CASE STUDY

STATE GOVERNMENT EMPLOYMENT AGENCY USES TENABLE IDENTITY EXPOSURE TO MODERNIZE AND SECURE ITS AD ARCHITECTURE

Industry: State and Local Government

Location: North America

Products used:

tenable Identity Exposure

Active Directory (AD) is the central source of truth for the most critical business applications and services within an organization. Its complexity and ever-changing attack surface make AD the favored target for attackers to elevate privileges and facilitate lateral movement by leveraging known flaws and misconfigurations.

Working from an outdated AD architecture that was designed based on best practices from more than 20 years ago, this state employment agency was concerned about increased exposure and security risk for the organization, as well as the employers and clients that depend on its services. The agency is using Tenable Identity Exposure (formerly Tenable.ad) to reduce risk and eliminate attack paths before attackers can find a way to exploit them.

"AD is a seriously under-investigated attack vector," says the agency's security systems engineer (SSE). "We have to get visibility on these things and have a discussion about them. Tenable Identity Exposure helps you with that."

Behind Every Breach Headline is an Insecure AD Deployment

Dedicated to helping workers and businesses succeed during challenging times, this large agency is tasked with managing the state's unemployment system.

Following decades-old security protocols from the early 2000s, all of the state's government agencies were connected to a single Active Directory root domain, and the employment department was just one of nearly 35 subdomains.

While it's not uncommon for an Active Directory to be in place for 20 years or even longer, the agency recognized that the interdependencies of the services and entitlements in AD could reveal the personal identity information of the agency, employees, clients and businesses. Even the smallest oversight, misconfiguration or mistake in entitlement anywhere within the subdomains could be catastrophic, and expose users to identify theft, fraud or even ransomware attacks.

"We are all beholden to the worst security practices of the smallest agency. And because we're a public agency, attackers have won half the battle because they can get our usernames in the public domain," notes the SSE. "As a result, the agency is particularly susceptible to password attempts, phishing and password spraying."

Knowing that changes were required to bring Active Directory in line with the latest security practices, but not having the ability to make them, the security team needed to gain visibility across several thousand assets in order to have an informed discussion with senior management.

According to the SSE, "People don't realize how vulnerable Active Directory is as a mechanism of cross-walking into other environments until they're caught in an incident. If an attacker gains account credentials for a known account, it is very difficult to determine if the activity is normal business operations, or somebody living off the land, collecting data, and doing malicious things. My stance, frankly, is we're breached. We've always been breached, and we need to rebuild the domain."

To get the required visibility, the agency implemented Tenable Identity Exposure, a security platform that continuously scans AD for new weaknesses and attacks, and alerts users to issues in real-time.

This proactive, risk-based approach to AD security provides complete visibility into Active Directory, including all vulnerabilities and attack activity. The security team can predict which pathways attackers may target, and act to detect, shut down and prevent attacks in real time.

Tenable Identity Exposure also enables the agency to proactively discover and prioritize weaknesses within the existing Active Directory domains and reduce exposure by following Tenable Identity Exposure's step-by-step remediation guidance. By hardening Active Directory, the agency can stop attackers in their tracks, eliminate their potential movements and ensure that fewer breaches result in escalated privileges, lateral movement, or malware execution.

Agency Uses Tactical and Contextually Aware Remediation Findings to Reveal Active Directory Weaknesses Before Attacks Happen

Almost immediately following deployment of Tenable Identity Exposure, the security team discovered that a domain administrator was patching domain controllers with patches obtained from a rogue patch repository. Working with Microsoft's Active Directory support engineers to rebuild the domain controllers, the team cleaned up the Active Directory environment based on Tenable Identity Exposure's findings.

This included deleting a few hundred group policies supported by the tactical and contextually aware remediation recommendations from Tenable Identity Exposure. These efforts made a significant improvement to the security posture of the state's Active Directory.

For security issues the team is unable to address itself, Tenable Identity Exposure provides visibility into indicators of risk and a user-friendly interface that gets people excited about doing their job. Having successfully presented the issues to senior leadership, the state is now one year into an 18-month long process of remediating risks in its Active Directory.

Tenable Identity Exposure also enables the security team to provide evidence of poor operational practices to get behavior in line with best security practices.

For example, a domain admin had set up a scheduled task on a member server running domain administrator credentials. The administrator wasn't willing to make any changes until the team pointed to the exposure as detailed in Tenable Identity Exposure, along with the clear mitigation instructions.

> **The SSE says, "Tenable Identity Exposure makes my job so easy. It eliminates all of the excuses people give for not doing the remediation work. It gives them confidence and assurance that what they're doing is correct. You don't get that with any other product."**

The security team is pleased with the support and innovation coming out of Tenable. "During the pandemic, support from a competitive vulnerability management vendor just tanked," notes the SSE. "I can't compliment Tenable enough. The support staff and security engineers are sterling. We have four best-of-breed vendors that I'm really happy with, and Tenable is one of them."

About Tenable

Tenable® is the Exposure Management company. More than 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.

Learn more: www.tenable.com/products/tenable-ad