CIRT.GY Guyana National Computer Incident Response Team

T2025_10 Use Group-Based NT Logins to Manage Desktop Privileges Securely (April 7th, 2025)

To maintain strong security and streamline user access, network administrators should utilize Active Directory (AD) groups to manage NT logins and desktop privileges. Instead of assigning access rights individually, assign users to security groups that define what resources or privileges they are entitled to. This approach ensures consistent permission management, reduces human error, and simplifies audits. For example, only authorized users in a specific ‘Admin Tools Access’ group should have access to system-level tools or sensitive applications on workstations. Regularly review group memberships to ensure users only have the access necessary for their roles following the principle of least privilege. Automating access provisioning based on group roles also enhances security and operational efficiency.

References

- Dansimp. (2025, January 15). Active Directory security groups. Retrieved from Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups
- Patton, B. (2025, January 16). 8 ways to secure your Active Directory environment. Retrieved from The Quest Blog. https://blog.quest.com/8-ways-to-secure-your-active-directory-environment/