ZERO Networks

MITRE | ATT&CK®

MITRE'S POST-BREACH BLUEPRINT FOR CYBER PREVENTION:

Harden Your Network via Segmentation and MFA

The Incident

In January 2024, threat actors exploited two Ivanti Connect Secure zero-day vulnerabilities in MITRE's VPN infrastructure, gaining unauthorized access to their network.

After initial infiltration via the VPN vulnerability, the attackers then followed the classic, tried-and-true playbook of leveraging a compromised admin account to move laterally within MITRE's network, establishing persistent access and harvesting credentials. Despite addressing the zero-day vulnerability promptly, MITRE failed to detect the lateral movement, leading to a false sense of security.

15 years ago, MITRE experienced a major cyber incident that proved to be a pivotal moment for them (and for cyber defense writ large). This event spurred the creation of the MITRE ATT&CK framework, a seminal contribution to understanding and combating cyber threats. Now, faced with another breach, MITRE is once again reflecting on the nature of modern threats and reevaluating their detection and incident response strategies.

MITRE's Best Practice Tips on Hardening Your Networks

As a result of MITRE's extensive internal investigation of the incident, they released the following recommendations as high-level strategies to harden networks:

- **Strong Authentication (M1032):** Implement robust access controls, including strong multi-factor authentication mechanisms and least privilege principles.
- **Regular Patch Management (M1051):** Keep systems and software up to date to mitigate known vulnerabilities.
- **Network Segmentation (M1030):** Employ network segmentation to limit the impact of a potential breach and contain malicious activity.
- **Least Privilege Access (M1026):** Restrict user privileges to limit the impact of compromised credentials.
- **Vulnerability Assessments (M1016):** Conduct regular security assessments and penetration testing to identify and address weaknesses proactively.
- **Threat Intelligence Program (M1019):** Read and act on published reporting from trusted sources such as CISA's cybersecurity advisories, which include detection and mitigation techniques.

> **"We further commit to working across our stakeholders in the U.S. government, industry, and the public to... broadly deploy zero trust architectures with robust multifactor authentication and micro-segmentation."**
>
> Charles Clancy
> CTO, MITRE

Charles Clancy and Lex Crupton, *"Advanced Cyber Threats Impact Even the Most Prepared"*

Identity & Network Security for a Modern Cyber Threat Landscape

These recommendations align closely with Zero Networks' offering via its unified platform for simple, fully automated zero trust segmentation and remote access. In fact, 50% of MITRE's "Best Practice Tips on Hardening Your Networks" are encompassed by Zero Network's unified platform: Network Segmentation, Least Privilege Access, and Strong Authentication.

Specifically:

- **Zero Networks'** Network Segmentation solution is radically simple micro-segmentation in-a-click to stop lateral movement in its tracks. Fully segment your network in 30 days without breaking anything.
- **Zero Networks'** Identity Segmentation solution stops privileged account abuse by restricting access to operational needs only. It revokes logon rights for all admin and service accounts and then provisions them based on least privilege, enhanced by multi-factor authentication (MFA).
- **Zero Networks'** Secure Remote Access solution connects employees and vendors to the network but leaves no open ports for attackers to exploit, all while maintaining maximum performance.

Zero Networks' platform enables organizations to adopt zero trust architectures efficiently, enhancing their cybersecurity posture and mitigating the risk of cyber threats. Whether an organization is just beginning to implement MITRE's recommendations or seeking to enhance its existing defenses, Zero Networks is ready to partner with them.

The Bottom Line

The recent cyberattack on MITRE serves as a stark reminder of the persistent and evolving nature of cyber threats and the need for organizations to continuously adapt and strengthen their defenses. The full incident summary can be found here.

By heeding MITRE's recommendations and leveraging solutions such as Zero Networks' unified platform, organizations can bolster their defenses and navigate today's modern threats with confidence.

Zero Networks stands ready to assist organizations in their journey towards implementing robust cybersecurity measures and achieving a zero-trust environment. Request a demo today and embark on the path to fortified cybersecurity defenses.

Request a demo

ZERO Networks