Supply Chain Attacks Are a Risk to Your Organization

Overview
A supply chain attack is a cyber-attack that targets less secure elements in a supply chain. Supply chain management experts recommend strict control of an organization's supply network to prevent potential damage from cyber criminals.

Vulnerabilities
IT security teams generally have a limited grasp of the risks posed by software supply chains. In addition, suppliers, vendors, and third-party service providers are vulnerable to supply chain attacks:

- Any company that produces software or hardware for other organizations is a potential target of attackers.
- Recent supply chain attacks show that any supplier, vendor, or third-party service provider is vulnerable and could be compromised.

Supply Chain Controls
If you aren't aware of the risks, you won't be able to implement the proper security controls. The first step in implementing supply chain controls is to increase security awareness among management, network administrators, software development staff, and quality control staff.

Executive management should ensure that security is integrated into all phases of a network and software lifecycle. Staff should document supply chain dependences, be aware of the appropriate vulnerability disclosures, and patch security vulnerabilities in a timely manner.

Where possible, organizations should:

- Reduce the attack surface by limiting the number of suppliers, vendors, and service providers.
- Impose strict controls over the supply chain and ensure the suppliers, vendors, and service providers implement and maintain approved security controls and protocols.
- Build security into the design of networks and software using an iterative testing process that ensures the solution is properly hardened.
- Ensure all elements of the supply chain have security audits. This includes the organization, suppliers, vendors, and service providers. Review security audit reports and remediation action plans to ensure the appropriate corrective action occurs.

Publication Information

Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.