Proactive AD Security: Leveraging Risk Assessment and Attack Path Analysis

Active Directory (AD) is an important part of many firms' IT infrastructure, making it a popular target for cyber attackers. The rise of targeted attacks has resulted in increasingly advanced approaches for compromising AD. These attacks target vulnerable points in AD security, which can seriously disrupt operations. To mitigate these threats, businesses must take a holistic approach that includes active directory risk assessment and attack path analysis.

The Importance of Active Directory Risk Assessment

Assessing your AD environment is crucial for maintaining robust security. Here's why:

The Power of Effective AD Risk Assessment

Active Directory risk assessment is a proactive method that identifies vulnerabilities before they can be exploited by attackers. This assessment is essential for determining and enhancing an organization's security posture. Organizations can strengthen their defenses against potential threats by conducting a rigorous analysis of AD for potential threats.

Here are a few significant points of a good AD risk assessment:

- **Early detection of vulnerabilities** allows for early correction, lowering the chance of successful attacks.
- **Comprehensive security posture analysis** provides a thorough overview of the present security situation, indicating areas for improvement.
- By identifying the most significant AD vulnerabilities, businesses can **prioritize their security efforts and resources**.
- **Regular risk assessments** guarantee that the organization follows industry norms and standards, which frequently necessitate periodic security audits.
- Understanding vulnerabilities and potential attack vectors enables **faster and more effective incident response and recovery methods**.
- Regular assessments **create a feedback loop for continual security** improvement, allowing you to respond to new threats and changing circumstances.
- Clear risk assessment reports assist stakeholders, including management and board members, to **understand the security posture and make educated decisions**.

Leveraging AD Risk Assessment to Secure Privileged Accounts

Privileged accounts are often the primary targets of attackers due to the extensive access they provide. AD risk assessment assists in identifying and securing these accounts, ensuring they are safeguarded from potential threats. This includes auditing account privileges, ensuring proper usage, and enforcing tight security standards to reduce the risks associated with these accounts. Here are some additional points about safeguarding privileged accounts:

- **Conduct a thorough audit** to identify all privileged accounts and keep an updated inventory. This includes accounts with administrative privileges or access to sensitive systems and data.
- **Limit privileged accounts' access rights** to the bare minimum required for their jobs. This limits the possible damage if an account is compromised.

- **Make MFA mandatory** for all privileged accounts to add an extra layer of security.
- **Periodically examine the access rights** of privileged accounts to ensure they are still needed and cancel those that are no longer required.
- **Use tools like Fidelis Endpoint® to secure and monitor sessions** started by privileged accounts, ensuring that they are not hijacked or misused.
- **Privileged Access Management (PAM) solutions** are used to regulate and manage access to privileged accounts while also offering extra security measures such as session recording and credential vaulting.
- Provide **frequent training to users with privileged access** to ensure they understand security best practices.

For further in-depth insights on how you can best maintain the hygiene of your Active Directory, download our whitepaper.

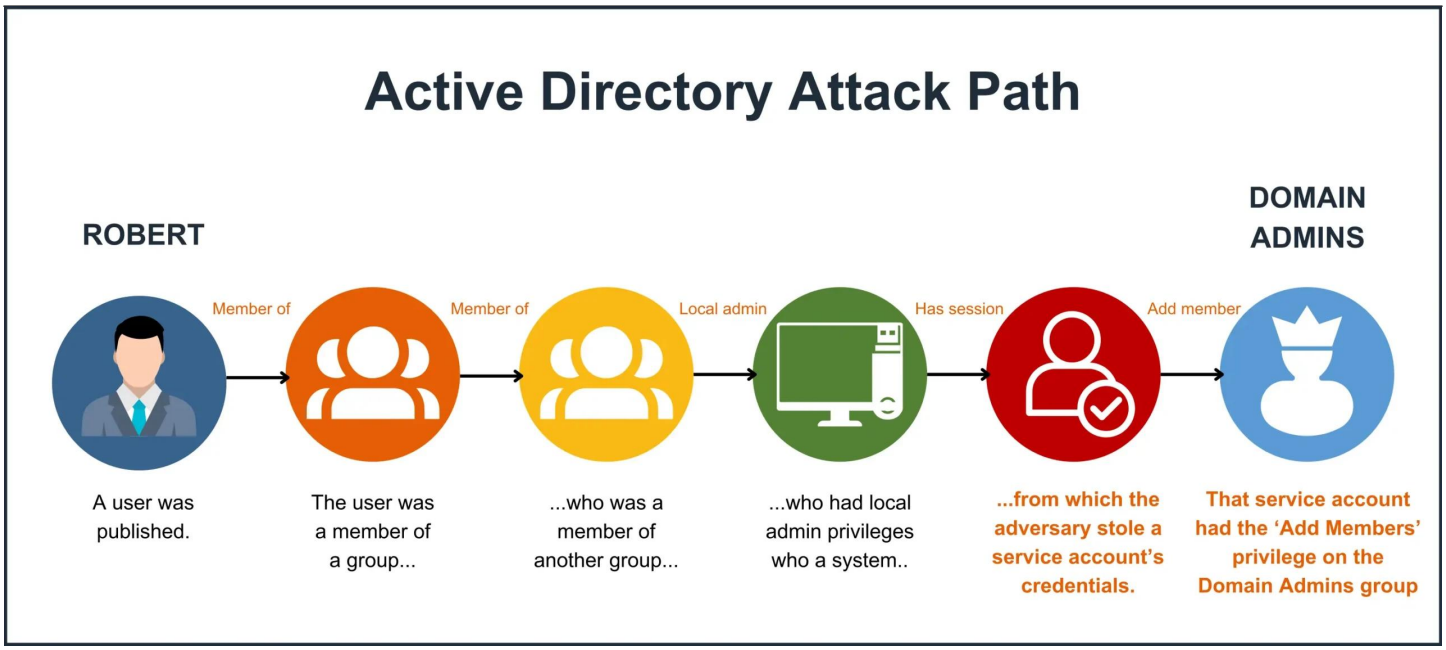
Security Checklist: Hardening
Your Active Directory with
Advanced Strategies

