OTORIO Pen-Testers Help a World-Leading Maritime Company Correct Critical Security Flaws

A global maritime company asked OTORIO to conduct a security assessment of one of their cruise ships. They wanted to see their level of protection against cyber attacks.

OTORIO's Role

OTORIO's penetration testing teams come from Israel's elite technological units and are experienced in successfully defending mission-critical, cyber-physical systems. The team employs unique penetration techniques that are non-disruptive and can be carried out with maximum efficiency, with zero impact on daily operations.

OTORIO was tasked with:

- Estimating the security level of the vessel
- Identifying critical risk vulnerabilities
- Mapping attack vectors
- Recommending remediation steps that will address the critical and major findings

In particular, OTORIO was instructed to explore ways to access the ship's engine-room, balance controls, and other mission-critical systems.

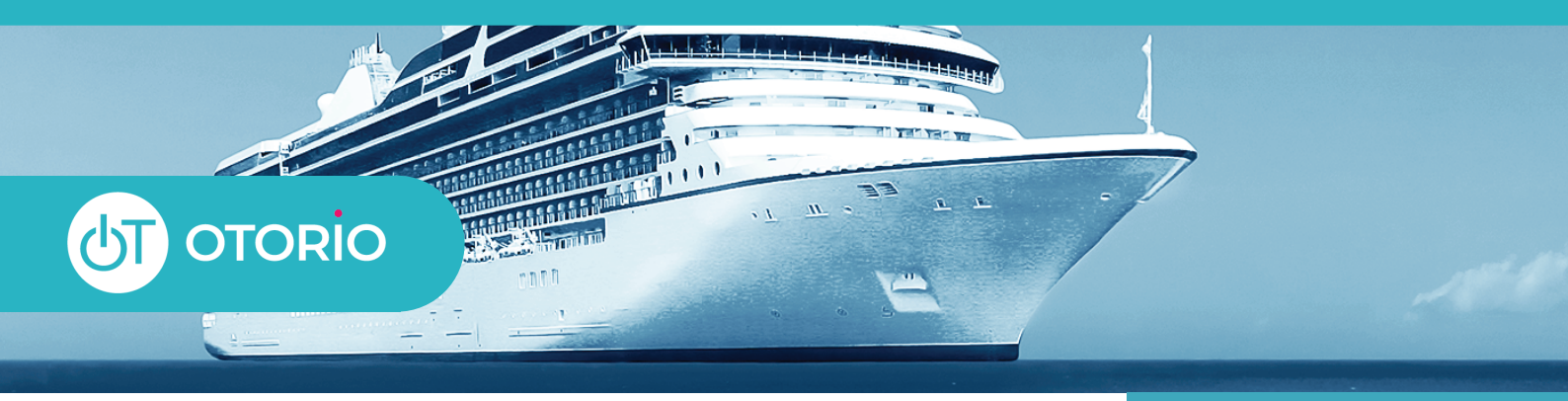
Acting Like Hackers

OTORIO pen-testers were not given access to any of the ship's IT or operational networks. Instead, they needed to act like attackers, searching for covert entryways and cracks in the ship's cyber-security.

As testing was restricted to the public facing areas, such as the business centers, bars, casino, restaurants, and an internet café, the team was able to reach only a limited number of machines. Despite this limitation, they were able to gain access to some of the ship's most valuable operational assets in only a few hours. The team was then able to gain access to the master computer, achieve keylogging capabilities on it, and collect hashed credentials of more than ten users - including the administrator of the domain.

Background

The customer runs a number of luxury cruise ships. OTORIO's penetration testing security team spent close to 3 days in a dry dock environment, with a "black-box" approach, to identify security gaps. They had no prior knowledge of the internal network and their goal was to determine if an on-board passenger could potentially gain access to the ship's crown jewels.



Our Findings

While some solid security practices were in place, the team found a number of security issues that enabled OTORIO to bypass these measures. Most importantly, OTORIO pen-testers were able to gain access, undetected, to the ship's balance control systems. Had this been achieved by a malicious actor, it would have given them complete control over the ship's flotation and balancing systems, placing the entire craft, and the people on it, in danger.

These included:

- Misconfigured account lockout procedures
- Ten hashed credentials - including those of the domain administrator
- Gaining access to the ship's controls via public internet access

OTORIO pen-testers were able to gain access to the ship's controls

With no account lockout configured in the domain, attackers can easily obtain users' passwords using brute force. Additionally, the team found outdated and End-of-Life versions of software tools, which exposed the system to many security issues, gave attackers the ability to perform malicious activities, and gain control of the systems.

Moving forward

OTORIO's assessment gave this company a solid awareness of their current security posture and specific implementation guidelines. This will enable them to protect their passengers's safety and privacy and prevent financial loss and IP theft. .

Recommendations

The team made 18 mitigation steps to remediate the risks and help the company stay safe from any dramatic reputational, financial or privacy & identity implications. Some of the recommendations included:

- Upgrade the application OS, or use Microsoft methodology
- Replace the current screen share technology
- Restrict access to the cashier printers using network protection
- Configure the domain account lockout policy
- Use network segmentation
- Enforce a password policy