Active Directory Security

An Executive Summary for the U.S. Government

From the White House to the U.S. Capitol, at the foundation of cyber security and privileged access of all branches and departments of the U.S. Government lie their Active Directory deployments.

These Active Directory deployments are the foundation of cyber security and privileged access because the entirety of their building blocks of cyber security i.e. all user accounts and passwords, and all computers and security groups are stored, managed and secured inside Active Directory.

Should a department's or agency's foundational Active Directory be compromised, the foundation and bedrock of the organization's cyber security would have been compromised, and the entirety of all IT resources of that department or agency could be exposed to the risk of compromise.

In particular, three specific high-value threats, notably, the compromise of even just one privileged user account, the instantaneous unleashing of ransomware on thousands of computers via group policy pushed out from Active Directory, and the instant compromise of everyone's credentials via the use of the Mimikatz DCSync hacking tool, merit the highest concern and immediate attention.

In summary, the numerous Active Directory deployments of the U.S. Government are likely their most important, valuable and strategic assets, which is why their security is absolutely paramount, and must be amongst the highest executive, organizational and cyber security priority at all times.

Active Directory Security

Active Directory Security is Paramount

As the foundation of an organization's cyber security, Active Directory is an extremely high-value organizational asset and its adequate protection and security are paramount to business today.

Active Directory is the very foundation of IT and cyber security and the heart of privileged access in every organization whose IT infrastructure is powered by Microsoft's Windows Server platform -

1. In Windows Server based networks, all the three A's of cyber security i.e. **A**uthentication, **A**uthorization and **A**uditing are completely integrated with and rely on Active Directory.

2. All the building blocks of cyber security i.e. all organizational user accounts (and passwords,) and computers (accounts,) and all security groups used to provision access to the entirety of the organization's IT resources are all stored, managed and protected in Active Directory.

3. The security of all domain-joined computers can be easily and instantly controlled from Active Directory via Group Policy. (An unfortunate ramification is that today anyone with sufficient privileged access in Active Directory could use it to unleash ransomware).

4. In addition, numerous mission-critical IT services and applications such as DNS, Cloud-integration, email (Exchange), remote access etc. all rely on Active Directory.

5. The *Keys to the Kingdom* i.e. the most powerful privileged access, reside in Active Directory.

Consequently, should an organization's foundational Active Directory be compromised, the very foundation and bedrock of the organization's cyber security would have been compromised, and the security of the entirety of an organization's IT resources could be instantly jeopardized.

Active Directory is thus an organization's single most important and valuable asset, and as a result its security is absolutely paramount and must be the highest organizational priority at all times.

Active Directory Security

Recommended Reading for the U.S. Government

Active Directory is an organization's single most important and valuable asset, and thus its security is absolutely paramount and must undoubtedly be the highest organizational priority at all times.

The following 10 helpful and valuable pointers are intended to help all federal CISOs, IT personnel and cyber security analysts gain a deeper understanding of Active Directory security -

1. What is Active Directory ?
2. A Matter of National Security – Trillion Dollar Cyber Security Insight for President Trump
3. Active Directory Security is Paramount – Cyber Security 101 for the C-Suite
4. The Keys to the Kingdom – Privileged Access in Active Directory
5. The Keys to Privileged Access in Active Directory – Active Directory Effective Permissions
6. The #1 Threat to Active Directory Deployments – Active Directory Privilege Escalation
7. How should organizations Correctly Audit Privileged Access in Active Directory ?
8. How should organizations secure Active Directory ? – An Active Directory Security Checklist
9. A Real-world Scenario – A Massive Breach at a Company while it was Considering the Cloud
10. Essential reading for Citizens, CISOs, IT Managers, IT Admins, IT Auditors and Pen-Testers

In conclusion, today every organization is only as cyber secure as its foundational Active Directory.