- Statistics and Trends
- Security Checklist
- Advanced Strategies for AD Security

Download the Whitepaper Now!

Mapping and Managing AD Attack Paths

Understanding possible attack vectors is critical for comprehensive AD security. Mapping attack paths involves identifying and assessing the many routes an attacker could take via your network to compromise indispensable assets. This approach aids in the visualization of potential gaps and the effective prioritization of security solutions. Identifying these channels allows you to proactively block or monitor key points that could be misused, improving their overall security posture.



Here are some methods for attack path mapping:

- **Identifying Privileged Account Access:** Knowing which accounts have elevated privileges is critical since they are frequently targeted by attackers. Analyzing how these accounts interact with different systems and data might help to identify potential vulnerabilities.
- **Analyzing Trust Relationships:** Understanding the relationships between different domains and systems is important. Trust relationships can be used for lateral movement, which allows attackers to migrate from one compromised system to another inside the network. Analyzing these relationships helps to find weak links that need to be strengthened.
- **Reviewing Network Segmentation:** It can reveal potential attack paths. Proper segmentation restricts an attacker's ability to move laterally and access important assets.
- **Reviewing Access Controls and Permissions:** Examining access controls and permissions can reveal excessive privileges that could be misused. Ensuring that permissions adhere to the principle of least privilege is essential for risk mitigation.
- **Assessing Security Policies and Configurations:** Doing so helps in identifying misconfigurations that could be exploited. Regular assessments guarantee that policies and configurations are up to date and secure.

There are several tools that can assist in mapping attack paths, providing detailed insights into potential vulnerabilities and visualizing the most likely routes attackers might take. One such solution is Fidelis NDR, enhancing threat detection and response across the entire attack path, providing a layered defense strategy.

Measuring the Impact of Risk Assessment and Mitigation

Key metrics for assessing the effectiveness of risk assessment and mitigation efforts include reduced vulnerabilities and improved detection rates. These metrics can help decision-makers justify security spending by highlighting the benefits of preventative measures. Fidelis Network® provides sophisticated analytics and reporting capabilities for tracking key KPIs and demonstrating the impact of security improvements.

Bonus: Top 5 AD Attack Paths in 2025 and How to Conquer Them

1. Password Spraying and Weak Credentials

Password spraying is a common attack vector. Enforcing strong password policies and establishing multi-factor authentication (MFA) helps in mitigating the risk.

2. Phishing and Social Engineering.

Social engineering strategies, particularly phishing, are quite effective. Mitigation includes providing comprehensive security awareness training and using DMARC to prevent email spoofing.

3. Exploiting Unpatched Vulnerabilities

Patching known vulnerabilities as soon as possible is crucial in preventing their exploitation. Implementing strong vulnerability management procedures for AD can help to mitigate these threats.

4. Misconfigured Privileged Accounts

Misuse of privileged accounts poses a big concern. Strategies such as ensuring least privilege access and ongoing monitoring of privileged accounts are essential.

