How transport and logistics businesses can strengthen their cyber defenses

BY ANNA HAMMOND · APRIL 22, 2024 · LAST UPDATED ON MARCH 6, 2025

The transport and logistics (T&L) industry is a crucial player in today's interconnected world, enabling the seamless movement of goods across long distances with exceptional efficiency.

However, this very efficiency has also made the industry a prime target for cyber attacks. As T&L companies rely increasingly on digital technologies to optimize operations, they become vulnerable to cyber threats that can disrupt supply chains, compromise sensitive data, and even threaten the safety of their customers and employees.

In this article, we explore the complex landscape of cybersecurity within the T&L sector, examine the limitations of traditional approaches like pentesting, and discuss why a transformative shift towards continuous security testing is what the industry needs.

Transport and logistics: the current cybersecurity landscape

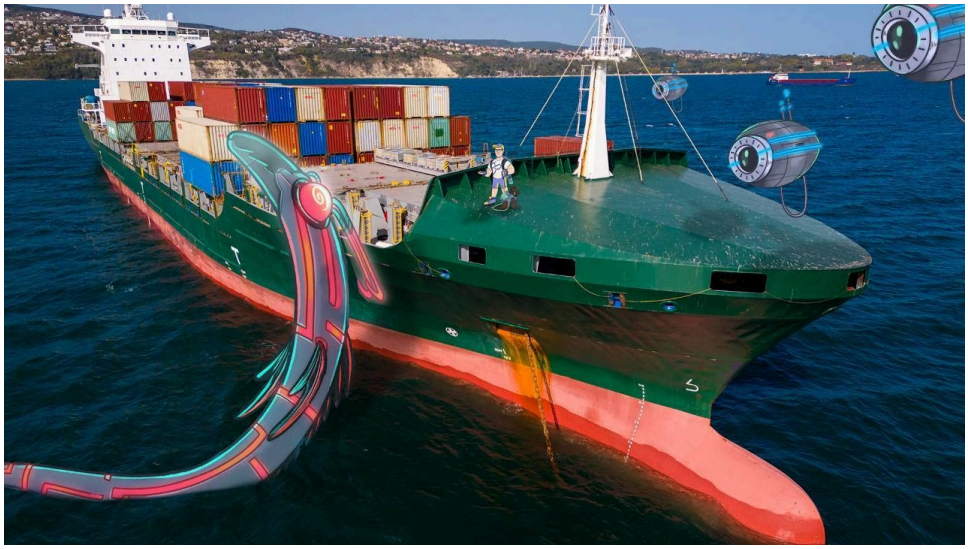
The T&L industry operates within a digital ecosystem characterized by interconnected networks, sophisticated software systems, and IoT devices. From GPS tracking and fleet management to warehouse automation and inventory control, technology underpins every aspect of T&L operations.

While these advancements have undoubtedly enhanced efficiency and productivity, they have also introduced new vulnerabilities. Cyber attacks targeting the T&L sector can have far-reaching consequences, including operational disruptions, financial losses, damage to reputation, and regulatory penalties. Moreover, the interconnected nature of T&L networks means that a breach in one area can cascade throughout the entire supply chain, amplifying the impact of cyber incidents.

Unfortunately, we've seen incidents like this unfolding in recent years. In 2022, Expeditors International, a global logistics company, had to shut down most of its systems worldwide following a cyberattack. The incident cost Expeditors $47 million in extra charges for prolonged use of shipping containers at depots and terminals.

A year later, KNP Logistics suffered a major ransomware attack in June 2023 which impacted key systems, processes and financial information. Unfortunately, the business went into administration shortly after the cyberattack.

This notable increase in cyberattacks targeting transportation and logistics companies means that organizations must prioritize cybersecurity as a fundamental aspect of their operations.



Pentesting and its limitations

In response to these threats, many T&L companies have turned to pentesting as a cybersecurity measure. During a penetration test (or 'pentest'), a trained cybersecurity professional (also known as a pentester or ethical hacker) attempts to exploit vulnerabilities in the target system using a variety of techniques, tools, and methodologies.

By conducting these controlled assessments, pentesters can uncover weaknesses before malicious actors exploit them, enabling transport and logistics organizations to take remedial action and strengthen their defenses.

However, while pentesting is an essential component of cyber defense, it's not without its limitations. One of the primary drawbacks of pentesting is its episodic nature. Pentests are typically conducted at predetermined intervals, leaving large gaps during which new vulnerabilities may emerge. In today's rapidly evolving threat landscape, where cyber attacks are becoming more sophisticated and frequent, this periodic approach is no longer sufficient.

Additionally, relying solely on pentesting to identify existing vulnerabilities may not be enough to uncover zero-day exploits or novel attack vectors that exploit previously unknown weaknesses. As a result, T&L companies may be blindsided by emerging threats that evade detection during pentesting assessments.

The modern solution: continuous security testing

To address these limitations, T&L companies need to adopt a more proactive and adaptive approach to cybersecurity. This means transitioning from a reactive pentesting model to a continuous security testing approach.

Continuous security testing offers ongoing surveillance and detection of threats in real-time. Rather than relying solely on periodic assessments or reactive measures, continuous security testing empowers organizations to proactively identify and address vulnerabilities as they arise, minimizing the window of exposure to potential threats.

One way for companies to continuously test their assets is by running a bug bounty program. A bug bounty program leverages the collective expertise of ethical hackers to identify vulnerabilities within an organization's systems, applications, and infrastructure. By offering monetary rewards (bounties) or other incentives for valid vulnerability submissions, bug bounty programs incentivize the discovery and responsible disclosure of security flaws.

This crowdsourced approach to security testing lets T&L companies tap into a diverse pool of talent and perspectives on an ongoing basis, uncovering vulnerabilities that may have gone undetected through traditional testing methods like pentesting alone.

Bridging the gap with hybrid pentesting

Another approach that would be beneficial for transport and logistics companies is hybrid pentesting. Hybrid pentests represent a cutting-edge approach to security testing, seamlessly integrating the strengths of both traditional pentests and bug bounty programs.

Like with traditional pentesting, researchers will undertake a thorough and dedicated analysis of the target system's security posture, producing a report with the all the findings. But unlike traditional pentesting, this hybrid approach means that companies gain access to the exceptional expertise of the broader research community. Additionally, they can use a 'pay for impact' approach, where costs align directly with the significance of the findings (with a mutually agreed upper limit). This leads to enhanced cost-effectiveness compared to traditional pentesting methods.

Transport and logistics businesses need to adopt a continuous approach to security testing

By adopting proactive defense strategies, transport and logistics businesses can mitigate potential risks and protect their operations, reputation, and bottom line.

To learn more about bug bounty programs and hybrid pentesting for the transport and logistics industry, get in touch.