Prepared for

semperis

Unknown Vulnerabilities Become the Top Active Directory Security Posture Concerns

January 2022 EMA White Paper
By Paula Musich

EMA™
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Key Takeaways

Most concerning risks

- Native Microsoft security flaws
- Social engineering attacks, such as phishing
- Attackers moving between AD on-premises and cloud

Top AD recovery concerns

- Not having a post-cyber-attack recovery plan
- The inability to recover quickly
- Not having a defined responsibility for AD recovery

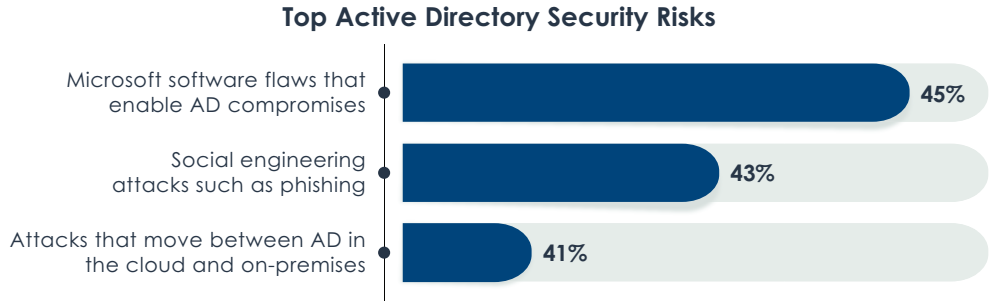
Responding to the SolarWinds attack

- 45% of organizations increased collaboration between operational and security teams
- 44% increased focus on closing AD security gaps, detecting attacks, and ensuring malware-free backups
- 37% added skilled practitioners to address AD security weaknesses

Introduction

As any security practitioner will tell you, trying to close exposures in Microsoft's Active Directory (AD) is like trying to fill in the holes of a constantly morphing block of Swiss cheese. Because Active Directory's configuration is in a continual state of flux, bad actors perpetually find new ways to exploit vulnerabilities to achieve their illicit aims. It's no wonder that the top Active Directory security posture concern for most IT security practitioners is unknown AD vulnerabilities, followed closely by known but unaddressed AD vulnerabilities, according to new research conducted by Enterprise Management Associates on behalf of Semperis.

Practitioners are confronted by a wide range of risks when it comes to Active Directory security. Topping the list of risks they see as most concerning are security flaws in Microsoft software, such as the Windows Print Spooler service and Exchange Server vulnerabilities, that open the door to compromises of Active Directory, the world's most widely used directory system. This is no surprise, given the prevalence of AD as an attack vector, the challenges with staying up to date with current security patches, and the amount of coverage the issue of AD security has been given over the last several months. The second most cited risk—social engineering attacks, such as phishing—is also common sense, given that people are usually the weakest link in the security chain. Phishing remains a highly successful means of entry, and the ease with which attackers can gain enough information to mount credible attacks is well documented. The third most cited risk—attackers being able to move between Active Directory in the cloud and on-premises—is getting much more attention and is becoming top of mind because this tactic was implicated in both the high-profile SolarWinds and Colonial Pipeline attacks.



Ransomware that exploits vulnerabilities in Active Directory is an increasing threat to organizations, especially with the development of the LockBit 2.0 ransomware as a service exploit, which can now automatically distribute itself across a domain when executed on a domain controller. The impact of such attacks (if successful) is especially damaging to organizations. When asked what the impact would be from an attack that took down their organization's domain controllers, the largest percentage of respondents at 37% said the impact would be significant, resulting in business disruption of more than one day. Twenty-one percent said it would be severe, with more than 10 days of business disruption. The majority of respondents said the impact of an attack that wiped out the domain controllers would range from significant to catastrophic.

Balancing Active Directory Security in the Cloud and On-Premises

As organizations continue to move a greater percentage of their workloads and applications to the cloud, additional threats and challenges confront security teams. Concerns about the security of cloud environments has not stopped the transition to the cloud, and it will only accelerate. Today, just under half of EMA study participants said the majority of their organization's mix of assets and services were mostly on-premises, but they had some cloud-based services, such as Microsoft 365 (formerly Office 365). They anticipate that would shift to 45%, with more than half of those assets and services in the cloud, by 2025. This finding suggests that the hybrid mode of computing services will be with us for some time. Organizations will be challenged to adequately secure those hybrid environments.

The skill level those internal security teams bring to managing and securing those hybrid environments does not quite match the ratings they give themselves in securing assets, either on-premises or exclusively in the cloud. While about 47% describe their ability to manage and secure Active Directory on-premises and in the cloud (Azure AD) as very competent, only 37% gave that rating for managing and securing hybrid deployments. Thirty-one percent rated that hybrid skill level as merely adequate. Should a cyber-attack take down their Azure AD service, 55% of respondents expressed a medium level of confidence in their organization's ability to restore its cloud-based resources, such as users, groups, roles, and policies. Curiously, when it comes to recovering Active Directory after a cyber-attack, respondents (for the most part) indicated the same level of concern over which aspects of the recovery they worried about most between on-premises deployments and Azure Active Directory in the cloud. On a five-point scale, where five was extremely concerned and one not at all concerned, respondents' top concerns for recovering both deployment types were not having a post-cyber-attack recovery plan, an inability to recover quickly, and not having a defined responsibility for AD recovery, all at between 3.76 and 3.71.

Less than 40% feel very competent managing and securing hybrid AD deployments.

Addressing Active Directory Security Concerns

So, what are organizations doing to address their concerns about recovering from an attack? For organizations that have implemented an Active Directory cyber disaster recovery plan, testing that process is key.

How organizations respond to new types of attacks and risks to Active Directory is an important element in putting such recovery plans in place. One of the newer high-profile attack types, the SolarWinds attack, raised awareness of the dominant directory system as an attack vector. In reacting to that new threat, 45% of respondent organizations have increased the level of collaboration between their operational and security teams; 44% have increased their teams' focus on closing Active Directory security gaps, detecting attacks, and ensuring malware-free backups; and 37% added skilled practitioners to address Active Directory security weaknesses.

Although it's encouraging to see these evolving security practices and increased focus on securing Active Directory, there is still much work to be done. Forty-one percent of EMA respondents said that just now, securing Active Directory is starting to be included in security strategy discussions, and 3% said their organizations view Active Directory as an operational resource and manage it as such. Those laggards will have an uphill climb in catching up to the 56% of respondent organizations that make Active Directory core to their overall security strategy.

About Semperis

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 50 million identities from cyber-attacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyber-attacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4151.011022