TIPS TO MANAGE ACCESS CONTROL & LEAST PRIVILEGE

A strong access control and least privilege strategy can help you reduce costs, improve security and reduce the risk of data exploitation. Here, we share our top tips for managing access control and exercising least privilege.

IMPLEMENT 2FA

Mandating two-factor authentication keeps attackers out, even when they've stolen passwords.

EXERCISE LEAST PRIVILEGE

Providing users with the bare minimum of access and privilege necessary limits the damage if compromised.

REMOVE USERS FROM THE LOCAL ADMINISTRATORS GROUP

Prevent privilege escalation attempts. Automatically reduces Microsoft vulnerability exploits by 80%.

AVOID CREDENTIAL OVERLAP ACROSS SYSTEMS

Prevent lateral movement opportunities if valid credentials are obtained.

DISABLE CREDENTIAL CACHING

Prevent storage of credentials - anytime credentials are stored provides attackers with an opportunity to steal them.

APPLY ACCOUNT LOCKOUT POLICIES AND/OR PROGRESSIVE DELAYS FOR LOGINS

Prevents brute force attempts.

ENABLE ADMIN APPROVAL MODE

Enforces UAC for the built-in Administrator, prevents privilege escalation and lateral movement attempts.

DISABLE ANONYMOUS LOGIN

Prevents ability to use File Transfer Protocol (FTP) and further spread an attack to other users on the network.

USE HIGHEST UAC ENFORCEMENT LEVEL

Enforcing UAC setting to "always notify," will trigger prompts whenever a program attempts to make changes to Windows settings or the machine.

AVOID STAYING LOGGED-IN ON REMOTE SYSTEMS

Prevent attackers from hijacking admin access and privileges.

For information or advice for securing your inbox, get in touch with us at contact@ka2.io