Radiflow

Use Case

Cybersecurity for Transportation

In May 2017, Deutsche Bahn, the German national rail network, suffered a ransomware attack (namely, WannaCry) that affected 450 of its computers. The attack brought down the company's passenger information and other systems. Soon after, the same attack, which originated in North Korea, hit the national railway systems in both Russia and China.

The rise of autonomous and "smart" transportation technologies, intelligent GPS systems and other transformative technologies has revolutionized the worldwide supply chain of goods and have dramatically improved safety, efficiency, availability of assets and overall performance.

However, as with other industries transitioning to IIoT-based technologies and devices, the adoption of digital technologies also dramatically increased exposure to cyber-risk, often posed by sophisticated, state-sponsor hacking groups.

Adding to the complexity, transportation systems – railways and other forms of ground transportation, as well as sea and to some extent air transportation – were designed without taking into consideration the need to protect devices from external threats. Making things worse, much of the equipment used in transportation systems has a very long lifetime (30 years or more for trains, and even longer for railway signaling systems), creating a patchwork of inadequately-protected devices and subsystems.

Who’s Threatening the Transportation Industry, and What is its State of Preparedness?

While the majority of attacks on transportation firms focused on stealing financial and other business-related information or extorting money through ransomware attacks (that take advantage of the criticality of transportation systems), some attacks, perpetrated by state-sponsored hackers as a means of cyber-warfare, were aimed directly at OT operations to disrupt operations, often using the IT-OT barrier as the gateway into the OT network.

However, even with the writing clearly apparent on the wall, the transportation industry has not put in place adequate mechanisms to tackle cyber attacks. According to an 2020 SJSU/MTI study, about half of all transit companies surveyed experienced a cyber attack of some sort (either by directly phishing for information, data breaches, ransomware or supply chain attacks). Yet, only 60% actually have a cybersecurity preparedness program; 43% do not believe they have the resources necessary for cybersecurity preparedness; and only 47% audit their cybersecurity program at least once per year.

What's Behind the Transportation Industry's Vulnerabilities?

As recent cyberattacks on transportation companies reveal, by and large the transportation industry is ill-equipped to handle the risks it's facing, due largely to a number of factors: interconnectivity with external systems, inadequate regulation (compared to other national-critical infrastructure like power generation), lack of awareness among decision makers and the overarching shortage of OT-security experts.

By nature, cybersecurity system for transportation needs to interoperate with passenger information systems (PIS), physical security, customer service, BMS systems at stations or depots (for managing electricity, HVAC, escalators etc.) and more. Much of this connectivity, e.g. in rail or metro systems, is done over the internet, often over wireless/cellular connections. This greatly increases the attack surface of the transportation utility, creating numerous potential attack vectors toward exploiting vulnerabilities in OT and other systems.

As mentioned, the transition to IIoT-based automation, communications and operation management systems has increased the attack surface in the transportation sector. This is due to the large amount of data and interconnected systems that they handle, which makes them prime targets for hackers.

For example, the International Maritime Organization' (IMO) strategic transition to navigation allows continuously collecting, integrating, and analyzing ship and container information to track ships' locations, cargo details, maintenance issues and more; this means that a breach into the e-navigation system would affect the entire spectrum of shipping operations. The same goes to for the numerous other interconnected OT systems in ships and ground transportation vehicles and facilities, that are increasingly relying on edge device operation rather than relying on centralized, system-wide management, thanks to the adoption of 5G technologies, which further increase the probability of an attack.

