XM Cyber

7 Mistakes to Avoid With Identity and Access Security

Identity and access security is a complex landscape that is a vital part of every organization's security program. Here are seven common pitfalls that XM Cyber can help you to avoid.

1 Treating Identity As a Silo

Organizations often manage identities separately from vulnerabilities and asset security posture management. They may fix a weak password but not see that the user has access to an unpatched, high-value database or could allow an attacker to move from on-prem to cloud.

2 Prioritizing by Severity Instead of Impact

It's natural to assume that an issue flagged as high severity is a priority - but can it actually be exploited? Does it lead to business critical assets? It might not be the Tier 1 Admin account with an old password that threat actors can exploit.

3 Relying on Point-in-Time Audits

With attackers moving faster than ever before thanks to AI, relying on static checks can be a higher risk approach. Ideally, teams should continuously assess access permission levels and identity security posture.

4 Losing Track of What Is Where

Identity professionals have a lot to keep track of, which means sometimes things get forgotten. Being able to see shadow accounts and identities and assess the risk they could pose to critical assets is a key consideration.

5 Not Cracking Down On Credentials

Threat actors love to target credentials and identities in order to breach and move laterally across an organization's environment. Understanding where credentials are exposed, cached and reused is key.

6 Setting and Forgetting Critical Controls

Initial deployment went well, permissions were assigned correctly and PAM tool controls configured. But two months later is everything performing as expected? Is there any configuration drift or unexpected behavior? Are elevated permissions actually being used?

7 Neglecting Non-Human Identities (NHI)

Most organizations have significant quantities of machine and now AI identities. Typically they have higher privileges than most human users but often are subject to less scrutiny. They should be assessed to the same high standard of security.

Learn how XM Cyber can help you proactively address these issues at xmcyber.com

XM Cyber