CASE STUDY
Utility

El Paso Electric

Gained Peace of Mind with RiskSense

CUSTOMER PROFILE

El Paso Electric Company is an electric utility providing generation, transmission, and distribution service to approximately 400,000 retail and wholesale customers, as well as local governments.

"Excellent technical capabilities demonstrated and superb customer service. We will continue to work with RiskSense in the future."

– Rick Bernal, Information Security Manager, El Paso Electric

The Electric Company
El Paso Electric

THE CHALLENGE

In recent years, the utility industry has become increasingly aware of the potential for critical attacks against its infrastructure, such as electrical grids and water disbursement facilities. These attacks are detrimental not only to the utility company itself but its entire customer base, which is reliant on these companies for the most vital of services. To that end, El Paso Electric was intent on obtaining detailed information about its security posture through vulnerability scanning and penetration testing of its network, applications, firewall and wireless environments; garnering workable information from this activity in order to remediate vulnerabilities; and developing a thorough plan for responding to critical incidents.

THE SOLUTION

The RiskSense security analyst team was able to provide a complete system and application components review, to include evaluation of the following security areas: configuration, audit logging, directory structures and volumes, patches and hotfixes, ports and protocols, endpoint procedures (HIPS, antivirus technologies), access/password/account controls, and registry settings.

In the wireless assessment, the team attempted attacks through multiple vectors in order to assess security strength. This included passive and active attacks, denial-of-service attacks, man-in-the-middle attacks and ARP cache poisoning attacks.

The RiskSense Platform was a significant component in analyzing the collected data and generating detailed reports that provided concrete direction for vulnerability remediation. Incident response is a complex animal in the information technology jungle. It takes an extremely experienced team to create a plan that sets out a specific process for recovery and remediation after an incident or breach. The foremost goal is to stop attacks in progress and mitigate any impacts. To address these multifaceted elements, RiskSense uses its proprietary tools and analysis methods to determine the ports, protocols, services, and payloads used by the attack and develops customized response plans to minimize or eliminate effects of future and similar attacks. El Paso Electric's plan included the following phases: malicious code analysis (rapid detection and behavioral based analysis and web mining and link analysis) and analysis of suspicious

The RiskSense Platform facilitated a targeted, prioritized approach to vulnerability remediation.

executables and anatomy of identified malware (forensics of infected machines and reverse engineering). Lastly, El Paso Electric was assured that the RiskSense team would be able to perform sensitive data recovery and quantify and catalog said data in the case of a breach or incident.

THE RESULTS

Since becoming a RiskSense customer, El Paso Electric has ramped up its remediation efforts and has applied corrective measures to hundreds of severe vulnerabilities (CVSS score of 10). Access and use of the platform has significantly altered El Paso Electric's security posture for the better. This was achieved through a targeted and prioritized approach to remediation, which was facilitated by the analytics provided via RiskSense. El Paso Electric has also gained a priceless component in regards to the future of its organization and the safety of its infrastructure: peace of mind. Having a strong incident response team to rely upon in the case of exploitation or breach is invaluable, and the RiskSense team is proud to be able to provide this as one of many critical cybersecurity services.

NEXT STEPS

El Paso Electric focuses on visibility into their risk posture with the goal of continuously improving their security programs. The team uses the RiskSense Platform to monitor and improve their risk resiliency. Additionally, El Paso Electric with the RiskSense Platform is further protected against potential breaches through active incident response and phishing exercises. Instead of solely monitoring their risk, they are also proactive about being prepared so they know how to respond quickly to mitigate any damage if a breach were to happen.

WHY RISKSENSE

Detailed info about security posture through vulnerability scanning and penetration testing.
Complete system and application components review with various types of attempted attacks.
Near real-time detailed reports with workable information for remediation.
Platform to analyze and collect data with concrete remediation directions.
Incident preparedness: RiskSense's ability to perform data recovery in case of a breach.

RISKSENSE®
Contact Us Today to Learn More About RiskSense
RiskSense, Inc. | +1 844.234.RISK | +1 505.217.9422 | info@RiskSense.com

CONTACT US | SCHEDULE A DEMO | READ OUR BLOG