REGIONAL UTILITY EXPOSES, CLOSES MAJOR SECURITY GAPS

Security gaps found at a small, rural utility spurred the decision to add SecureWorks services to remediate those vulnerabilities

Industry: Utilities | **Country:** United States

BUSINESS NEED

Successive reports from smaller cybersecurity firms that its overall security posture was flawless led the utility to seek deeper visibility into its cyberdefense layers.

SOLUTION

The utility commissioned a SecureWorks Advanced Penetration Test, which uncovered numerous security gaps and prompted a broader SecureWorks engagement to help close those gaps and guard against new ones.

BENEFITS

- Exposed extensive vulnerabilities and risks
- Closed a hidden link to potential threat actors in Asia
- Strengthened cyberprotections and PCI compliance

PRODUCTS | SecureWorks Advanced Penetration Test | SecureWorks Social Engineering Testing | SecureWorks Advanced Endpoint Threat Detection

THE U.S. DEPARTMENT OF HOMELAND SECURITY (DHS) CONSIDERS ALL UTILITIES — FROM THOSE SERVING MILLIONS OF URBAN CUSTOMERS TO SMALL, RURAL UTILITIES SERVING A FEW THOUSAND OR LESS — PART OF WHAT IT CALLS “CRITICAL INFRASTRUCTURE.”

This designation also applies to the transportation, communications, manufacturing and other key sectors of the U.S. economy that are vulnerable to either physical attacks or cyberattacks.

To help protect the nation’s electric grid against the latter, the DHS publishes cybersecurity standards known as “NERC-CIP” (North American Electric Reliability Corporation–Critical Infrastructure Protection). These are best practices for utilities of all sizes to help ensure they have sufficient safeguards in place to protect them from threat actors both inside and outside the United States.

But putting a solid defense-in-depth cybersecurity model in place and then keeping it up to date can be quite a challenge. That’s especially true for smaller utilities, which often have limited IT staffs whose members are typically IT generalists with security as just one of their varied duties. Such was the case of a small, rural utility, which provides its customers with both electricity and communications services, including internet, voice, television and home security.

SKEPTICISM SPURS ACTION

To supplement the IT staff’s limited cybersecurity expertise and gain an independent view of the situation, the chief technology officer of the utility had engaged a number of security consultants in recent years to assess the utility’s security posture. Each reported that the utility’s defenses were good and found no major flaws.

While most recipients would have peace of mind after such findings, the CTO was skeptical. Despite the successive all-clear reports from consultants, he suspected that their own expertise might be limited and that they had not gone deep enough to find hidden or low-level gaps in the company’s defense layers. That’s why he called SecureWorks.

The first service he ordered was an Advanced Penetration Test, conducted by the SecureWorks Security & Risk Consulting (SRC) practice. According to the SRC team, the depth and extent of that Advanced Penetration Test was between its standard Penetration Test, which he described as “checking the front door locks” of an organization’s cyberdefenses, and SecureWorks Red Team Testing, which simulates an all-out, real-world cyberattack.

SIMULATING A REAL-WORLD CYBERATTACK

In performing the Advanced Penetration Test, the SecureWorks SRC team used many of the same tools that determined threat actors might use to attempt a breach of the utility’s safeguards and then drive deeper into its network and move laterally for making other system attacks. The team started with basic port scans of the utility’s firewalls and other external-facing network devices.

It didn’t take long for them to find an opening via a web services appliance on the network. They were able to intercept and decrypt some authentication traffic containing login credentials for several server administrators. This information enabled them to expand their reach across the utility’s network and gain access to a Secure Shell server, where they helped themselves to even more credentials to many other systems.

One alarming discovery was an active network connection to an IP address in Asia, which was found to have a history of malicious activity. The SRC team reported it immediately so incident response could begin investigating how long the connection had been open and what intellectual property or other data might have been stolen or compromised.

ACTION PLAN AND NEXT STEPS

At that point, the SecureWorks SRC team had proven the other security firms’ assessments wrong and compiled their findings into a detailed report for the CTO, who shared it with his executive team. In effect, the report’s findings and recommendations became an action list with steps the utility can take to strengthen its security.

The Advanced Penetration Test report also prompted the CTO to implement two other SecureWorks services. One was Managed Phishing from the SecureWorks SRC Social Engineering portfolio. This tests users’ security awareness — sometimes called the “human firewall” — by inducing them to click on email links that could otherwise open the network to threat actors. Periodic phishing exercises have helped the utility raise awareness among employees.

The second service was Advanced Endpoint Threat Detection (AETD) from the SecureWorks Managed Services portfolio. AETD uses the on-premises solution from Carbon Black, which has a strategic relationship with SecureWorks. It provides 24x7 endpoint monitoring with support for Windows, Linux, and Mac OSX and powered by a subset of SecureWorks Counter Threat Unit (CTU) intelligence as well as Carbon Black’s CTU intelligence. It differs from SecureWorks’ own Red Cloak AETD service, which is a cloud-hosted service that supports only Windows at this time.

AETD has also helped the utility comply with the Payment Card Industry (PCI) data security standards of major credit card issuers. More importantly, the utility’s cyberdefenses are now better aligned with the U.S. NERC-CIP security standards for critical infrastructure. And its CTO can sleep better at night, knowing he has SecureWorks to enhance and supplement the security expertise of his own IT staff, while providing a valuable backstop against threat actors in the future.