Radiflow

Securing the Operational Technology

Supply Chain

May 2024

THIS CONTROLLED DOCUMENT IS THE PROPERTY OF RADIFLOW LTD.

This document contains proprietary information. Any duplication, reproduction or transmission to unauthorized parties without prior permission of Radiflow is strictly prohibited.

Table of Contents

Introduction

Today, industrial and critical infrastructure operations, as well as industrial machine building, involve multiple hardware and software products and services from a variety of suppliers, creating a mesh of supply chains across their networks. While boosting productivity substantially, these elaborate supply chains come at a cost.

Leveraging their multiple interconnections, cyber attackers are increasingly exploiting supply chains as their initial point of compromise to reach lucrative targets. This trend is rising rapidly. According to Mandiant's M-Trends 2022 report, attacks designed to compromise supply chains were the second most prevalent initial-infection vector.

Consequences of successful cyberattacks on operational technology (OT) supply chains are often significant and may lead to disruptions to operations, productivity and financial losses, and safety risks to personnel and the public.

Cognizant of the sharp increase in attacks on supply chain suppliers, regulators are now requiring that OT entities restrict their activities with supply chain companies to those complying with tightening cybersecurity standards. As a result, cybersecurity compliance is transitioning from a voluntary best practice to a mandatory requirement, reflecting the critical role that supply chains play in digitized operations. This welcome shift toward more secure OT supply chains strengthens overall cybersecurity.

Supply Chain Challenges

Organizations are facing two primary supply chain challenges: visibility and management of security risks posed by third-party vendors. Organizations must balance security and operational efficiency to ensure that their OT supply chains are secure and resilient against cyberattacks. **Common cyber threats to the supply chain include:**

Third-Party Vendors

Today, OT operators acquire hardware and software products from third-parties to automate various aspects of their operations. Among these are:

- Machine builders
- Providers of physical components like sensors, actuators, controllers, and other devices
- IIoT device makers
- Networking equipment suppliers
- Computer suppliers
- Software creators (applications, operating systems)
- System integrators

But the operators do not have cyber visibility into these products. If the third-party suppliers do not maintain strict and effective cybersecurity measures, their products can turn into welcoming vectors for cyberattacks by hackers who may target them to gain access to the operator's network and assets. Some of the tactics and techniques that hackers might use include:

Phishing and Social Engineering

Attackers may use phishing emails or social engineering tactics to trick employees along the supply chain into divulging sensitive information or downloading malicious software. These tactics can compromise the integrity of the supply chain.

Malware and Ransomware

Malicious software can infect a supplier's systems, spreading to other parts of the supply chain. Ransomware attacks can encrypt critical data, causing disruptions until a ransom is paid.

Supply Chain Interception

Attackers may infiltrate the supply chain's communication channels or software updates to inject malware, compromise data, or manipulate orders. This can lead to counterfeit or tampered products entering the supply chain.

Physical Attacks

Cyberattacks can also have physical consequences, such as compromising the integrity of hardware components or industrial control systems within the supply chain.

Insider Threats

Disgruntled employees or contractors with access to the supply chain can intentionally or unintentionally cause harm by leaking sensitive information or introducing vulnerabilities.

Zero-Day Vulnerabilities

Attackers may discover and exploit unknown vulnerabilities (zero-days) in supply chain software or hardware. This can be particularly challenging to defend against since there are no patches available.

Data Breaches

Breaches of sensitive data within the supply chain can lead to the exposure of trade secrets, customer data, or proprietary information. This can have severe legal and financial repercussions.

Inadequate Security Practices

Poor cybersecurity practices within the supply chain, such as weak password policies, lack of regular updates, and insufficient employee training, can create vulnerabilities.

Connections with IT Systems

OT operators pay attention to industrial control systems – controllers, sensors, logic solvers, and associated communications processors. Systems and devices used for manufacturing operations such as historians and engineering workstations also require attention since they typically exchange information with business IT systems. As these systems are connected to the enterprise network, they introduce additional attack vectors.