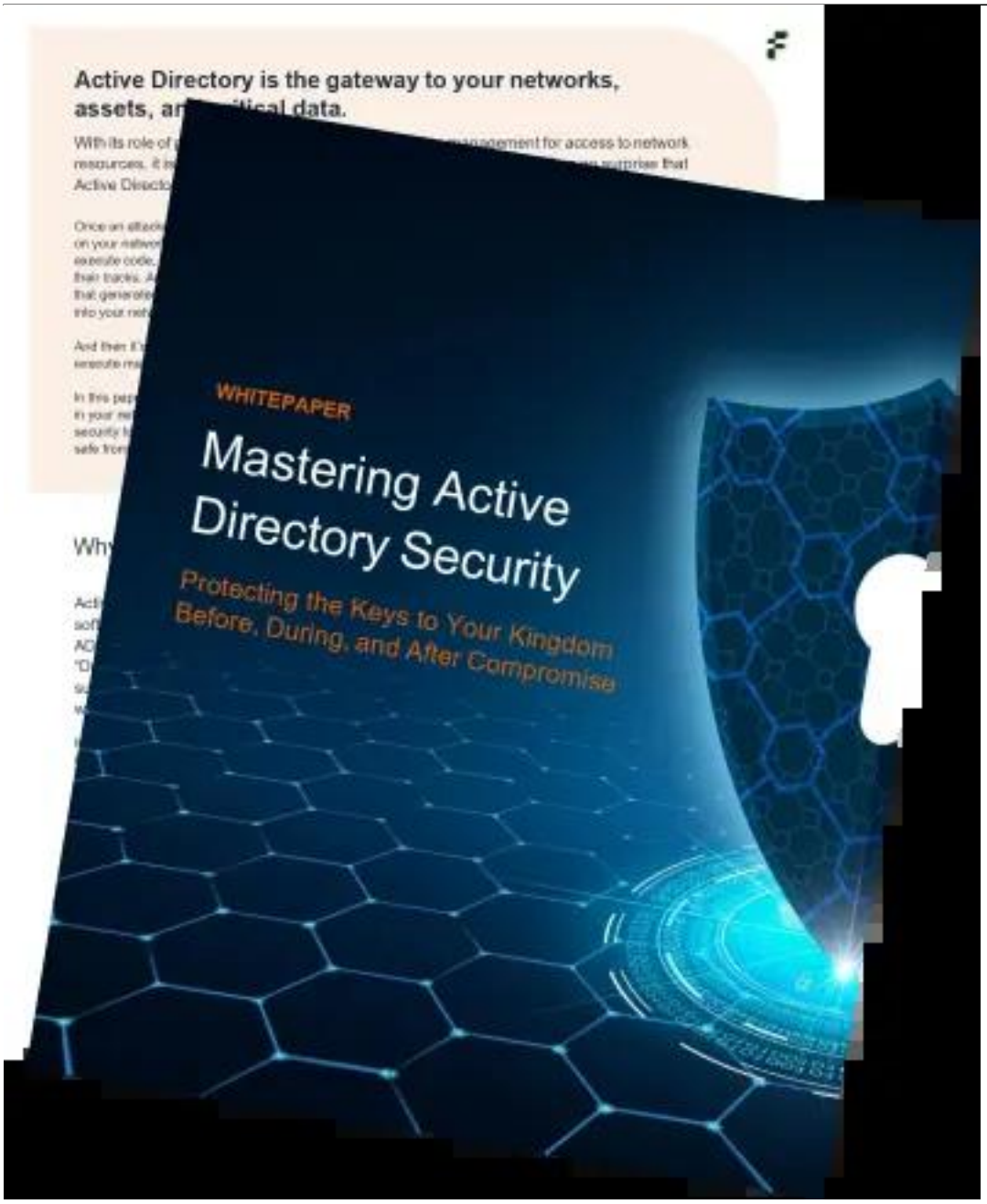
5. Weak Lateral Movement Controls

Attackers use weak network segmentation to migrate laterally. To avoid this, improve network segmentation and install strong security controls at network boundaries. Fidelis Network® can help to monitor and secure network segments, lowering the risk of lateral movement.

Mastering Active Directory Defense: Proactive Strategies to Thwart Attacks

- Continuous Visibility
- Ensure Compliance Against Misconfiguration
- Proactive AD Defense

Download Whitepaper



Conclusion

Active Directory risk assessment and attack path analysis are crucial steps in safeguarding AD infrastructures. These proactive approaches play critical roles in detecting and limiting potential attack vectors. By implementing these practices and using solutions such as Fidelis Elevate®, Fidelis Network®, and Fidelis Endpoint®, organizations can drastically improve their security posture, assuring powerful defense against sophisticated AD attacks.