DIRECTDEFENSE

CASE STUDY

TESTING SECURITY AND COMPLIANCE FOR A BATTERY MANAGEMENT SYSTEM

How DirectDefense Identified Security Vulnerabilities Within a Major Critical Infrastructure

A multinational corporation was developing a battery energy storage system (BESS) that would enable the company's vendors and integrators to manage the voltage and power output for massive batteries. This major critical infrastructure component required testing of its SCADA architecture to ensure compliance with tight government-level regulations.

Our team was able to identify less-than-satisfactory security around the system's critical infrastructure, as well as areas requiring patches and upgrades to bring the system in line with NERC-CIP and ISA99/IEC62443 compliance regulations.

NERC-CIP requirements fall at different levels, and this particular asset is considered "high" because of the way it operates. Therefore, it needed to comply with the highest level of regulation under NERC-CIP, which is important both for our client and the asset's end users.

Our Key Findings:

01. Microsoft Patching Issues:
We identified outdated Microsoft Windows systems that would increase the attack surface and risk of compromise.

02. Configuration Vulnerabilities:
Two Windows systems were left vulnerable to a man-in-the-middle attack concerning traffic moving between the servers and the network, leaving credentials potentially exposed.

03. Network Segmentation Deficiencies:
Our assessment revealed that the internal SCADA network wasn't sufficiently segmented, allowing attackers to move throughout the network environment if access is gained.

Preparation

Setting Up the Testing Environment

Having performed SCADA assessments at multiple critical infrastructures, including those serving federal government entities, DirectDefense is well-positioned to know what to look for and test to identify vulnerabilities.

For this particular engagement, we were able to provide a deeper perspective because of our 50 years' combined experience working with critical infrastructure. As such, we could ensure compliance with the specific guidelines of NERC-CIP and ISA99/IEC62443, and identify vulnerabilities unique to a battery energy storage system.

To kick off this assessment, the client provided a testing environment inclusive of white-box access and a network diagram. This environment allowed us to conduct a thorough review of the SCADA system's security.

Execution

Identifying System and Network Vulnerabilities

Using the remote testing environment, our team took a mixed white-box and red team approach and attempted to expose gaps in the network. Because the battery energy system needed to meet a high level of compliance under NERC-CIP, being able to compromise the network quickly would be a serious red flag, which is why our testing is so important.

The client needed to ensure compliance before shipping the product, and our assessment uncovered less-than-satisfactory security around the system's critical infrastructure.

Because we identified network segmentation deficiencies within the SCADA network, we were able to make the important recommendation to lock down the plant network and the SCADA network to avoid attackers being able to move freely between each.

Another major vulnerability we uncovered was a Windows configuration issue that left the network open to attack, putting credentials at risk. A significant problem can arise from a man-in-the-middle attack where an adversary is able to manipulate traffic between the server and the network.

If attackers gain access to the network, they can cause a system failure that results in serious physical damage, or worse – especially if the outage occurs while the asset is powering business-critical operations.

DirectDefense is committed to helping organizations obtain greater security through a manageable project plan, with strategic implementations over time.

If attackers gain access to the network, they can cause a system failure that results in serious physical damage, or worse.

Maintenance

Focusing on Becoming ISA/IEC Certified

As part of our ongoing engagement with this client, we're helping them work toward achieving ISA99/IEC62443 security compliance so they can move forward with the distribution of the battery energy storage system.

As part of the ISA99/IEC62443 certification, we'll be performing a web application audit and a secondary audit on a key component of the battery system to ensure updates were made following our initial assessment.

We will also be vetting their third-party vendor for security compliance by performing a third-party risk management assessment.

The Key Takeaway for SCADA Security

Our assessment successfully identified vulnerabilities within the critical infrastructure system. We were able to start our client on the road to compliance and tighten security gaps that could cause big problems for their business, and their end users' businesses, down the road.

This particular client was proactive in seeking ISA99/IEC62443 certification and retained us to perform the pre-certification testing. In our line of work, we often see critical infrastructures that have not been updated for upwards of two decades or more, so conducting testing to eliminate the issues that can come from legacy systems is simply a smart move.

For critical infrastructures, security is about protecting your business, but also protecting your customers' businesses. Any time that critical infrastructure is involved, there are risks of serious disruptions to everyday life, liability, and even loss of life following an attack.

Getting security right the first time around saves time, money, and your reputation.

Contact Us Today!

SCADA systems were not designed to secure the level of automation occurring within organizations today. If you'd like to know how you can make your organization more secure inside and out, let's talk. Visit directdefense.com or call 1 888 720 4633.