PROTECTING YOUR ORGANIZATION FROM SUPPLY CHAIN ATTACKS STARTS WITH THE CLOUD

October 25, 2022 • Cloud & SaaS Awards • Kevin Beasley

More than 60% of security breaches in 2021 happened at weak points in the supply chain — a nearly 20% increase from the previous year. The impact of software supply chain attacks is far-reaching since these attacks not only affect the targeted organization, but its partners and customers as well. With organizations continuing to rely on remote work and IT outsourcing, systems can be more vulnerable to hidden threats in third-party software.

Businesses must respond by creating a comprehensive cybersecurity plan to stay ahead of cybercriminals. But what does that involve? Well, it starts with moving operations to the cloud. The added layers of security in the cloud typically extend well beyond what is available on-premise, allowing organizations to effectively implement advanced threat:

- *Prevention;*
- *Detection;*
- *Mitigation.*

Supply chain attacks are changing the cybersecurity landscape

Supply chain attacks happen when a bad actor attacks a first- and/or third-party vendor's supply chain technology with malware, impacting the organization and its clients. For example, cybercriminals often gain access by attacking well-known and commonly used management software, such as SolarWinds' network management software, and inserting malicious code into the system to create a backdoor.

Case Study

SolarWinds unknowingly distributed the code to its clients in the system's routine software update. For several months, additional malware was embedded into the system to spy on SolarWinds and its clients, including cybersecurity firms and government agencies such as the Department of Homeland Security and the Department of Energy.

As in the case of the SolarWinds attack, software supply chain attacks can result in additional consequences in the form of compromised and lost data, identity theft, and revenue loss. In fact, the average cost of a data breach reached $4.35 million in 2022, and McKinsey estimates cybercrime expenses will reach $10.5 trillion a year by 2025. Ultimately, cyberattacks lead to broken trust with customers and investors, diminish organizations' reputation, and damage business continuity.

The growth of IT outsourcing for remote and hybrid work has significantly contributed to the rise of cyberattacks. Outsourced processes rely on organizations granting vendors privileged access to their networks through

remote-access software. These decentralized operations increase the chances of cybercriminals exploiting vulnerabilities within systems.

Additionally, software supply chain attacks are difficult to detect. Cybercriminals can target networks at any stage of the software development cycle with advanced tactics like malware infections disguised as legitimate products. Along with deceptive techniques, cybercriminals often use advanced technologies — AI, machine learning, and automation — to increase the longevity and severity of cyberattacks.

4 ways cloud-based services enhance cybersecurity

In today's cybersecurity landscape, cloud-based services can provide vital security against software supply chain attacks. Cloud providers adhere to the latest cybersecurity policies and protocols, ensuring systems and networks meet regulatory compliance standards. Additionally, cloud providers monitor your data in real time and provide 24/7 support.

Cloud-based services also improve cybersecurity performance in several other ways:

1. **Regular penetration testing for vulnerabilities:** Cloud providers regularly conduct penetration testing, also known as pen testing, to analyze your network's security posture and regulatory compliance. During these tests, individuals imitate the methods of cybercriminals to identify network vulnerabilities such as entry points into a system's infrastructure. Regular pen testing can help pinpoint possible cyberattacks your network could face and identify the strengths and weaknesses of your systems, so you and your provider can work together to implement necessary system upgrades.

2. **Proactive patch management:** If vulnerabilities are detected, cloud providers can secure systems and networks to prevent potential cyberattacks. The process involves identifying, testing, and installing patches — usually code changes — to fix network bugs, address system vulnerabilities, or add security features. As a result, cloud providers offer networks streamlined software updates to improve your cybersecurity performance. This process also increases network software compatibility with hardware devices and ensures compliance with security regulations.

3. **Disaster Recovery and High availability:** Cloud providers with disaster recovery (DR) and high availability (HA) can quickly respond to and recover from data breaches and shutdowns. Networks with DR and HA deploy highly redundant infrastructure to ensure proper scaling and maintain automated online backup systems to protect critical data. DR and HA also minimize the impact of downtime if your organization experiences system failures, which can help improve productivity, reduce data loss, and protect brand reputation. For instance, if your network experienced a cyberattack, a cloud provider with DR and HA can move your operations to another data center location to prevent cybercriminals from accessing critical business data. This backup mode can also keep your organization up and running despite the initial breach.

4. **Privileged access management:** To mitigate cybersecurity risks, cloud

providers with privileged access management (PAM) can limit network access. Essentially, providers regulate the data, accounts, and systems vendors have access to in the cloud. PAM also sets parameters based on business attributes such as job functions, circumstances, and geography. For instance, if an employee who works in the marketing department wants to access accounts related to IT, the employee would need to be granted permission beforehand. The system must authenticate the identity of the employee and decide whether to allow access to the IT accounts based on business needs and other factors. Subsequently, PAM reduces the risks of cybercriminals compromising networks by constant monitoring and limiting who has access to your data.

Develop proactive strategies to protect your organization against cyberattacks

Cloud-based services are critical for enhancing your cybersecurity plan. There are additional measures you can take now to bolster protection against software supply chain attacks.

- **Continue ongoing investments** in your IT department to install and test security software;
- **Vet your vendors** to ensure they meet your business needs and security expectations. Ask questions regarding the vendor's expertise level, certifications, security operation compliance (SOC), and security approaches, like annual basis testing. Consult the vendor's references and track record for a closer look.
- **Conduct ongoing training sessions** for all employees to raise awareness about preventable cybersecurity risks. Often, human error is involved with cyberattacks, especially through phishing and social engineering.
- **Update your hardware** frequently to meet regulatory requirements and prevent outdated components from causing network vulnerabilities.
- **Subscribe** to common vulnerabilities and exposure (CVE) notifications to receive the latest news on cybersecurity risks and solutions.

By adopting cloud-based services and following cybersecurity best practices, you can enhance your organization's response to cyberthreats with proactive policies and protocols. To stay a step ahead of cybercriminals, upgrade your cybersecurity capabilities with cloud technologies to protect your business operations and critical infrastructure.