Notable Incidents

To understand the severity and depth of security challenges faced by supply chains, here are some notable cyber incidents utilizing this attack vector. These incidents highlight the potential vulnerability of supply chain companies as entry points for sophisticated cyberattacks on Industrial Automation Control System (IACS) companies.

- In a report issued last month after an investigation, the U.S. House Committee on Homeland Security and the House select committee on China focused on the more than 200 Chinese-made cranes installed at US ports. These cranes contain communications equipment with no clear purpose or record of their installation, heightening concerns that the cranes could be used for surveillance or sabotage. House lawmakers found that the equipment installed on the cranes — cellular modems that can be used for remote communication — were not mentioned in any contract between U.S. ports and Chinese crane maker, ZPMC.
- In February of this year, attackers successfully infiltrated AnyDesk's production systems, extracting sensitive source code and private code-signing keys. This breach poses significant risks as it enables malicious actors to potentially create harmful versions of the software embedded with backdoors and other vulnerabilities. Remote access software like AnyDesk is widely used in OT environments.
- In July 2023, Rockwell Automation reported a security vulnerability in one of its products that is widely deployed in OT settings. Collaborating with the U.S. government, the company identified a state-backed hacking operation with the capability to run malicious code on industrial-controller communication modules.
- In late November 2023, advisories from the U.S. cybersecurity agency, CISA, and Trend Micro's Zero Day Initiative (ZDI) highlighted four vulnerabilities in Delta's InfraSuite Device Master. Two deemed 'critical severity' allow remote, unauthenticated attackers to execute arbitrary code. Two additional 'high severity' vulnerabilities enable remote code execution and the acquisition of sensitive information. Delta's InfraSuite Device Master is a data center facility monitoring software product designed for real-time oversight of critical devices that govern power and cooling systems and building sensors along with industrial control systems (ICS) such as programmable logic controllers (PLCs) and power meters.
- In May 2023, ABB, a global manufacturer and supplier of IACS solutions, was targeted by a Black Basta ransomware attack. The attack had significant impact, affecting numerous workstations, disrupting operations, causing project delays, and affecting factories. ABB took steps to mitigate the incident, including the termination of VPN connections with its customers.

- In February 2022, Kojima Industries, a key player in Toyota's supply chain, fell victim to a cyberattack. A serious incident caused a significant disruption in Toyota's operations, forcing the company to halt production of a third of its global manufacturing output for at least a day. The impact of the cyberattack resulted in a reduction of 13,000 units – 5% – of production.

All of the above incidents occurred in the last two years. Prior to these incidents were several infamous attacks that caused considerable damage.

- One of the most significant supply chain attacks in history, the SolarWinds attack, involved a compromise of SolarWinds' software updates, which were then distributed to thousands of their customers, including major IACS operators. This breach allowed threat actors, believed to be associated with Russian intelligence, to gain access to sensitive data and systems across multiple organizations.

- Initially thought to be ransomware, NotPetya was a destructive malware attack that primarily targeted Ukraine but also affected organizations worldwide. The attack began with the compromise of a Ukrainian accounting software company, M.E.Doc, whose product was used by many organizations in the country. The malware spread through software updates and caused extensive damage to global supply chains.

- Maersk, the world's largest shipping company, also suffered the consequences of a NotPetya attack which disrupted global trade and resulted in $300 million in damages. The malware infiltrated Maersk's systems through one of its suppliers.

We could list dozens of other such incidents that underscore the importance of securing the OT supply chain. Attackers often target trusted vendors or service providers to gain access to their intended targets. Supply chain attacks can have far-reaching consequences, affecting not only the compromised organization directly, but also its customers and partners.

