CASE STUDY: ASSESSING ENTERPRISE-WIDE IT AND OT RISKS AT A LARGE ENERGY COMPANY

Situation

Over the past several years, we have worked closely with a large energy company as a trusted advisor on security matters. In 2014, the client decided to move beyond one-off security engagements to develop a broader picture of the enterprise risk and security posture of its information technology (IT) and operational technology (OT). The breadth of technologies, requirements and regulatory concerns required us to leverage our experience in risk management, cybersecurity, physical security, smart-grid technologies, application architecture, mesh networks and wireless backhaul links.

Solution

We worked closely with the client to determine a program of customized tactical services that, when combined, would support the executive team's strategic decision-making. Our solution included the following assessments:

Smart-meter testing

We conducted lab testing and in-field random testing on the client's smart meters using the open source tool Termineter, which was developed by SecureState. Termineter uses the ANSI C12.18 standard for communication with the smart meter over the optical interface. This testing was performed to determine the risk that is posed by unsupervised access of customers to the smart meters. Given that many smart meters are used in residential areas, easily accessible by users, security flaws could allow them to change the data stored in the table, such as energy usage. Interacting with meters over the optical interface is a very common attack vector as it does not require the meter to be removed from its mounting, making it much safer than attacking the hardware.

Smart-grid component testing

We also assessed the client's smart-grid components beyond the smart meters. This included physical and logical security reviews of connected grid routers, capacitor bank controllers, reclosers, voltage regulators and serial-to-Ethernet devices. We performed a physical review of each device to determine the location of potential points of access including, but not limited to, serial and Ethernet ports. We used public and proprietary documentation to identify connection methods for each target device. We then commenced attack and penetration testing to simulate an attack against each of the devices. When performing penetration tests, we start with simplistic attacks that a basic hacker or beginner would attempt, then gradually increase the sophistication of the attacks to identify a wide spectrum of vulnerabilities.

Network architecture reviews

We reviewed the security of the client's smart grid and associated networks through vulnerability scans, documentation reviews, attack and penetration tests, and interviews with client staff. We assessed how information flows between the head-end servers to the smart meters. We performed a device configuration review to scan network devices for administration, authentication and best practice standards based upon current system hardening guidelines provided by CIS, NIST and DISA in addition to client-specific guidelines. This assessment exposed potential misconfigurations and vulnerabilities, allowing us to tailor a prioritized remediation plan targeting critical and high-risk issues.

We also assessed the security of cellular networks used by smart-grid devices. We reviewed the architecture and implementation of the cellular data connection used by the pole mount and collar mount cellular relay backhaul devices. During this assessment, we reviewed the design and assessed the possibility of an attacker gaining access to assets through the connection. Since intercepting and modifying cell network traffic is illegal, we were limited in what we could test.

Internal and external network penetration testing

We conducted penetration testing to determine the ability of an attacker to compromise the client's data on its internally and externally facing networks. Although we did not compromise the systems, we did identify that some systems were running out-of-date operating systems and had missing patches.

Web application security (WAS) assessments

We performed WAS assessments on a variety of internally and externally facing applications. These assessments helped identify security flaws and helped the client clarify the business logic and flow of the applications.

Results

Our assessments encompassed technologies and processes across the client's enterprise. Like many energy companies, security staff had insight primarily into the IT environment, with little knowledge of the OT environment. By assessing horizontally across technologies and internal organizations, we were able to identify security trends that affect both IT and OT systems. The most significant issue was that the client had not adequately prepared for organizational changes in its IT, security and OT infrastructure teams. Lack of end-to-end documentation and ineffective communication among the client's heavily siloed organizations meant that knowledge was lost when employees departed.

Our consistent role as a security advisor meant that, in several cases, we had the most comprehensive understanding of how the client's processes and technologies integrated. This is a common issue among large organizations, particularly energy companies that integrate a high number of technologies that are in production for long periods of time. The scope of the client's technologies also showed systemic vulnerabilities that could be remediated and managed by a vulnerability management program (VMP). This included inconsistent patching, outdated operating systems, and default or weak passwords.

There are several steps that we recommended to significantly decrease the risks facing the organization. These included improved documentation, more mature knowledge management processes, strong security policy enforcement and organization-wide collaboration on security issues. We continue to work with the client to determine the best course toward implementing the recommended improvements.

This was a complex engagement that required buy-in from the client's executive leadership down to its technical support staff. If your organization is similar to this client, you should look internally to see if you are facing similar issues of IT/OT siloing and inconsistent knowledge retention. If you are, you should consider conducting enterprise-wide reviews to determine how vulnerabilities are putting your organization at risk, and then developing an effective remediation road map.

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed. RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International. RSM® and the RSM logo are registered trademarks of RSM International Association. *The power of being understood*® is a registered trademark of RSM US LLP.