Defending Against Identity-Based Attacks

Identity systems are the foundation of enterprise security, making them a top target for cybercriminals. Attackers exploit vulnerabilities in these systems to infiltrate networks, escalate privileges, and access critical resources. Business Email Compromise (BEC) is one of the most common and costly outcomes, with billions lost each year to these attacks.

Fenix24 takes a proactive, battle-tested approach to Active Directory (AD) hardening. We identify and remediate misconfigurations, close security gaps, and fortify controls to minimize risk and prevent unauthorized access. Backed by experience from hundreds of real-world breach scenarios, our team delivers actionable, proven solutions that safeguard organizations against evolving threats.

Why It Matters

THE GROWING THREAT OF BUSINESS EMAIL COMPROMISE

BEC remains one of the most effective and costly attack methods used by cybercriminals. By infiltrating identity systems, attackers can impersonate trusted executives, vendors, or employees with access to financial transactions. These highly targeted schemes exploit human psychology—leveraging urgency and familiarity—to manipulate victims into transferring funds or disclosing sensitive information, resulting in significant financial and reputational damage.

Successful BEC attacks often lead to the compromise of Active Directory. Fenix24 has identified the most common AD vulnerabilities exploited by threat actors and developed a rapid hardening response to help prevent these attacks before they occur.

OUR SOLUTION

Fenix24 is the leader in AD hardening, with unmatched expertise from countless breach responses. We quickly assess and fortify identity systems, closing security gaps before attackers strike. Here's what we deliver:

- Identification of accounts bypassing security policies.
- Enhanced visibility into identity profiles for key stakeholders.
- Activation and improvement of existing security controls.
- Separation of privileged accounts from regular user accounts.
- Dedicated security accounts for administrative tasks.

Drawing from hundreds of real-world incidents, Fenix24 ensures your identity management systems are resilient.

FENIX24

Active Directory (AD) Hardening: Strengthening the Core of Enterprise Security

AD is the backbone of enterprise IT environments. It manages authentication, permissions, and access to critical resources. Its central role, however, also makes it a high-value target for cyberattacks. A compromised AD can lead to catastrophic consequences, including ransomware propagation, data breaches, and loss of operational control. AD hardening is essential for minimizing vulnerabilities and maintaining a strong security posture.

CURRENT CHALLENGES IN AD SECURITY

1. **Misconfigurations:** Excessive privileges, dormant accounts, and inadequate access controls leave AD environments exposed.

2. **Lack of Visibility:** Many organizations struggle to monitor and audit changes within their AD, creating blind spots for attackers to exploit.

3. **Outdated Protocols and Practices:** Legacy authentication methods and unpatched vulnerabilities increase the risk of compromise.

4. **Sophisticated Attack Vectors:** Techniques such as Kerberoasting, Pass-the-Hash, and Golden Ticket attacks exploit AD weaknesses to escalate privileges and maintain persistence.

Fenix24's Approach to AD Hardening

Fenix24 delivers a proactive and systematic approach to securing AD environments, leveraging industry best practices and advanced tools to detect, mitigate, and prevent vulnerabilities. Our methodology includes:

1. **Comprehensive Review:**
   - Evaluate the current health of AD configurations, access policies, and account hygiene.
   - Identify vulnerabilities and misconfigurations.

2. **Privileged Access Management (PAM):**
   - Implement least privilege principles and secure administrative accounts.
   - Leverage Just-In-Time (JIT) and Just-Enough-Administration (JEA) models.

3. **Incident Response Integration:**
   - Rapidly contain and remediate incidents to minimize the impact of a breach.
   - Develop and test recovery plans to ensure business continuity.

Best Practices for AD Security

- **Audits:** Fenix24 reviews AD configurations, policies, and permissions.
- **Password Policies:** Enforce strong passwords, implement multi-factor authentication (MFA), and eliminate password reuse.
- **Account Hygiene:** Remove inactive accounts and enforce expiration dates for temporary accounts.
- **Group Policy Management (GPO):** Fenix24 centralizes and standardizes security settings through GPOs.

Why Choose Fenix24?

Fenix24 combines industry expertise, innovative tools, and a commitment to strengthening your AD environment. Our team partners with organizations to:

- Proactively reduce attack surfaces.
- Strengthen detection and response capabilities.
- Align AD security strategies with organizational goals.

Let's Get Started

For more information or to schedule a consultation, call 423.305.7890 (press option 2) or email us at rapidresponse@fenix24.com.