OTORIO strengthens the security posture of global energy group

A global energy group asked OTORIO to conduct a security assessment for five of their Geothermal Production Field power plants. They needed to understand their current security posture as measured against commonly accepted industry standards, such as the ISA/IEC 62443 and NIST standards.

05
Critical Risks
DETECTED

08
Medium Level Risks
DETECTED

20
Plan Put in Place
MITIGATION STEPS

Identifying and Bridging Security and Compliance Gaps

Using the qualitative risk assessment approach defined by the National Institute of Standards and Technology (NIST), OTORIO provided recommendations for each of the findings and provided short and long-term recommendations. OTORIO generated an implementation plan to enhance the company's overall security posture.

The plan takes into account both prioritized findings and the means to comply with the IEC 62443 standards.

Background

The customer is a leader in the geothermal energy industry. The company is involved in the exploration and production of steam-based power generation for commercial use.
They develop steam fields and power generation projects.

OTORIO was tasked with:

- Reviewing the customer's architecture diagrams
- Analyzing the plants' data flows
- Interviewing the engineers to understand their daily operations and future plans
- Identifying security and compliance gaps
- Providing mitigation plans and an implementation roadmap

Key Findings

While the organization had some effective security measures in place to protect against external threats, we found some security risks.
For example, one high priority risk was the lack of patch management processes for systems used by OT in the plant operations, including client and server operating systems, AV software, and DCS software. Patch management is an important security control that ensures that devices and software systems are upgraded to the latest versions continuously. This includes firmware updates for network and process devices, as well as security and software updates for the DCS components and workstation clients.

Compared to IT networks, applying patches to OT components is more challenging. This is because many OT components are not redundant and thus cannot be taken offline for a reboot - which is a common and basic requirement for many security or software upgrades. In addition, as a result of the processes' sensitivity and the safety requirements, applying a patch or update must be tested prior to being deployed in production.

Testing patches is a common practice in the IT world to ensure that nothing breaks once the update is installed. However, given the circumstances, testing patches in an OT environment must be executed with increased caution. Patching can be a problem for most OT environments that lack such test environments. Patches, when applied, are usually installed directly in production.

Other findings included:

- Lack of compliance with the basic requirements (Security Level 1) of the IEC 62443 standard
- Missing Network Access Control Systems for device identification and authentication
- Missing a centralized Identity and Access Management Solution
- Lack of Application Whitelisting
- Weak passwords for local accounts

The bottom line

OTORIO's assessment gave this company a clear picture of their current security posture and the practical tools and strategies to improve it.
These controls reduce the risk of exposing data to external parties, while at the same time, provide senior management with the information they need to make informed business decisions.

Recommendations & Implementation Roadmap

OTORIO recommended implementing a few key processes, including designing and implementing an OT specific patch management program, provisioning a centralized identity and access management platform, and deploying network access control mechanisms throughout their plants.