Expanding Regulations

Regulators in many industrial sectors are beginning to demand that regulated entities limit their relations to supply chain companies who comply with the highest cybersecurity standards. Such regulations are spreading across the globe. Here are several recent major initiatives in the US, EU, and Australia:

United States

The 2021 Cybersecurity Executive Order (EO 14028) establishes a clear framework for how the government and private sector should work together to improve cybersecurity in government systems. The EO requires developers to maintain greater visibility into their software and make security data available publicly.

A new update to the National Institute of Standards and Technology's (NIST) foundational cybersecurity supply chain risk management (C-SCRM) guidance intends to help organizations protect themselves as they acquire and use technology products and services. The revised publication, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, provides guidance on identifying, assessing, and responding to cybersecurity risks throughout the supply chain at all levels of an organization. It forms part of NIST's response to Executive Order 14028.

European Union

In November 2022, the EU adopted the updated the Network and Information Security 2 (NIS2) Directive, a broad initiative designed to standardize cybersecurity measures across member states. NIS2 includes a significant focus on supply chain security and supplier relationships by requiring individual entities to address relevant cybersecurity risks, including vulnerabilities specific to each direct supplier and service provider as well as their secure development procedures.

American and Asian suppliers to EU companies subject to NIS2 may be subject themselves.

Australia

In April 2021, the Australian Department of Health issued a regulatory guidance document detailing the cybersecurity responsibilities and requirements for medical device manufacturers.

Regulators also focus on the cybersecurity of supply chains in many industrial sectors. While this paper lacks space to list them all, here are some examples:

Critical Infrastructure

In April 2023, Oliver Dowden, UK Secretary of State in the Cabinet Office, stated that the UK is actively exploring strategies that will include all private sector businesses involved in critical national infrastructure under the scope of cybersecurity resilience regulations.

Defense

In 2020, the U.S. Department of Defense (DoD) published the Cybersecurity Maturity Model Certification (CMMC), a regulation for cybersecurity of supply chains used by the Defense industry. The regulation requires that all Defense contractors be certified according to their level of cyber maturity.

Medical Devices

In April 2022, the U.S. Food and Drug Administration (FDA) published a Draft of Guidance on Cybersecurity for Medical Devices, a regulation covering cybersecurity across the entire life cycle of such devices.

In 2018, the FDA published a guide for data integrity also known as the ALCOA Principles for the medical industry supply chain and manufacturers responsible for data integrity.

Energy

In July 2020, the North American Electric Reliability Corporation (NERC) issued its Critical Infrastructure Protection (CIP) standard, CIP-013-1. This now-enforced standard focuses on addressing vulnerabilities and threat vectors present within the supply chains of Bulk Electric Systems (BES).

Maritime

International Association of Classification Societies (IACS) has adopted a new Unified Requirement (UR) that applies to supply chains in the sector:

"UR E27 aims to ensure system integrity is secured and hardened by third-party equipment suppliers. This UR provides requirements for cyber resilience of onboard systems and equipment and provides additional requirements relating to the interface between users and computer-based systems onboard, as well as product design and development requirements for new devices before their implementation onboard ships."

Securing the OT Supply Chain

Supply chains continue to grow; organizations now work with an average of 27 third parties. Securing all these chain links is essential for critical infrastructure and industrial operators to ensure the integrity, reliability, and safety of products and services. A secure supply chain helps protect against various risks, including cybersecurity threats, counterfeit products, disruptions, safety problems, and more.

Cyber threats to the supply chain are dynamic and evolving, so organizations must continually adapt their cybersecurity strategies to address emerging threats and vulnerabilities. Securing OT supply chains requires vigilance, collaboration, and proactive measures to mitigate risks and protect critical infrastructure.

Here is a comprehensive list of actions that OT organizations should undertake:

Asset Visibility

- Use automated processes (passive monitoring and/or active scanning) to map the landscape of digital and physical devices.
- Map the communications from, to, and between assets.

