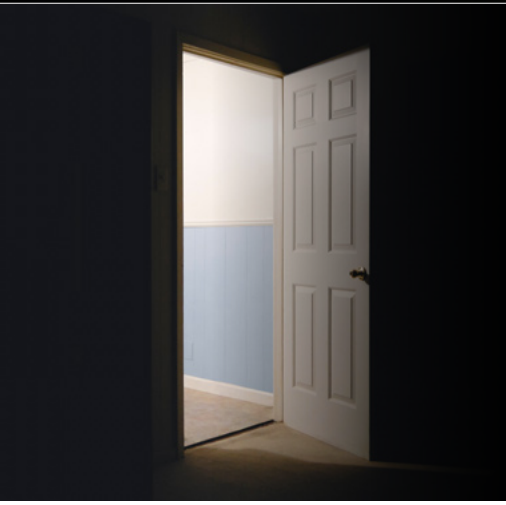
FAST FACTS

Manufacturing Cybersecurity Briefing

Supply Chain Attack Avoidance Checklist



What happened with SolarWinds?

SolarWinds is a US company that provides IT and network management software. In March 2020, an advanced, persistent threat actor hacked into the SolarWinds platform and placed sophisticated zero-day malware in the company's Orion network monitoring software product. SolarWinds unknowingly distributed it to 18,000 of their customers via standard software updates.

The malicious code was able to tell when it had been installed on a customer's system. When the customer opened the Orion software, it activated the SUNBUSRT backdoor code, which carried out cyber-espionage activities.

Implications for the manufacturing community, even if you don't use SolarWinds

Supply chain attacks are immune to many traditional detection and defense measures. This means that you can no longer trust the software updates of your trusted suppliers of IT and OT products. You cannot assume that applications and data inside the corporate perimeter and behind the firewall are safe.

SolarWinds was used to distribute cyber-espionage malware, but this attack vector could also carry a ransomware or DDoS attack, either of which could inflict significant financial and operational damage.

Manufacturing firms should particularly pay attention, even if they don't use SolarWinds, as the attackers targeted centrally situated control systems. While SolarWinds was the target in this instance, the implications are clear that state-sponsored adversaries are placing high value on such systems, including other network management tools and Industrial Control Systems (ICS). The SolarWinds attack may foreshadow follow-on campaigns against manufacturing firms.

To reduce your risk, consider taking a range of technology, process, and policy controls to defend against supply chain attacks.

Supply chain risk management best practices

The National Institute for Standards and Technology (NIST), part of the US Department of Commerce, has published a useful no-cost guide to Supply Chain Risk Management Practices. This guide is primarily intended for government agencies, but it's equally applicable to manufacturing companies. It advises that the best way to identify, assess, and mitigate against ICT supply chain risks is for organizations to:

1. Integrate ICT supply chain risk management into your overall organizational risk management approach
2. Implement security controls across 20 aspects of operations as defined by NIST in SP 800-53i, including:
   - Access control
   - Awareness and training
   - Audit and accountability
   - Security assessment and authorization
   - Configuration management
   - Contingency planning
   - Identification and authentication
   - Incident response
   - Maintenance
   - Media protection
   - Physical and environmental protection
   - Planning
   - Program management
   - Personnel security
   - PII processing and transparency
   - Risk assessment
   - System and services acquisition
   - System communications protection
   - System and information integrity
   - Supply chain risk management
3. Identify supply chain threat scenarios, including telecommunications counterfeits, industrial espionage, malicious code insertion, and unintentional compromise
4. Develop and implement a supply chain risk management plan using the template the document provides

CHECKLIST: AVOID SUPPLY CHAIN ATTACKS

There's no single countermeasure to mitigate a supply chain attack.

Your preparation must consider people and processes, as well as technologies. We recommend that you:

- ☐ Routinely review intelligence from Information Sharing and Analysis Centers (ISACs), national and regional Community Emergency Response Teams (CERTS), and suppliers of IT and OT management software
- ☐ Adopt a risk-based vulnerability management approach by using:
  - threat intelligence capabilities
  - business asset identification, monitoring, and maintenance
  - risk scoring based on the business-criticality of the assets
- ☐ Ensure correct implementation of encryption for storage, transmission, and processing (tokenization)
- ☐ Review supply chain risk management standards and adopt best practices. Two publications that can be referenced are NIST-SP 800-161 "Supply Chain Risk Management" and the 20 operational domains in NIST 800-53 Implement a zero-trust architecture and policy (see Atos publication On the Road to Zero Trust)
- ☐ Rehearse business continuity and disaster recovery plans physically or in tabletop exercises
- ☐ Deploy advanced threat detection capabilities, including those supported by artificial intelligence
- ☐ Define processes to report a breach to your local crime complaint center

Schedule a Smart Factory Studio session

Take the next step to developing a robust risk management strategy with a session at the Atos Smart Factory Studio. We'll help you to unleash the power of ideas, by combining expertise, innovation, and a powerful virtual collaboration environment that brings together experts from across the globe to brainstorm, develop, and define the industrial cybersecurity solutions that will protect your business for years to come.

Schedule your studio experience now at **www.atos.net/manufacturing** and let us help with your Smart Defense