removal.

- Prevents unauthorised access to key information assets.
- Prevents fraudulent activity by managing segregation of duties.

How can i-confidential help?

Our PAM and recertification specialists help clients to protect their critical assets and applications, meet audit and compliance requirements, and prevent data breaches and potential service disruptions.

We have helped several leading organisations successfully address this issue. Some key activities include:

- Providing a structured approach to addressing PAM's complexity and risk.
- Identifying and onboarding unique user accounts into a PAM solution.
- Operating a recertification process and planning the removal of inappropriate user accounts.

For more information about how we can help your business, please contact us

i-confidential
Building Trust, Reducing Risk

www.i-confidential.com
info@i-confidential.com
0131 445 1458