OTORIO

Pulp and Paper

OTORIO Pen-testers Help a Global Paper Manufacturer Protect its Critical Assets

Case Study

A global pulp & paper manufacturer asked OTORIO to conduct a security assessment of their network as it would be seen by an external attacker. The manufacturer wanted OTORIO to gain access to their internal network without any prior knowledge of it.

Findings And Mitigation

02
ATTACK SCENARIOS

11
TECHNICAL FINDINGS

24
MITIGATION SUGGESTIONS

Our Findings

OTORIO tested the network using various attack scenarios, based on the network's current structure. The findings included:

- Lack of network hardening between sites and zones
- No patch management
- No security monitoring
- Reusing passwords

Background

The customer manages over 100 manufacturing sites around the globe. OTORIO's Penetration Testing team probed the resilience of the manufacturer's "most critical site". OTORIO tested the magnitude of the damage that could be caused to the manufacturer with no prior knowledge or access to the network. OTORIO's Penetration Testing security team spent approximately two weeks identifying the security gaps utilizing a "black-box" approach.

OTORIO

Pulp and Paper

OTORIO's Role

OTORIO was tasked with:

- Assessing the organization's external attack surface.
- Testing the network's resilience.
- Identifying critical risk vulnerabilities.
- Mapping attack vectors.
- Utilizing real-world scenarios and methods that can impact production and daily operations.
- Recommending remediation steps that will address the critical and major findings.

Moving forward

OTORIO's assessment gave this company a solid, short and long-term mitigation plan to increase awareness of their security posture with implementation guidelines. This proactive approach will ensure business continuity, prevent financial loss, and protect them against IP theft.

Recommendations

The team provided mitigation steps to remediate the risks and help the company avoid any negative impact upon reputation, finances, privacy, or identity. Some of the recommendations included:

- Enforcing password policies.
- Increasing awareness of proper cybersecurity conduct.
- Updating OS and tracking security updates.
- Creating policies for update management.
- Reconfiguring GPPs.
- Auditing sensitive and abnormal activity.
- Reinforcing firewall policies and defining a detailed set of rules.
- Reconfiguring the whitelist IP policy.

About OTORIO

OTORIO has pioneered an industrial-native OT security platform that enables its customers to achieve an integrated, holistic security strategy for industrial control systems (ICS) and cyber-physical systems (CPS).

Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. The company's platform provides automated and consolidated visibility of the entire operational network, enabling companies to take control of their security posture, eliminate critical risks, and deliver immediate business value across the organization.

OTORIO's global team combines the extensive mission-critical experience of top nation-state cyber security experts with deep operational and industrial domain expertise.

CN 120520