Asset Management

- Identify devices running legacy operating systems.
- Employ an asset management system that tracks patching of vulnerabilities over the lifecycle of assets, logs security events, and delivers recovery capabilities.

Risk Assessments

- Identify potential risks and vulnerabilities in the supply chain including third-party vendors. This includes physical, cyber, and operational risks.
- Consider natural disasters, supplier dependencies, and regulatory changes.
- Conduct regular (monthly or quarterly) risk assessments and track the changes.

Supplier Selection

- Limit the number of suppliers.
- Carefully vet and select suppliers based on their reputation, financial stability, and commitment to security and quality.
- Assess their cybersecurity measures and supply chain security practices regularly.

Supplier Agreements

- Establish clear contractual agreements that outline security expectations, quality standards, and compliance requirements.
- Include provisions for audits, inspections, and penalties for non-compliance.

Supplier Tracking

- Regularly monitor supplier adherence to security applicable security standards and industry best practices.

Monitoring and Detection

- Deploy intrusion detection systems and security monitoring tools to identify unusual activities and potential threats.
- Stay up-to-date with the latest threat intelligence to understand emerging cybersecurity risks in the supply chain. This can help to identify new threats and vulnerabilities and take proactive measures to prevent incidents before they occur.

Patching

- Exploiting known vulnerabilities in unpatched software is a favorite tactic of hackers. Update operating systems, firmware, and software as releases become available.

Physical Security

- Secure physical access to warehouses, manufacturing facilities, and distribution centers.
- Implement access controls, surveillance systems, and alarm systems.

Quality Assurance

- Implement quality control and testing procedures to ensure that products meet specifications and safety standards.
- Conduct regular inspections and audits.

Resilience Planning

- Develop business continuity and disaster recovery plans to address supply chain disruptions.
- Diversify suppliers and have contingency plans for for disruptions to critical components.

Backup and Recovery

- Regularly back up critical data and systems.
- Develop and test recovery procedures to minimize downtime in case of an attack.

Incident Response Plan

- Develop an incident response plan to respond to cybersecurity incidents quickly and effectively.
- Keep the plan up to date and test it periodically.

Compliance

- Stay informed about relevant regulations and standards in the industry and ensure compliance with them.
- Conduct regular compliance audits.

Security Awareness Training

- Train employees and supply chain partners on security protocols, best practices, and reporting procedures for security incidents.
- Repeat the training periodically for new employees and partners.

Communications

- Maintain open lines of communication with suppliers, customers, and stakeholders.
- Promptly share information about security incidents and disruptions.
- Collaborate with other organizations and industry groups to share threat intelligence and best practices related to supply chain security.
- Encourage open reporting.

Continuous Improvement

- Regularly review and update supply chain security measures to adapt to changing threats and technologies.
- Learn from past incidents and make improvements accordingly.

Third-Party Assessments

- Consider third-party assessments and certifications (e.g., ISO 28000 for supply chain security, NIS2) to validate internal security practices.

Cyber threats to the supply chain are dynamic and always evolving. Securing it is an ongoing process that requires vigilance and adaptability. By proactively addressing potential risks and continuously improving security measures, OT organizations can enhance the resilience and reliability of their supply chains.

Radiflow Solutions for the Supply Chain

Radiflow helps critical infrastructure and industrial operators to combat inevitable supply chain attacks by:

- Providing comprehensive protection for both their operational technology (OT) and their many supply chains, including machine builders.
- Offering continuous monitoring and endpoint protection for OT devices of all types, new, legacy, IIoT, etc.
- Delivering solutions that allow machine builders and device manufacturers to be more cybersecurity transparent with their customers and compliant with the emerging standards and regulations.