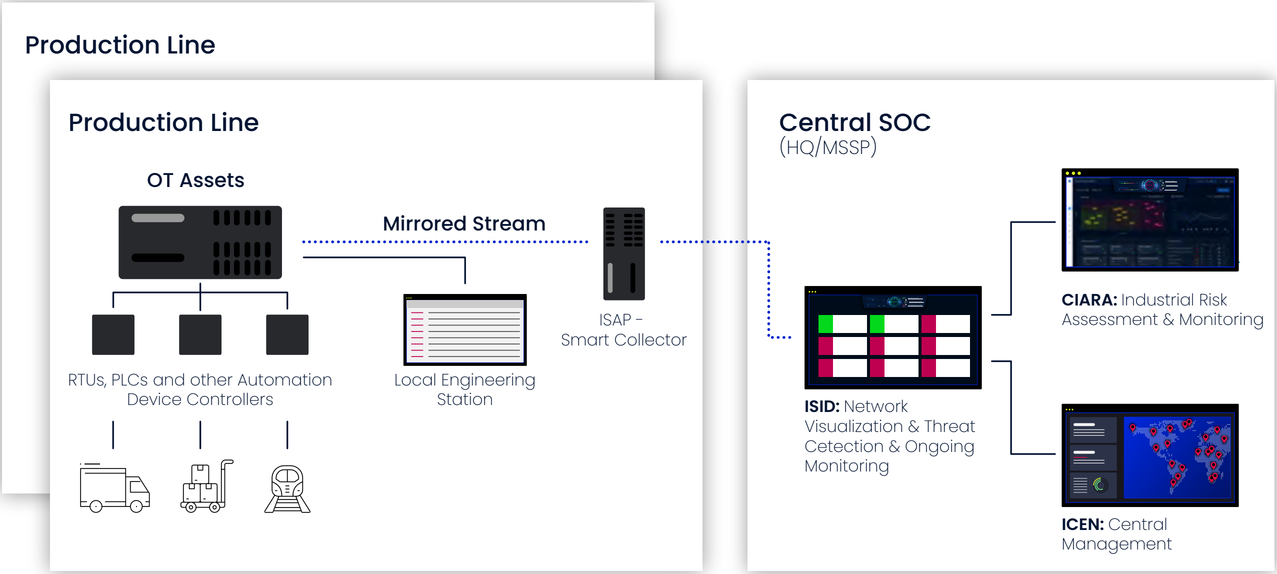
As for regulation, despite the sector's global operations—or perhaps because of them—regulators have had a hard time agreeing or focusing on a set of cybersecurity standards that transportation companies should follow wherever they operate. Among the regulations proposed or already established are the EU's Network and Information Security (NIS) directive and the soon-to-be-implemented CLC/TS 50701 and EN 50126 standards for railroads, as well as a series of rules for ships promulgated by the International Maritime Organization.

Finally, the transportation sector is competing with practically all other OT and IT sectors over a small pool of cybersecurity talent. As many as four million cyber specialist jobs were unfilled in 2020, according to the ISC2 International Information System Security Certification Consortium, and the relatively slow-moving transportation industry seems to have little appeal to recent information security graduates, who tend to be drawn to industries that involve more innovation and creativity.

Operations

Whether protecting a railway company's electrification system or a train station's BMS, the framework for efficient protection is the same:

- Visibility into the network: in order to protect the network you need to know what it's made of. Ideally you'll have a detailed network visualization maps that provide easy access to each device's properties, state, vulnerabilities and potential inter-zone attack vectors.
- Risk assessment: by simulating breach and attack scenarios (using a network digital image for device and topology information and threat intelligence for attacker capability and tactics), and accounting for the impact of a debilitating attack on each and every operational unit, transportation operators can get a clear picture of their exposure to risk, and which mitigation measures provide the best level of protection.
- Implementation: the results of the risk assessment serve as the basis for a prioritized protection plan for the OT-IT network, which should allow for optimization based on budget and operational needs. As implementation of the plan, including architectural changes, may take years to complete, it's important to install sufficient threat protection and ongoing network monitoring mechanisms, at the corporate or at an MSSP's SOC.
- Long-term security management: Continuous monitoring for threats and network anomalies, as well as ongoing risk management for the entire IT-OT infrastructure is required to provide adequate network protection and set in place protection, detection and respond measures, in the face of the ever-changing threat environment, device vulnerabilities and operational needs.



Radiflow Solutions for Transportation Operations

Radiflow offers a variety of products and services for protecting and improving the resiliency of transportation operations, which allow you to:

- Map OT network assets and connections and group the assets into zones and business processes, using Radiflow's threat detection tool.
- Assess the risk posture, per business unit, and for the network overall, by simulating relevant attack techniques on the digital image of the site (using Radiflow's unique OT BAS (Breach Attack Simulation) tool. Radiflow's risk assessment platform supports multi-site analysis so you can see in one glance the risk-status in your overall domain.
- Generate an optimized network hardening plan, which prioritizes mitigation controls by their contribution to reaching the user's security and/or other goals (e.g. focus on critical industrial units only or budgetary constraints).
- Continuously monitor the OT network for anomalies as well as for changes in the risk posture due to the changes in the threats landscape and in the site.

Radiflow's industrial cybersecurity platform enables users to take advantage of a host of sector-specific integrated solutions (like signaling network cyber security platforms), as well as solutions for asset and asset lifecycle management, specialty firewalls, security event management platforms and more. Radiflow's solutions were also designed for OT-MSSP operation, which allows small-to-medium transportation operators to outsource monitoring and ongoing risk assessment operations to cloud based security providers.

About

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital

resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6000 sites around the globe.

Radiflow | For more info: radiflow.com