Radiflow solutions provide effective mechanisms for:

Asset Visibility and Management

Radiflow iSID passively monitors the ICS network, discovering and identifying assets along with their communications and behaviors. Complementing the passive monitoring capabilities of iSID, Radiflow Active Scanner employs targeted scans (rather than querying the entire network, typical of IT scanning solutions) for specific groups of industrial assets (e.g., PLCs) to identify live as well as silent devices, and to collect additional information from existing devices. Radiflow solutions tightly integrate with third-party CMDB systems like ServiceNow.

Network Monitoring and Visibility

Radiflow iSID starts by providing comprehensive network monitoring and visibility. It learns network and device behavior to create a normal baseline. Then, it continuously monitors the OT network to identify anomalies, unauthorized access, and potential threats. This visibility helps supply chain operators understand their network's status and detect any unusual activities.

Threat Detection

Radiflow iSID employs various techniques to detect threats and anomalies within the supply chain's OT infrastructure. These may include signature-based detection, anomaly detection, and behavior analysis to identify deviations from normal network behavior, potentially indicating a cyberattack or malicious activity.

Vulnerability Assessment

Identifying and addressing vulnerabilities within the supply chain's OT systems is crucial. Radiflow conducts vulnerability assessments and penetration testing to identify weaknesses in the infrastructure that could be exploited by attackers. Once vulnerabilities are identified, organizations can prioritize and remediate them.

Access Control and Authentication

Through native integrations with other security solutions (e.g., Cyolo), Radiflow helps manage access to critical OT components by implementing strong authentication mechanisms, role-based access control (RBAC), ensuring that only authorized personnel can access and modify sensitive systems. This reduces the risk of unauthorized access and insider threats.

Network Segmentation

Network segmentation is a fundamental security measure that Radiflow employs to isolate critical OT systems and devices from the broader enterprise network. By segmenting the network, the impact of a breach can be limited, as it becomes more difficult for attackers to move laterally within the infrastructure. Radiflow conducts a study of the network and recommends segmentations that maximize protection against incidents and comply with standards and best practices.

Incident Response and Threat Mitigation

When a security incident is detected, Radiflow iSID facilitates a rapid response, determining affected components, containing the threat, and mitigating its impact. iSID collects forensic data that aids in reporting per NIS2 and other regulatory requirements.

Risk Management

Radiflow's data-driven CIARA, automates risk assessments, enabling OT organizations to conduct them frequently, quickly, and accurately. Mitigation measures are quantified by their contribution to lowering risk and their optimal use of the security budget.

CIARA automatically discovers and learns key risk indicators, and accurately evaluates per-site and overall security posture and risk. It determines how to direct the OT security budget to maximize the effectiveness of threat-mitigation controls based on cybersecurity standards like IEC 62443 and NIST CSF.

CIARA provides full network visibility maps and reports, displaying all network segments, zones, conduits, assets, asset properties, protocols, links, and vulnerabilities. As the environment changes, data-driven CIARA automatically updates its knowledgebase.

Conclusion

High-value targets, OT operations, assets, and data are very attractive to nation-state adversaries and hacker syndicates who spend enormous amounts of time and resources to defeat security barricades.

Because the threat landscape is constantly evolving, supply chain cybersecurity necessitates a ceaseless, comprehensive effort. Organizations must remain vigilant, collaborate with their partners, and invest in the necessary personnel, technologies, and processes to secure their supply chains effectively now and in the future.

The entire OT community – operators, machine builders, MSSPs, auditors, vendors, system integrators, and other participants in the supply chain – must work together to defend critical infrastructure and industrial operation from the onslaught of security threats they all face.

Fortified by a rapidly growing body of pertinent regulations, all these stakeholders must familiarize themselves with the long list of security activities provided in this paper.

The road to OT security is a long one and there is no silver bullet. Organizations cannot go from high-risk to low-risk overnight. With an iron will, they need to implement the processes, solutions, and activities that will close the security gaps that hackers inevitably try to exploit.

Radiflow offers many of the solutions to the twin-requirements of bolstering OT security posture while complying with regulations, directives, and best practices. Together, we will succeed.